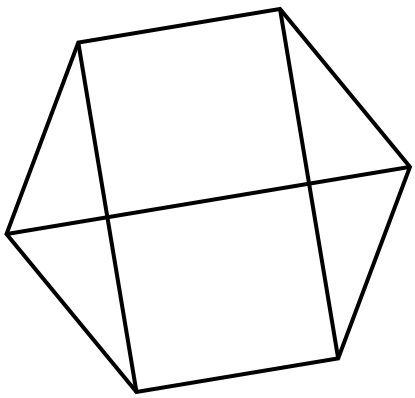
Quantum States and their Marginals:
From Multipartite Entanglement to Quantum Error-Correcting Codes

Felix Huber



Quantum States and their Marginals: From Multipartite Entanglement to Quantum Error-Correcting Codes

DISSERTATION

zur Erlangung des Grades eines Doktors
der Naturwissenschaften

vorgelegt von:

Felix Michael Huber

eingereicht bei der Naturwissenschaftlich-Technischen Fakultät
der Universität Siegen,
Siegen 2017

Gutachter:

Prof. Otfried Gühne

Prof. Jens Siewert

Prüfer:

Prof. Otfried Gühne

Prof. Jens Siewert

Prof. Mohamed Barakat

Prof. Christof Wunderlich

Datum der mündlichen Prüfung:

15.12.2017

Abstract

At the heart of the curious phenomenon of quantum entanglement lies the relation between the whole and its parts. In my thesis, I explore different aspects of this theme in the multipartite setting by drawing connections to concepts from statistics, graph theory, and quantum error-correcting codes: first, I address the case when joint quantum states are determined by their few-body parts and by Jaynes' maximum entropy principle. This can be seen as an extension of the notion of entanglement, with less complex states already being determined by their few-body marginals. Second, I address the conditions for certain highly entangled multipartite states to exist. In particular, I present the solution of a long-standing open problem concerning the existence of an absolutely maximally entangled state on seven qubits. This sheds light on the algebraic properties of pure quantum states, and on the conditions that constrain the sharing of entanglement amongst multiple particles. Third, I investigate Ulam's graph reconstruction problems in the quantum setting, and obtain legitimacy conditions of a set of states to be the reductions of a joint graph state. Lastly, I apply and extend the weight enumerator machinery from quantum error correction to investigate the existence of codes and highly entangled states in higher dimensions. This clarifies the physical interpretation of the weight enumerators and of the quantum MacWilliams identity, leading to novel applications in multipartite entanglement.

Zusammenfassung

Für das Phänomen der Quantenverschränkung sind die Beziehungen zwischen dem Ganzen und dessen Teilen zentral. In dieser Dissertation untersuche ich verschiede Aspekte dieser Thematik im Hinblick auf Mehrteilchen-Systeme, und ziehe Verbindungen zu Konzepten der Statistik, der Graphentheorie, und der Quantenfehlerkorrektur. Als Erstes untersuche ich die Bedingungen, unter denen Quantenzustände durch ihre Reduktionen auf kleine Subsysteme zusammen mit der Anwendung von Jaynes' Maximum-Entropie-Methode bestimmt sind. Dies kann als eine Ausweitung des Verschränkungsbegriffes gesehen werden, wobei ein weniger komplexer Zustand bereits durch seine Subsysteme kleiner Größe festgelegt ist. Zweitens erörtere ich notwendige Bedingungen an die Existenz von gewissen hoch verschränkten Zuständen. Insbesondere präsentiere ich die Lösung einer langjährigen bisher noch ungelösten Frage zur Existenz eines absolut maximal verschränkten Zustandes, welcher aus sieben Quantenbits besteht. Dies wirft neues Licht auf die algebraischen Eigenschaften von reinen Quantenzuständen und auf die Restriktionen, welche das Teilen von Verschränkung unter mehreren Parteien limitieren. Drittens untersuche ich gewisse Fragestellungen für Quantenzustände, welche dem Rekonstruktionproblem von Ulam in der Graphentheorie ähneln. Dies führt zu neuen Bedingungen, damit eine Sammlung von Marginalien einem gemeinsamen Zustand entstammt. Zuletzt wende ich die Theorie der Gewichtszähler aus der Quantenfehlerkorrektur auf Fragen der Existenz von hoch verschränkten höher-dimensionale Zuständen und von fehlerkorrigierenden Codes an. Dies klärt die physikalische Interpretation der Gewichtszähler und der quantum MacWilliams identität, und führt zu neuartigen Anwendungen in der Theorie der Mehrteilchen-Verschränkung.

Contents

List of Illustrations

Figures

Tables

Preface

Quantum mechanical states exhibit the two peculiar and closely related phenomena of superposition and entanglement. Exploring the ramifications of these phenomena has been a major scientific challenge during the last century. In particular, the discovered applications of quantum mechanics to information theory have spawned a whole new field of physics that is now known as quantum information theory. It includes all aspects of information processing and computation by means of quantum states, and led to algorithms in the quantum domain which are widely thought to outperform their classical counterparts.

Entanglement was recognized early to be one of the key resources for quantum information processing and computation tasks. Loosely speaking, entanglement is present when the 'best possible knowledge of a *whole* does not necessarily include the best possible knowledge of all of its *parts*, even though they may be entirely separated and therefore virtually capable of being "best possibly known"'[1]. Thus the individual parts of a quantum system cannot be described independently from each other, making a joint description of all involved particles necessary.

However, the characterization of entanglement and of its related notions such as steering and non-locality has turned out to be a far more difficult endeavor than one could have initially anticipated. In particular, there cannot exist any simple means to determine whether any given state is entangled or not [2, 3]. While the understanding of entanglement occurring between two particles has seen strong advances, the deeper investigation of entanglement between multiple parties is a rather recent undertaking. In particular, it has been recognized that entanglement cannot be shared arbitrarily amongst all particles, but that its distribution is constrained in various ways.

This thesis explores aspects of multipartite entanglement by drawing connections to concepts from statistics, graph theory, and the theory of quantum error-correcting codes. First, I address the case when quantum states are already determined by their few-body marginals and by Jaynes' maximum entropy principle [A]. This can be seen as an extension of the notion of entanglement, with less complex states being already determined by their few-body marginals. Our methods permit to detect states that cannot be obtained as thermal or ground states of few-body Hamiltonians. This furthermore answers questions about which states are unlikely to appear in naturally occurring equilibrium systems. Together with my co-authors, I subsequently treated questions concerning the quantum marginal problem of four-partite systems [B], and provided methods for pure qubit states to be reconstructed from their even- or odd-body correlations only [C]. Second, I address conditions for certain highly entangled multipartite states, that exhibit maximal entanglement across every bipar-

tition, to exist. These states are also called absolutely maximally entangled, or perfect tensors. Here, I present the solution of a long-standing open problem concerning the existence of an absolutely maximally entangled state on seven qubits [D]. The methods used shed light on the algebraic properties of pure states, and on the conditions that constrain the distribution of entanglement amongst multiple particles. It furthermore highlights the usefulness of the Bloch decomposition for also representing pure quantum states, as it directly incorporates the correlations as exhibited by the state. Third, I investigate Ulam's graph reconstruction problem in the quantum setting [E]. The classical graph-theoretic problem consists of reconstructing a graph from the knowledge of its vertex-deleted subgraphs; I address analogous questions concerning reductions of a class of quantum states called graph states. This yields conditions for a set of states to originate from a common joint state. Lastly, I use approaches from the theory of quantum error correction and adopt the weight enumerator machinery to investigate questions in multipartite entanglement [F]. This offers a physical interpretation of the quantum weight enumerators, and clarifies a remarkable relation known as the quantum MacWilliams identity. With the shadow inequalities as introduced by Rains, I provide a systematic approach to disprove the existence of many higher-dimensional absolutely maximally entangled states. These inequalities can be seen as an exponentially large family of constraints for quantum correlations, and provide a fine-graining of the reduction map known from multipartite entanglement.

This thesis is based on the following projects and publications:

[A] Felix Huber and O. Gühne,
Characterizing Ground and Thermal States of Few-Body Hamiltonians.
Phys. Rev. Lett. **117**, 010403 (2016).

[B] N. Wyderka, Felix Huber, and O. Gühne,
Almost all four-particle pure states are determined by their two-body marginals.
Phys. Rev. A **96**, 010102(R) (2017).

[C] N. Wyderka, Felix Huber, and O. Gühne,
Constraints on correlations in qubit systems.
arXiv:1710.00758 (2017).

[D] Felix Huber, O. Gühne, and J. Siewert,
Absolutely Maximally Entangled States of Seven Qubits Do Not Exist.
Phys. Rev. Lett. **118**, 200502 (2017).

[E] Felix Huber and S. Severini,
Some Ulam's reconstruction problems for quantum states.
In preparation (2017).

[F] Felix Huber, C. Eltschka, J. Siewert, and O. Gühne,
Bounds on absolutely maximally entangled states from shadow inequalities, and the quantum MacWilliams identity.
arXiv:1708.06298 (2017).

Chapter 1

Basic concepts

In this first part, I introduce basic notions of quantum information and multipartite entanglement.

1.1 Fundamentals

1.1.1 Quantum states

A pure quantum state having D levels can mathematically be represented by a unit vector in the complex Hilbert space $\mathcal{H} = \mathbb{C}^D$. [4]. It is commonly written as a *ket* $|\phi\rangle$, and can be expanded in any orthonormal basis $\{|\alpha\rangle\}$ of $\mathcal{H}$ as

$$|\phi\rangle = \sum_{\alpha=0}^{D-1} c_\alpha \, |\alpha\rangle \ . \tag{1.1}$$

Its adjoint is written as a *bra* $\langle\phi|$. Normalization demands that the inner product fulfills $\langle\phi|\phi\rangle = 1$, and thus $\sum |c_\alpha|^2 = 1$. Often, an expansion in the *computational basis* is of interest,

$$|\phi\rangle = \sum_{i=0}^{D-1} c_i \, |i\rangle \ , \tag{1.2}$$

where

$$|i\rangle = (0, \ldots, 0, \underbrace{1}_{\text{i'th position}}, 0, \ldots, 0)^T . \tag{1.3}$$

Statistical probability distributions of pure quantum states (so-called *mixed states*) in turn are represented by positive [1] operators in the space $\mathcal{B}(\mathcal{H})$ of bounded operators on $\mathcal{H}$ having trace one, denoted as *density matrices*,

$$\varrho = \sum_i p_i |\phi_i\rangle\langle\phi_i|. \tag{1.4}$$

In order that the density matrix ϱ is indeed positive $\varrho \geq 0$ and of trace one, one requires that $\sum_i p_i = 1$ and $p_i \geq 0$. By the spectral theorem, Hermitian operators

[1] Throughout this text, we often refer to Hermitian operators with non-negative eigenvalues as *positive*, instead of the more precise but somewhat cumbersome term *positive semi-definite* or *non-negative*.

can be diagonalized, having real eigenvalues. The eigenvalues of density matrices λ_i must thus be real and non-negative, with

$$\mathrm{Tr}(\varrho) = \sum_i \lambda_i = 1\,. \tag{1.5}$$

While the *expectation value* of an observable represented by a Hermitian operator $\hat{A}$ is from the Born's rule given by $\langle \hat{A} \rangle_{|\phi\rangle} = \langle\phi|\,\hat{A}\,|\phi\rangle$, it is obtained from $\langle \hat{A} \rangle_{\varrho} = \mathrm{Tr}(\hat{A}\varrho)$ for density matrices.

Convex combinations, as done here in the transition from pure to mixed states, is a common way to incorporate classical statistical probabilities on top of the underlying description of quantum objects. Generally, given a set of quantum states $\{|\phi_i\rangle\}$, its *convex hull* is formed by taking all possible statistical mixtures,

$$\mathrm{conv}(\{|\phi_i\rangle\}) = \{\sigma \mid \sigma = \sum_i p_i |\phi_i\rangle\langle\phi_i|\,, \sum_i p_i = 1\,,\, p_i \geq 0\}\,. \tag{1.6}$$

1.1.2 Multiple particles

Pure quantum states of n particles (or parties), having the local dimensions $D_1, \ldots, D_n$, are represented by complex unit vectors in the Hilbert space $\mathcal{H} = \mathbb{C}^{D_1} \otimes \ldots \otimes \mathbb{C}^{D_n}$. Given independent pure quantum states $\{|\phi_i\rangle \in \mathcal{H}_i\}$, their joint description is obtained by taking the tensor product

$$|\phi\rangle = |\phi_1\rangle \otimes \cdots \otimes |\phi_n\rangle \qquad \in \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n\,. \tag{1.7}$$

A multipartite state can be expanded in any orthonormal basis, in particular in the computational basis which is obtained by the tensor product of the local computational bases. Often, the symbols for the tensor products are then left out, or the individual kets are grouped together into a single one,

$$\begin{aligned} |i_1\rangle \otimes |i_2\rangle \otimes \cdots \otimes |i_n\rangle &= |i_1\rangle\,|i_2\rangle \ldots |i_n\rangle \\ &= |i_1 i_2 \ldots i_n\rangle\ . \end{aligned} \tag{1.8}$$

A crucial operation in quantum information is the mathematical "forgetting" of individual parties, which is done by taking a *partial trace*. If V and W are complex Hilbert spaces, the partial trace Tr_W over subsystem W is defined as follows: For all operators M and N on V and $V \otimes W$ respectively, $\mathrm{Tr}_W(\cdot)$ is the unique operation such that

$$\mathrm{Tr}[(M_V \otimes \mathbb{1}_W)N] = \mathrm{Tr}[M_V\,\mathrm{Tr}_W(N)]\,. \tag{1.9}$$

Given an orthonormal basis $\{|i_S\rangle\}$ of subsystem S, the partial trace is usually written as

$$\begin{aligned} \mathrm{Tr}_S(X) &= \sum_i (\langle i_S| \otimes \mathbb{1}_{S^c}) X (|i_S\rangle \otimes \mathbb{1}_{S^c})\,, \\ &= \sum_i \langle i_S|\,X\,|i_S\rangle\ , \end{aligned} \tag{1.10}$$

where S^c denotes the complement of S in $\{1 \ldots n\}$. In particular, by taking the partial trace, independent pure quantum states can be decomposed into their parts

again. If $|\phi\rangle = |\phi_1\rangle \otimes \ldots \otimes |\phi_n\rangle$, the density matrix of an individual subsystem $|\phi_i\rangle\langle\phi_i|$, a *marginal* or *reduction* can be recovered by taking the partial trace over the remaining parties,

$$|\phi_i\rangle\langle\phi_i| = \mathrm{Tr}_{(1,\ldots,i-1,i+1,\ldots,n)}(|\phi\rangle\langle\phi|)\,. \tag{1.11}$$

After preforming a partial trace, one does not necessarily recover a pure state, but a (mixed) density matrix. Tracing over the subsystems in S^c, one thus writes

$$\varrho_S = \mathrm{Tr}_{S^c}(|\phi\rangle\langle\phi|)\,. \tag{1.12}$$

1.1.3 Operators and maps

A Hermitian operator on $\mathcal{B}(\mathcal{H})$ is *positive*, $A \geq 0$, if all its eigenvalues are non-negative, $\lambda_i \geq 0$ [5]. Correspondingly, $A \geq B$ if $(A-B) \geq 0$. Positive operators form a *cone*, as any convex combination $pA + (1-p)B$ for positive operators A and B with $0 \leq p \leq 1$ remains positive. Because every positive operator corresponds up to a normalization of the trace to a density matrix, the set of density matrices corresponds to a hyperplane through the cone of positive operators. The identity operator is denoted by $\mathbb{1}$, or id if emphasis is placed on its nature as a map. A decomposition of the identity $\sum_i E_i = \mathbb{1}$ in terms of positive operators $\{0 \leq E_i \leq \mathbb{1}\}$ is called a *positive operator-valued measure (POVM)*. POVMs are the most general form of describing measurements in quantum mechanics, with an *effect* E_i having the expectation value $\langle E_i \rangle_\varrho = \mathrm{Tr}(E_i \varrho)$. Finally, note that unitary operators U with $U^\dagger = U^{-1}$ map pure states to pure states.

A map $\mathcal{L}[\cdot]$ is *positive* if positive operators (e.g. density matrices) stay positive under its action,

$$\varrho \geq 0 \quad \Longrightarrow \quad \mathcal{L}[\varrho] \geq 0\,. \tag{1.13}$$

However, a quantum system may consist of multiple systems, including a possible environment. This necessitates the definition of *completely positive* maps.

Definition 1. *Consider a map $\mathcal{L}$ acting on $\mathcal{B}(\mathcal{H}_A)$. $\mathcal{L}$ is completely positive, if for all $\mathcal{H}_B$ and all positive $\varrho \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$,*

$$(\mathcal{L}_A \otimes \mathrm{id}_B)[\varrho] \geq 0\,. \tag{1.14}$$

If additionally the trace is preserved under the action of a map $\mathcal{L}$, it is called a *completely positive trace preserving map (CPTP)*, or *quantum channel*, mapping quantum states to quantum states. Completely positive maps can be represented in the *Kraus form* as [6–8]

$$\varrho \longrightarrow \mathcal{L}[\varrho] = \sum_i A_i \varrho A_i^\dagger\,, \tag{1.15}$$

where $\{A_i\}$ are the *Kraus operators*. In order that the map also be trace-preserving, one has the additional requirement of

$$\sum_i A_i^\dagger A_i = \mathbb{1}\,. \tag{1.16}$$

According to Stinespring's dilation theorem, any completely positive map on $\mathcal{H}_A$ can always be represented in a larger Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ as a unitary map followed by a partial trace,

$$\mathcal{L}(\varrho_A) = \mathrm{Tr}_B[U_{AB}(\varrho_A \otimes |0\rangle\langle 0|_B)U_{AB}^\dagger)]\,. \tag{1.17}$$

Finally, a map is called *decomposable*, if it can be written as

$$\mathcal{L}[\cdot] = \mathcal{L}_1[\cdot] + \mathcal{L}_2 \circ \mathcal{T}[\cdot]\,, \tag{1.18}$$

where $\mathcal{T}$ is the transpose map.

Allowing for certain sets of operations only gives rise to different classifications of quantum states. *Local unitary operations* (LU) connect n-partite states that can be transformed by tensor products of local unitaries,

$$|\phi\rangle = U_1 \otimes \cdots \otimes U_n\,|\psi\rangle\ . \tag{1.19}$$

This can be seen as a different choice of local basis to represent the state. *Local operations* (LO) are of the form

$$(\Phi_1 \otimes \cdots \otimes \Phi_n)[\varrho] = \sum_{i\ldots r} \left(A_1^{(i)} \otimes \cdots \otimes A_n^{(r)}\right) \varrho \left(A_1^{(i)\,\dagger} \otimes \cdots \otimes\ A_n^{(r)\,\dagger}\right). \tag{1.20}$$

If one additionally allows for the exchange of classical communication amongst the parties between rounds of local operations, one arrives at a class called *local operations and classical communication* (LOCC). The LOCC conversion of pure states is characterized by majorization: A state ϱ is said to *majorize* a state σ, in shorthand $\varrho \succ \sigma$, if their eigenvalues sorted in descending order fulfill for all k that

$$\sum_{i=1}^{k} \lambda_i^{\downarrow}(\varrho) \geq \sum_{i=1}^{k} \lambda_i^{\downarrow}(\sigma)\,. \tag{1.21}$$

This leads to the following theorem.

Theorem 1 ([9]). *A bipartite pure state $|\psi\rangle$ can be converted by LOCC into another state $|\phi\rangle$, if and only if the eigenvalues of $\varrho_{A,\phi} = \mathrm{Tr}_B(|\phi\rangle\langle\phi|)$ majorize those of $\varrho_{A,\psi} = Tr_B(|\psi\rangle\langle\psi|)$,*

$$|\psi\rangle \xrightarrow{LOCC} |\phi\rangle \quad \Longleftrightarrow \quad \varrho_{A,\psi} \prec \varrho_{A,\phi}\,. \tag{1.22}$$

Note that the majorization induces a partial order only; thus there exist mutually inconvertible states.

Stochastic local Operations and classical communications (SLOCC) extends this set of operations to also allow for a probabilistic conversion between states. Mathematically, SLOCC operations can be represented by

$$|\phi\rangle = A_1 \otimes \cdots \otimes A_n\,|\psi\rangle\ , \tag{1.23}$$

where the matrices $A_1, \ldots, A_n$ must be invertible.

The above maps represent the key idea of operations which may only create classical correlations, but no *entanglement* (c.f. Sect. 1.1.4). As an example, a key task

in quantum information is to *distill* or concentrate entanglement using LOCC only. Given k copies of a bipartite state ϱ, the aim is to obtain a singlet,

$$\underbrace{\varrho \otimes \cdots \otimes \varrho}_{k \text{ copies}} \quad \xrightarrow{LOCC} \quad \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)\,. \tag{1.24}$$

A state ϱ for which this is not possible for any number of copies is called *undistillable*; undistillable but entangled states are *bound entangled*. A sufficient criterion for undistillability is for a state to have a positive partial transpose (c.f. Sect. 1.1.6) [10]. If on the other hand a state violates the reduction criterion, it is distillable [11].

Finally, one may desire to copy an unknown quantum states, similarly as to copying classical bits. This however turns out to be impossible [12, 13]. Suppose one wished to copy an unknown state $|\psi\rangle$, such that

$$|\psi\rangle \otimes |t\rangle \xrightarrow{U} |\psi\rangle \otimes |\psi\rangle\ , \tag{1.25}$$

under a necessarily unitary evolution U, and where $|t\rangle$ is an arbitrary target state. Then this copying procedure must also work for another state $|\phi\rangle$, and we have

$$\begin{aligned} U(|\psi\rangle \otimes |t\rangle) &= |\psi\rangle \otimes |\psi\rangle\ , \\ U(|\phi\rangle \otimes |t\rangle) &= |\phi\rangle \otimes |\phi\rangle\ . \end{aligned} \tag{1.26}$$

The inner product of the above equations yields $\langle\psi|\phi\rangle = (\langle\psi|\phi\rangle)^2$, whose only two solutions can either be $\langle\psi|\phi\rangle = 0$ or $|\psi\rangle = |\phi\rangle$. Therefore it may be possible to construct devices copy from a specific set of mutually orthogonal states, but the cloning of arbitrary states is forbidden. This is known as the *no-cloning theorem*.

1.1.4 Entanglement

Entanglement is the notion of quantum states which are not simply built up from their constituents in any classical way. Loosely speaking, these are states in the tensor product space (of say, Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$), that are not statistical mixtures of tensor-product vectors. Thus entangled quantum states exhibit non-classical correlations, whose classification and quantification is of interest.

Bipartite entanglement

Consider two quantum states $|\phi_A\rangle$ in $\mathcal{H}_A$ and $|\phi_B\rangle$ in $\mathcal{H}_B$ of two independent subsystems A and B. Their joint description is obtained by taking their tensor product, forming a *product state* in $\mathcal{H}_A \otimes \mathcal{H}_B$,

$$|\phi_{AB}\rangle = |\phi_A\rangle \otimes |\phi_B\rangle\ . \tag{1.27}$$

If the quantum states on subsystems A and B are mixed themselves, the product state is represented by a density matrix,

$$\varrho_{AB} = \varrho_A \otimes \varrho_B\,. \tag{1.28}$$

Taking a statistical mixture of product states, one obtains a *separable state*. These are of the form

$$\varrho_{AB} = \sum_i p_i \varrho_A^{(i)} \otimes \varrho_B^{(i)} \,, \tag{1.29}$$

where $p_i \geq 0$ and $\sum_i p_i = 1$. Thus the set of separable states SEP forms the convex hull of product states. Any correlations appearing in separable states between the different parties are of purely classical nature. However, not every bipartite quantum state (that is, consisting of two subsystems) can be written in such way: These states are called *entangled* [14].

Definition 2. *A bipartite quantum state ϱ_{AB} is entangled, if it cannot be written as a convex combination of product states.*

$$\varrho_{AB} \neq \sum_i p_i \varrho_A^{(i)} \otimes \varrho_B^{(i)} , \tag{1.30}$$

for all choices of convex weights p_i, and density matrices $\varrho_A^{(i)}$, $\varrho_B^{(i)}$.

For pure joint states, this reduces to

Definition 3. *A pure bipartite quantum state $|\phi_{AB}\rangle$ is entangled, if it cannot be written as*

$$|\phi_{AB}\rangle \neq |\phi_A\rangle \otimes |\phi_B\rangle \tag{1.31}$$

for all choices of $|\phi_A\rangle$ and $|\phi_B\rangle$.

The paradigmatic example of an entangled state on two subsystems having two levels each is the *Bell state* (or Einstein-Podolsky-Rosen pair),

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \,, \tag{1.32}$$

exhibiting strong non-classical correlations between the subsystems. Three other states complete the set of Bell states,

$$\begin{aligned} |\phi^-\rangle &= (|00\rangle - |11\rangle)/\sqrt{2} \,, \\ |\psi^+\rangle &= (|01\rangle + |10\rangle)/\sqrt{2} \,, \\ |\psi^-\rangle &= (|10\rangle - |01\rangle)/\sqrt{2} \,, \end{aligned} \tag{1.33}$$

having the same entanglement features as $|\phi^+\rangle$. The last state in above list is also called a singlet. For pairs of higher dimensional states, the Bell state generalizes to

$$|\Omega\rangle = \frac{1}{\sqrt{D}} \sum_{i=0}^{D-1} |i_A\rangle \otimes |i_B\rangle \ . \tag{1.34}$$

In fact, every state that shows maximal entanglement across a bipartition $A|B$ can be written as $|\phi\rangle = (\mathbb{1} \otimes U)\,|\Omega\rangle$, where U is a suitable unitary [15]. An interesting property for bipartite states with maximal entanglement is that any operation on the first party can also be performed by acting on the second party,

$$A \otimes \mathbb{1}\,|\Omega\rangle = \mathbb{1} \otimes A^T\,|\Omega\rangle \ . \tag{1.35}$$

In particular, it holds that $U \otimes \bar{U}\,|\Omega\rangle = |\Omega\rangle$ for all unitaries U.

Schmidt decomposition

An important aspect of bipartite states is their *Schmidt decomposition* [14].

Theorem 2. *For every pure state $|\phi\rangle$ in $\mathcal{H}_A \otimes \mathcal{H}_B$, there exist orthonormal bases $\{|\alpha_i\rangle\}$ in $\mathcal{H}_A$ and $\{|\beta_i\rangle\}$ in $\mathcal{H}_B$, such that the state can be expressed as*

$$|\phi\rangle = \sum_{i=1}^{K} \sqrt{\lambda_i}\, |\alpha_i\rangle \otimes |\beta_i\rangle \ , \tag{1.36}$$

with $K = \min(\dim(\mathcal{H}_A), \dim(\mathcal{H}_B))$. The Schmidt coefficients *$\{\sqrt{\lambda_i}\}$ are non-negative and normalized, fulfilling $\lambda_i \geq 0$ and $\sum_{i=1}^{K} \lambda_i = 1$. The number of nonzero Schmidt coefficients is called the* Schmidt rank*, and a state $|\phi\rangle$ is entangled if and only if its Schmidt rank is strictly larger than one.*

In the Schmidt decomposed form, the reductions of $|\phi\rangle$ can be written as

$$\varrho_A = \mathrm{Tr}_B\, |\phi\rangle\langle\phi| = \sum_{i=1}^{K} \lambda_i |\alpha_i\rangle\langle\alpha_i| \,, \tag{1.37}$$

$$\varrho_B = \mathrm{Tr}_A\, |\phi\rangle\langle\phi| = \sum_{i=1}^{K} \lambda_i |\beta_i\rangle\langle\beta_i| \,. \tag{1.38}$$

Note that the spectrum of the reductions $\sigma(\varrho_A) = \sigma(\varrho_B) = (\lambda_1, \ldots, \lambda_K)$ is given by the Schmidt coefficients, up to additional vanishing eigenvalues. Conversely, every mixed state can be *purified* on a larger system. This works in the following way: let $\varrho_A = \sum_{i=1}^{K} \lambda_i |\alpha_i\rangle\langle\alpha_i|$ be the spectral decomposition of a state ϱ_A on $\mathcal{H}_A$. Given an orthonormal basis $\{|\beta_i\rangle\}$ for $\mathcal{H}_B$ of $\dim(\mathcal{H}_B) \geq K$, a pure state can be constructed by

$$|\psi_{AB}\rangle = \sum_{i=1}^{K} \sqrt{\lambda_i}\, |\alpha_i\rangle \otimes |\beta_i\rangle \ . \tag{1.39}$$

The state $|\psi_{AB}\rangle$ has indeed ϱ_A as its marginal on subsystem A.

A bipartite state is called *maximally entangled*, if all $\lambda_i = K^{-1}$. This follows from the fact that every other state of the same dimension can be obtained by means of *local operations and classical communication* (c.f. Thm. 1). Note that the reduced density matrices of maximally entangled states are proportional to the identity on the supported subspace of dimension K. Indeed the Bell state [Eq. (1.32)] and its generalization to higher dimensions [Eq. (1.34)] are maximally entangled. Its one-party marginal states are *maximally mixed*, being proportional to the identity matrix.

$$\begin{aligned} \mathrm{Tr}_2(|\phi^+\rangle\langle\phi^+|) &= \mathbb{1}/D \,, \\ \mathrm{Tr}_1(|\phi^+\rangle\langle\phi^+|) &= \mathbb{1}/D \,. \end{aligned} \tag{1.40}$$

Thus while the joint state is definite (in the sense of not being a classical mixture of states), any measurement performed single reductions alone yield completely random outcomes. However, performing the same measurement on both parties,

one can see that their outcomes are strongly correlated. It can be shown that this type of correlations cannot have classical origins [16].

While maximal entanglement can be defined in different ways for multipartite systems, having maximally mixed reductions is a typical feature of highly entangled pure states. For systems consisting of more than two parties this will lead to the notion of *absolutely maximally entangled states* (AME), which will be the subject of Sect. 1.2.3 and Chpt. 3.

Multipartite entanglement

Considering more than two parties, product states, separable states, and entangled states are defined similarly [14]: *Pure product states* of n parties are of the form

$$|\phi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle \otimes \cdots \otimes |\phi_n\rangle \ , \tag{1.41}$$

while *mixed product states* can be written as

$$\varrho = \varrho_1 \otimes \varrho_2 \otimes \cdots \otimes \varrho_n \, . \tag{1.42}$$

Accordingly, *separable states* are obtained by taking statistical mixtures of product states,

$$\varrho^{\text{fs}} = \sum_i p_i \varrho_1^{(i)} \otimes \varrho_2^{(i)} \otimes \cdots \otimes \varrho_n^{(i)} \, , \tag{1.43}$$

where again, $p_i \geq 0$ and $\sum_i p_i = 1$. These states are also called *fully separable*, in contrast to states which are separable only when some subsystems are grouped together. Multi-partite states are called *entangled*, if they are not fully separable.

Definition 4. *A multipartite state is called entangled, if it cannot be written as a convex combination of product states.*

$$\varrho \neq \sum_i p_i \varrho_1^{(i)} \otimes \varrho_2^{(i)} \otimes \cdots \otimes \varrho_n^{(i)} \, , \tag{1.44}$$

for all choices of convex weights p_i, and density matrices $\varrho_1^{(i)}, \ldots, \varrho_n^{(i)}$.

Biseparable states can be written as the convex combination of pure states $|\psi_k^{\text{bs}}\rangle$ that are separable across some bipartition, but which are not fully separable.

$$\varrho^{\text{bs}} = \sum_k p_k |\psi_k^{\text{bs}}\rangle\langle\psi_k^{\text{bs}}| \, . \tag{1.45}$$

Note that the individual $|\psi_k^{\text{bs}}\rangle$ might be biseparable with respect to different bipartitions. If a multipartite state cannot be written as a fully separable or a biseparable state, the state is called *genuinely multipartite entangled*.

While the entanglement properties of pure bipartite states are well understood, multipartite states allow for more freedom in the distribution of quantum correlations between the different parties. This gives rise to different classifications of multipartite entanglement with respect to different entanglement properties or operational procedures. As an example, considering *local operations and classical communications (LOCC)* (c.f. Sect. 1.1.3), this gives in the case of three two-level

systems (termed *qubits*) rise to two entanglement classes, which are represented by the W- and the Greenberger-Horne-Zeilinger (GHZ) states,

$$\begin{aligned} |W\rangle &= (|001\rangle + |010\rangle + |100\rangle)/\sqrt{3}\,, \\ |GHZ_3\rangle &= (|000\rangle + |111\rangle)/\sqrt{2}\,. \end{aligned} \tag{1.46}$$

Lastly, note that many further notions of entanglement and quantum correlations, such as steering, non-locality, genuine multi-level entanglement, and other notions are naturally defined with the convex hull picture: considering a set of states which do not show a certain type of correlation, the convex hull is taken to incorporate classical mixtures thereof. It is then of interest to understand what states lie outside of the so constructed convex hull.

1.1.5 Entropy and distance measures

Non-orthogonal quantum states cannot be distinguished with certainty. However, it is still interesting to understand how far "apart" two states are. Thus it is of interest to have suitable distance measures on the state space, and to be able to compare them. These can then also be used in perturbation proofs, as e.g. done in Obs. 18. Similarly, measures to quantify mixedness of quantum states are crucial to understand the amount of classical uncertainty about a state.

A short note about matrix functions: these are defined in the eigenbasis on the eigenvalues. That is, given a matrix A that is diagonalizable as $A = ZDZ^{-1}$, the matrix function is understood as operating on the spectrum $\{\lambda_i\}$,

$$f(A) = Z \begin{pmatrix} f(\lambda_1) & & \\ & \ddots & \\ & & f(\lambda_n) \end{pmatrix} Z^{-1}\,. \tag{1.47}$$

With this, the *absolute value* of an operator A is defined as

$$|A| = \sqrt{AA^\dagger}\,. \tag{1.48}$$

For finite-dimensional bounded operators this equals to $|A| = \sum_i |\lambda_i|$ [2]. With it, the L_p-norm of an operator is given by

$$||A||_p = \Big[\operatorname{Tr}(|A|^p)\Big]^{\frac{1}{p}}\,, \tag{1.49}$$

or in terms of its eigenvalues, $||A||_p = \left(\sum |\lambda_i|^p\right)^{1/p}$. The *trace norm* of an operator is its L_1-norm,

$$||A||_{\mathrm{Tr}} = ||A||_1 = \operatorname{Tr}|A| = \operatorname{Tr}\sqrt{AA^\dagger}\,. \tag{1.50}$$

The *trace distance* between two Hermitian operators is then obtained by the trace norm of their difference,

$$D_{\mathrm{Tr}}(\varrho,\sigma) = \frac{1}{2}||\varrho-\sigma||_{\mathrm{Tr}} = \frac{1}{2}\operatorname{Tr}\sqrt{(\varrho-\sigma)^2}\,. \tag{1.51}$$

[2] In this text, I will consider finite-dimensional bounded operators only.

The physical interpretation of the trace distance is that of distinguishing quantum states by an optimal measurement [17]. It fulfills,

$$D_{\mathrm{Tr}}(\varrho,\sigma) = \max_{0\leq E\leq \mathbb{1}} \mathrm{Tr}[E(\varrho-\sigma)]\,, \tag{1.52}$$

where $0 \leq E \leq \mathbb{1}$ is an effect (c.f. Sect. 1.1.3). Accordingly, the average optimal success probability of distinguishing ϱ from σ is $[1 + D_{\mathrm{Tr}}(\varrho,\sigma)]/2$.

The *fidelity* is defined by

$$F(\varrho,\sigma) = \left(\mathrm{Tr}\sqrt{\sqrt{\varrho}\sigma\sqrt{\varrho}}\right)^2. \tag{1.53}$$

While it is not apparent from the formulation above, the fidelity is symmetric in its two arguments. For pure states, the fidelity is equal to the overlap $F(|\phi\rangle, |\psi\rangle) = |\langle\phi|\psi\rangle|^2$. This generalizes to mixed states, where it corresponds to the maximum overlap of purifications $|\phi\rangle$ and $|\psi\rangle$ of ϱ and σ. This follows from Uhlmann's theorem [18],

$$F(\varrho,\sigma) = \max_{|\phi\rangle,|\psi\rangle} |\langle\phi|\psi\rangle|^2\,. \tag{1.54}$$

In the following $0 \leq a \leq 1$. The fidelity has further nice properties,

1. **Positivity.** $0 \leq F(\varrho,\sigma) \leq 1$, and $F(\varrho,\sigma) = 1 \iff \varrho = \sigma$. $F(\varrho,\sigma) = 0$ if and only if the support of ϱ is orthogonal to that of σ.

2. **Symmetry.** $F(\varrho,\sigma) = F(\sigma,\varrho)$.

3. **Unitary invariance.** $F(U\varrho U^\dagger, U\sigma U^\dagger) = F(\varrho,\sigma)$.

4. **Concavity.** $F(\varrho, a\sigma_1 + (1-a)\sigma_2) \geq aF(\varrho,\sigma_1) + (1-a)F(\varrho,\sigma_2)$.

5. **Multiplicativity.** $F(\varrho_1\otimes\varrho_2, \sigma_1\otimes\sigma_2) = F(\varrho_1,\sigma_1)F(\varrho_2,\sigma_2)$.

6. **Monotonicity under CPTP maps.** $F(\mathcal{L}[\varrho],\mathcal{L}[\sigma]) \leq F(\varrho,\sigma)$ for any CPTP map $\mathcal{L}$. In particular, this includes monotonicity under the partial trace.

The *quantum relative entropy* originates from the classical relative entropy. It is defined as

$$S(\varrho||\sigma) = \mathrm{Tr}[\varrho(\ln\varrho - \ln\sigma)]\,. \tag{1.55}$$

It is per se not a distance measure, but rather a divergence, as it is generally not symmetric in its arguments, $S(\varrho||\sigma) \neq S(\sigma||\varrho)$. It has the following properties [17]:

1. **Positivity**. $S(\varrho||\sigma) \geq 0$, where equality implies $\varrho = \sigma$.

2. **Unitary invariance**. $S(U\varrho U^\dagger||U\sigma U^\dagger) = S(\varrho||\sigma)$.

3. **Joint convexity**.

$$S(a\varrho_1 + (1-a)\varrho_2||a\sigma_1 + (1-a)\sigma_2) \;\leq\; aS(\varrho_1||\sigma_1) + (1-a)S(\varrho_2||\sigma_2)\,.$$

4. **Additivity.** $S(\varrho_1\otimes\varrho_2||\sigma_1\otimes\sigma_2) = S(\varrho_1||\sigma_1) + S(\varrho_2||\sigma_2)$.

5. **Superadditivity [19].**

$$\big(1+2||H(\sigma_{AB})||_\infty\big)D(\varrho_{AB}||\sigma_{AB}) \geq D(\varrho_A||\sigma_A)+D(\varrho_B||\sigma_B)\,, \tag{1.56}$$

where $H(\sigma_{AB}) = (\sigma_A^{-1/2}\otimes\sigma_B^{-1/2})\sigma_{AB}(\sigma_A^{-1/2}\otimes\sigma_B^{-1/2})-\mathbb{1}_{AB}$. Note that $H(\sigma_{AB}) = 0$ if $\sigma_{AB} = \sigma_A\otimes\sigma_B$.

6. **Monotonicity under CP maps**. $S(\mathcal{L}[\varrho]||\mathcal{L}[\sigma]) \leq S(\varrho||\sigma)$ for any CPTP map $\mathcal{L}$, such as e.g. the partial trace.

The *von Neumann entropy* of a state ϱ is defined as

$$S(\varrho) = -\operatorname{Tr}(\varrho\log\varrho)\,, \tag{1.57}$$

which in terms its eigenvalues λ_i reads as $S(\varrho) = -\sum_i \lambda_i\log\lambda_i$. It is related to the quantum relative entropy by $S(\varrho||\mathbb{1}/D) = \ln(D) - S(\varrho)$, where D is the dimension of the Hilbert space. It has the properties

1. **Positivity.** $0 \leq S(\varrho) \leq S(\mathbb{1}/D) = \ln D$.
2. **Unitary invariance.** $S(U\varrho U^\dagger) = S(\varrho)$.
3. **Concavity.** $S(a\varrho+(1-a)\sigma) \geq aS(\varrho)+(1-a)S(\sigma)$.
4. **Subadditivity.** $S(\varrho_{12}) \leq S(\varrho_1)+S(\varrho_2)$.
5. **Araki-Lieb Triangle inequality.** $|S(\varrho_1)-S(\varrho_2)| \leq S(\varrho_{12})$.
6. **Strong Subadditivity.** $S(\varrho_{123})+S(\varrho_2) \leq S(\varrho_{12})+S(\varrho_{23})$.

The strong subadditivity of the von Neumann entropy, the weak monotonicity of the quantum relative entropy, and the joint convexity of the quantum relative entropy are equivalent [20]. The operational significance of the von Neumann entropy stems from *Schumacher's noiseless coding theorem*, where it can be seen that the von Neumann entropy of $\varrho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$ is a measure of the information contained in a string of pure states $|\psi_i\rangle$ occurring with probabilities p_i [21]. Furthermore, the von Neumann entropy quantifies the distillable entanglement and the entanglement cost for pure states (c.f. Sect. 1.1.6). It can also be used to measure the mixedness of quantum states: it vanishes for pure states, $S(|\psi\rangle) = 0$, while for maximally mixed states $S(\mathbb{1}/D) = \ln(D)$ holds.

One can establish inequalities and continuity bounds between the different distance and entropy measures. The *quantum Pinsker inequality* relates the trace distance and the quantum relative entropy,

$$S(\varrho||\sigma) \geq 2\,D_{\mathrm{Tr}}(\varrho,\sigma)^2\,. \tag{1.58}$$

The *Fannes' Lemma* upper bounds a change in trace distance to the change in the von Neumann entropy: If $D_{\mathrm{Tr}}(\varrho,\sigma) \leq \epsilon \leq 1$, then

$$|S(\varrho)-S(\sigma)| \leq \begin{cases} \epsilon\log(D-1)+h(\epsilon) & \text{if } \epsilon \leq 1-D^{-1} \\ \log D & \text{if } \epsilon > 1-D^{-1}\,, \end{cases} \tag{1.59}$$

where D is the dimension of the Hilbert space, and $h(x) = -x\log x - (1-x)\log(1-x)$ is the binary entropy. The *Fuchs-Van-de-Graaf inequalities* relates the fidelity and trace distance [22],

$$1 - \sqrt{F(\varrho,\sigma)} \leq D_{\mathrm{Tr}}(\varrho,\sigma) \leq \sqrt{1 - F(\varrho,\sigma)}\,. \tag{1.60}$$

Many more inequalities for distance measures and entropies have been derived [23], including continuity bounds on conditional relative entropies [24–27].

Often, the mixedness of quantum states is of interest: Given a pure joint state, the extent of the impurity of its reductions signal entanglement. The *purity* can be used to define such mixedness of a state,

$$\mathrm{Tr}(\varrho^2) = \sum_i \lambda_i^2\,, \tag{1.61}$$

where λ_i are the eigenvalues of ϱ. A state ϱ is pure if and only if $\mathrm{Tr}(\varrho^2) = 1$. The *linear entropy* is related to the purity and approximates the von Neumann entropy [Eq. (1.57)] by its first leading order terms in the Mercator series,

$$S_L(\varrho) = \frac{D}{D-1}[1 - \mathrm{Tr}(\varrho^2)]\,. \tag{1.62}$$

The normalization is chosen such that $0 \leq S_L(\varrho) \leq 1$. The marginals of the maximally entangled Bell states have, in contrast to pure product states, a minimal purity and a maximal linear entropy. While their operational significance is not as clear the one of the von Neumann entropy, they are often used as a measure of entanglement. In Sect. 5.11.3, I will present a subadditivity-like expression for the purity and linear entropy that constrains the possible correlations of three-partite states.

1.1.6 Entanglement detection and measures

In order to determine whether a given state is entangled or not, it has to be tested if it can be written as a separable state. This is the so-called *separability problem*. Unfortunately, this is a computationally difficult task, being NP-hard [2, 3]. Therefore, various separability criteria and entanglement measures have been developed to detect and quantify entanglement. A common approach is that entanglement cannot be created locally, and that entangled quantum states can be seen as a resource for certain operational tasks. Here, I mention those which are necessary for the later Chapters.

Witnesses

Given a convex set, it can be delineated by a hyperplane: the Banach-Hahn separation theorem guarantees that a closed convex set can always be separated from a point outside of it by a continuous linear functional. Hence, an entangled state, lying outside of the convex set of separable states, can be delineated by a *witness* [28]. This is a Hermitian operator $\mathcal{W}$, such that

$$\begin{aligned} &\mathrm{Tr}(\mathcal{W}\sigma) \geq 0 && \text{for all separable states } \sigma\,, \\ &\mathrm{Tr}(\mathcal{W}\varrho) < 0 && \text{for at least one entangled state } \varrho\,. \end{aligned} \tag{1.63}$$

Then, $\mathcal{W}$ is said to detect the entangled state ϱ. As an example, given any entangled state $|\psi\rangle$, a projector-based witness can be constructed from

$$\mathcal{W} = \alpha \mathbb{1} - |\psi\rangle\langle\psi| \,, \tag{1.64}$$

where α is obtained by maximizing the overlap to separable states,

$$\alpha = \max_{\varrho \in \text{SEP}} \text{Tr}(\varrho|\psi\rangle\langle\psi|) = \max_{|\phi\rangle = |\phi_A\rangle \otimes |\phi_B\rangle} |\langle\psi|\phi\rangle|^2 \,. \tag{1.65}$$

If then $\text{Tr}(\sigma\mathcal{W}) < 0$ is measured, then the state σ must be entangled. There are other strategies to construct suitable witnesses, and in general multiple witnesses are able to detect the same state. Often specific witnesses are designed in such way as to optimize the type and number of measurements necessary [29, 30].

Positive maps

Another method to detect entanglement are *positive but not completely positive maps* [14]. Recall that a map $\mathcal{L}[\cdot]$ is positive if all positive operators (e.g. density matrices) stay positive under its action,

$$M \geq 0 \quad \Longrightarrow \quad \mathcal{L}(M) \geq 0 \,. \tag{1.66}$$

Naturally, if a map $\mathcal{L}$ is positive but not completely positive (c.f. Sect. 1.1.3), then there must exist a state ϱ_{AB}, such that

$$(\mathcal{L}_A \otimes \text{id}_B)[\varrho_{AB}] \ngeq 0 \,. \tag{1.67}$$

Necessarily, such a state ϱ_{AB} must be entangled: If it would be separable, then

$$(\mathcal{L}_A \otimes \text{id}_B)\big[\sum_i p_i \varrho_A^{(i)} \otimes \varrho_B^{(i)}\big] = \sum_i p_i \big(\mathcal{L}_A[\varrho_A^{(i)}] \otimes \varrho_B^{(i)}\big) \tag{1.68}$$

would be positive, contrary to the assumption. It has been shown that a state ϱ is separable, if and only if $(\mathcal{L} \otimes \text{id})[\varrho] \geq 0$ for all positive maps $\mathcal{L}$ [28].

An example of a positive but not completely positive map is the *reduction map* [11].

$$\mathcal{R}[X] = \text{Tr}(X)\mathbb{1} - X \,. \tag{1.69}$$

With it, one can detect entanglement, this is called the *reduction criterion*: Clearly, this map is positive, mapping pure states to the mixture of orthogonal states. However, it is not completely positive. This can be seen by choosing ϱ_{AB} to be equal to the Bell state $|\phi^+\rangle\langle\phi^+|$. Then

$$(\mathcal{R}_A \otimes \text{id}_B)[\varrho_{AB}] = \mathbb{1} \otimes \varrho_B - \varrho_{AB} = \mathbb{1}/2 - |\psi^+\rangle\langle\psi^+| \ngeq 0 \,, \tag{1.70}$$

having one negative eigenvalue. If a state violates the reduction criterion, it is distillable [11] (c.f. Sect. 1.1.3).

Another example is the *Breuer-Hall map* or *extended reduction criterion* [31, 32],

$$\mathcal{R}_{BH}[X] = \text{Tr}(X)\mathbb{1} - X - UX^TU^\dagger. \tag{1.71}$$

for any U with $U^T = -U$ and $U^\dagger U \leq \mathbb{1}$. This map is positive, but in contrast to the reduction map, not necessarily *decomposable*. Recall that a decomposable map can be written as

$$\mathcal{L}[\cdot] = \mathcal{L}_1[\cdot] + \mathcal{L}_2 \circ \mathcal{T}[\cdot]\,, \tag{1.72}$$

where $\mathcal{T}$ is the transpose map. If U in Eq. (1.71) is unitary, $\mathcal{R}_{BH}$ cannot be written in such a way and is therefore non-decomposable [3]. Note that decomposable maps correspond to decomposable witnesses, which have the form $\mathcal{W} = P + Q^{T_A}$ for positive observables P and Q [14, 15]. However, decomposable witnesses cannot detect entangled states that have a positive partial transpose (so-called bound entangled states), and decomposable witnesses and maps are generally weaker than the PPT criterion for detecting entanglement (see also the next Section).

Interestingly, the reduction map can be extended to multiple parties [4] [33, 35–37], called the *universal state inversion*.

Definition 5. *The universal state inversion map is given by*

$$\mathcal{I}[\varrho] = \sum_{S\subseteq\{1\ldots n\}} (-1)^{|S|} \varrho_S \otimes \mathbb{1}_{S^c}\,, \tag{1.73}$$

where $\varrho_S = \mathrm{Tr}_{S^c}(\varrho)$.

It can also be written as $\mathcal{I}[\cdot] = \bigotimes_j (\mathbb{1}_j \,\mathrm{Tr}_j - \mathbb{1})[\cdot]$. In case of qubits, the inversion is also given by $\mathcal{I}[\varrho] = \sigma_y^{\otimes n} \sigma^T \sigma_y^{\otimes n}$. This map will play a major role in Chapters 3 and 5, with the *shadow enumerator* generalizing the constraints originating from the non-negative overlap $\mathrm{Tr}(\mathcal{I}[\varrho]\varrho)$. A proof of the positivity of the universal state inversion and an extension of this map are presented in Sect. 5.11.1.

Further separability criteria

The *positive partial transpose (PPT)* or Peres-Horodecki criterion detects entanglement from the eigenvalues of a partially transposed state. Given a bipartite state expanded as

$$\varrho = \sum_{ijkl} C_{ij,kl}\, |i\rangle\langle j| \otimes |k\rangle\langle l|\,, \tag{1.74}$$

its partial transposition with respect to its first subsystem is given by

$$\varrho^{T_A} = \sum_{ijkl} C_{\underline{ji},kl}\, |i\rangle\langle j| \otimes |k\rangle\langle l|\,. \tag{1.75}$$

In terms of the Bloch decomposition (c.f. Sect. 1.1.7), the partial transpose simply maps Y to $-Y$ in the transposed party. The PPT-criterion can also be regarded as a positive but not completely positive map $\mathcal{L} = \mathcal{T} \otimes \mathbb{1}$, where $\mathcal{T}$ is the partial transposition. If ϱ^{T_A} is not positive, ϱ must be entangled. In particular, if the system is composed of two qubits, or of one qubit and one qutrit, a positive partial transpose

[3] Note that anti-symmetric unitaries can only be found in even dimensions.

[4] A two-partite version of the universal state inversion already appeared in Refs. [33, 34].

is a necessary and sufficient criterion for states to be separable [28]. Additionally, a positive transpose implies undistillability for all bipartite systems [10]..

The *computable cross norm* or *realignment* (CCNR) criterion uses the Schmidt decomposition of operators: A density matrix can be decomposed as

$$\varrho = \sum_i \mu_i G_i^A \otimes G_i^B \,. \tag{1.76}$$

Above, $\mu_i \geq 0$ and G_i^A, G_i^B form orthonormal bases of $\mathcal{H}_A$ and $\mathcal{H}_B$ with respect to the Hilbert-Schmidt inner product. The CCNR criterion states, that if ϱ is separable, then its operator Schmidt coefficients μ_i fulfill

$$\sum \mu_i \leq 1 \,. \tag{1.77}$$

Thus a state with $\sum_i \mu_i > 1$ must be entangled.

The *majorization criterion* states, that if ϱ_{AB} is separable, the decreasingly ordered eigenvalues $\lambda_i^{\downarrow}$ of ϱ_{AB} and of its reductions ϱ_A and ϱ_B fulfill

$$\begin{aligned} \sum_{i=1}^{k} \lambda_i^{\downarrow}(\varrho_{AB}) &\leq \sum_{i=1}^{k} \lambda_i^{\downarrow}(\varrho_A) \,, \\ \sum_{i=1}^{k} \lambda_i^{\downarrow}(\varrho_{AB}) &\leq \sum_{i=1}^{k} \lambda_i^{\downarrow}(\varrho_B) \qquad 1 \leq k \leq D \,. \end{aligned} \tag{1.78}$$

This type of ordering is called *majorization*, and one writes above inequalities as $\varrho_{AB} \prec \varrho_A$ and $\varrho_{AB} \prec \varrho_B$.

The *reshuffling criterion* states, that if ϱ is separable, then

$$||\varrho^R||_{\mathrm{Tr}} \leq ||\varrho||_{\mathrm{Tr}} \,, \tag{1.79}$$

where the reshuffled matrix ϱ^R is obtained in the following way: Expand the state ϱ as

$$\varrho = \sum_{ijkl} C_{ij,kl} \, |i\rangle\langle j| \otimes |k\rangle\langle l| \;, \tag{1.80}$$

the reshuffled state is then defined as

$$\varrho^R = \sum_{ijkl} C_{i\underline{k},\underline{j}l} \, |i\rangle\langle j| \otimes |k\rangle\langle l| \;. \tag{1.81}$$

Entanglement measures

Besides detecting entanglement, it is also of interest to quantify it. Thus the need for *entanglement measures*. For an entanglement measure $E(\varrho)$, all or some of the following requirements are desirable [14, 17].

1. **Faithfulness.** $E(\varrho) = 0$ if and only if ϱ is separable.
2. **Monotonicity.** Entanglement cannot be created by local operations and classical communication (LOCC), $E(\Lambda^{\mathrm{LOCC}}[\varrho]) \leq E(\varrho)$.

3. **Unitary invariance.** $E(U\varrho U^\dagger) = E(\varrho)$ for all unitaries $U = U_1 \otimes \ldots \otimes U_n$.

4. **Convexity.** $E(a\varrho + (1-a)\sigma) \leq aE(\varrho) + (1-a)E(\sigma)$ for $0 \leq a \leq 1$.

5. **Additivity.** $E(\varrho \otimes \sigma) = E(\varrho) + E(\sigma)$.

Many entanglement measures fulfill variants of these requirements. As an example, a *weakly discriminant* entanglement measure may not only vanish for all separable, but additionally also for some entangled states; the criterion of monotonicity under LOCC may be replaced by the stronger condition of *monotonicity under probabilistic* LOCCs Φ^{LOCC} of the form

$$\sum_k p_k E(\Phi_k[\varrho]) \leq E(\varrho)\,, \qquad \sum_k p_k = 1\,, \qquad p_k \geq 0\,, \tag{1.82}$$

where Φ^{LOCC} maps ϱ to $\Phi_k[\varrho]$ with probability p_k.

The *convex roof construction* can be used to extend entanglement measures defined on pure states by a decomposition of mixed into pure states. Given a measure $E(|\psi\rangle)$, its convex roof is given by

$$E(\varrho) = \inf_{p_k, |\phi_k\rangle} \sum_k p_k E(|\phi_k\rangle)\,, \tag{1.83}$$

where $\varrho = \sum_k p_k |\phi_k\rangle\langle\phi_k|$, $\sum_k p_k = 1$, and $p_k \geq 0$. The convex roof is often difficult to compute.

Entanglement measures: Examples

Below I list some bipartite entanglement measures. It is possible to roughly distinguish between geometric & entropic measures, operational measures, and algebraic measures; however there is significant overlap between these classes as e.g. certain operational measures can be interpreted in different ways.

Examples of *geometric & entropic* measures are [14, 17]:

1. **Geometric measure of entanglement.**

$$D_G(|\phi\rangle) = 1 - \sup_{|\psi\rangle = |\psi_1\rangle \cdots |\psi_n\rangle} |\,\langle\phi|\psi\rangle\,|^2\,. \tag{1.84}$$

   Its extension to mixed states is obtained by the convex roof construction.

2. **Relative entropy of entanglement.** $D_R(\varrho) = \min_{\sigma \in \text{SEP}} S(\varrho||\sigma)$.

3. **Entanglement of formation.**

$$E_F(\varrho) = \inf_{p_k, |\psi_k\rangle} \sum_k p_k S[\text{Tr}_B(|\psi_k\rangle)] \tag{1.85}$$

   is the convex roof construction of the von Neumann entropy of reductions as an entanglement measure of pure states. Thus the minimization is performed over all decompositions $\varrho = \sum_k p_k |\phi_k\rangle\langle\phi_k|$ with $\sum_k p_k = 1$ and $p_k \geq 0$.

Operational measures are often defined in terms of rates converting one type of state into another one. Examples are [14, 17]:

4. **Entanglement cost.**

$$E_C(\varrho) = \inf_{\text{LOCC}} \lim_{n\longrightarrow\infty} \frac{n_{\text{in}}}{n_{\text{out}}}\,, \tag{1.86}$$

where n_{in} is the minimal number of singlets needed to create n_{out} copies of ϱ under an optimal LOCC operation.

5. **Distillable Entanglement.**

$$E_D(\varrho) = \inf_{\text{LOCC}} \lim_{n\longrightarrow\infty} \frac{n_{\text{in}}}{n_{\text{out}}}\,, \tag{1.87}$$

where n_{out} is the maximal number of singlets obtained from n_{in} copies of ϱ under an optimal LOCC operation.

Naturally, $E_D(\varrho) \leq E_C(\varrho)$. For pure states, equality holds, and $E_D(\varrho) = E_C(\varrho) = S(\varrho_A)$ [38]. If $E_D(\varrho) = 0$, no singlets can be distilled. Accordingly, ϱ is called *undistillable*. This is in particular the case if a bipartite state has a positive partial transpose [10]. Entangled but undistillable states are called *bound entangled*.

Examples of *algebraic* measures are [14, 17]:

6. **Negativity.** $\mathcal{N}_T(\varrho) = (||\varrho^{T_A}||_1 - 1)/2$, which measures the violation of the positive partial transpose criterion [c.f. Eq. (1.75)].

7. **Reshuffling negativity.** $\mathcal{N}_R(\varrho) = (||\varrho^R||_1 - 1)/2$, which measures the violation of positivity after reshuffling ϱ to ϱ^R [c.f. Eq. (1.81)].

8. **Concurrence.** For a mixed two-qubit state, $\mathcal{C}(\varrho) = \max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}$, where $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ are the square roots of the eigenvalues of the operator $\sqrt{\varrho}\tilde{\varrho}\sqrt{\varrho}$ in descending order, and the spin-flipped state is $\tilde{\varrho} = (\sigma_y \otimes \sigma_y)\varrho^T(\sigma_y \otimes \sigma_y)$. For pure states $\varrho = |\psi\rangle\langle\psi|$, the concurrence simplifies to $\mathcal{C}(\varrho) = \sqrt{\text{Tr}(\varrho\tilde{\varrho})}$.

1.1.7 Bloch representation

Density matrices are positive Hermitian operators, having trace one. They can be expanded in a suitable operator basis. This is called the *Bloch (or Bloch-Fano) representation* [39, 40].

One qubit

Let us first consider a multipartite system composed of two-level subsystems, called *qubits*. A single pure qubit can be written as

$$|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\ . \tag{1.88}$$

Its associated density matrix then reads

$$|\phi\rangle\langle\phi| = \begin{pmatrix} \alpha^2 & \alpha\bar{\beta} \\ \bar{\alpha}\beta & \beta^2 \end{pmatrix}\ . \tag{1.89}$$

Any qubit density matrix (also those which are not pure) can be expanded in terms of the Hermitian *Pauli matrices*. These are the matrices

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{1.90}$$

The Pauli matrices $\sigma_0, \sigma_1, \sigma_2, \sigma_3$ are often also denoted by I, X, Y, Z. Following properties are crucial for what follows.

$$\begin{aligned} \sigma_i^\dagger &= \sigma_i \\ \mathrm{Tr}(\sigma_i) &= 0 \qquad\qquad \text{for } i = 1, 2, 3\,, \\ \sigma_i \sigma_j &= \delta_{ij}\sigma_0 + i\epsilon_{ijk}\sigma_k\,, \end{aligned} \tag{1.91}$$

where ϵ_{ijk} is the Levi-Civita symbol. They form an orthonormal basis with respect to the Hilbert-Schmidt inner product $\langle A, B\rangle = \mathrm{Tr}(A^\dagger B)$,

$$\mathrm{Tr}(\sigma_i \sigma_j) = 2\delta_{ij}\,. \tag{1.92}$$

A density matrix can then be expanded as

$$\varrho = \frac{1}{2}\sum_i \mathrm{Tr}(\sigma_i \varrho)\sigma_i\,. \tag{1.93}$$

Many qubits: the Pauli basis

This similarly works for multipartite states. By forming tensor products of Pauli matrices, one obtains the n-qubit *Pauli basis* of Hermitian operators acting on $(\mathbb{C}^2)^{\otimes n}$,

$$\mathcal{P}_n = \{\sigma_\alpha | \sigma_\alpha = \sigma_{\alpha_1} \otimes \ldots \otimes \sigma_{\alpha_n}\} \tag{1.94}$$

From the orthonormality of the Pauli matrices, $\mathrm{Tr}(\sigma_\alpha \sigma_\beta) = \delta_{\alpha_1\beta_1} \ldots \delta_{\alpha_n\beta_n} 2^n$ follows. Often we will write X_j, Y_j, Z_j for the Pauli matrices acting on particle j alone. Define by the $\mathrm{supp}(\sigma_\alpha)$ the support of an operator $\sigma_\alpha \in \mathcal{P}_n$, that is, the parties on which the operator σ_α acts not with the identity σ_0. The weight of an operator is then size of its support, $\mathrm{wt}(\sigma_\alpha) = |\,\mathrm{supp}(\sigma_\alpha)|$. A density matrix ϱ on n qubits can be expanded in terms of the Pauli basis as

$$\varrho = 2^{-n}\sum_{\sigma_\alpha \in \mathcal{P}_n} \mathrm{Tr}[\sigma_\alpha \varrho]\sigma_\alpha\,. \tag{1.95}$$

Given a quantum state ϱ, we obtain its reduction on parties S by acting with the partial trace on its complement S^c

$$\varrho_S = \mathrm{Tr}_{S^c}(\varrho)\,. \tag{1.96}$$

Let ϱ be expanded as in Eq. (1.95). The reduction tensored by the identity can also be written as

$$\varrho_S \otimes \mathbb{1}_{S^c} = \frac{1}{2^{|S|}}\sum_{\mathrm{supp}(\sigma_\alpha)\subseteq S} \mathrm{Tr}[\sigma_\alpha \varrho]\sigma_\alpha^\dagger\,. \tag{1.97}$$

This follows from the fact that $\mathrm{Tr}_{S^c}(\sigma_\alpha) = 0$ if $\mathrm{supp}(\sigma_\alpha) \not\subset S$.

Bloch representation in higher dimensions

Operators and density matrices in higher (but finite) dimensions can also be expanded in the Bloch representation - only an orthonormal basis has to be chosen.

A particularly nice [5] basis is the unitary but non-Hermitian *Heisenberg-Weyl* or *displacement basis* [40, 43, 44]. Define the shift and clock operators on a basis $\{|j\rangle, j = 1, \ldots, D-1\}$ for $\mathbb{C}^D$ by

$$\begin{aligned} X|j\rangle &= |j+1 \mod D\rangle \,, \\ Z|j\rangle &= \omega^j |j\rangle \,, \end{aligned} \tag{1.98}$$

where $\omega = e^{2\pi i/D}$ is a root of unity. X, Z, and ω generate the *generalized single-qubit Pauli group* $\mathcal{G}_1 = \{\omega^r X^s Z^t\}$ [45]. For even dimensions, sometimes also $\{\sqrt{\omega}^r X^s Z^t\}$ is used. The operators X and Z satisfy the relation

$$ZX = \omega XZ \,. \tag{1.99}$$

In particular, $Z^\alpha X^\beta = \omega^{\alpha\beta} X^\beta Z^\alpha$. In the case of $D = 2$, these simply reduce to the Pauli matrices, where $ZX = -XZ$. The Heisenberg-Weyl basis consists of the displacement operators

$$D(\mu, \nu) = \omega^{\mu\nu/2} X^\mu Z^\nu \,. \tag{1.100}$$

It is orthonormal, $\mathrm{Tr}[D(\mu,\nu)^\dagger D(\alpha,\beta)] = D\delta_{\mu\nu}\delta_{\alpha\beta}$. With it, operators on $\mathbb{C}^D$ can be expanded by

$$\varrho = \frac{1}{D} \sum_{\mu,\nu=0}^{D-1} \mathrm{Tr}[D(\mu,\nu)^\dagger \varrho] D(\mu,\nu) \,. \tag{1.101}$$

Another useful basis is the *generalized Gell-Mann* basis. It is given by [40, 46]

$$\begin{aligned} x_{jk} &= \sqrt{\frac{D}{2}} \big(|j\rangle\langle k| + |k\rangle\langle j| \big) \,, && 0 \le j < k < D \,, \\ y_{jk} &= \sqrt{\frac{D}{2}} \big(-i|j\rangle\langle k| + i|k\rangle\langle j| \big) \,, && 0 \le j < k < D \,, \\ z_l &= \sqrt{\frac{D}{l(l-1)}} \Big(\sum_{i=0}^{l-1} |i\rangle\langle i| - l|l\rangle\langle l| \Big) && 1 \le l < D \,. \end{aligned} \tag{1.102}$$

There are $D(D-1)/2$ symmetric elements $\{x_{jk}\}$, $D(D-1)/2$ antisymmetric elements $\{y_{jk}\}$, and $(D-1)$ diagonal elements $\{z_l\}$. The Gell-Mann basis is Hermitian and orthonormal,

$$\begin{aligned} \mathrm{Tr}(x_{ab}\, x_{\mu\nu}) = \mathrm{Tr}(y_{ab}\, y_{\mu\nu}) &= \delta_{a\mu}\delta_{b\nu} D \,, \\ \mathrm{Tr}(z_a\, z_\mu) &= \delta_{a\mu} D \,, \end{aligned} \tag{1.103}$$

with all other inner products vanishing. If $D = 2$, this basis reduces to the Pauli basis for qubits, where $x_{01} = X$, $y_{01} = Y$, and $z_1 = Z$.

[5] In fact, the Heisenberg-Weyl basis is a so-called *nice error basis*: Its elements form - up to a complex phase - a group [41, 42].

Given a basis $\{e_\alpha\}$ for a single particle, a *tensor-product basis* is obtained by taking tensor products

$$E_\alpha = e_{\alpha_1} \otimes e_{\alpha_2} \otimes \cdots \otimes e_{\alpha_n} . \tag{1.104}$$

Operators such as many-party density matrices can then be expanded as

$$\varrho = \frac{1}{D^n} \sum_\alpha \mathrm{Tr}[E_\alpha^\dagger \varrho] E_\alpha . \tag{1.105}$$

A local basis spanned by $\{D(\mu, \nu)\}$ turns out to a particularly suitable error basis for quantum error-correcting codes. Similarly as in the case of qubits, define by $\mathrm{supp}(E_\alpha)$ the support of an operator, i.e. the parties it acts non-trivially on. The weight is then the size of the support, $\mathrm{wt}(E_\alpha) = |\mathrm{supp}(E_\alpha)|$.

Lastly, the *generalized Pauli group* on n qubits $\mathcal{G}_n$ is formed by tensor-products of the single-qubit generalized Pauli group. That is, its elements are of the form

$$\omega^r X^{s_1} Z^{t_1} \otimes \cdots \otimes X^{s_n} Z^{t_n} , \tag{1.106}$$

or sometimes for even dimensions

$$(\sqrt{\omega})^r X^{s_1} Z^{t_1} \otimes \cdots \otimes X^{s_n} Z^{t_n} . \tag{1.107}$$

The necessity of $\sqrt{\omega}$ in the case of even dimensions can be seen in the case of qubits: The term $\pm 1 X^s Z^t$ can never be equal to $\pm Y$. Thus an additional phase i is needed to generate the Pauli group for 2-level systems, $\langle \pm i, \pm 1, X^s Z^t \rangle$.

1.2 Further notions

1.2.1 Graph states

Graph states are a type of states on n parties with prime dimension D each, which are completely defined by a corresponding graph [47, 48]. These states are often highly entangled [6], and can be used to construct *stabilizer codes* (also called *graph* or *additive* codes), which are a type of quantum error-correcting codes [54–56]. Additionally, graph states are a resource for measurement-based quantum computation [57, 58]. Nevertheless, they can be described by simple means - that is, by their corresponding graph. This makes them particularly useful.

A graph $G(V, E)$ is a collection of vertices $v \in V$, connected by edges $e \in E$. For each vertex i, the neighborhood $N(i)$ is defined to be the set of vertices j connected by an edge. Considering graph states on D-level systems, each edge can appear multiple times, having an up to $(D-1)$-fold multiplicity m_e (or m_{ij}). Given a graph $G = (V, E)$ of n vertices, its corresponding graph state $|G\rangle$ is defined as the common and unique $(+1)$-eigenstate of the n commuting operators $\{g_i\}$,

$$g_i = X_i \bigotimes_{j \in N(i)} Z_j^{m_{ij}} . \tag{1.108}$$

[6] Many highly entangled graph states can be obtained from graphs having a *circulant* adjacency matrix [49–52]. Also see the tables in Ref. [53].

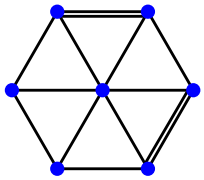


Figure 1.1: A graph state of seven qutrits. This is also an absolutely maximally entangled (AME) state (c.f. Sect. 1.2.3) [48].

Above, X and Z are the shift and clock operators,

$$\begin{aligned} X\left|j\right\rangle &= \left|j+1 \mod D\right\rangle , \\ Z\left|j\right\rangle &= \omega^{j}\left|j\right\rangle , \end{aligned} \tag{1.109}$$

where $\omega = e^{2\pi i/D}$ is a root of unity. In the case of $D = 2$, these simply reduce to the Pauli matrices. The set $\{g_i\}$ is called the *generator*. To obtain $|G\rangle\langle G|$ in the Bloch decomposition, the notion of its stabilizer is helpful. The *stabilizer* S is the Abelian group obtained by the multiplication of generator elements,

$$S = \left\{ \prod g_1^{i_1} g_2^{i_2} \cdots g_n^{i_n} \;\middle|\; i_1, \ldots, i_n \in \{1, \ldots, D-1\} \right\}. \tag{1.110}$$

Each of its D^n elements are said to stabilize the state, that is, $g_i\left|G\right\rangle = \left|G\right\rangle$ for all g_i. The stabilizer forms a subgroup of the *generalized Pauli group* (c.f. Sect. 1.1.7). In the case of qubits, this group simply reduces to the n-party Pauli-group $\mathcal{G}_n$, which consists of all elements in $\mathcal{P}_n$ in addition to a complex phase $\{\pm 1, \pm i\}$. With the notion of the stabilizer, the graph state can be written as

$$|G\rangle\langle G| = \frac{1}{2^n} \sum_{s_a \in S} s_a \,. \tag{1.111}$$

On the other hand, it can be shown that the graph state can also be written as

$$\left|G\right\rangle = \prod_{e \in E} \mathrm{CZ}_e^{m_e} \left|\bar{0}\right\rangle^{\otimes n} . \tag{1.112}$$

Above, the generalized controlled-Z gate CZ acting on the two parties of edge $e = (i, j)$ reads,

$$\mathrm{CZ}_{ij} = \sum_{k=0}^{D-1} |k\rangle\langle k|_i \otimes Z_j^k = \sum_{k,l=0}^{D-1} \omega^{kl} |k\rangle\langle k|_i \otimes |l\rangle\langle l|_j \,. \tag{1.113}$$

Furthermore, $\left|\bar{0}\right\rangle$ is obtained by the Fourier gate, $\left|\bar{k}\right\rangle = F^\dagger \left|k\right\rangle$, where

$$F = \frac{1}{\sqrt{D}} \sum_{k,l=0}^{D-1} \omega^{kl} \left|k\right\rangle \left\langle l\right| . \tag{1.114}$$

Therefore, $\left|\bar{0}\right\rangle = \frac{1}{\sqrt{D}} \sum_i \left|i\right\rangle$. To obtain the graph state, the state is initialized in $\left|\bar{0}\right\rangle^{\otimes n}$ and conditional phase gates CZ_{ij} are applied corresponding to the graph. In the

case of qubits, $|\bar{0}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, and CZ_{ij} is the controlled Z gate

$$\mathrm{CZ}_{ij} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} . \tag{1.115}$$

Local unitary equivalence of graph states

Let us for now focus on graph states for qubits. To understand when two non-isomorphic graphs give non-identical but comparable quantum states, let us make a small detour: When comparing quantum states, equivalence up to local unitaries (LU) is often considered. That is, two n-qubit states ϱ and σ are said to be *LU-equivalent* if there exist the unitaries $U_1, \ldots, U_n \in SU(2)$, such that

$$\varrho = U_1 \otimes \cdots \otimes U_n \; \sigma \; U_1^\dagger \otimes \cdots \otimes U_n^\dagger . \tag{1.116}$$

If no such unitaries exist, the states are said to be LU-inequivalent.

An interesting subset of unitaries to consider is the so-called *local Clifford group* $\mathcal{C}_n^l$. It is obtained by the n-fold tensor product of the one-qubit Clifford group $\mathcal{C}_1$, generated by

$$\mathcal{C}_1 = \left\langle H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \right\rangle . \tag{1.117}$$

The group $\mathcal{C}_1$ maps the one-qubit Pauli group $\mathcal{G}_1 = \langle \pm i, \pm 1, X, Y, Z \rangle$ to itself under conjugation. The n-qubit local Clifford group $\mathcal{C}_n^l = \mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_1$ (n times) then similarly maps the n-qubit Pauli group $\mathcal{G}_n = \mathcal{G}_1^{\otimes n}$ to itself under conjugation. Interestingly, it was shown that the action of local Clifford operations on a graph state can be understood as a sequence of *local complementations* on the corresponding graph [59]. This works in the following way: Given a graph G, the local complementation with respect to vertex j is defined as the complementation of the subgraph in G consisting of all vertices in its neighborhood $N(j)$ and their associated edges. That is, each edge occurring in the neighborhood of vertex j is removed, while previously missing edges are added. We conclude, that for two graphs being in the same local complementation orbit, their corresponding graph states must be equivalent under the action of local Clifford operations, and vice versa. Thus they must also be LU-equivalent. The contrary however is not necessarily true: It has been shown that there are LU-equivalent graph states that are not also local Clifford equivalent [60, 61].

1.2.2 Quantum exponential families

Considering a quantum state of interest, one might ask, whether or not this state could possibly exist in naturally occurring systems. Similarly, an experimentalist would be interested in preparing a desired state in the laboratory. However, both the experimentalist as well as nature mostly have access to *local interactions* only - this is because higher-order interactions are both suppressed in quantum field theory, as well as difficult to engineer artificially. Additionally, under sufficient conditions, physical systems thermalize when left alone for long enough [62]. That is, they have

the form of a *thermal state* $\varrho = e^{-\beta H}/\operatorname{Tr}(e^{-\beta H})$, where H is the Hamiltonian of the system and β the inverse temperature. In the limit of $\beta \to \infty$, the density matrix becomes proportional to the projector onto the *ground state* space. This Section is concerned with the classification of thermal states according to the interaction structure present in their Hamiltonians. This leads to the notion of *quantum exponential families*, and to that of *irreducible correlations*.

This approach is also of interest for aspects of statistical physics: According to Jaynes' *maximum entropy principle*, the classical probability distribution that describes the current knowledge best is the one that maximizes the Shannon entropy [63, 64]. Thus given expectation values $\mathbb{E}[A_i(x)] = a_i$ of functions A_i, one wishes to solve the optimization problem

$$\text{maximize} \qquad -\int_x p(x)\log p(x) d\mu(x) \tag{1.118}$$

$$\text{subject to} \qquad \int_x p(x) A_i(x) d\mu(x) = \mathbb{E}[A_i(x)] = a_i \tag{1.119}$$

$$\int_x p(x) d\mu(x) = 1\,, \qquad p(x) \geq 0\,. \tag{1.120}$$

The resulting probability distribution can be seen as being maximally unbiased or non-committal with respect to missing information, while being consistent with all known constraints. Starting with a set of observables $\{A_i\}$, this results in the classical *exponential families*, a class of distributions with parameters $\{\theta_i\}$ having the form

$$p_\theta(x) = \exp\left[\sum_i \theta_i A_i(x) - \psi(\theta)\right], \tag{1.121}$$

$$\psi(\theta) = \log \int \exp[\sum_i \theta_i A_i(x) d\mu(x)]\,. \tag{1.122}$$

A similar reasoning can be applied to density matrices: the maximization of the von Neumann entropy (c.f. Sect. 1.1.5) under a set of constraints $\{\langle A_i\rangle\}$ singles out thermal states of the form

$$\varrho = \frac{\exp(\sum \lambda_i A_i)}{\operatorname{Tr}\exp(\sum \lambda_i A_i)} \tag{1.123}$$

as the maximally unbiased description of physical states [65]. The development of quantum exponential families as part of information geometry was then strongly shaped by the work of Amari for classical exponential families [66, 67]: A hierarchy of exponential families is defined, obtained by considering increasingly local correlation structures. This led to the notions of the classical information projection, the k-body irreducible interactions, and a Pythagorean relation for the classical relative entropy (also called Kullback-Leibler divergence). In the following, the corresponding constructions are presented for quantum states.

Thermal states of few-body Hamiltonians

Let us consider systems of spin-$1/2$ particles. A two-local (or two-body) Hamiltonian of a system consisting of N particles can be written as

$$H = \sum\nolimits_{i,j=1}^{N} \sum\nolimits_{\alpha\beta} \lambda_{\alpha\beta}^{(ij)} \sigma_\alpha^{(i)} \otimes \sigma_\beta^{(j)}\,, \tag{1.124}$$

where $\sigma_\alpha^{(i)}$ denotes a Pauli matrix $\{\mathbb{1}, \sigma_x, \sigma_y, \sigma_z\}$ acting on the i-th particle. Note that the identity matrix is included, so H can also contain single particle terms. We denote the set of all possible two-local Hamiltonians by $\mathcal{H}_2$ and in an analogous manner the set of k-local Hamiltonians by $\mathcal{H}_k$. An example for a two-local Hamiltonian is the Heisenberg model having nearest-neighbor interactions. However, this approach generally ignores any geometrical arrangement of the particles. This motivates the following definition for the so-called *quantum exponential family*.

Definition 6. *The exponential family $\mathcal{Q}_2$ of thermal states of two-local Hamiltonians is given by*

$$\mathcal{Q}_2 = \left\{ \tau \,\middle|\, \tau = \frac{e^{-\beta H}}{\mathrm{Tr}[e^{-\beta H}]}, H \in \mathcal{H}_2 \right\}. \tag{1.125}$$

Ground states can be reached in the limit of infinite inverse temperature β [7]. For any k, the exponential families $\mathcal{Q}_k$ can be defined in a similar fashion. The set $\mathcal{Q}_1$ consists of mixed product states, the set $\mathcal{Q}_N$ of the full state space. The exponential families form the hierarchy $\mathcal{Q}_1 \subseteq \mathcal{Q}_2 \subseteq \cdots \subseteq \mathcal{Q}_N$, and a suitable βH can be seen as a way of parameterizing a specific density matrix $\tau = e^{-\beta H}/\,\mathrm{Tr}[e^{-\beta H}]$. The question arises, what states are in $\mathcal{Q}_k$? And for those which are not, what is their best approximation by states in $\mathcal{Q}_k$? This will lead to the concepts of the *information projection* and of *irreducible higher-order interactions*.

To make connections with concepts of recent interest, it was shown that states in $\mathcal{Q}_2$ whose individual Hamiltonian interaction terms are so-called shield commuting are equivalent to quantum Markov networks [71]: if a state can be written as $\tau = e^H/\,\mathrm{Tr}(e^H)$, where $H = H_{AB} + H_{BC}$ with $[H_{AB}, H_{BC}] = 0$, then ϱ shows a vanishing conditional mutual information between the two regions A and C that are shielded by the region B,

$$I(A:C|B) = S(\varrho_{AB}) + S(\varrho_{BC}) - S(\varrho_{ABC}) - S(\varrho_B) = 0\,. \tag{1.126}$$

One says that $A-B-C$ forms a quantum Markov chain. This result [8] resonates with the Hammersley-Clifford theorem, which shows that classical Markov networks, whose nodes are only dependent on their direct neighbors, can be expressed as a classical thermal state with local two-body interactions only [76, 77].

Information projection

Here I present some results on the characterization of quantum exponential families [78, 79]. Given a state ϱ, consider its distance from the exponential family $\mathcal{Q}_2$ in terms of the relative entropy (or divergence) $S(\varrho||\tau) = \mathrm{Tr}[\varrho(\log(\varrho) - \log(\tau))]$ (c.f.

[7] Note that in general, calculating ground or thermal states is numerically and analytically hard [68–70].

[8] Furthermore, it has recently been shown that also *approximate* Markov chains on one-dimensional lattices can be represented by thermal states of (geometrically) local Hamiltonians [72], and that Gibbs states of local Hamiltonians on lattices can be well-approximated by certain tensor network methods [73]. If the mutual information [Eq. 1.126] is not too large for some state ϱ_{ABC}, then a positive map $\mathrm{id}_A \otimes \mathcal{T}_{B\to BC}$ can be found to approximately reconstruct ϱ_{ABC} from its marginal ϱ_{AB} [74]. Further interesting aspects regarding local Hamiltonians, such as area laws and the spreading of correlations (so-called Lieb-Robinson bounds), can be found in Ref. [75].

Sect. 1.1.5). As the closest state to ϱ in $\mathcal{Q}_2$, one obtains the so-called *information projection* $\tilde{\varrho}_2$.

Definition 7. *The information projection $\tilde{\varrho}_k$ of a state ϱ is the unique closest state in $\mathcal{Q}_k$ in terms of the relative entropy,*

$$\tilde{\varrho}_k = \mathrm{argmin}_{\tau\in\mathcal{Q}_k} S(\varrho||\tau)\,. \tag{1.127}$$

Following equivalent characterizations of the information projection are known:

Proposition 1 ([78, 79])**.** *Let ϱ be a quantum state, and $\tilde{\varrho}_k$ its information projection. Then (a) $\tilde{\varrho}_2$ is the unique minimizer of the relative entropy of ϱ from the set $\mathcal{Q}_2$,*

$$\tilde{\varrho}_2 = \mathrm{argmin}_{\tau\in\mathcal{Q}_2} S(\varrho||\tau)\,. \tag{1.128}$$

(b) Of the set of states having the same two-body reduced density matrices (2-RDMs) as ϱ, denoted by $\mathcal{M}_2(\varrho)$, $\tilde{\varrho}_2$ has a maximal von Neumann entropy

$$\tilde{\varrho}_2 = \mathrm{argmax}_{\mu\in\mathcal{M}_2(\varrho)} S(\mu)\,. \tag{1.129}$$

(c) Finally, $\tilde{\varrho}_2$ is the unique intersection of $\mathcal{Q}_2$ and $\mathcal{M}_2(\varrho)$.

From (b) it follows that if for a state σ another state ϱ of higher entropy but having the same 2-RDMs can be found, then σ must lie outside of $\mathcal{Q}_2$. This fact will be used in Chpt. 2 to characterize the convex hull $\mathrm{conv}(\mathcal{Q}_2)$.

Irreducible interactions

The *irreducible higher-order interaction* of a state is defined by its relative entropy distance to $\mathcal{Q}_k$,

$$D_k(\varrho) = S(\varrho||\tilde{\varrho}_k)\,. \tag{1.130}$$

States not in $\mathcal{Q}_2$ are said to have irreducible interactions of order three or higher, because they contain information which is not already present in their 2-RDMs. This can be seen from the characterization in Eq. (1.129): The 2-RDMs are then already sufficient to reconstruct the global state from its marginals, according to Jaynes' maximum entropy principle [63, 80]. This is conceptionally nice, but also has certain drawbacks. Importantly, the irreducible interaction, as quantified by the relative entropy, is not continuous, as shown in Ref. [81]. In addition, the relative entropy is difficult to estimate experimentally without doing state reconstruction, so other distances such as the fidelity are preferable. These properties make the relative entropy somewhat problematic and give further reasons why we will consider the convex hull $\mathrm{conv}(\mathcal{Q}_k)$ in Chpt. 2.

From the Pythagorean relation [c.f Eq. (1.139)] [82], one has

$$S(\varrho||\tilde{\varrho}_1) = S(\varrho||\tilde{\varrho}_{n-1}) + S(\tilde{\varrho}_{n-1}||\tilde{\varrho}_{n-2}) + \cdots + S(\tilde{\varrho}_2||\tilde{\varrho}_1)\,. \tag{1.131}$$

Thus the correlations of a state can be decomposed into

$$\begin{aligned} D_k(\varrho) &= D_{n-1}(\varrho) + D_{n-2}(\tilde{\varrho}_{n-1}) + \cdots + D_k(\tilde{\varrho}_{k+1}) \\ &= C_n(\varrho) + C_{n-1}(\varrho) + \cdots + C_{k+1}(\varrho)\,, \end{aligned} \tag{1.132}$$

where $C_i(\varrho) = D_{i-1}(\tilde{\varrho}_i)$. Because the quantities $D_{k\geq 2}$ can increase under local operations, the $C_i(\varrho)$ as attributable to i-body interactions should be seen as measuring complexity, rather than as measuring entanglement [78].

Quantum information geometry

The *marginal set* $\mathcal{M}_k(\varrho)$ consists of quantum states having the same k-party reduced density matrices (k-RDMs) as ϱ

$$\mathcal{M}_k(\varrho) = \{\mu \,|\, \mu_A = \varrho_A \text{ for all } |A| \leq k\}\,, \tag{1.133}$$

where μ_A is the reduced state obtained by tracing out all subsystems not contained in A. This set is convex, as states stay in the marginal family under convex combination. Recall that the exponential family $\mathcal{Q}_k$ consists of thermal states of k-local Hamiltonians

$$\mathcal{Q}_2 = \left\{\tau \,\middle|\, \tau = \frac{e^H}{\mathrm{Tr}[e^H]}\,, H \in \mathcal{H}_2\right\}. \tag{1.134}$$

In contrast to the marginal set, the exponential families $\mathcal{Q}_k$ are, apart from $\mathcal{Q}_n$, not convex. To see this, note that $\mathrm{conv}(\mathcal{Q}_1)$ is the set of separable states, having a volume and a number of free parameters corresponding to the dimension of the state space. In addition, $\mathrm{conv}(\mathcal{Q}_k)$ is larger than the set of separable states for $k \geq 2$. However, $\mathcal{Q}_k$ has not as many free parameters and is a set of measure zero. Thus $\mathcal{Q}_k \subsetneq \mathrm{conv}(\mathcal{Q}_k)$, and $\mathcal{Q}_k$ cannot be convex.

The relations between the marginal set and the exponential family originate in two special ways to parametrize a quantum state [83]. These are the affine (also called mixed) and the exponential representations

$$\begin{aligned} \varrho_{\text{aff}} &= \mathbb{1}/D + \eta_i A_i\,, & \eta &\in [-1,1]^{D^2-1}\,, \\ \varrho_{\exp} &= \exp[\theta_i A_i - \psi(\theta)]\,, & \theta &\in \mathbb{R}^{D^2-1}\,, \end{aligned} \tag{1.135}$$

where D is the dimension of the system, $\{A_i\}$ is a suitable orthonormal basis of the operator space, and we sum over repeated indices. The Massieu function $\psi(\theta) = \log \mathrm{Tr}[\exp H]$ is not only required for normalization, but also defines, together with the potential $\phi(\eta) = -S(\eta) = \mathrm{Tr}[\varrho \log \varrho]$, a Legendre transform $\psi(\theta) + \phi(\eta) - \theta_i \eta_i = 0$. The relations

$$\eta_i = \frac{\partial \psi(\theta)}{\partial \theta_i} = \mathrm{Tr}[\varrho A_i] \qquad \text{and} \qquad \theta_i = \frac{\partial \phi(\eta)}{\partial \eta_i} = \mathrm{Tr}[H A_i] \tag{1.136}$$

follow. For any two states $\varrho(\eta)$ and $\varrho'(\theta')$, the following *Pythagorean relation* for the relative entropy holds [82]

$$S(\varrho||\varrho') = \phi(\eta) + \psi(\theta') - \eta_i \theta'_i\,, \tag{1.137}$$

and its repeated application yields

$$S(\varrho||\varrho'') = S(\varrho||\varrho') + S(\varrho'||\varrho'') + (\eta_i - \eta'_i)\cdot(\theta'_i - \theta''_i)\,. \tag{1.138}$$

Recall that the *information projection* $\tilde{\varrho}_k$ of ϱ is the element in $\mathcal{M}_k(\varrho)$ having the largest von Neumann entropy. Given ϱ, its information projection $\tilde{\varrho}_k$, and a $\tau \in \mathcal{Q}_k$, the Pythagorean relation then simplifies to

$$S(\varrho||\tau) = S(\varrho||\tilde{\varrho}_k) + S(\tilde{\varrho}_k||\tau)\,. \tag{1.139}$$

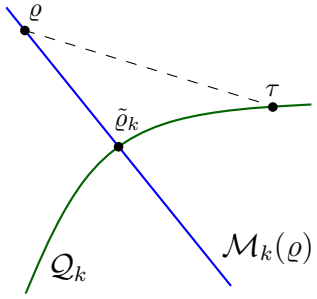


Figure 1.2: The information projection $\tilde{\varrho}_k$ lies in the unique intersection of $\mathcal{Q}_k$ and $\mathcal{M}_k(\varrho)$. It is also the minimizer of the relative entropy $S(\varrho||\cdot)$ in $\mathcal{Q}_k$.

Thus the above definition of the information projection is equivalent to $\tilde{\varrho}$ being in the unique intersection of the exponential family $\mathcal{Q}_k$ with $\mathcal{M}_k(\varrho)$, and to

$$\tilde{\varrho}_k = \operatorname{argmin}_{\tau\in\mathcal{Q}_k} S(\varrho||\tau)\,. \tag{1.140}$$

This is illustrated in Fig. 1.2.

Let us consider two examples. First, consider the five-qubit ring cluster state $|C_5\rangle$ (c.f. Fig. 1.2.3) and its information projection onto $\mathcal{Q}_2$. The state $|C_5\rangle$ has maximally mixed 2-body marginals, and of the set $\mathcal{M}_2(|C_5\rangle)$, the maximally mixed state has the highest entropy. Second, consider the one-parameter family of states $|GHZ_\alpha\rangle = (|000\rangle + e^{i\alpha}|111\rangle)/\sqrt{2}$. All of its two-party reduced states are equal to $(|00\rangle\langle 00| + |11\rangle\langle 11|)/2$. Also,

$$\begin{aligned}\gamma &= \int_\alpha |GHZ_\alpha\rangle\langle GHZ_\alpha|\,\mathrm{d}\alpha \\ &= (|000\rangle\langle 000| + |111\rangle\langle 111|)/2\end{aligned} \tag{1.141}$$

has the same 2-RDMs and is thus an element of the marginal set $\mathcal{M}_2(|GHZ_\alpha\rangle)$. Additionally, γ is the information projection of $|GHZ_\alpha\rangle$ onto $\mathcal{Q}_2$, as it is the element of maximum entropy in $\mathcal{M}_2(|GHZ_\alpha\rangle)$. As known from Ref. [84], almost all three qubit states are determined by their 2-RDMs, and thus the irreducible three-body correlation is discontinuous at $|GHZ_\alpha\rangle$. More examples can be found in Ref. [79].

1.2.3 Absolutely maximally entangled (AME) states

Multiparticle entanglement is central for the understanding of the possible quantum advantages in metrology or information processing. When investigating multiparticle entanglement as a resource, the question arises which quantum states are the most entangled. Considering pure bipartite states, maximally entangled states have maximally mixed reductions, such as the Bell state in Eq. (1.32). Considering bipartite entanglement measures, one can argue that states which are maximally entangled across any bipartition show the strongest form of entanglement [85, 86]. Accordingly, these states are also known as *absolutely maximally entangled* (AME) [44, 48, 87–101]. The following definition makes this precise.

Definition 8 (AME states)**.** *A pure state of n parties, having D levels each, is called* absolutely maximally entangled *(AME), if all reductions to $\lfloor \frac{n}{2} \rfloor$ parties are maximally mixed.*

Then maximal possible entanglement is present across each bipartition. Note that when writing an AME state in its Schmidt decomposition across a bipartition $A|B$ with $k = |A| \leq |B|$, it can with the help of Eq. (1.35) be brought into the following form [88],

$$|\phi_{n,D}\rangle = \sum_{i_1 i_2 \ldots i_k} |i_1\rangle |i_2\rangle \ldots |i_k\rangle |\phi_{i_1 i_2 \ldots i_k}\rangle \ . \tag{1.142}$$

Here, $|i_1\rangle, \ldots |i_k\rangle$ form a computational basis for the parties $\{1 \ldots k\}$, and the states $\{|\phi_{i_1 i_2 \ldots i_k}\rangle\}$ are mutually orthogonal.

Well-known examples of AME states are the Bell and GHZ states [Eqs. (1.32) and (1.46)] on two and three parties respectively. AME states have been shown to be a resource for a variety of quantum information-theoretic tasks that require maximal entanglement amongst many parties, such as open-destination teleportation, entanglement swapping, and quantum secret sharing [102, 88, 99]. They can be seen as quantum error-correcting codes having parameters $((n, 1, \lfloor \frac{n}{2} \rfloor + 1))_D$ (c.f. Def. 9), and are key building blocks for holographic quantum error-correcting codes [103–105] [9]. Thus, it is a natural question to ask for what number of parties and local dimensions such states may exist [44, 85, 86].

The existence of AME states composed of two-level systems was until recently still unresolved: Qubit AME states were known to exist for $n = 2, 3, 5,$ and 6 parties, all of which can be expressed as graph or stabilizer states, see Fig. 1.2.3 [44]. Of particular interest was the case of four parties: While the existence of an AME state was ruled out [86], best approximations (where not all reductions are maximally mixed) have been presented [10] [96]. The existence of AME states of eight or more qubits was excluded by linear programming bounds, using the so-called shadow enumerator [44, 106, 107]; see also the bounds in Eq. (1.165) and Chpt. 5. The last case concerning seven qubits was a long-standing open problem, first raised by Calderbank et. al in a seminal article on the connection between qubit stabilizer codes and classical codes over $GF(4)$ [108] (c.f. Sect. 1.2.4). I will address this question in Chpt. 3, where the existence of such a state is ruled out. This solves the problem of AME states in the case of qubits [109].

Concerning larger local dimensions, the existence of AME states is only partially resolved. Scott obtained the following bound on the existence of AME states [44].

Proposition 2 (Scott bound)**.** *An AME state of n parties having D levels each fulfills*

$$n \leq \begin{cases} 2(D^2 - 1) & n \text{ even}, \\ 2D(D+1) - 1 & n \text{ odd}. \end{cases} \tag{1.143}$$

I will present a proof of this bound in Sect. 3.3. Curiously enough, AME states exist for any number of parties, if the dimension of the subsystems is chosen large enough [99]. Furthermore, different constructions for such states have been put forward, based on graph states [47, 48], classical maximum distance separable codes [99, 110], and combinatorial designs [91, 111]. As an example, the rightmost

[9] AME states are also called *perfect tensors* in this context.

[10] The case of four parties remains intriguing; an open problem concerns the four-party AME state with $D = 6$.

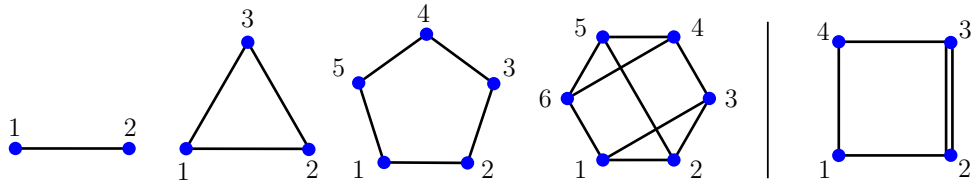


Figure 1.3: Left: qubit AME states on $n = 2, 3, 5, 6$ parties can be expressed as graph states. Right: from this graph, AME states for all odd prime dimensions can be obtained.

graph depicted in Fig. 1.2.3 is a four-party AME state for all odd prime dimensions [48]. However, for many cases it is still unknown if AME states can exist: For the current status of this question, see Table 5.2 in Chpt. 5 and Problem 35 in the list of Open Quantum Problems of the IQOQI Vienna [112].

1.2.4 Quantum error-correcting codes

Quantum information processing inevitably happens in the presence of disturbance from the environment. This can introduce errors on the information carriers, which are quantum states. In order to subsequently recover the information from these disturbances, some sort of error-correction has to be performed. *Quantum error-correcting codes* (QECC) allow for such a mechanism. More precisely, a QECC is a subspace of the Hilbert space, that can be reconstructed completely if only certain types of disturbances occur. The mere existence of such error-correcting techniques in the quantum domain is already highly surprising for several reasons [113, 114]:

1. Quantum errors: While classical errors are discrete, quantum errors are continuous by nature. Thus it is unclear if any methods from the theory of discrete classical error-correcting codes can be adapted to quantum errors.

2. No-cloning: The information has to be encoded in some sort of redundant way. However, the no-cloning theorem forbids to simply copy an unknown state (c.f. Sect. 1.1.3).

3. Measurement: In order to correct an error, information about it has to be acquired. A measurement of the system however will collapse the wave function and is likely to destroy the information encoded in the state.

To address these challenges, consider the simplest error-correcting code, the three-qubit bit-flip code: Define the two logical states

$$\begin{aligned} |0_L\rangle &= |000\rangle \ , \\ |1_L\rangle &= |111\rangle \ . \end{aligned} \tag{1.144}$$

During the encoding, any superposition $\alpha\,|0\rangle + \beta\,|1\rangle$ will thus be mapped to $\alpha\,|000\rangle + \beta\,|111\rangle$ [11]. Any (qu)bit-flip on a single party, e.g. a on the third party, mapping $|000\rangle$ to $|001\rangle$ and $|111\rangle$ to $|110\rangle$, can be detected by majority voting. Note that in order

[11] Note that this is not the same as making two additional copies of the state, as in $(\alpha\,|0\rangle + \beta\,|1\rangle\,) \longrightarrow (\alpha\,|0\rangle + \beta\,|1\rangle)(\alpha\,|0\rangle + \beta\,|1\rangle)(\alpha\,|0\rangle + \beta\,|1\rangle)$.

to do this, we cannot simply measure each qubit - this would collapse the state, destroying the encoded information. Instead, a *syndrome measurement* is done: By performing the parity measurements Z_1Z_2 and Z_2Z_3, the position of the bit-flip error can be identified. In practice, this is done by coupling a helper qubit, termed *ancilla*, by conditional gates $\mathrm{CZ}_{ij} = \mathrm{diag}(1,1,1,-1)$ between parties i and j. To implement the parity measurement e.g. Z_1Z_2, the ancilla (on position 4) is coupled with the gates CZ_{14} and CZ_{24}. Measuring the ancilla with Z_4, the outcome will be $+1$ if the first and second qubit are in the same state, and -1 otherwise. The parity measurement Z_2Z_3 is performed in a similar way. Crucially, the logical states, being eigenvectors of Z_1Z_2 and Z_2Z_3, are left undisturbed. After the identification of the error, it can subsequently be corrected by a recovery operation, which in the case of $\langle Z_1Z_2\rangle = 1$ and $\langle Z_2Z_3\rangle = -1$ consists of an X_3 gate on the third qubit.

With this, the problem of cloning quantum states and of state collapse by the measurement is circumvented. The continuous nature of quantum errors can further be addressed by recognizing that any error can linearly be decomposed into a discrete set of errors. If a code is able to correct these, their linear combination can also be corrected [115].

Definition of QECC

From the operational perspective, a subspace $\mathcal{C}$ is a quantum error-correcting code if there exists a recovery procedure $\mathcal{R}$ which corrects the error map $\mathcal{E}$. Thus one requires that

$$\mathcal{R} \circ \mathcal{E} \propto \mathcal{I} \quad \text{on } \mathcal{C}\,. \tag{1.145}$$

The errors or noise acts on states in $(\mathbb{C}^D)^{\otimes n}$ as a completely positive trace preserving (CPTP) superoperator $\mathcal{E}(\cdot)$. As any CPTP map, $\mathcal{E}$ can be decomposed in the Kraus representation (c.f. Sect. 1.1.3) [8],

$$\mathcal{E}(\cdot) = \sum_\mu E_\mu(\cdot)E_\mu^\dagger\,, \qquad \text{with } \sum_\mu E_\mu^\dagger E_\mu = \mathbb{1}\,, \tag{1.146}$$

with Kraus operators $\{E_\mu\}$. The recovery map $\mathcal{R}$ is often explicitly given, however for the definition of the code, only its existence is required. This is guaranteed if the following requirements, the so-called Knill Laflamme conditions, are met.

Theorem 3 (Knill-Laflamme [116])**.** *Let $\Pi_\mathcal{C}$ be the projector onto the code $\mathcal{C}$. A necessary and sufficient condition for the existence of an error-recovery operation $\mathcal{R}$ to correct a set of errors $\{E_\alpha\}$ is that*

$$\Pi_\mathcal{C} E_\mu^\dagger E_\nu \Pi_\mathcal{C} = C_{\mu\nu}\Pi_\mathcal{C}\,, \tag{1.147}$$

where the matrix $C = (C_{\mu\nu})$ is Hermitian.

If the set of errors $\{E_\mu\}$ can be corrected, then so can the error map $\mathcal{E}(\cdot) = \sum_\mu E_\mu(\cdot)E_\mu^\dagger$. This can be seen by the linear decomposition of $\mathcal{E}$ in terms of error operators E_μ. Thus the problem of correcting a continuum of errors is turned into one of correcting a discrete set.

For the purposes of this thesis we are concerned with any kind of local but independent errors. Thus we adapt a notion which is derived from Thm. 3, where the concept of a specific error map is replaced with that of local errors. A *local error*

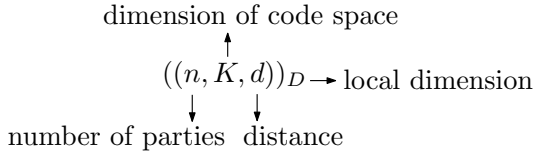


Figure 1.4: Parameters of quantum codes.

basis $\{E_\alpha\}$ is given by the n-fold tensor product of a single-particle operator basis $\{e_j\}$, which includes the identity, $e_0 = \mathbb{1}$. Then the notion of the *weight* $\mathrm{wt}(E_\alpha)$ of a basis element is well-defined, which is the number of sites it acts non-trivially on. A suitable basis is the Heisenberg-Weyl basis, as introduced in Sect. 1.1.7. Note however that the notions that follow are independent of any particular local error basis chosen, as long as as the identity is included in the basis. A quantum error-correcting code is then defined in the following way.

Definition 9 (QECC [44, 117])**.** *A quantum error-correcting code $\mathcal{C}$ with distance d on a system of n parties having local dimension D each is defined as a K-dimensional subspace $\mathcal{C}$, such that for any orthonormal basis $\{|j_\mathcal{C}\rangle\}$ of $\mathcal{C}$ the Knill-Laflamme error conditions hold for all errors of weight less than d,*

$$\langle i_\mathcal{C}| E_\alpha |j_\mathcal{C}\rangle = \delta_{ij} C(E_\alpha) \qquad \forall E_\alpha \in \{E_\alpha\} : \mathrm{wt}(E_\alpha) < d\,. \tag{1.148}$$

Thus any error E_α of weight less than the distance d affects all states lying in the code space in the same way. The notation $((n, K, d))_D$ is used to refer to such codes, see Fig. 1.4. If $K = D^k$ for some integer k, this can be seen as encoding k logical quDits into n physical quDits, and the parameters are then often written as $[[n, k, d]]_D$ [12]. If $C(E) = \mathrm{Tr}(E)/D^n$, the code is called *pure*. By convention, codes with $K = 1$ (also called *self-dual*) are only considered codes if they are pure. Thus a self-dual code of distance d, described by a projector $\Pi_\mathcal{C} = |\psi\rangle\langle\psi|$, fulfills $\mathrm{Tr}(E_\alpha|\psi\rangle\langle\psi|) = 0$ for all $E_\alpha \neq \mathbb{1}$ of weight smaller than d. Therefore these are simply pure quantum states whose reductions onto $(d-1)$ parties are all maximally mixed, and are also called $(d-1)$-uniform states. In particular, AME states, whose reductions onto $\lfloor \frac{n}{2} \rfloor$ parties are maximally mixed, are self-dual QECC having the parameters $((n, 1, \lfloor \frac{n}{2} \rfloor + 1))_D$.

A code with distance d can then be used to correct $t = \lfloor (d-1)/2 \rfloor$ errors. This leads to an equivalent formulation for a quantum error-correcting code to have distance d, the requirement being

$$\langle i_\mathcal{C}| E_\alpha^\dagger E_\beta |j_\mathcal{C}\rangle = C_{\alpha\beta}\delta_{ij} \tag{1.149}$$

for any orthonormal code basis $\{|i_\mathcal{C}\rangle\}$ spanning $\mathcal{C}$ and all E_α, E_β with weights not larger than $t = \lfloor (d-1)/2 \rfloor$.

Making new codes from old

Often, new codes can be created from known ones. Taking the partial trace over subsystems of a pure code, its *reduction* can be obtained.

[12] Sometimes this notation is exclusively used for stabilizer codes, which will be introduced in Sect.1.2.4.

Theorem 4 (Rains [118], Theorem 20). *Suppose $\mathcal{C}$ is a pure $((n, K, d))_D$ code with $n, d \geq 2$. Then there exists a pure $((n-1, DK, d-1))_D$.*

Two codes can also be *concatenated*, that is, the encoding is performed in series. This new code is constructed by encoding each system of dimension D_2 of an *outer code* $\mathcal{C}_2$ using an *inner code* $\mathcal{C}_1$ having $K_1 = D_2$ codewords [119, 120].

Theorem 5 (Rains [118], Theorem 21). *Let $\mathcal{C}_1$ be a $((n_1, K_1, d_1))_{D_1}$ and $\mathcal{C}_2$ be $((n_2, D_1, d_2))_{D_2}$. Let $\mathcal{C} = \mathcal{C}_2(\mathcal{C}_1)$ be any concatenation of $\mathcal{C}_1$ and $\mathcal{C}_2$. Then $\mathcal{C}$ is a $((n_1 n_2, K_1, d))_{D_2}$, with a minimal distance d of at least $d_1 d_2$.*

As an example, the *Shor code* [115] is a concatenation of a three-qubit outer code, protecting against single-qubit phase-flips,

$$\begin{aligned} |0\rangle &\longrightarrow |{+}{+}{+}\rangle \\ |1\rangle &\longrightarrow |{-}{-}{-}\rangle \ , \end{aligned} \tag{1.150}$$

with a three-qubit inner code that protects against single-qubit bit-flips,

$$\begin{aligned} |+\rangle &\longrightarrow |000\rangle + |111\rangle \\ |-\rangle &\longrightarrow |000\rangle - |111\rangle \ . \end{aligned} \tag{1.151}$$

Concatenated, they protect against any error on a single qubit, and thus form a $((9, 2, 3))_2$. The code space is spanned by the *logical vectors* $|0_L\rangle$ and $|1_L\rangle$, where

$$\begin{aligned} \frac{1}{\sqrt{2}}\big(\,|0_L\rangle + |1_L\rangle\,\big) &\propto \big(\,|000\rangle + |111\rangle\,\big)\big(\,|000\rangle + |111\rangle\,\big)\big(\,|000\rangle + |111\rangle\,\big)\,, \\ \frac{1}{\sqrt{2}}\big(\,|0_L\rangle - |1_L\rangle\,\big) &\propto \big(\,|000\rangle - |111\rangle\,\big)\big(\,|000\rangle - |111\rangle\,\big)\big(\,|000\rangle - |111\rangle\,\big)\,. \end{aligned} \tag{1.152}$$

The *logical operations* on the encoded qubit with the basis states $|0_L\rangle$ and $|1_L\rangle$ are given by $X_L = X^{\otimes 9}$ and $Z_L = Z^{\otimes 9}$,

$$\begin{aligned} X_L\,|0_L\rangle &= |1_L\rangle & \qquad Z_L\,|0_L\rangle &= |0_L\rangle \ , \\ X_L\,|1_L\rangle &= |0_L\rangle & \qquad Z_L\,|1_L\rangle &= -\,|1_L\rangle \ . \end{aligned} \tag{1.153}$$

Stabilizer codes

A particularly useful type of QECC are *stabilizer codes*. To introduce it, recall that the *generalized Pauli group* $\mathcal{G}_N$ consists of the elements

$$\omega^r X^{s_1} Z^{t_1} \otimes \cdots \otimes X^{s_n} Z^{t_n} \ , \tag{1.154}$$

or sometimes

$$(\sqrt{\omega})^r X^{s_1} Z^{t_1} \otimes \cdots \otimes X^{s_n} Z^{t_n} \tag{1.155}$$

in even dimensions. Here, X and Z are the shift and clock operators in D dimensions, and ω is the D'th root of unity (also see Sect. 1.1.7).

As with graph states, a stabilizer code is defined by its *stabilizer*, which is an Abelian subgroup of $\mathcal{G}_n$ [13] [45] .

Given k generator elements $g_1, \ldots, g_k \in \mathcal{G}_n$, the *stabilizer* S is the Abelian group obtained by the multiplication of generator elements [45],

$$S = \left\{ \prod g_1^{i_1} g_2^{i_2} \cdots g_k^{i_k} \;\middle|\; i_1, \ldots, i_k \in \{1, \ldots, D-1\} \right\} . \tag{1.156}$$

The code space $\Pi_{\mathcal{C}}$ is then the $(+1)$-eigenspace of all stabilizer elements,

$$s_a \Pi_{\mathcal{C}} s_a = \Pi_{\mathcal{C}} \qquad \forall s_a \in S \, . \tag{1.157}$$

Consider a stabilizer code on n parties. Given a generator with $(n-k)$ elements, the stabilizer will contain D^{n-k} elements. If the dimension D is prime, the associated coding space will have dimension D^k. Therefore, such a code will encode k qu$D$its into n qu$D$its, denoted by $[[n, k, d]]_D$. However, if D is not prime, this does not necessarily need to be the case anymore [45].

Let us restrict on prime dimensions. The *logical operators* are obtained by extending the generator with a complete independent set of commuting operators $\overline{Z}_i$. If the generator consists of $(n-k)$ elements, this will consist of k elements $\overline{Z}_1, \ldots, \overline{Z}_k$. The remaining logical operators are given by the additional k operators $\overline{X}_1, \ldots, \overline{X}_k$ having the properties

$$\begin{aligned} \overline{X}_i s_a &= s_a \overline{X}_i \, , && \forall s_a \in S \, , \\ \overline{X}_i \overline{Z}_j &= \overline{Z}_j \overline{X}_i \, , && \text{if } i \neq j \, , \\ \overline{X}_i \overline{Z}_i &= \omega^{-1} \overline{Z}_i \overline{X}_i \, . \end{aligned} \tag{1.158}$$

The logical operators $\overline{X}_i, \overline{Z}_i$ are in the *normalizer* $N(S) = \{n \in \mathcal{G}_n \,|\, nS = Sn\}$, Thus their action on the code space cannot be detected, and they can be used to perform logical operations on the encoded states.

As an example, the Shor code [115] (introduced in the previous section) is a stabilizer code, having the *generator matrix*

$$\begin{array}{ccccccccc} \mathrm{X} & \mathrm{X} & \mathrm{X} & \mathrm{X} & \mathrm{X} & \mathrm{X} & \mathrm{I} & \mathrm{I} & \mathrm{I} \\ \mathrm{I} & \mathrm{I} & \mathrm{I} & \mathrm{X} & \mathrm{X} & \mathrm{X} & \mathrm{X} & \mathrm{X} & \mathrm{X} \\ \mathrm{Z} & \mathrm{Z} & \mathrm{I} & \mathrm{I} & \mathrm{I} & \mathrm{I} & \mathrm{I} & \mathrm{I} & \mathrm{I} \\ \mathrm{I} & \mathrm{Z} & \mathrm{Z} & \mathrm{I} & \mathrm{I} & \mathrm{I} & \mathrm{I} & \mathrm{I} & \mathrm{I} \\ \mathrm{I} & \mathrm{I} & \mathrm{I} & \mathrm{Z} & \mathrm{Z} & \mathrm{I} & \mathrm{I} & \mathrm{I} & \mathrm{I} \\ \mathrm{I} & \mathrm{I} & \mathrm{I} & \mathrm{I} & \mathrm{Z} & \mathrm{Z} & \mathrm{I} & \mathrm{I} & \mathrm{I} \\ \mathrm{I} & \mathrm{I} & \mathrm{I} & \mathrm{I} & \mathrm{I} & \mathrm{I} & \mathrm{Z} & \mathrm{Z} & \mathrm{I} \\ \mathrm{I} & \mathrm{I} & \mathrm{I} & \mathrm{I} & \mathrm{I} & \mathrm{I} & \mathrm{I} & \mathrm{Z} & \mathrm{Z} \\ \hline \mathrm{X} & \mathrm{X} & \mathrm{X} & \mathrm{X} & \mathrm{X} & \mathrm{X} & \mathrm{X} & \mathrm{X} & \mathrm{X} \\ \mathrm{Z} & \mathrm{Z} & \mathrm{Z} & \mathrm{Z} & \mathrm{Z} & \mathrm{Z} & \mathrm{Z} & \mathrm{Z} & \mathrm{Z} \end{array} \, . \tag{1.159}$$

Each of the eight top rows is a generator element, thus the encoded space has dimension $2^{9-8} = 2$. The last two rows are the logical operators X_L and Z_L that act on the encoded logical qubit. These commute with all generators, and are in the normalizer $N(S)$ of the stabilizer. The Shor code, being able to correct for one error, is a $[[9, 1, 3]]_2$.

[13] This is reminiscent of the graph states introduced in Sect. 1.2.1. In fact, graph states are simply stabilizer codes with $K = 1$ [54].

Pauli	$GF(4)$
I	0
X	1
Y	ω
Z	ω^2
tensor products	vectors
multiplication	addition
$[M_{\boldsymbol{x}}, N_{\boldsymbol{y}}] = 0$	$\langle \boldsymbol{x}, \boldsymbol{y} \rangle = 0$
nothing	multiplication
phases	nothing

Table 1.1: Correspondences between qubit stabilizer codes and additive codes over $GF(4)$. The table is from Ref. [117].

Stabilizer codes and classical codes

Stabilizer codes are also called *additive*, because of their connection to classical codes. In particular, qubit stabilizer codes are related to classical additive codes over the finite field $GF(4)$ that have a Hermitian trace inner product [106, 108]. If a qubit stabilizer code has codewords of even weight only, the code is of type II, being of type I otherwise. These types are sometimes denoted by 4_I^{H+} and 4_{II}^{H+} respectively.

This works in the following way [108]: Take $GF(4)$ to consist of $\{0, 1, \omega, \omega^2\}$, with $\omega^2 = \omega + 1$ and $\omega^3 = 1$. The code consists of codewords that are vectors of elements in $GF(4)$, $\boldsymbol{c} = c_1 \dots c_n \in GF(4)^n$. The weight $\mathrm{wt}(\boldsymbol{x})$ of a vector $\boldsymbol{x}$ is the number of its nonzero components. The conjugation of vectors is $\bar{\mathbf{x}} = \mathbf{x^2}$, thus

$$\begin{aligned} \bar{0} &= 0 & \bar{1} &= 1\,, \\ \bar{\omega} &= \omega^2 & \bar{\omega}^2 &= \omega\,. \end{aligned} \tag{1.160}$$

The trace is given by $\mathrm{Tr}(\mathbf{x}) = \mathbf{x} + \mathbf{x^2}$, therefore $\mathrm{Tr}(0) = \mathrm{Tr}(1) = 0$ and $\mathrm{Tr}(\omega) = \mathrm{Tr}(\omega^2) = 1$. The *Hermitian trace inner product* of two vectors $\boldsymbol{x} = x_1 \dots x_n$ and $\boldsymbol{y} = y_1 \dots y_n$ is given by

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \sum_i \mathrm{Tr}(x_i \bar{y}_i)\,. \tag{1.161}$$

A code is *additive*, if the addition of two codewords yields a codeword again. Table 1.1 relates elements and operations on stabilizer codes with those of additive codes over $GF(4)$ [117]. The Pauli matrices are associated with elements of $GF(4)$ by the mapping $\{I \to 0, X \to 1, Y \to \omega, Z \to \omega^2\}$. The multiplication of Pauli elements, neglecting phases, corresponds to the addition of vectors over $GF(4)$; their commutator corresponds to the Hermitian trace inner product. If a code $\mathcal{C}$ is additive, its *dual* code $\mathcal{C}^\perp$ is additive again, spanned by $\mathcal{C}^\perp = \{\boldsymbol{x} \in GF(4) \,|\, \langle \boldsymbol{x}, \boldsymbol{c} \rangle = 0 \ \forall \boldsymbol{c} \in \mathcal{C}\}$. A code with $\mathcal{C} \subseteq \mathcal{C}^\perp$ is called self-orthogonal, a code with $\mathcal{C} = \mathcal{C}^\perp$ *self-dual*.

Stabilizer codes can also be expressed as graph codes, and if $K = 1$, these are the graph states introduced in Sect. 1.2.1 [54]. Thus graph states correspond to *self-dual additive codes over* $GF(4)$. While a single graph states (having $K = 1$) cannot be used to encode anything, they are however often highly entangled. As an example, the six-qubit absolutely maximally entangled graph state of Fig. 1.2.3 corresponds to

the classical *hexacode* [44]. It is generated by the rows of the generator matrix

$$\begin{bmatrix} 1 & 0 & 0 & 1 & \omega & \omega \\ 0 & 1 & 0 & \omega & 1 & \omega \\ 0 & 0 & 1 & \omega & \omega & 1 \\ \omega & 0 & 0 & \omega & \bar{\omega} & \bar{\omega} \\ 0 & \omega & 0 & \bar{\omega} & \omega & \bar{\omega} \\ 0 & 0 & \omega & \bar{\omega} & \bar{\omega} & \omega \end{bmatrix} . \tag{1.162}$$

The code space consists of all the codewords that can be generated by the addition of rows. In terms of a quantum code, this corresponds to the $[[6, 0, 4]]_2$ qubit stabilizer code obtained from the generator matrix

$$\begin{bmatrix} X & I & I & X & Y & Y \\ I & X & I & Y & X & Y \\ I & I & X & Y & Y & X \\ Y & I & I & Y & Z & Z \\ I & Y & I & Z & Y & Z \\ I & I & Y & Z & Z & Y \end{bmatrix} . \tag{1.163}$$

In the matrix above, each row represents a generator. Its stabilizer corresponds, up to local unitaries, to the stabilizer of the six-qubit AME graph state depicted in Fig. 1.2.3. Finally, note that expressing stabilizer codes in terms of graph states and codes generalizes to prime power dimensions $q = p^l$; stabilizer codes in q dimensions are one-to-one related to classical additive codes over $GF(q^2)$ [121, 122].

Bounds on QECC

It is interesting to know for what parameters QECC can possibly exist. Here, I will list some bounds on the existence of QECC.

Theorem 6 (Quantum Singleton bound [123])**.** *Let $\mathcal{C}$ be a quantum code with parameters $((n, K, d))_D$. Then*

$$K \leq D^{n-2d+2} . \tag{1.164}$$

If equality holds, then $\mathcal{C}$ is pure to weight $(n - d + 2)$, that is $A_j = 0$ for all $j < n - d + 2$.

Codes reaching equality in the quantum singleton bound are called *quantum maximum distance separable (QMDS)*, with parameters $((n, D^{n-2d+2}, d))_D$.

From the *shadow inequalities* (see Chpt. 5), Rains derived bounds for qubit codes. Self-dual additive codes on qubits (i.e graph states) are called type II, if all its codewords have even weight, and type I otherwise (also see Chpt. 5). Denote by d_{II}, d_I their distances. The following bounds hold [44, 124, 125] [14]:

$$d_I \leq \begin{cases} 2\lfloor n/6 \rfloor + 1 & \text{if } n = 0 \mod 6 \\ 2\lfloor n/6 \rfloor + 3 & \text{if } n = 5 \mod 6 \\ 2\lfloor n/6 \rfloor + 2 & \text{otherwise} , \end{cases} \tag{1.165}$$

$$d_{II} \leq 2\lfloor n/6 \rfloor + 2 . \tag{1.166}$$

[14] Also see Table 11.1 in Ref. [106].

Codes meeting the bound are called *extremal*. In fact, these bounds are general, and carry over to non-additive codes.

Theorem 7 (Shadow bound: Theorem 13.4.1. in [106]). *If a pure* $((N,1,d))_2$ *exists, then*

$$d \leq \begin{cases} 2\lfloor n/6 \rfloor + 3 & \text{if } N = 5 \mod 6\,, \\ 2\lfloor n/6 \rfloor + 2 & \text{otherwise.} \end{cases} \tag{1.167}$$

If a pure $((N,K,d))_2$ *exists for* $K > 1$*, with* $0 \leq l \leq 5$*, then*

$$d \leq \begin{cases} 2\lfloor n/6 \rfloor + 2 & \text{if } N = 4 \mod 6\,, \\ 2\lfloor n/6 \rfloor + 1 & \text{otherwise.} \end{cases} \tag{1.168}$$

Thus, qubit AME states having the parameters $((n,1,\lfloor \frac{n}{2} \rfloor + 1))_2$ may only exist if $n = 2,3,5,6,7$. However, as I will show in Chpt. 3, an AME state of seven qubits having the parameters $((7,1,4))_2$ is ruled out.

The *quantum Hamming bound* is a type of sphere packing bound, obtained by a counting argument.

Theorem 8 (Quantum Hamming bound [126, 127]). *Let* $\mathcal{C}$ *be a pure* $((n,K,d))_D$*. Then*

$$K \sum_{j=0}^{\lfloor (d-1)/2 \rfloor} \binom{n}{j} (D^2-1)^j \leq D^n\,. \tag{1.169}$$

Proof. For $\mathcal{C}$ spanned by some orthonormal basis $\{|j_\mathcal{C}\rangle\}$ to be pure,

$$\langle i_\mathcal{C}|\, E_\alpha^\dagger E_\beta\, |j_\mathcal{C}\rangle = \mathrm{Tr}(E_\alpha^\dagger E_\beta)/D^n \tag{1.170}$$

for all errors $E_{\alpha,\beta} \in \mathcal{E}$ with $\mathrm{wt}(E_{\alpha,\beta}) < \lfloor (d-1)/2 \rfloor$. Thus the elements in the set $\{E_\alpha\, |i_\mathcal{C}\rangle\}$ must be mutually orthogonal. Note that there are D^2-1 different error operators for on each site. Distributing exactly j local errors onto n sites must lead to $\binom{n}{j}(D^2-1)$ orthogonal vectors. Summing over all possible errors of weight up to $t = \lfloor (n-1)/2 \rfloor$, one obtains the bound. □

The *Quantum Gilbert-Varshamov bound* is an existence bound on codes that must not necessarily be pure.

Theorem 9 (Quantum Gilbert-Varshamov [126]). *A* $((n,K,d))_D$ *exists, if*

$$K \sum_{j=0}^{2t} \binom{n}{j} (D^2-1)^j \geq D^n\,, \tag{1.171}$$

where $t = \lfloor (n-1)/2) \rfloor$.

Because this bound does not imply purity of the code, this bound however does not give sufficient conditions for the existence of AME states.

Quantum weight enumerators

Here I introduce *quantum weight enumerators*. These are polynomials that are useful to characterize QECC. A thorough presentation is given in Chapter 3. The *Shor-Laflamme (weight) enumerators* [118, 128] are defined for any two given Hermitian operators M and N acting on $(\mathbb{C}^D)^{\otimes n}$, and are local unitary invariants. Their (unnormalized) coefficients are given by [15].

$$A_j(M,N) = \sum_{\mathrm{wt}(E)=j} \mathrm{Tr}(EM)\,\mathrm{Tr}(E^\dagger N)\,, \tag{1.172}$$

$$B_j(M,N) = \sum_{\mathrm{wt}(E)=j} \mathrm{Tr}(EME^\dagger N)\,, \tag{1.173}$$

where $\{E\}$ is an local error basis that includes the identity (c.f. Sect. 1.1.7). The list of coefficients $(A_0,\ldots,A_n)$ is also called a *weight distribution*. The corresponding enumerator polynomials are

$$A_{MN}(x,y) = \sum_{j=0}^{n} A_j(M,N)x^{n-j}y^j\,, \tag{1.174}$$

$$B_{MN}(x,y) = \sum_{j=0}^{n} B_j(M,N)x^{n-j}y^j\,. \tag{1.175}$$

While it might not be obvious from the definition, these enumerators are independent of the local error-basis $\mathcal{E}$ chosen, and are thus local unitary invariants. As an example, it can be shown that for absolutely maximally entangled states (AME) of n parties having D levels each (c.f. Sect. 1.2.3), the weight enumerator is given by [44]

$$A_j(|\phi_{n,D}\rangle) = \frac{n!}{(n-j)!} \sum_{k=\lfloor \frac{n}{2}\rfloor+1}^{j} \frac{(-1)^{j-k}(D^{2k-n}-1)}{k!(j-k)!}\,. \tag{1.176}$$

The *quantum MacWilliams identity* relates $A_j(M,N)$ and $B_j(M,N)$.

Theorem 10 (quantum MacWilliams identity, Rains [106, 118])**.** *Given two Hermitian operators M and N acting on n systems having D levels each, then*

$$A_{MN}(x,y) = B_{MN}\Big(\frac{x+(D^2-1)y}{D}, \frac{x-y}{D}\Big)\,. \tag{1.177}$$

Considering a QECC with parameters $((n,K,d))_D$, one sets $M=N$ to be equal to the projector $\Pi_{\mathcal{C}}$ onto the code space. The following results concerning QECC and their Shor-Laflamme enumerators are known [118]: The coefficients $A_j = A_j(\Pi_{\mathcal{C}})$ and $B_j = B_j(\Pi_{\mathcal{C}})$ are non-negative, and

$$KB_0 = A_0 = K^2\,, \tag{1.178}$$

$$KB_j \geq A_j\,, \tag{1.179}$$

with equality in the second equation for $j<d$. In fact, these conditions are not only necessary but also sufficient for a projector $\Pi_{\mathcal{C}}$ to be a QECC.

[15] In fact, for higher dimensions, we chose a definition that is different, but equivalent, to the original definition as found in Ref. [118].

Theorem 11 ([118]). *Let $\Pi_{\mathcal{C}}$ be a projector of rank K. Then $\Pi_{\mathcal{C}}$ is a code of distance d if and only if*

$$KB_j(\Pi_{\mathcal{C}}) = A_j(\Pi_{\mathcal{C}}) \qquad \forall j < d\,. \tag{1.180}$$

The *shadow enumerator* further constrains the values that the weight distribution can take. Given $A_{MN}(x, y)$, is it obtained by

$$S_{MN}(x, y) = A_{MN}\left(\frac{(D-1)x + (D+1)y}{D}, \frac{y-x}{D}\right). \tag{1.181}$$

Its coefficients S_j must be non-negative [107, 129]. In Chapter 5, I show how the shadow enumerator constrains the correlations in quantum codes. In fact, it turns out to be a type of *monogamy relation* that originates in the universal state inversion map (c.f. 1.1.6), constraining the purities of reductions.

Given the parameters of a hypothetical quantum code, one can formulate a *linear program* to find hypothetical weight distributions that satisfy Eqs. (1.177), (1.178), (1.180), and (1.181). If no valid weights $A_j(\Pi_{\mathcal{C}})$ can be found, a code with the proposed parameters cannot exist. This therefore represents a way to prove the non-existence of certain hypothetical states and QECC.

Theorem 12 (LP bound for general QECC, Thm. 21 in Ref. [108] and Thm. 10 in Ref. [107]). *If a $((n, K, d))_D$ exists, then there is a solution to the following set of linear equations and inequalities for A_i, B_i, and S_i with $0 \leq j \leq n$:*

$$\begin{aligned}
A_i, B_i, S_i &\geq 0 \\
A_0 &= K^2 \\
KB_i &= A_i \quad (i < d) \\
KB_i &\geq A_i \quad (i \geq d)\,, \\
B_i &= D^{-n} \sum_{0 \leq k \leq n} K_i(k; n, 1, D^2 - 1) A_k \\
S_i &= D^{-n} \sum_{0 \leq k \leq n} (-1)^k K_i(k; n, D-1, D+1) A_k
\end{aligned} \tag{1.182}$$

For pure codes, the third constraint above is strengthened to

$$KB_j = A_j = 0 \quad \textit{for all } j < d\,. \tag{1.183}$$

The Krawtchouk-like polynomial in Eq. (1.182) is given by (c.f. Appendix 5.12),

$$K_m(k; n, E, F) = \sum_{\alpha} (-1)^{\alpha} \binom{n-k}{m-\alpha} \binom{k}{\alpha} E^{[(n-k)-(m-\alpha)]} F^{m-\alpha}\,. \tag{1.184}$$

For qubit stabilizer codes, one additionally has that [108] (also see Sect. 4.4)

$$\sum_{i \text{ even}} A_i = 2^{n - \log_2 K - 1} \quad \text{for type } I \text{ codes.} \tag{1.185}$$

$$\sum_{i \text{ even}} A_i = 2^{n - \log_2 K} \quad \text{for type } II \text{ codes,} \tag{1.186}$$

1.2.5 Semidefinite programming

Semidefinite programming (SDP) is a type of convex optimization [16], that can efficiently be solved and the result of which is *certifiable* [130–133]. It is of use in various fields such as convex constrained optimization, control theory, and combinatorial optimization. In quantum information, it can be used to study distillable entanglement [134], nonlocal correlations [135, 136], separability [137], steering [138], and measurement compatibility [139] amongst other applications, often approximating NP-hard problems [140].

A semidefinite program is in its *primal* form defined as [17]

$$\begin{aligned} \underset{x\in\mathbb{R}^m}{\text{minimize}} \quad & c^T x \\ \text{subject to} \quad & F_0 + \sum_{i=1}^{m} x_i F_i \geq 0\,. \end{aligned} \tag{SDP-P}$$

where the optimization is performed over the variable $x \in \mathbb{R}^m$, $c = (c_1, \ldots, c_m)^T \in \mathbb{R}^m$ is the problem vector, and $\{F_i\}$ are Hermitian problem matrices. To every primal SDP an associated *dual* problem is given by

$$\begin{aligned} \underset{Z\in\mathcal{B}_+^n}{\text{maximize}} \quad & -\operatorname{Tr}(F_0 Z) \\ \text{subject to} \quad & Z \geq 0 \\ & \operatorname{Tr}(F_i Z) = b_i \quad \text{for } i = 1, \ldots, m\,, \end{aligned} \tag{SDP-D}$$

where the optimization of Z is performed over the cone of positive semi-definite matrices $\mathcal{B}_+^n$ of size $n \times n$. An SDP is *feasible* if a solution, called *feasible point*, exists. Note that the set of feasible points is always convex. For $c = 0$, the primal problem reduces to a problem of feasibility instead of minimization. If the primal and dual problem are both feasible, their difference in objective values is

$$\begin{aligned} c^T x - [-\operatorname{Tr}(F_0 Z)] &= \sum_{i=1}^{m} c_i x_i + \operatorname{Tr}(F_0 Z) \\ &= \sum_{i=1}^{m} \operatorname{Tr}(F_i Z) x_i + \operatorname{Tr}(F_0 Z) \\ &= \operatorname{Tr}[(\sum_{i=1}^{m} x_i F_i + F_0) Z] \geq 0\,. \end{aligned} \tag{1.187}$$

This difference is called the *duality gap*, and its non-negativity is known as *weak duality*: The solution of the dual problem lower bounds any solution to the primal

[16] Convex optimization concerns itself with the optimisation of convex functions over convex sets.

[17] Note that there are different equivalent formulations of SDPs to be found in the literature. In particular, the notions of the primal and dual program can be interchanged, and it is possible to formulate them in a completely symmetric way [140]. Often, the primal problem is minimized, while the dual problem is maximized. I choose to take the approach and notation as used in Refs. [130] and [141].

problem, and vice versa. If the feasible sets of both the primal and the dual problem are non-empty, then for every $\epsilon > 0$ there exists feasible x and Z such that

$$\mathrm{Tr}(c^T x) + \mathrm{Tr}(F_0 Z) < \epsilon \,. \tag{1.188}$$

Then the solutions x and Z are known to be ϵ-suboptimal. Consequently, ϵ serves as a stopping criterion in numerical algorithms. *Strong duality* holds if the primal and dual program achieve the same optimal value. This is the case if both the primal and dual problem are strictly feasible, that is, when there exist x with $F(x) > 0$ and $Z > 0$ with $Tr(F_i Z) = c_i$ [130]. Then one has the complementary slackness condition of a vanishing duality gap,

$$\mathrm{Tr}\left[\big(\sum_{i=1}^{m} x_i F_i + F_0\big) Z\right] = 0 \,. \tag{1.189}$$

If the primal problem is infeasible, a *certificate* Z can be given in the following way: If there exists an operator $Z \geq 0$, such that $\mathrm{Tr}(F_i Z) = 0$ for all $i = 1, \ldots, m$ while $\mathrm{Tr}(F_0 X) < 0$, the duality gap would be *negative*: then the primal problem must be *infeasible*. In entanglement theory, a certificate for a suitable primal program can take the role of a witness (c.f. Sect. 1.1.6) [141, 142].

Note that the primal problem in Eq. (SDP-P) can be seen as a Bloch decomposition of a positive operator (c.f. Sect. 1.1.7), such as a quantum state. Further constraints on the state, such as certain marginals or a positive partial transpose, can naturally be stated in terms of the Bloch coefficients. Interestingly, also quadratic constraints can be incorporated: Terms of the form $(Ax + b)^T (Ax + b) - c^T x - d \leq 0$ can be written as

$$\begin{pmatrix} \mathbb{1} & Ax + b \\ (Ax + b)^T & c^T x + d \end{pmatrix} \geq 0 \,. \tag{1.190}$$

Such additional constraints $G^{(i)}$ are included into the primal SDP by enlarging the term $F(x) = F_0 + \sum_{i=1}^{m} x_i F_i \geq 0$ such that is has the block-diagonal form

$$F(x) \oplus G^{(1)}(x) \oplus \cdots \oplus G^{(k)}(x) \geq 0 \,. \tag{1.191}$$

Many NP-hard problems admit a *convex relaxation* as an SDP. As an example, the problem of minimizing a quadratic form over the vertices of a hypercube is NP-hard [132]:

$$\begin{aligned} &\underset{x}{\text{minimize}} && x^T Q x \\ &\text{subject to} && x_i \in \{+1, -1\} \quad \text{for all } i = 1, \ldots, n \,, \end{aligned}$$

where $Q = Q^T$ is a symmetric matrix of size $n \times n$. Its optimal solution can be lower bounded by solving the SDP-pair of the primal program given by

$$\begin{aligned} &\underset{X}{\text{minimize}} && \mathrm{Tr}(QX) \\ &\text{subject to} && X \geq 0 \\ & && X_{ii} = 1 \quad \text{for all } i = 1, \ldots, n \,, \end{aligned} \tag{1.192}$$

and its dual

$$\begin{aligned} \underset{\Lambda}{\text{maximize}} \quad & \mathrm{Tr}(\Lambda) \\ \text{subject to} \quad & \Lambda \text{ diagonal} \\ & Q - \Lambda \geq 0\,. \end{aligned} \tag{1.193}$$

This can be seen as follows: Writing $X = xx^T$, the original objective function in Eq. (1.192) reads $x^T Q x = \mathrm{Tr}(Qxx^T) = \mathrm{Tr}(QX)$. The feasible set is then given by $\{X \,|\, X \geq 0, X_{ii} = 1, \mathrm{rank}(X) = 1\}$. By dropping the rank constraint, one obtains the SDP above.

Finally, note that *linear programs (LP)* of the form

$$\begin{aligned} \underset{x \in \mathbb{R}^m}{\text{minimize}} \quad & c^T x \\ \text{subject to} \quad & Ax + b \geq 0\,. \end{aligned} \tag{LP}$$

with componentwise inequalities are a special case of SDPs, where the problem matrix A is diagonal. In this view, semidefinite programs are a natural extension of linear programs, where componentwise inequalities are replaced by matrix inequalities. While the feasible sets of LPs are polyhedral with planar faces, the feasible sets of SDPs are spectrahedral, having additional curved boundaries.

1.2.6 The quantum marginal problem

The relation between the whole to its parts lies at the heart of quantum entanglement. Namely, if a many-party pure quantum state is not the tensor product of its individual parts, the state is said to be entangled. A particularly intriguing consequence is, that given a set of quantum marginals, it is not clear from the outset if and how they can be assembled into a joint pure state. This is the so-called *quantum marginal problem* (QMP) which will resurface in the following Chapters in various disguises.

Originally coined the *N-representability problem* by Coleman, its first formulation asks how to recognize when a putative two-party reduced density matrix is a reduction of a N-particle system of indistinguishable fermions [143]. In fact, the N-representability problem has been highlighted as one of the most prominent research challenges in theoretical and computational chemistry [144]. If it was resolved, it would e.g. allow to efficiently calculate the binding or ground state energy of molecules.

Coleman gave a necessary and sufficient constraint for the QMP in the case of one-body marginals of fermions.

Theorem 13 (Coleman [36, 143])**.** *A density matrix ϱ is the reduced one-body marginal of a system of n fermions, if and only if each of its eigenvalues λ satisfies $0 \leq \lambda \leq 1/n$.*

This question was subsequently expanded to the case of distinguishable particles, and in particular, to systems of qubits. In the case of the marginals being disjoint, the conditions for the existence of a pure joint qubit state has been completely characterized: it is given by the so-called *polygon inequalities*, which constrain the spectra of reductions.

Theorem 14 (Polygon inequalities, Higuchi et al. [145]). *Let $\varrho_1, \ldots, \varrho_n$ be one-qubit density matrices, and denote by λ_i the smaller eigenvalue of ϱ_i. Then there exists a compatible pure n-qubit state with the one-body marginals $\{\varrho_i\}$, if and only if the eigenvalues $\{\lambda_i\}$ satisfy the polygon inequalities*

$$\lambda_i \leq \sum_{j \neq i} \lambda_j \,. \tag{1.194}$$

Constraints for the existence of a mixed joint state on two qubits have subsequently been obtained by Ref. [146], and for the case of a joint pure three qutrit case by Ref. [147]. Solving the QMP in case of disjoint marginals completely, Klyachko extended the spectral conditions for the existence of a mixed joint state on n parties of arbitrary local dimensions [148, 149]. However, these conditions result already for more than four qubits in thousands of inequalities [36]. The QMP in the Gaussian setting was settled in Ref. [150].

The quantum marginal problem with overlapping marginals has turned out to be intractable - only necessary conditions for the general case are known [36, 151–153], some of which are based on entropic inequalities. Let us consider the case of overlapping two-party reductions of three particles. The strong subadditivity states that (c.f. Sect. 1.1.5),

$$S_{12} + S_{23} \geq S_{123} + S_2 \,, \tag{1.195}$$

where $S_{12} = S(\varrho_{12})$, etc. Discarding the non-negative term S_{123} yields the requirement

$$S_{12} + S_{23} \geq S_2 \,. \tag{1.196}$$

By purification of Eq.(1.195), one obtains an equivalent, but, in the context of the QMP, stronger relation,

$$S_{12} + S_{23} \geq S_1 + S_3 \,. \tag{1.197}$$

However, this is only a sufficient condition for the QMP on three parties: it has been shown that there exist ϱ_{12} and ϱ_{23} that satisfy above condition, but for which no valid extension ϱ_{123} can be found [152].

Another criterion for the tripartite case is an inequality obtained by Butterley et al. for qubits.

Theorem 15 (Quantum Bell-Wigner inequality [36]). *Suppose $\varrho_{12}, \varrho_{23}$ and ϱ_{13} are two-qubit reductions of a three qubit state, with compatible one-body marginals. Then*

$$0 \leq \Delta \leq \mathbb{1} \,, \tag{1.198}$$

where $\Delta = \mathbb{1} - \varrho_1 - \varrho_2 - \varrho_3 + \varrho_{12} + \varrho_{13} + \varrho_{23}$.

Subsequently, it has been shown that while this requirement is necessary, it is not sufficient [37]. This is in stark contrast to the classical case, where an analogous requirement is indeed also sufficient for a joint probability distribution to exist [36]. Above relation will be extended in Sect. 5.11.2 to a family of inequalities for all finite local dimensions and an arbitrary number of parties.

Interestingly, the special case of the symmetric extension of two qubits, where a two-party density matrix ϱ_{AB} is extended to a tripartite state $\varrho_{ABB'}$ that satisfies $\mathrm{Tr}_B(\varrho_{ABB'}) = \mathrm{Tr}_{B'}(\varrho_{ABB'})$, has completely been characterized.

Theorem 16 ([154]). *A two qubit state ϱ_{AB} admits a symmetric extension $\varrho_{ABB'}$ if and only if*

$$\mathrm{Tr}(\varrho_B^2) \geq \mathrm{Tr}(\varrho_{AB}^2) - 4\sqrt{\det \varrho_{AB}}\,. \tag{1.199}$$

Further constraints on the QMP are imposed by relations involving entanglement measures. The key idea is that entanglement cannot be shared arbitrarily amongst the individual subsystems: rather, so-called *monogamy of entanglement* relations constrain the possible correlations which quantum states can exhibit [155, 156]. In its most basic form, this concept can be expressed as follows: If two parties A and B are maximally entangled with each other, then neither A nor B can also be entangled with a third party C. Monogamy relations are different formulations of this concept, imposing restrictions on how quantum correlations can be shared by multiple parties. This was first made precise for 2-level systems in a seminal article by Coffman, Kundu, and Wootters [156]: consider states of two qubits, and define the spin-flipped state as $\tilde{\varrho} = (\sigma_y \otimes \sigma_y)\varrho^T(\sigma_y \otimes \sigma_y)$ [18]. Recall that the concurrence for a two qubit mixed state ϱ_{AB} is given by $\mathcal{C}_{AB} = \max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}$, where $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ are the square roots of the eigenvalues of the operator $\sqrt{\varrho}\tilde{\varrho}\sqrt{\varrho}$ in descending order (c.f. Sect. 1.1.6). The concurrence is an entanglement monotone, being non-increasing under stochastic LOCC operations. The following relation holds:

Theorem 17 (Coffman-Kundu-Wootters monogamy [156]). *For all pure three-qubit states $|\psi\rangle$ it holds that*

$$\mathcal{C}_{AB}^2 + \mathcal{C}_{AC}^2 \leq \mathcal{C}_{A(BC)}^2\,, \tag{1.200}$$

where $\mathcal{C}_{A(BC)}^2 = 4\det(\varrho_A)$.

Note that above, $\mathcal{C}_{A(BC)}^2$ can be seen as the concurrence on an effective two-qubit pure state: because ϱ_{ABC} is pure, the reduction ϱ_{BC} can only have at most rank two. Considering the three-partite states introduced in Eq. (1.46), the W-state reaches equality in above equation. In contrast, the GHZ state does not reach equality; its so-called tangle is non-zero and the state contains essential three-way entanglement. A conjecture extending the Coffman-Kundu-Wootters inequality [Eq. (1.200)] to more parties was later proven by Osborne and Verstraete [157], and similar relations constraining multipartite quantum correlations have been found for other measures such as squashed entanglement, entanglement negativity, and non-local correlations [158–162].

Related to the QMP are conditions for joint states to be unique, given their marginals - a question we will address in Chpt. 2. This is motivated by a naturally arising physical question: Considering a Hamiltonian having local interactions only, its ground state is non-degenerate only if no other states with the same local reductions exist. In this context, Linden et al. showed that almost every pure state of three qubits is completely determined by its two-particle reduced density matrices [84, 163]. This result was extended to systems of n qubits, where it was shown that having access to a certain subset of all marginals of size $\lfloor \frac{n}{2} \rfloor + 1$ is already enough to uniquely specify a joint pure state [164].

[18] This is the universal state inversion as encountered in Eq. (1.73).

Despite many efforts, a general necessary and sufficient condition for the QMP with overlapping marginals is still lacking. We want to add that, while the QMP can be stated as a semidefinite program in principle [165], its formulation scales exponentially in system size. In fact, the quantum marginal problem has been shown to be QMA-complete, being too hard to solve, even when having access to a quantum computer [166, 167].

Chapter 2

Ground and thermal states of local Hamiltonians

The question whether a given quantum state is a ground or thermal state of a few-body Hamiltonian can be used to characterize the complexity of the state and is important for possible experimental implementations. We provide methods to characterize the states generated by two- and, more generally, k-body Hamiltonians as well as the convex hull of these sets. This leads to new insights into the question which states are uniquely determined by their marginals and to a generalization of the concept of entanglement. Finally, certification methods for quantum simulation can be derived. This Chapter is based on Project [A].

2.1 Introduction

Interactions in quantum mechanics are described by Hamilton operators. The study of their properties, such as their symmetries, eigenvalues, and ground states, is central for several fields of physics. Physically relevant Hamiltonians, however, are often restricted to few-body interactions, as the relevant interaction mechanisms are local. But the characterization of generic few-body Hamiltonians is not well explored, since in most cases one starts with a given Hamiltonian and tries to find out its properties.

In quantum information processing, ground and thermal states of local Hamiltonians are of interest for several reasons: First, if a desired state is the ground or thermal state of a sufficiently local Hamiltonian, it might be experimentally prepared by engineering the required interactions and cooling down or letting thermalize the physical system [168–174]. For example, one may try to prepare a cluster state, the resource for measurement-based quantum computation, as a ground state of a local Hamiltonian [175]. Second, on a more theoretical side, ground states of k-body Hamiltonians are completely characterized by their reduced k-body density matrices. The question which states are uniquely determined by their marginals has been repeatedly studied and is a variation of the representability problem, which asks whether given marginals can be represented by a global state [143]. It has turned out that many pure states have the property to be uniquely determined by a small set of their marginals [84, 163, 164], and for practical purposes it is relevant

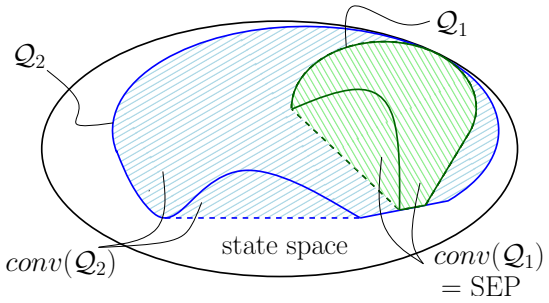


Figure 2.1: Schematic view of the state space, the exponential families $\mathcal{Q}_1$ and $\mathcal{Q}_2$, and their convex hulls. While the whole space of mixed states is convex, the exponential families are non-convex low-dimensional manifolds. The convex hull of $\mathcal{Q}_1$ are the fully separable states and our approach allows to characterize the convex hull for arbitrary $\mathcal{Q}_k$.

that often entanglement or non-locality can be inferred by considering the marginals only [142, 176, 177].

In this Chapter we present a general approach to characterize ground and thermal states of few-body Hamiltonians. We use the formalism of exponential families, a concept first introduced for classical probability distributions by Amari [66] and extended to the quantum setting in Refs. [78, 79, 82, 83] (also see Sect. 1.2.2). This offers a systematic characterization of the complexity of quantum states in a conceptionally pleasing way. We derive two methods that can be used to compute various distances to thermal states of k-body Hamiltonians: The first method is general and uses semidefinite programming, while the second method is especially tailored to cluster and, more generally, graph states. In previous approaches it was only shown that some special states are far away from the eigenstates of local Hamiltonians [178], but no general method for estimating the distance is known.

Our approach leads to new insights in various directions. First, it has been shown that cluster and graph states can, in general, not be exact ground states of two-body Hamiltonians [175], but it was unclear whether they still can be approximated sufficiently well. Our method shows that this is not the case and allows to bound the distance to ground and thermal states. Second, as shown in Ref. [84], almost all pure states of three qubits are completely determined by their two-party reduced density matrices. As we prove, for $N \geq 5$ qubits or four qutrits this is not the case, but we present some evidence that the fact might still be true for four qubits. Finally, our method results in witnesses, which can be used in a quantum simulation experiment to certify that a three-body Hamiltonian or a Hamiltonian having long-range interactions was generated.

2.2 The setting

Let us recall the notion of quantum exponential families (c.f. Sect. 1.2.2). A two-local (or two-body) Hamiltonian of a system consisting of N spin-1/2 particles can be written as

$$H = \sum_{i,j=1}^{N} \sum_{\alpha\beta} \lambda_{\alpha\beta}^{(ij)} \sigma_{\alpha}^{(i)} \otimes \sigma_{\beta}^{(j)} , \tag{2.1}$$

where $\sigma_\alpha^{(i)}$ denotes a Pauli matrix $\{\mathbb{1}, \sigma_x, \sigma_y, \sigma_z\}$ acting on the i-th particle etc. Note that the identity matrix is included, so H can also contain single particle terms. We denote the set of all possible two-local Hamiltonians by $\mathcal{H}_2$ and in an analogous manner the set of k-local Hamiltonians by $\mathcal{H}_k$. An example for a two-local Hamiltonian is the Heisenberg model having nearest-neighbor interactions. However, our approach generally ignores any geometrical arrangement of the particles. Finally, for an arbitrary multi-qubit operator A we call the number of qubits where it acts on non-trivially the *weight* of A. In practice, this can be determined by expanding A in terms of tensor products of Pauli operators and looking for the largest non-trivial product.

The set we aim to characterize is the so-called exponential family $\mathcal{Q}_2$, consisting of thermal states of two-local Hamiltonians

$$\mathcal{Q}_2 = \left\{ \tau \,\middle|\, \tau = \frac{e^{-\beta H}}{\mathrm{tr}[e^{-\beta H}]}, H \in \mathcal{H}_2 \right\}. \tag{2.2}$$

Ground states can be reached in the limit of infinite inverse temperature β. For any k, the exponential families $\mathcal{Q}_k$ can be defined in a similar fashion. The set $\mathcal{Q}_1$ consists of mixed product states, the set $\mathcal{Q}_N$ of the full state space. The exponential families form the hierarchy $\mathcal{Q}_1 \subseteq \mathcal{Q}_2 \subseteq \cdots \subseteq \mathcal{Q}_N$, and a suitable βH can be seen as a way of parameterizing a specific density matrix $\tau = e^{-\beta H} / \mathrm{tr}[e^{-\beta H}]$. The question arises, what states are in $\mathcal{Q}_k$? And for those which are not, what is their best approximation by states in $\mathcal{Q}_k$?

It turns out to be fruitful to consider the convex hull

$$\mathrm{conv}(\mathcal{Q}_2) = \left\{ \sum\nolimits_i p_i \, \tau_i \mid \tau_i \in \mathcal{Q}_2 \,, \sum\nolimits_i p_i = 1 \,, \, p_i \geq 0 \right\},$$

and ask whether a state is in this convex hull or not (see also Fig. 2.1). The convex hull has a clear physical interpretation as it contains all states that can be generated by preparing thermal states of two-body Hamiltonians stochastically with probabilities p_i. In this way, taking the convex hull can be seen as a natural extension of the concept of entanglement: The thermal states of one-body Hamiltonians are just the mixed product states and their convex hull are the fully separable states of N particles [14]. In this framework, the result of Linden et al. [84] can be rephrased as stating that all three-qubit states are in the closure of the convex hull $\mathrm{conv}(\mathcal{Q}_2)$, since nearly all pure states are ground states of two-body Hamiltonians.

Finally, the characterization of the convex hull leads to the concept of witnesses that can be used for the *experimental* detection of correlations [14]. Witnesses are observables which have positive expectation values for states inside a given convex set. Consequently, the observation of a negative expectation value proves that a state is outside of the set. We will see below that such witnesses can be used to certify quantum simulation.

2.3 Characterization of $\mathrm{conv}(\mathcal{Q}_k)$ via semidefinite programming

Our first method to estimate the distance of a given state to the convex hull of $\mathcal{Q}_2$ relies on semidefinite programming [179]. This optimization method is insofar

useful, as semidefinite programs are efficiently solvable and their solutions can be certified to be optimal. Moreover, ready-to-use packages for their implementation are available.

As a first step we formulate a semidefinite program to test if a given pure $|\psi\rangle$ state is outside of $\mathcal{Q}_2$. Recall that it has been shown that the following three characterizations for the information projection $\tilde{\varrho}_2 \in \mathcal{Q}_2$ are equivalent (c.f. Sect. 1.2.2) [78]: (a) $\tilde{\varrho}_2$ is the unique minimizer of the relative entropy of ϱ from the set $\mathcal{Q}_2$,

$$\tilde{\varrho}_2 = \operatorname{argmin}_{\tau\in\mathcal{Q}_2} S(\varrho||\tau)\,. \tag{2.3}$$

(b) Of the set of states having the same two-body reduced density matrices (2-RDMs) as ϱ, denoted by $\mathcal{M}_2(\varrho)$, $\tilde{\varrho}_2$ has a maximal von Neumann entropy

$$\tilde{\varrho}_2 = \operatorname{argmax}_{\mu\in\mathcal{M}_2(\varrho)} S(\mu)\,. \tag{2.4}$$

(c) Finally, $\tilde{\varrho}_2$ is the unique intersection of $\mathcal{Q}_2$ and $\mathcal{M}_2(\varrho)$. From the characterization in Eq. (2.4), it follows that it suffices to find a different state ϱ having the same 2-RDMs as $|\psi\rangle$. If ϱ is mixed, its entropy is higher than that of $|\psi\rangle$, meaning that $|\psi\rangle$ cannot be its own information projection and therefore lies outside of $\mathcal{Q}_2$. If ϱ is pure, consider the convex combination $(|\psi\rangle\langle\psi| + \varrho)/2$, again having a higher entropy. To simplify notation we define for an arbitrary N-qubit operator X the operator $R_k(X)$ as the projection of X onto those operators, which can be decomposed into terms having at most weight k. In practice, $R_k(X)$ can be computed by expanding X in Pauli matrices, and removing all terms of weight larger than k. Note that $R_k(\varrho)$ may have negative eigenvalues.

The following semidefinite program (c.f. Sect. 1.2.5) finds a state with the same k-body marginals as a given state $|\psi\rangle$,

$$\begin{aligned} \underset{\varrho}{\text{minimize}} \quad & \operatorname{tr}(\varrho|\psi\rangle\langle\psi|) \\ \text{subject to} \quad & R_k(\varrho) = R_k(|\psi\rangle\langle\psi|) \\ & \operatorname{tr}[\varrho] = 1, \quad \varrho = \varrho^\dagger, \quad \varrho \geq \delta\mathbb{1}\,. \end{aligned} \tag{2.5}$$

While this program can be run with $\delta = 0$, it is useful to choose δ to be strictly positive. Then, a strictly positive ϱ may be found, which is guaranteed to be distant from the state space boundary. Consequently, if $|\psi\rangle$ is disturbed, one can still expect to find a state with the same reduced density matrices in the vicinity of ϱ. This can be used to prove that the distance to $\mathcal{Q}_2$ is finite, and will allow us to construct witnesses for proving irreducible correlations (or interactions) in $|\psi\rangle$. We make this rigorous in the following Observation. For that, let $\mathcal{B}(|\psi\rangle)$ be the ball in trace distance $D_{\mathrm{Tr}}(\mu,\eta) = \frac{1}{2}\operatorname{tr}(|\mu-\eta|)$ centered at $|\psi\rangle$.

Observation 18. *Consider a pure state $|\psi\rangle$ and a mixed state $\varrho \geq \delta\mathbb{1}$ with $R_k(\varrho) = R_k(|\psi\rangle\langle\psi|)$. Then, for any state σ in the ball $\mathcal{B}_\delta(|\psi\rangle)$ a valid state $\tilde{\varrho}$ in $\mathcal{B}_\delta(\varrho)$ can be found, such that their k-party reduced density matrices match. Moreover, the entropy of $\tilde{\varrho}$ is larger than or equal to the entropy of σ. This implies that the ball $\mathcal{B}_\delta(|\psi\rangle)$ contains no thermal states of k-body Hamiltonians.*

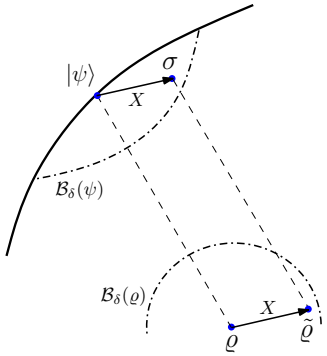


Figure 2.2: Illustration of Observation 18: If a strictly positive ϱ can be found, then for a given perturbation σ of $|\psi\rangle$ one can find a corresponding $\tilde{\varrho}$ in the vicinity of ϱ, such that the reduced density matrices of σ and $\tilde{\varrho}$ are the same.

Proof. Any σ in the trace ball $\mathcal{B}_\delta(|\psi\rangle)$ can be written as $\sigma = |\psi\rangle\langle\psi| + X$, with a traceless X. The trace can be decomposed as $\mathrm{tr}(X) = \langle\psi|\, X\, |\psi\rangle + \sum_i \langle\psi_i^\perp|X|\psi_i^\perp\rangle = 0$, where the $|\psi_i^\perp\rangle$ are orthogonal to $|\psi\rangle$. The second term of this expression is positive, since

$$\begin{aligned}\sum_i \langle\psi_i^\perp|X|\psi_i^\perp\rangle &= \sum_i \langle\psi_i^\perp|(X + |\psi\rangle\langle\psi|)|\psi_i^\perp\rangle \\ &= \sum_i \langle\psi_i^\perp|\sigma|\psi_i^\perp\rangle \geq 0\,. \end{aligned} \tag{2.6}$$

So we must have $\langle\psi|X|\psi\rangle \leq 0$. Furthermore, X can only have one negative eigenvalue λ_-, otherwise there would be also $|\psi_i^\perp\rangle$ with $\langle\psi_i^\perp|X|\psi_i^\perp\rangle < 0$, which is in contradiction to $\sigma \geq 0$. From $\mathrm{tr}(X) = 0$ it follows that λ_- has the largest modulus of all eigenvalues and consequently $\mathrm{tr}(|X|) = 2|\lambda_-|$. Since $D_{\mathrm{Tr}}(|\psi\rangle\langle\psi|, \sigma) = \mathrm{tr}\,|X|/2 \leq \delta$, it follows that $|\lambda_-| \leq \delta$. For $\sigma \in \mathcal{B}_\delta(|\psi\rangle)$ we choose $\tilde{\varrho} = \varrho + X$ as a candidate having the k-RDMs of σ. We have

$$R_k(\sigma) = R_k(|\psi\rangle\langle\psi| + X) = R_k(\varrho + X) = R_k(\tilde{\varrho})\,. \tag{2.7}$$

Furthermore, $\tilde{\varrho}$ is a positive semidefinite density matrix, because of $\tilde{\varrho} = \varrho + X \geq (\delta - |\lambda_-|)\mathbb{1} \geq 0$. Thus, for any state σ in $\mathcal{B}_\delta(|\psi\rangle)$ there exists a state $\tilde{\varrho}$ in $\mathcal{B}_\delta(\varrho)$, such that the k-RDMs of σ and $\tilde{\varrho}$ match.

Now we show that the entropy of $\tilde{\varrho}$ is larger than or equal to the entropy of σ, as this ensures that σ is not in $\mathcal{Q}_k$. Namely, if the entropy of $\tilde{\varrho}$ is larger, a state with the same k-RDMs but of higher entropy than σ has been found, and σ is outside of $\mathcal{Q}_k$. If on the other hand equality holds, then again $\sigma \notin \mathcal{Q}_k$ due to the uniqueness of the information projection and because of $\sigma \neq \tilde{\varrho}$. First, note that if ϱ fulfills the condition $S(\varrho) \geq 2C_\delta$, where

$$C_\delta = -\delta \log(\tfrac{\delta}{D-1}) - (1-\delta)\log(1-\delta)\,, \tag{2.8}$$

then also as required $S(\tilde{\varrho}) \geq S(\sigma)$. This follows from the sharp Fannes-Audenaert inequality (c.f. Sect. 1.1.5) [25]

$$|S(\eta) - S(\mu)| \leq -d \log\big(\frac{d}{D-1}\big) - (1-d)\log(1-d)\,, \tag{2.9}$$

where $d = D_{\mathrm{Tr}}(\eta, \mu)$ and $D = 2^N$ is the dimension of the system. Recall that $\sigma \in \mathcal{B}_\delta(\psi)$ and $\tilde{\varrho} \in \mathcal{B}_\delta(\varrho)$. Thus the entropy of σ can be at most C_δ, and the entropy of $\tilde{\varrho}$ must be at least $S(\varrho) - C_\delta$. Requiring $S(\varrho) \geq 2C_\delta$ therefore ensures that the entropy of $\tilde{\varrho}$ is higher than or equal to that of σ.

It remains to show that ϱ indeed fulfills this condition. For that, note that the eigenvalues of ϱ are larger than δ but smaller than $1/N$ due to the normalization of ϱ. Furthermore assume $D \geq 8$, since we are considering at least three qubits. From the bounds on the eigenvalues it follows that the entropy of ϱ is bounded by

$$\begin{aligned} S(\varrho) \geq & -[1-(D-1)\delta]\log[1-(D-1)\delta] \\ & -(D-1)\delta\log(\delta) \equiv \Gamma\,. \end{aligned} \tag{2.10}$$

So, we consider the function $\mathcal{F}(\delta, D) = \Gamma - 2C_\delta$ and have to show its positivity. Let us first fix D. Taking the second derivative of $\mathcal{F}$ with respect to δ one directly finds that this second derivative is strictly negative. This implies that $\mathcal{F}$ assumes only one maximum in the interval $[0, 1/D]$ and that the minima are assumed at the borders. We have $\mathcal{F}(0, D) = 0$ and it remains to prove that $\mathcal{G}(D) = \mathcal{F}(1/D, D)$ is positive. For $D = 8$ one can directly check that $\mathcal{G}$ as well as its derivative is positive. Furthermore, the second derivative of $\mathcal{G}(D)$ with respect to D is strictly positive for any $D \geq 8$, which proves the claim. □

In the Observation, we considered the trace distance, but a ball in fidelity instead of trace distance can be obtained: Consider a state σ near $|\psi\rangle$, having the fidelity $F(\sigma, \psi) = \alpha \geq 1 - \delta^2$, where $F(\varrho, \psi) = \mathrm{tr}[\varrho|\psi\rangle\langle\psi|] = \langle\psi|\,\varrho\,|\psi\rangle$. Then from the Fuchs-van-de-Graaf inequality (see Sect. 1.1.5) [22] follows that

$$D_{\mathrm{Tr}}(\sigma, |\psi\rangle\langle\psi|) \leq \sqrt{1 - F(\sigma, \psi)} \leq \delta\,. \tag{2.11}$$

Thus Observation 18 is applicable.

The usage of the fidelity as a distance measure has a clear advantage from the experimental point of view, as it allows the construction of witnesses for multiparticle correlations. Indeed the observable

$$\mathcal{W} = (1 - \delta^2)\mathbb{1} - |\psi\rangle\langle\psi| \tag{2.12}$$

has a positive expectation value on all states in $\mathcal{Q}_k$ and, due to the linearity of the fidelity, also on all states within the convex hull $\mathrm{conv}(\mathcal{Q}_k)$. So, a negative expectation value signals the presence of k-body correlations. Witnesses for entanglement have already found widespread applications in experiments [14].

Numerical results

Equipped with a method to test whether a pure state is in $\mathrm{conv}(\mathcal{Q}_2)$ or not we are able to tackle the question whether the results of Ref. [84] can be generalized. Recall that in this reference it has been shown that nearly all pure states of three qubits are uniquely determined (among all mixed states) by their reduced two-body density matrices. This means that they are ground states of two-body Hamiltonians. Consequently, the closure of the convex hull $\mathrm{conv}(\mathcal{Q}_2)$ contains all pure states and therefore also all mixed states, and the semidefinite program in Eq. (2.5) will not

δ	10^{-3}	10^{-4}	10^{-5}	10^{-6}	10^{-7}
5qb	0.0040	0.1325	0.2976	0.3729	0.4000
6qb	0.7680	0.8872	0.8897	1.0000	1.0000

Table 2.1: Fraction of pure five and six qubit states which are outside of the convex hulls of $\mathcal{Q}_2$, as detected by the semidefinite program from Eq. (2.5). See the text for further details.

be feasible for δ strictly positive. The question is whether this result holds for more qubits too.

Let us first consider states of five and six qubits. We report in Table 2.1 numerical results for the fraction of pure states lying outside of $\mathrm{conv}(\mathcal{Q}_2)$, with the condition of positive definiteness δ ranging from 10^{-3} to 10^{-7}. We tested $300'000$ ($30'000$) random five-qubit (six-qubit) states distributed to the Haar measure [180] for each setting δ with our semidefinite program using the solver MOSEK [1]As can be seen from the Table, at least 40% of all tested five-qubit states and 100% of all tested six-qubit states lie outside of $\mathrm{conv}(\mathcal{Q}_2)$. Thus, a similar result as in Ref. [84] does not hold in the cases of five and six qubits. Concerning $\mathrm{conv}(\mathcal{Q}_3)$, a single five-qubit state and no six-qubit state has been detected to lie outside. We ascribe the latter result to a rather weak statistics, as states in the vicinity of $|M_6\rangle$ are easily detected by our semi-definite program (cf. Fig. 2.3).

Let us now turn to the case of four qubits. Here, none of 8 million random pure states have been found to be outside of $\mathrm{conv}(\mathcal{Q}_2)$. The numerical result suggests that this is a general feature of four-qubit systems. We also tested special examples of highly entangled four-qubit states, such as the cluster state, classes of hypergraph states [181], the Higuchi-Sudbery $|M_4\rangle$ state [86] or the $|\chi\rangle$-state [14] (also see Eq. (7.76) in [182] or Eq. (16) in [183]. While many of theses states can be shown to be outside of $\mathcal{Q}_2$, we were not able to prove analytically or with the help of the semidefinite program that they have a finite distance to $\mathcal{Q}_2$. This implies that they might be approximated by thermal states of two-body Hamiltonians.

To summarize: concerning pure five-qubit states, we numerically found a fraction of 40% to be outside of $\mathrm{conv}(\mathcal{Q}_2)$. In the case of pure four-qubit states however, no tested random state has been found to lie outside of $\mathrm{conv}(\mathcal{Q}_2)$. Given the fact that the test works well in the cases of five and six qubits, this leads us to conjecture that nearly all pure four qubit states are in $\mathrm{conv}(\mathcal{Q}_2)$, and hence also in $\mathcal{Q}_2$. This would imply that a similar result as the one obtained by Ref. [84] holds in the case of four qubits: almost every pure state of four qubits is completely determined by its two-particle reduced density matrix. Indeed, we have subsequently shown a similar result, namely, that almost all four-particle pure states are determined amongst pure states by their two-body marginals (see Sect. 2.6.3) [184].

[1] We used the software MOSEK (MOSEK ApS, The MOSEK Python optimizer, API manual Version 7.1 (Revision 39), 2015) with a solver tolerance of 10^{-8} and the python wrapper PICOS (PICOS, A Python Interface for Conic Optimization Solvers, v. 1.1.1). For five to six qubits, a single problem instance takes around $5-10$ seconds to solve on a desktop computer.

2.4 Characterization via the graph state formalism

The family of graph states includes cluster states and GHZ states, and furthermore has turned out to be important for measurement-based quantum computation and quantum error correction [47, 58]. Due to their importance, the question whether graph states can be prepared as ground states of two-body Hamiltonians has been discussed before [175]. Generally, graph states have shown to not be obtainable as unique non-degenerate ground states of two-local Hamiltonians. Further, any ground state of a k-local Hamiltonian H can only be ϵ-close to a graph state $|G\rangle$ with $m(|G\rangle) > k$ at the cost of H having an ϵ-small energy gap relative to the total energy in the system [175]. Here $m(|G\rangle)$ is the minimal weight of any element in the stabilizer S of state $|G\rangle$ (see also below). But as pointed out in Ref. [175], this does not imply that graph states cannot be approximated in general, as ϵ is a relative gap only.

Let us recall the construction of graph states (also see Sect. 1.2.1). A graph consists of vertices and edges (see Fig. 2.3). This defines the generators

$$g_a = \sigma_x^{(a)} \prod_{b \in N(a)} \sigma_z^{(b)}, \tag{2.13}$$

where the product of the $\sigma_z^{(b)}$ runs over all vertices connected to vertex a, called neighborhood $N(a)$. The graph state $|G\rangle$ can be defined as the unique eigenstate of all the g_a, that is $|G\rangle = g_a |G\rangle$. This can be rewritten with the help of the stabilizer. The stabilizer S is the commutative group consisting of all possible 2^N products of g_a, that is $S = \{s_i = \prod_{a \in I} g_a\}$. Then, the graph state can be written as $|G\rangle\langle G| = 2^{-N} \sum_{s_i \in S} s_i$ [47]. This formula allows to determine the reduced density matrices of graph states easily, since one only has to look at the products of the generators g_a.

For instance, all stabilizer elements of the five-qubit ring cluster state $|C_5\rangle$ (c.f. Fig. 2.3) have at least weight three, and therefore the 2-RDMs of $|C_5\rangle$ are maximally mixed. By choosing $\delta = 2^{-5}$ in Observation 18, the maximum overlap to $\mathrm{conv}(\mathcal{Q}_2)$ is bounded by $F_{\tau \in \mathcal{Q}_2}(|C_5\rangle, \tau) \leq 1 - \delta^2 \approx 0.99902$. Note that Ref. [185] has demonstrated a slightly better bound $F(|C_5\rangle, \tau) \leq 1/32 + \sqrt{899/960} \approx 0.99896$. However, both bounds are by far not reachable in current experiments. In fact, one can do significantly better. In the following, we will formulate a stricter bound by first considering $\mathcal{Q}_2$ and the ring cluster state $|C_N\rangle$ for an arbitrary number of qubits $N \geq 5$, but the result is general.

A bound on the overlap of maximally entangled states to $\mathrm{conv}(\mathcal{Q}_k)$

Observation 19. *The maximum overlap between the N-qubit ring cluster state $|C_N\rangle$ and an N-qubit state $\tau \in \mathcal{Q}_2$ is bounded by*

$$\sup_{\tau \in \mathcal{Q}_2} \langle C_N | \tau | C_N \rangle = \sup_{H \in \mathcal{H}_2} \mathrm{tr}\left[\frac{e^H}{\mathrm{tr}[e^H]} |C_N\rangle\langle C_N|\right] \leq \frac{D-1}{D}, \tag{2.14}$$

where $D = 2^N$ is the dimension of the system. More generally, for an arbitrary pure state with maximally mixed reduced k-party states in a $d^{\otimes N}$-system, the overlap with $\mathcal{Q}_k$ is bounded by $(d^N - 1)/d^N$.

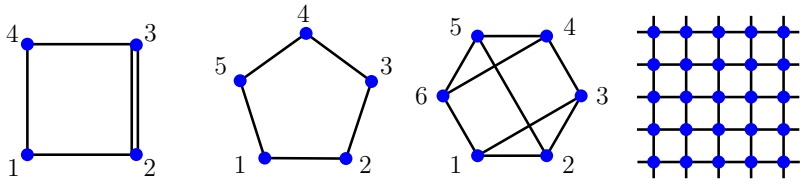


Figure 2.3: Examples of graphs discussed in this section. Left: A graph state of four qudits. In odd dimensions, this state can be used as a witness to detect states outside of $\mathrm{conv}(\mathcal{Q}_2)$. Center Left: The five-qubit ring-cluster graph. The corresponding ring-cluster state $|C_5\rangle$ has a finite distance to the exponential family $\mathcal{Q}_2$. Center Right: The maximally entangled six-qubit $|M_6\rangle$ state is not in the convex hull of $\mathcal{Q}_3$. Right: The 2D periodic 5×5 cluster state $|C_{5\times5}\rangle$ is not in $\mathrm{conv}(\mathcal{Q}_4)$.

Proof. We consider first only the ring cluster state, the generalization is then straightforward. For $N \geq 5$, the ring cluster state $|C_N\rangle$ has $m(|C_N\rangle) = 3$, that is, all the two-body reduced density matrices are maximally mixed [175]. Since the family of thermal states is invariant under the addition of the identity $\tau(H) \mapsto \tau(H + \theta\mathbb{1})$, we can choose H to be traceless when maximizing the overlap. So $\mathrm{tr}[H] = 0$ and $\mathrm{tr}[H|C_N\rangle\langle C_N|] = 0$ follows. Note that this is the only part in the proof where the property of $|C_N\rangle$ having maximally mixed 2-RDMs is required.

We write H and $|C_N\rangle\langle C_N|$ in the eigenbasis $\{|\eta_i\rangle\}$ of H,

$$H = \sum_i \eta_i |\eta_i\rangle\langle\eta_i| \,, \tag{2.15}$$

$$|C_N\rangle\langle C_N| = \sum_{ij} c_i c_j \, |\eta_i\rangle\langle\eta_j| \,, \tag{2.16}$$

and obtain following conditions, where the second results from the normalization of the ring cluster state:

$$f_1 = \sum_i \eta_i = 0 \,, \tag{2.17}$$

$$f_2 = \sum_i p_i - 1 = 0 \,, \qquad p_i = |c_i|^2 \geq 0 \,, \tag{2.18}$$

$$f_3 = \sum_i p_i \eta_i = 0 \,. \tag{2.19}$$

Under these conditions, we have to maximize

$$\mathcal{F} = \frac{\sum_i p_i e^{\eta_i}}{\sum_i e^{\eta_i}}. \tag{2.20}$$

If H is nontrivial, it must have both some positive and negative eigenvalues. Then at least two of the p_i must be nonzero. We use the method of Lagrange multipliers and consider

$$\Lambda = \frac{\sum_i p_i e^{\eta_i}}{\sum_i e^{\eta_i}} + \lambda_1 f_1 + \lambda_2 f_2 + \lambda_3 f_3 \,. \tag{2.21}$$

If the maximum is attained for some value p_k which is not at the border of the domain $[0,1]$, we then must have

$$\frac{\partial \Lambda}{\partial p_k} = \frac{e^{\eta_k}}{\sum_i e^{\eta_i}} + \lambda_2 + \lambda_3 \eta_k = 0\,. \tag{2.22}$$

For a given spectrum of H, $\{\eta\} = (\eta_1, \ldots, \eta_D)$, Eq. (2.22) has a solution for at most two values, η_+ and η_-. For any η_i not equal to η_+ or η_-, the corresponding variable p_i has to lie at the boundary of the domain $[0,1]$, which implies that $p_i = 0$ if $\eta_i \notin \{\eta_+, \eta_-\}$. The eigenvalues η_+ and η_- can be l and l' fold degenerate, with corresponding $p_+^l, p_-^{l'}$. But then, it is easy to see that it is optimal to maximize one of those by taking $p_+ = \sum_l p_+^l$ and $p_- = \sum_{l'} p_-^{l'}$ and setting the others to zero. Second, considering the set of $\eta_i \notin \{\eta_+, \eta_-\}$ where $p_i = 0$ one can further see with Jensen's inequality that it is optimal to take all of the η_i equal, that is $(D-2)\eta_i = -(\eta_+ + \eta_-)$. So, the whole problem reduces to a problem with four variables,

$$\max_{p_i, \eta_i} \mathcal{F} = \max_{p_\pm, \eta_\pm} \frac{p_+ e^{\eta_+} + p_- e^{\eta_-}}{e^{\eta_+} + e^{\eta_-} + (D-2) e^{-(\eta_+ + \eta_-)/(D-2)}}\,. \tag{2.23}$$

From the conditions it follows that we can choose $\eta_+ > 0$, which implies that $\eta_- = -\eta_+ p_+ / p_- < 0$. We have to prove that the upper bound is $(D-1)/D$. Rewriting $p_- = \frac{\eta_+}{\eta_+ - \eta_-}$, we aim to show that

$$\frac{\left(1 - \frac{\eta_+}{\eta_+ - \eta_-}\right) e^{\eta_+} + \frac{\eta_+}{\eta_+ - \eta_-} e^{\eta_-}}{e^{\eta_+} + e^{\eta_-} + (D-2) e^{-(\eta_+ + \eta_-)/(D-2)}} \leq \frac{D-1}{D}\,. \tag{2.24}$$

This can be rewritten to

$$\begin{aligned} &(D-1)(\eta_+ - \eta_-)\left[e^{\eta_+} + e^{\eta_-} + (D-2) e^{-(\eta_+ + \eta_-)/(D-2)}\right] \\ &- D(\eta_+ e^{\eta_-} - \eta_- e^{\eta_+}) \geq 0\,. \end{aligned} \tag{2.25}$$

Regrouping terms leads to

$$\begin{aligned} &\underbrace{(D-1)(D-2)(\eta_+ - \eta_-) \exp\left(-\frac{\eta_+ + \eta_-}{D-2}\right)}_{t_1} \\ &\underbrace{-\left[\eta_+ + (D-1)\eta_-\right] \exp(\eta_-)}_{t_2} \\ &\underbrace{+\left[\eta_- + (D-1)\eta_+\right] \exp(\eta_+)}_{t_3} \geq 0\,. \end{aligned} \tag{2.26}$$

The term t_1 is always positive, while the signs of t_2 and t_3 depend upon the choice of η_+ and η_-. So consider the following three cases:

1. Case: $(D-1)\eta_+ < |\eta_-|$: Then $t_2 \geq 0$, but $t_3 < 0$. However, we have $t_1 + t_3 \geq 0$ because of
$$-(\eta_+ + \eta_-) = -\eta_+ + |\eta_-| \geq (D-2)\eta_+ \tag{2.27}$$

and

$$\begin{aligned}(D-1)(D-2)(\eta_+ - \eta_-) \\ \geq (D-1)(D-2)|\eta_-| \geq 2|\eta_-| \\ \geq |\eta_-| + (D-1)\eta_+ \geq |\eta_- + (D-1)\eta_+| \,. \end{aligned} \tag{2.28}$$

2. Case: $(D-1)^{-1}\eta_+ \leq |\eta_-| \leq (D-1)\eta_+$: This case directly leads to $t_2 \geq 0$ and $t_3 \geq 0$.

3. Case: $|\eta_-| < (D-1)^{-1}\eta_+$: Then $t_3 \geq 0$, but $t_2 < 0$. However, we have $t_2 + t_3 \geq 0$, because of $e^{\eta_+} > e^{\eta_-}$ and

$$\begin{aligned}(D-1)\eta_+ + \eta_- \geq 3\eta_+ + \eta_- \\ \geq 2\eta_+ \geq \eta_+ + (D-1)\eta_- \,. \end{aligned} \tag{2.29}$$

This finishes the proof. □

In the case of five qubits, $F_{\tau\in\mathcal{Q}_2}(|C_5\rangle, \tau) \leq 31/32 \approx 0.96875$, which improves the bound on the distance to $\mathrm{conv}(\mathcal{Q}_2)$ by more than two orders of magnitude [2]. From Observation 19, we can construct the witness

$$\mathcal{W} = \frac{D-1}{D}\mathbb{1} - |C_N\rangle\langle C_N| \,, \tag{2.30}$$

which detects states outside of $\mathrm{conv}(\mathcal{Q}_2)$. In a similar fashion, any state having the maximally mixed state as k-particle RDMs can be used to construct a witness for $\mathrm{conv}(\mathcal{Q}_k)$. First, in all odd dimensions D there is a four-partite graph state (see Fig. 2.3) with maximally mixed 2-RDMs [91], which can be used to derive a witness for $\mathrm{conv}(\mathcal{Q}_2)$. The highly entangled six-qubit state $|M_6\rangle$ (see the graph in Fig. 2.3) has maximally mixed 3-RDMs, so $\mathcal{W} = \frac{63}{64}\mathbb{1} - |M_6\rangle\langle M_6|$ is a witness to exclude thermal states of three-body Hamiltonians. Third, consider a 5×5 2D cluster state with periodic boundary conditions. This state has $m(|C_{5\times5}\rangle) = 5$ [175], and can therefore serve as a witness $\mathcal{W} = \alpha\mathbb{1} - |C_{5\times5}\rangle\langle C_{5\times5}|$ for $\mathrm{conv}(\mathcal{Q}_4)$, where $\alpha = (2^{25}-1)/2^{25}$. It should be noted that this witness can also be used for $\mathrm{conv}(\mathcal{Q}_2)$, for which the value α might be improved [3].

Lower bounding the irreducible higher-order interactions

Note that the minimal fidelity distance from the convex hull $\mathrm{conv}(\mathcal{Q}_k)$ can be used to show the presence of irreducible interactions D_k. The minimal distance D_k to $\mathcal{Q}_k$ in terms of the relative entropy is bounded by

$$D_k(\varrho) \geq \min_{\sigma\in\mathrm{conv}(\mathcal{Q}_2)} S(\varrho||\sigma) \geq -\log \max_{\sigma\in\mathcal{Q}_2} F(\varrho,\sigma) \,. \tag{2.31}$$

[2] Numerical optimization by a stochastic basin-hopping algorithm yields a maximal overlap of $\approx 81\%$

[3] The reason is that in the proof of Observation 19 one has not only the constraint $\mathrm{tr}[H|C_{5\times5}\rangle\langle C_{5\times5}|] = 0$, but also $\mathrm{tr}[H^2|C_{5\times5}\rangle\langle C_{5\times5}|] = 0$.

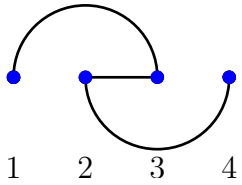


Figure 2.4: Graph of the linear cluster state η with particles 2 and 3 exchanged. This state cannot be approximated by Hamiltonians with nearest-neighbor interactions only.

This follows from a recent result on α-Rényi relative entropies [186],

$$S(\varrho||\sigma) \geq S_{1/2}(\varrho||\sigma) = -\log F(\varrho,\sigma)\,. \tag{2.32}$$

Therefore, the divergence of the five qubit ring cluster state from $\mathcal{Q}_2$ is bounded by $D_2(|C_5\rangle) \geq 0.0317$.

2.5 Quantum simulation as an application

The aim of quantum simulation is to simulate a physical system of interest by another well-controllable one. Naturally, it is crucial to ascertain that the interactions really perform as intended. Different proposals have recently come forward to engineer sizeable three-body interactions in systems of cold polar molecules [187], trapped ions [188], ultracold atoms in triangular lattices [189], Rydberg atoms [190] and circuit QED systems [191]. Using the ring cluster state witness $\mathcal{W} = \alpha\mathbb{1} - |C_N\rangle\langle C_N|$ derived above, it is possible to certify that three- or higher-body interactions have been engineered. This is done by letting the system under control thermalize. If then $\langle\mathcal{W}\rangle < 0$ is measured, one has certified that interactions of weight three or higher are present. At least five qubits are generally required for this, but by further restricting the interaction structure, four qubits can be enough for demonstration purposes. This can already be done with a fidelity of 93.75%, which is within reach of current technologies.

A four-qubit example

To certify that higher than two-body interactions have been engineered, a four qubit state can be used by further restricting the possible interaction structure of the system. As an example, consider an ion chain of four qubits in a linear trap, where the only two-body interactions allowed are of the nearest-neighbor type. Then the four-qubit linear cluster state η, which is a usual linear cluster state with a permutation of particles 2 and 3 (see Fig. 2.4), cannot be obtained as a ground or thermal state but only be approximated up to a fidelity of $\alpha = (N-1)/N = 15/16 = 93.75\%$. This value is within reach of current technologies.

To see why this state cannot be obtained, note that it has the generator

$$G = \{XIZI, IXZZ, ZZXI, IZIX\}\,,$$

where X, Y, Z, I stand for the Pauli matrices and the identity respectively. The stabilizer is then given by

$$\begin{aligned} S = \{&IIII, IXZZ, IYZY, IZIX, \\ &XIZI, XXIZ, XYIY, XZZX, \\ &YIYX, YXXY, -YYXZ, YZYI, \\ &ZIXX, -ZXYY, ZYYZ, ZZXI\} . \end{aligned} \tag{2.33}$$

The nearest-neighbor marginals of the graph state

$$\eta = 2^{-4} \sum_{s_a \in S} s_a \, , \tag{2.34}$$

which are η_{12}, η_{23}, and η_{34}, are all maximally mixed. The remaining two-party marginals do not need to be considered, as long-range interactions are precluded by the physical setup. Then an argument similar to as in Observation 2 can be made. It is again interesting to see what fraction of states cannot be ground states in such a setup. Our semidefinite program shows that 94% of pure states cannot be approximated as ground or thermal states of a linear spin chain having nearest-neighbor interactions only [4].However, when including next-to-nearest neighbor interactions, no unobtainable states were detected.

As an outlook, one may try to extend this idea of interaction certification to the unitary time evolution under local Hamiltonians. For instance, digital quantum simulation can efficiently approximate the time evolution of a time-independent local Hamiltonian and in Ref. [192] an effective 6-particle interaction has been engineered by applying a stroboscopic sequence of universal quantum gates. The process fidelity was quantified using quantum process tomography, however it would be of interest to prove that the same time evolution cannot be generated by 5-particle interactions only.

2.6 Further results

2.6.1 Further results on the information projection

The information projection of real states

The following observation is concerned with the information projection of states having real entries only.

Proposition 3. *Consider a real density matrix, $\varrho = \varrho^T$. Denote its information projection onto $\mathcal{Q}_k$ as $\tilde{\varrho}_k = e^{\tilde{H}} / \operatorname{tr}[e^{\tilde{H}}]$. Then $\tilde{\varrho}_k$ and $\tilde{H}$ must be real, too.*

Proof. From definition of the information projection, one has

$$\tilde{\varrho}_k = \operatorname{argmin}_{\tau \in \mathcal{Q}_k} S(\varrho || \tau) \, . \tag{2.35}$$

For any $\tau = e^H / \operatorname{tr}[e^H]$, consider $\tau' = e^{H'} / \operatorname{tr}[e^{H'}]$ with $H' = (H + H^T)/2$. If we can show that

$$S(\varrho || \tau') \leq S(\varrho || \tau) \, , \tag{2.36}$$

[4] We tested 3 million random pure states for $\delta = 10^{-7}$.

the claim holds. First, note that

$$\begin{aligned} S(\varrho||\tau)) &= \mathrm{tr}[\varrho\log\varrho - \varrho\log\tau] \\ &= \mathrm{tr}[\varrho\log\varrho - \varrho(H - \log\mathrm{tr}[e^H])]\,, \end{aligned} \tag{2.37}$$

and Eq. (2.36) thus corresponds to

$$-\mathrm{tr}[\varrho(H' - \log\mathrm{tr}[e^{H'}])] \leq -\mathrm{tr}[\varrho(H - \log\mathrm{tr}[e^H])]\,. \tag{2.38}$$

The first term on each side cancels because of $\mathrm{tr}[\varrho H'] = \mathrm{tr}[\varrho H]$, and we are left to show that

$$\mathrm{tr}\, e^{H'} \leq \mathrm{tr}\, e^H\,. \tag{2.39}$$

This is indeed the case: From the Golden-Thompson inequality [5], one obtains that

$$\mathrm{tr}\, e^{H'} = \mathrm{tr}\, e^{(H+H^T)/2} \overset{GT}{\leq} \mathrm{tr}[e^{H/2}\, e^{H^T/2}]\,. \tag{2.40}$$

Next, consider the Matrix-Hölder-Inequality (see e.g. Eq. 7.5 in [193]),

$$|\,\mathrm{Tr}(A^\dagger B)| \leq \|A\|_p \|B\|_q\,, \quad \frac{1}{p} + \frac{1}{q} = 1\,, \tag{2.41}$$

where $\|A\|_p = (\mathrm{tr}[|A|^p])^{1/p}$ with $|A| = \sqrt{A^\dagger A}$ (also Sect. 1.1.5). It follows with $H = H^\dagger$ and $e^H \geq 0$ that $|e^H| = e^H$, and thus

$$\mathrm{tr}[e^{H/2}e^{H^T/2}] \overset{MHI}{\leq} \|e^{H/2}\|_2\, \|e^{H^T/2}\|_2 = \mathrm{tr}\, e^H\,. \tag{2.42}$$

Therefore, $\tilde{H}_k$ has to be real, and so is $\tilde{\varrho} = e^{\tilde{H}_k}/\,\mathrm{tr}[e^{\tilde{H}_k}]$. This proves the claim. □

Analogously, if the state has some symmetry, say $\varrho = U^\dagger \varrho U$, then it follows that $\tilde{H} = U^\dagger \tilde{H} U$ and accordingly $\tilde{\varrho} = U^\dagger \tilde{\varrho} U$ [79]. This is can be seen by setting $H' = (H + U^\dagger H U)/2$, then $\mathrm{tr}[\varrho H] = \mathrm{tr}[\varrho H']$ and $\|e^{H/2}\|_2 = \|e^{U^\dagger HU/2}\|_2$, and the claim follows as in above proof.

Upper bounding the divergence to $\mathrm{conv}(\mathcal{Q}_k)$ by the irreducible interactions of decompositions

Proposition 4. *Consider a state, with a decomposition $\varrho = \sum_i p_i \varrho_i$. Its relative entropy divergence to $\mathrm{conv}(\mathcal{Q}_k)$ is upper bounded by the irreducible higher-order interactions to $\mathcal{Q}_k$ of its decompositions ϱ_i.*

$$\min_{\sigma\in\mathrm{conv}(\mathcal{Q}_k)} S(\varrho||\sigma) \quad \leq \quad \min_{\tau_i\in\mathcal{Q}_k} \sum_i p_i S(\varrho_i||\tau_i)\,. \tag{2.43}$$

Proof. Choose elements $\tau_i \in \mathcal{Q}_k$, such that they minimize the irreducible interactions $D_k(\varrho_i)$ to $\mathcal{Q}_k$,

$$\left\{\tau_i \middle| \tau_i = \mathrm{argmin}_{\tau_i\in\mathcal{Q}_k}\, S(\varrho_i||\tau_i)\right\}. \tag{2.44}$$

From the joint convexity of the relative entropy (see Sect. 1.1.5), it follows that

$$S(\varrho\,||\sum_i p_i\tau_i) \leq \sum_i p_i S(\varrho_i||\tau_i)\,. \tag{2.45}$$

But $\sum_i p_i \tau_i \in \mathrm{conv}(\mathcal{Q}_k)$, and thus also

$$\min_{\sigma \in \mathrm{conv}(\mathcal{Q}_k)} S(\varrho||\sigma) \leq S(\varrho \,||\, \sum_i p_i \tau_i)\,. \tag{2.46}$$

This ends the proof. □

2.6.2 Ground and excited states of local Hamiltonians

It is of interest to relate the exponential family $\mathrm{conv}(\mathcal{Q}_k)$ to the sets of ground and excited states of local Hamiltonians respectively. As mentioned, nondegenerate ground states of k-local Hamiltonians $H_k \in \mathcal{H}_k$ are determined by their k-RDMs and belong to the closure of $\mathcal{Q}_k$. Nondegenerate excited states of k-local Hamiltonians are completely determined by their $2k$-RMDs [173], and are therefore ground states of suitable $2k$-local Hamiltonians $H_{2k} \in \mathcal{H}_{2k}$. The argument rests on the fact that any eigenstate of a Hamiltonian H_k will also be the ground state of $(H_k - \lambda \mathbb{1})^2$, where λ is the corresponding eigenvalue. A similar argument also holds for nondegenerate ground and eigenstates. But as can be seen by parameter counting, there exist $2k$-local Hamiltonians which cannot be written as $H_{2k} = (H_k - \lambda \mathbb{1})^2$ with $H_k \in \mathcal{H}_k$. Thus the set of eigenstates of k-local Hamiltonians $\mathrm{ES}(\mathcal{H}_k)$ is a proper subset of the set of ground states of $2k$-local Hamiltonians $\mathrm{GS}(\mathcal{H}_{2k})$, $\mathrm{ES}(\mathcal{H}_k) \subsetneq \mathrm{GS}(\mathcal{H}_{2k})$. Finally, thermal states of k-local Hamiltonians are in the convex hull of $\mathrm{ES}(\mathcal{H}_k)$, and it follows that $\mathrm{conv}(\mathcal{Q}_k) \subsetneq \mathrm{conv}(\mathrm{GS}(\mathcal{H}_{2k}))$. Noting that $\mathrm{conv}(\mathrm{GS}(\mathcal{H}_{2k})) \subseteq \mathrm{conv}(\mathcal{Q}_{2k})$, a witness for $\mathrm{conv}(\mathcal{Q}_{2k})$ is therefore also a witness for $\mathrm{conv}(\mathrm{ES}(\mathcal{H}_k))$.

2.6.3 States of four parties

Let us consider a question that was raised from the work in the previous Section: namely, if states of four parties are uniquely determined by their two-body marginals. In such case, these states could be obtained as ground states of 2-body Hamiltonians. Here we consider this question in detail. This Section is based on Project [B].

When stating the question of uniqueness, it is important to specify the set of states that are under consideration. Usually, either the set of pure states or the set of all states are taken into account. This leads to two different kinds of uniqueness, namely to that of uniqueness among pure states (UDP) and to that of uniqueness among all states (UDA). We adopt here the definition of Ref. [194] and extend it by specifying which marginals are involved.

Definition 10. *A state $|\psi\rangle$ is called*

1) *k-uniquely determined among pure states (k-UDP), if there exists no other pure state having the same k-body marginals as $|\psi\rangle$.*

2) *k-uniquely determined among all states (k-UDA), if there exists no other state (mixed or pure) having the same k-body marginals as $|\psi\rangle$.*

Using this language, pure states are in $\mathcal{Q}_2$, if they are 2-UDA. In contrast, if a state $|\psi\rangle$ is 2-UDP but not 2-UDA, then there exists a state with the same two-body marginals, but of higher entropy. Then $|\psi\rangle$ cannot be a ground state of a two-body Hamiltonian and is not in $\mathcal{Q}_2$, according to Eq. (2.4). Therefore, the results of Ref. [84]

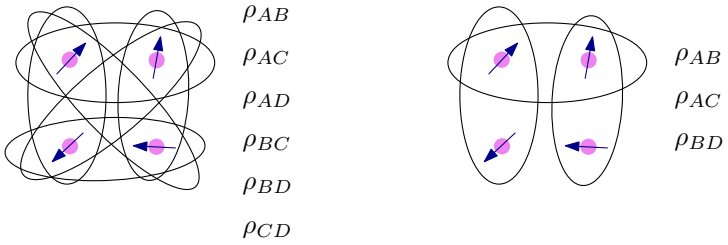


Figure 2.5: Illustration of two different sets of two-body marginals. Left: the set of all six two-body marginals. Right: a set of three two-body marginals that is shown to suffice to uniquely determine pure generic states. Illustration adopted from Proj. [C].

show that almost all three-qubit pure states are 2-UDA: given a random pure state $|\psi\rangle$, it is uniquely determined by its marginals ϱ_{AB}, ϱ_{AC} and ϱ_{BC}. Ref. [163] states that knowledge of just two of the three two-body marginals suffices to determine the state among all pure states (UDP). Later, the authors of Ref. [164] have shown that generic 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. While UDA implies UDP, the converse in general does not need to be true: there are examples of four-qubit states which are 2-UDP but not 2-UDA [195]. Other cases of UDP versus UDA are discussed in Ref. [194]. Note that in some cases a subset of all k-body marginals already suffices to show uniqueness, as in the case of almost all three-qubit states discussed above [163].

States of four parties are 2-UDP

In the case of four particles, it turns out that specific sets consisting of only three of the six two-body marginals suffice to determine generic pure states among all pure states.

Theorem 20 (N. Wyderka, FH, and O. Gühne [C])**.** *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.*

The proof relies on the Schmidt decomposition of a four qubit state state along different bipartitions, while requiring that it yields given reductions $\varrho_{AB}, \varrho_{CD}, \varrho_{BD}$ (illustrated in Fig.2.5). This in turn fixes all parameters of the joint four-qubit state. In fact, this theorem generalizes to all pure four-partite states whose subsystems are of equal dimensions.

Theorem 21 (N. Wyderka, FH, and O. Gühne [C])**.** *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.*

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

Corollary 1 (N. Wyderka, FH, and O. Gühne [C])**.** *For $n \geq 4$, almost all n-qudit pure states of parties $A, B, C, D, E_1, \ldots, E_{n-4}$ having dimension D each are uniquely*

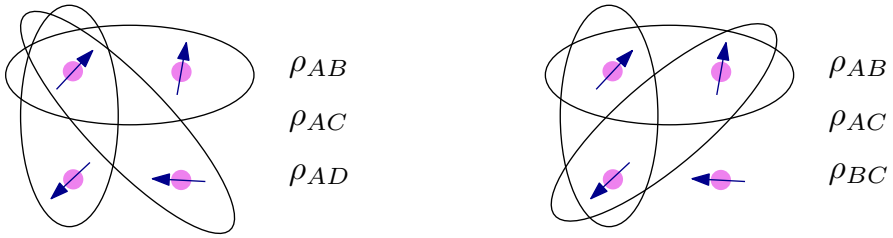


Figure 2.6: Illustration of the two other possible sets of three two-body marginals. Left: a set of marginals, which clearly does not determine the global state, as ϱ_D is not fixed. Right: a set of marginals to which our proof does not apply. Nevertheless, we have numerical evidence that these marginals still determine the state uniquely for qubits. Illustration adopted from Proj. [C].

determined among pure states by the three $(n-2)$*-body marginals of particles* $\varrho_{ABE_1\ldots}$, $\varrho_{CDE_1\ldots}$ *and* $\varrho_{BDE_1\ldots}$. *In particular, this implies that they are* $(n-2)$*-UDP.*

It should be stressed that the main statement of this Corollary is the fact that three marginals of size $(n-2)$ can already suffice. The fact that pure states are $(n-2)$-UDP is not surprising, as already less knowledge is generally sufficient for a pure state to be UDA [164].

Discussion

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, partially answering questions raised in main part of this Chapter. Interestingly, it also follows that pure states of an arbitrary number of qudits are determined by certain subsets of their marginals having size $n-2$. The proof required two marginals of distinct systems to be equal, 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. 2.6. 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 $\varrho_{\mathrm{ABC}} \otimes \varrho_{\mathrm{D}}$ 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 coincide on these marginals [5]. 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-qudit states are uniquely determined also among all *mixed* states by their two-body marginals. The results from Ref. [164] suggest that generic states are not necessarily UDA by their $\lfloor \frac{n}{2} \rfloor$-RDMs. Indeed, the discussion in Sect. 2.4 shows that for the case of four qutris, there exists a witness detecting states which are not UDA, namely the four qutrit AME state

[5] Here we used the semi-definite program from Sect. 2.3.

depicted in Fig. 1.2.3. This generalizes to all odd dimensions. On the other hand, the numerical procedure used in Sect. 2.3 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.

2.6.4 Even- and odd-body correlations of qubit states

Let us focus on aspects of the universal state inversion map applied to qubits. This answers questions about the uniqueness of quantum states, given certain sets of its correlations. In the first part in the Chapter the uniqueness of states from the knowledge of their *local* correlations was considered. In contrast, this Section deals with the uniqueness of states given all their odd- or even-body correlations, leading to extensions and variations of previous results [84, 163, 164, 184]. Additionally, we provide explicit relations between these sets of correlations. This section is based on Project [C].

The universal state inversion in the Bloch representation

Recall that a density matrix ϱ on n qubits can be expanded in terms of the Pauli basis as (c.f. Sect. 1.1.7)

$$\varrho = 2^{-n} \sum_{\sigma_\alpha \in \mathcal{P}_n} \mathrm{Tr}(\sigma_\alpha \varrho)\sigma_\alpha \,. \tag{2.47}$$

Let us group terms appearing in the decomposition according to their weight:

$$\varrho = 2^{-n} \sum_{j=0}^{n} P_j \,, \tag{2.48}$$

where P_j accounts for all j-body correlations

$$P_j = \sum_{\substack{\sigma_\alpha \in \mathcal{P}_n \\ \mathrm{wt}(\sigma_\alpha)=j}} \mathrm{Tr}(\sigma_\alpha \varrho)\sigma_\alpha \,. \tag{2.49}$$

Recall from Sect. 1.73 that the universal state inversion is given by

$$\mathcal{I}[\varrho] = \sum_{S \subseteq \{1 \ldots n\}} (-1)^{|S|} \varrho_S \otimes \mathbb{1}_{S^c} \,, \tag{2.50}$$

where $\varrho_S = \mathrm{Tr}_{S^c}(\varrho)$. Denote by the inverted state as $\tilde{\varrho} = \mathcal{I}[\varrho]$. The action of the universal state inversion on qubits corresponds to flipping all spins - thus introducing a minus sign for all odd-body correlations. This can be seen by understanding how $\mathcal{I}$ acts in the Bloch representation.

Proposition 5. *Given a state of n parties having D levels each expanded as $\varrho = D^{-n} \sum_{j=0}^{n} P_j$. Its (unnormalized) state inversion reads*

$$\tilde{\varrho} = \mathcal{I}[\varrho] = \frac{1}{D^n} \sum_{j=0}^{n} (-1)^j (D-1)^{n-j} P_j \,. \tag{2.51}$$

Proof. In Eq. (2.50), the subsystems of size k contribute to terms of weight j by a factor of $(-1)^k D^{n-k}\binom{n-j}{n-k}$. Here, the minus sign depends on the size k of the subsystem, the term D^{n-k} originates in the different normalization factor of the partially reduced states tensored by $\mathbb{1}^{\otimes n-k}$, and each P_j appears $\binom{n}{k}\binom{k}{j}/\binom{n}{j} = \binom{n-j}{n-k}$ times in the sum. Thus

$$\mathcal{I}[\varrho] = \frac{1}{D^n}\sum_{k=0}^{n}\sum_{j=0}^{k}(-1)^k D^{n-k}\binom{n-j}{n-k}P_j\,. \tag{2.52}$$

For $j = 0$, above expression is simply equal to $(D-1)^n$. Let us now consider a fixed $j > 0$. Using $\binom{n-j}{n-k} = 0$ if $j > k$, one obtains

$$\begin{aligned}\sum_{k=0}^{n}\binom{n-j}{n-k}(-1)^k D^{n-k} &= \sum_{k=0}^{n}\binom{n-j}{k}(-1)^{n-k}D^k \\ &= (-1)^j\sum_{k=0}^{n'}\binom{n'}{k}(-1)^{n'-k}D^k \\ &= (-1)^j(D-1)^{n'}\,,\end{aligned} \tag{2.53}$$

where $n' = n - j$. This ends the proof. □

A normalization of the state inversion, such that it is also trace-preserving, yields

$$\tilde{\varrho}_{\text{norm}} = \frac{1}{D^n}\sum_{j=0}^{n}(-1)^j(D-1)^{-j}P_j\,. \tag{2.54}$$

The normalized universal state inversion of a pure qubit state again pure; however this is not the case in higher dimensions. To see this, evaluate

$$\operatorname{Tr}(\tilde{\varrho}^2_{\text{norm}}) = D^{-2n}\sum_{j=0}^{n}(D-1)^{-2j}\operatorname{Tr}(P_j^2)\,. \tag{2.55}$$

where $\sum_j \operatorname{Tr}(P_j^2) = D^n$ because of $\operatorname{Tr}(\varrho^2) = 1$. Clearly, $\operatorname{Tr}(\tilde{\varrho}^2_{\text{norm}})$ will be strictly smaller than 1, except in the case of $D = 2$. Concerning the inversion for qubits, each term P_j with j being odd only acquires a minus sign, and $\mathcal{I}[\mathcal{I}[\varrho_{\text{norm}}]] = \tilde{\tilde{\varrho}}_{\text{norm}} = \varrho_{\text{norm}}$. This is in contrast to the universal state inversion map for $D \geq 3$, which is not involutory.

If the number of parties is odd and ϱ pure, then the state inversion $\tilde{\varrho}$ is orthogonal to ϱ in the Hilbert-Schmidt inner product.

Proposition 6 (N. Wyderka, FH, and O. Gühne [E])**.** *Given a pure state ϱ on an odd number of parties n, then*

$$\operatorname{Tr}(\varrho\tilde{\varrho}) = 0\,. \tag{2.56}$$

Proof. Consider the Schmidt decomposition of a pure state across a bipartition $A|B$. It can be seen that

$$(\varrho_A \otimes \mathbb{1}_B)\varrho_{AB} = (\mathbb{1}_A \otimes \varrho_B)\varrho_{AB}\,. \tag{2.57}$$

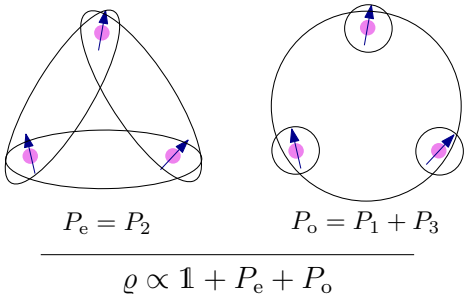


Figure 2.7: Visualization of the decomposition of a three-particle state ρ into even and odd-body correlations. A state ρ is expanded in Bloch representation as $\rho \propto \mathbb{1}+P_1+P_2+\ldots$, where P_j denotes all terms containing j-body correlations. We prove that the even-body correlations P_e are determined by the odd-body correlations P_o for pure states of an odd number of qubits, so the three qubit state is completely determined by P_o. The illustration is adopted from Proj. [E].

In Eq. (2.50), any two complementary terms ϱ_S and ϱ_{S^c} acquire opposite signs for all subsystems S. Consequently all terms cancel pairwise in

$$\mathrm{Tr}(\varrho\tilde{\varrho}) = \mathrm{Tr}\left(\varrho \sum_{S\subseteq\{1\ldots n\}} (-1)^{|S|}\varrho_S \otimes \mathbb{1}_{S^c}\right) = 0\,. \tag{2.58}$$

This ends the proof. □

Let us now focus on systems of qubits only. In order to obtain relations between correlations acting on even and odd subsystems respectively, we decompose a state of n qubits into

$$\varrho = 2^{-n}(\mathbb{1} + P_\mathrm{e} + P_\mathrm{o})\,. \tag{2.59}$$

Above, P_e and P_o contain only even-body (excluding the identity) and odd-body correlations respectively,

$$P_\mathrm{e} = \sum_{\substack{j \text{ even},\\ j\neq 0}} P_j\,, \tag{2.60}$$

$$P_\mathrm{o} = \sum_{j \text{ odd}} P_j\,. \tag{2.61}$$

This decomposition is visualized in Fig. 2.7 for the case of three qubits. Using such a decomposition, the state inversion can be written as

$$\tilde{\varrho} = 2^{-n}(\mathbb{1} + P_\mathrm{e} - P_\mathrm{o})\,, \tag{2.62}$$

where all odd-body correlations change sign. Interestingly, this can also be written as $\tilde{\varrho} = Y^{\otimes n}\varrho^T Y^{\otimes n}$ [196, 197]. In particular, for pure qubit states, the inversion can also be obtained from

$$|\tilde{\psi}\rangle = (i\sigma_y)^{\otimes n}\mathcal{C}\,|\psi\rangle\,, \tag{2.63}$$

where $\mathcal{C}$ is the complex conjugation. Note that $|\tilde{\tilde{\psi}}\rangle = -\,|\psi\rangle$ for n odd, and $\tilde{\varrho} = |\tilde{\psi}\rangle\langle\tilde{\psi}|$. Thus when considering pure qubit states on an odd number of parties, Eq. (2.56) reduces to

$$\langle\psi|\tilde{\psi}\rangle = 0\,. \tag{2.64}$$

States of an odd number of qubits

From Eq. (2.64) one can obtain interesting relations between P_{e} and P_{o} if the number of qubits is odd.

Proposition 7 (N. Wyderka, FH, and O. Gühne; Ref. [E]). *Let $\varrho = |\psi\rangle\langle\psi|$ be a pure state of an odd number of qubits, written in the even-odd decomposition of Eq.* (2.59)*. Then*

$$P_{\mathrm{o}}^2 = (\mathbb{1} + P_{\mathrm{e}})^2 \,, \tag{2.65}$$

$$P_{\mathrm{o}}^2 = 2^{n-1}(\mathbb{1} + P_{\mathrm{e}}) \,, \tag{2.66}$$

$$[P_{\mathrm{o}}, P_{\mathrm{e}}] = 0 \,, \tag{2.67}$$

$$\mathrm{spectrum}(P_{\mathrm{e}}) = (2^{n-1} - 1, 2^{n-1} - 1, -1, \ldots, -1) \,, \tag{2.68}$$

$$\mathrm{spectrum}(P_{\mathrm{o}}) = (2^{n-1}, -2^{n-1}, 0, \ldots, 0,) \,. \tag{2.69}$$

Proof. Expand

$$\begin{aligned} \varrho\tilde{\varrho} &= 2^{-2n}(\mathbb{1} + P_{\mathrm{e}} + P_{\mathrm{o}})(\mathbb{1} + P_{\mathrm{e}} - P_{\mathrm{o}}) \\ &= 2^{-2n}(\mathbb{1} + 2P_{\mathrm{e}} + P_{\mathrm{e}}^2 - P_{\mathrm{o}}^2) = 0 \,. \end{aligned} \tag{2.70}$$

This yields the first relation $P_{\mathrm{o}}^2 = (\mathbb{1} + P_{\mathrm{e}})^2$. From Eqs. (2.59) and (2.62), one obtains

$$\mathbb{1} + P_{\mathrm{e}} = 2^{n-1}(|\psi\rangle\langle\psi| + |\tilde{\psi}\rangle\langle\tilde{\psi}|) \,, \tag{2.71}$$

$$P_{\mathrm{o}} = 2^{n-1}(|\psi\rangle\langle\psi| - |\tilde{\psi}\rangle\langle\tilde{\psi}|) \,. \tag{2.72}$$

With the fact that $\langle\psi|\tilde{\psi}\rangle = 0$, the first two relations can directly be verified. Furthermore, P_{e} and P_{o} are diagonal in the same eigenbasis, and $[P_{\mathrm{e}}, P_{\mathrm{o}}] = 0$. The spectrum can simply be read of Eqs. (2.71) and (2.72). This ends the proof. □

From Eq. (2.66), it follows that a pure state of an odd number of qubits is uniquely determined amongst all pure states (UDP) by its odd-body correlations. Thus, one could ask if states are also uniquely determined by their odd-body correlations amongst all states (UDA), pure or mixed [194]. This is indeed the case.

Corollary 2 (N. Wyderka, FH, and O. Gühne [E]). *Let $|\psi\rangle$ be a pure state of an odd number of qubits. Then its odd-body correlations P_{o} uniquely determine $|\psi\rangle$ amongst all states (UDA).*

Proof. Let σ be a (possibly mixed) state having the same odd-body correlations as $|\psi\rangle\langle\psi|$. Expand σ in terms of pure states $\{|\phi_i\rangle\}$ as

$$\sigma = \sum_i p_i |\phi_i\rangle\langle\phi_i| = 2^{-n} \sum_i p_i (\mathbb{1} + P_{\mathrm{e}}^{(i)} + P_{\mathrm{o}}^{(i)}) \,, \tag{2.73}$$

with the convex weights p_i. By assumption, $\sum_i p_i P_{\mathrm{o}}^{(i)} = P_{\mathrm{o}}$. Note that all the rank-2 operators $P_{\mathrm{o}}^{(i)}$ share the same spectrum, having the non-vanishing eigenvalues $\pm 2^{n-1}$. In order that

$$\lambda_{\max}\Big(\sum p_i P_{\mathrm{o}}^{(i)}\Big) = \quad 2^{n-1} \qquad \text{and} \qquad \lambda_{\min}\Big(\sum p_i P_{\mathrm{o}}^{(i)}\Big) = -2^{n-1} \,, \tag{2.74}$$

the corresponding eigenvectors of all $P_{\mathrm{o}}^{(i)}$ must to be equal. It follows that $P_{\mathrm{o}}^{(i)} = P_{\mathrm{o}}$, and from Eq. (2.66), also $P_{\mathrm{e}}^{(i)} = P_{\mathrm{e}}$. Hence $\sigma = |\psi\rangle\langle\psi|$. This ends the proof. □

This result can be seen as a variation of the theme found in Ref. [84], where it was shown that almost all three-qubit states are UDA by P_1 and P_2. Corollary 4 shows that all three-qubit states are UDA by P_1 and P_3 , and it is remarkable that this generalizes to all odd numbers of parties.

Conversely, one could ask if the even-body correlations also uniquely determine the state. This is not the case, although the admissible odd-body correlations can easily be parametrized.

Corollary 3 (N. Wyderka, FH, and O. Gühne [E])**.** *Let $|\psi\rangle$ be a pure state of an odd number of qubits, and let its even-body correlations P_{e} be given. Then there is a two-parameter family of admissible odd-body correlations $P_{\mathrm{o}}(\theta,\phi)$ to retrieve a pure state again,*

$$\varrho(\theta,\phi) = 2^{-n}[\mathbb{1} + P_{\mathrm{e}} + P_{\mathrm{o}}(\theta,\phi)]\,. \tag{2.75}$$

Proof. From Eq. (2.71), recall that

$$\mathbb{1} + P_{\mathrm{e}} = 2^{n-1}(|\psi\rangle\langle\psi| + |\tilde{\psi}\rangle\langle\tilde{\psi}|)\,. \tag{2.76}$$

Let P_{e} be given. Then for any vector $|\eta\rangle$ lying in the two-dimensional subspace of the projector $(\mathbb{1} + P_{\mathrm{e}})$, one has also that $2^{n-1}(|\eta\rangle\langle\eta| + |\tilde{\eta}\rangle\langle\tilde{\eta}|) = (\mathbb{1} + P_{\mathrm{e}})$. Thus compatible odd-body correlations P_{o} can be reconstructed by

$$P_{\mathrm{o}} \;=\; 2^{n-1}(|\eta\rangle\,\langle\eta| - |\tilde{\eta}\rangle\,\langle\tilde{\eta}|). \tag{2.77}$$

Keeping $|\eta\rangle$ fixed, all valid solutions are parametrized in terms of real valued θ and ϕ as

$$\begin{aligned} P_{\mathrm{o}}(\theta,\phi) = 2^{n-1}[&\cos\theta(|\eta\rangle\langle\eta| - |\tilde{\eta}\rangle\langle\tilde{\eta}|) \\ &+ \sin\theta(e^{i\phi}\,|\tilde{\eta}\rangle\langle\eta| + e^{-i\phi}\,|\eta\rangle\langle\tilde{\eta}|)]\,. \end{aligned} \tag{2.78}$$

This ends the proof. □

Results for an even number of qubits

Let us now consider pure states ψ of an even number of qubits. Denote by α the absolute value of the overlap

$$\langle\tilde{\psi}|\psi\rangle = \alpha e^{i\varphi}\,. \tag{2.79}$$

Note that the phase φ is not a physical property of the state, as changing the state $|\psi\rangle$ to $e^{i\beta}\,|\psi\rangle$ changes the value of φ while describing the same state. The value α, however, is physical and the properties of the state depend on it. Indeed, for pure states and $n = 2$, α is the concurrence [197]. For pure states with $n \geq 2$, α is known as the n-concurrence of a state and is an entanglement monotone [198]. For our purposes, one can distinguish three cases: 1) If $\alpha = 0$, then results similar to those for an odd number of qubits hold. Examples for such states are fully separable states and the W state on n qubits. 2) If $\alpha = 1$, only even-body correlations are present. Examples of such states are graph states whose every vertex is connected to an odd number of other vertices [6], such as e.g. GHZ states of n qubits. These states correspond to self-dual additive codes of type II (c.f. Sect. 1.2.4). 3) If $0 < \alpha < 1$, one has the following:

[6] See Thm. 15 in Ref. [199].

	n even and $0 < a < 1$	n odd or $a = 0$
P_{o} given	One dimensional solution space for P_{e} (UDP)	P_{e} is uniquely determined (UDA)
P_{e} given	$\pm P_{\mathrm{o}}$ is uniquely determined up to the sign (UDP)	Two dimensional solution space for P_{o} (UDP)

Table 2.2: A summary of the relations between the even and odd components of the correlations as in this Section. Adopted from Proj. [E].

Proposition 8 (N. Wyderka, FH, and O. Gühne [E])**.** *Let $|\psi\rangle$ be a pure state of an even number of qubits with $|\langle\psi|\tilde{\psi}\rangle| = \alpha \neq 0$. Then*
(1) the even-body correlations P_{e} uniquely determine the odd-body correlations P_{o} amongst pure states up to a sign;
(2) the family of pure states having the same odd-body correlations P_{o} as $|\psi\rangle$ amongst pure states is one-dimensional. The even-body correlations can then be parameterized in terms of P_{o}.

The proof relies on determining the eigenvalues of P_{e} and P_{e}. Note that in contrast to the case of an odd number of qubits, a statement analogous to Cor. 2 is generally not true for an even number of parties. While P_{e} determines a state among all pure states up to a sign of P_{o}, it does not so among all states, except when $P_{\mathrm{o}} = 0$. This can be seen by convex combination of ϱ and $\tilde{\varrho}$, leading equal even-body but diminished odd-body correlations. Only in the case of $\alpha = 1$, where no odd-body correlations are present, is the state uniquely determined among all states by P_{e}. This can be seen from the fact that introducing additional odd-body correlations would lead to a purity $\mathrm{Tr}(\rho^2)$ greater than one. The results of all the previous Propositions and Corollaries are summarized in Table 2.2.

Applications

Our results have various applications. First, it can be shown that unique ground states of Hamiltonians having even-body interactions only cannot exhibit any odd-body correlations. This is seen from the fact that for any state $|\psi\rangle$, the state inversion $|\tilde{\psi}\rangle$ will have the same P_{e} and therefore the same energy. If n is odd however, this will not be possible. Thus ground states of even-body Hamiltonians on an odd number of qubits must necessarily be degenerate. This can be seen as an instance of Kramers degeneracy theorem [200]. Conversely, consider Hamiltonians having odd-body interactions only. Then it follows from Prop. 8 that their ground states can only be non-degenerate if $|\langle\tilde{\psi}|\psi\rangle| = \alpha = 0$.

Second, consider the unitary time evolution under Hamiltonians having odd-body interactions only. Then $\alpha^2 = \mathrm{Tr}(\rho\tilde{\rho})$ stays constant for all times. This can be seen by applying an adaption of Lemma 1 from Chapt. 3 to the decomposition of the time evolution into nested commutators. Interestingly, this is also true for mixed states, and the result also holds for the n-concurrence C_n as given by the convex roof construction of α [198]. This re-derives previously known results from Ref. [201]. Additionally, this can be used to test if three-body interactions such as proposed by Refs. [187, 202] truly have been engineered.

Finally, these results can be applied to the task of entanglement detection. Consider a pure state of an odd number of qubits. Then it can be checked for biseparability by its $(n-2)$-body marginals only: Consider any bipartition $A|B$. If A (B) contains an odd number of qubits, P_{e} can according to Prop. 7 be reconstructed and ϱ_A (ϱ_B) be tested for purity. Thus separability across any bipartition of pure states can be detected.

Further details on these application can be found in Proj. [E].

Discussion

We introduced the decomposition of multipartite qubit states in terms of even- and odd-body correlations. For pure states, we showed that the even- and odd-body correlations are deeply connected, and often one type of the correlations determines the other. This allowed to prove several applications, ranging from the unique determination of a state by its odd-body correlations to invariants under Hamiltonian time evolution and entanglement detection. It may be of interest to extend this theory to monogamy relations between the different sets of correlations.

2.7 Conclusion

In this Chapter, I have provided methods to characterize thermal and ground states of few-body Hamiltonians. The results can be used to test experimentally with a witness whether three-body or higher-order interactions are present. The concepts developed can also be seen as extending notions of entanglement, with less complex states already being determined by their few-body marginals. For future work, it would be desirable to characterize the entanglement properties of $\mathcal{Q}_2$, e.g. to determine whether the entanglement in these states is bounded, or whether they can be simulated classically in an efficient manner. Furthermore, it is of significant experimental relevance to develop schemes to certify that a unitary time evolution was generated by a k-body Hamiltonian.

In further projects, I 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 follows that almost all pure states of an arbitrary number of qudits are determined by a set of three marginals having size $(n-2)$.

An analysis of the Bloch decomposition of pure qubit states showed intricate relations between their even- and odd-body correlations. Given one set of correlations, the full state is often completely determined up to a few parameters, and an explicit reconstruction of the missing correlations can be given. These results are useful to deduce certain properties of ground states, to obtain invariants under unitary time evolution, and to simplify certain tasks of entanglement detection. It would be desirable to derive similar relations also for states having higher dimensions.

Chapter 3

AME state of seven qubits

This Chapter is concerned with the existence of an *absolutely maximally entangled* of seven qubits, as introduced in Chpt.1.2.3. These are states that show maximal possible entanglement across every bipartition. Accordingly, these states are also known as *absolutely maximally entangled* (AME) [44, 48, 87–100].

Definition 11 (AME states)**.** *A pure state of n parties, having D levels each, is called absolutely maximally entangled (AME), if all reductions to $\lfloor \frac{n}{2} \rfloor$ parties are maximally mixed.*

In the following, I will show the non-existence proof of the hitherto last open case concerning 2-level systems, the case of seven qubits. This Chapter is based on Project [D].

Let me summarize the known results concerning qubits: The three-qubit Greenberger-Horne-Zeilinger (GHZ) state is an AME state since all the single-qubit reduced states are maximally mixed. For four qubits it was shown that AME states do not exist [86] and best approximations of AME states (where not all reduced states are maximally mixed) have been presented [96]. Five- and six-qubit AME states are known [44, 93]. These can be represented as graph states and correspond to additive or stabilizer codes used in quantum error correction [44, 47]. For more than eight qubits, AME states do not exist [44, 106, 107, 118].

Despite many attempts, the case of seven qubits remained unresolved. Numerical results give some evidence for the absence of an AME state [93–95]. By exhaustive search, it was shown that such a state could not have the form of a stabilizer state [47]. Nevertheless, some approximation has been presented by making many but not all three-body marginals maximally mixed [98, 203].

As shortly mentioned, AME states are a type of pure *quantum error-correcting codes* (QECC), having the maximal distance allowed by the Singleton bound (see Thm. 6) [204]. In particular, AME states of n parties having local dimension D each correspond to a pure QECC in $(\mathbb{C}^D)^{\otimes n}$ of distance $\lfloor \frac{n}{2} \rfloor + 1$, denoted by $((n, 1, \lfloor \frac{n}{2} \rfloor + 1))_q$. Often, but not always, bounds on so-called non-additive (i.e. non-stabilizer) codes coincide with those for additive (stabilizer) codes. The seven qubit AME state would - if it existed - be one of the few examples where a non-additive code outperformed an additive one. This possibility was noted already in a seminal article by Calderbank et al. [108]. Up to $n = 30$, there are only three other instances known where this could be the case for one-dimensional codes on qubits: The existence of one-dimensional non-additive codes with parameters $((13, 1, 6))_2$, $((19, 1, 8))_2$, and

$((25,1,10))_2$ was still unresolved (see Table 13.3 in [106]). I will address these three cases in Chpt. 5, and show that these codes cannot exist either.

In the following, I provide a method to characterize AME states and their approximations, making use of the Bloch representation [39]. The usefulness of this tool may be surprising at first sight, as the Bloch representation is designed to be a tool for mixed states. We were motivated to choose this approach by the fact that monogamy equalities [96, 159] directly signal the non-existence of a four-qubit AME state, and the natural framework for deriving the monogamy equalities appears to be the Bloch representation [159].

3.1 The Bloch representation

As described in Sect. 1.1.7, any n-qubit state can be written as

$$\varrho = \frac{1}{2^n} \sum_{\alpha_1 \ldots \alpha_n} r_{\alpha_1,\ldots,\alpha_n} \sigma_{\alpha_1} \otimes \cdots \otimes \sigma_{\alpha_n} \,, \tag{3.1}$$

where the $\{\alpha_1, \ldots, \alpha_n\} \in \{0, x, y, z\}$ label combinations of the four Pauli matrices. For simplicity, we group the terms according to their weight, that is, their number of non-trivial (Pauli) operators. Let P_j be the sum over terms of weight j, then the state can be written as

$$\varrho = \frac{1}{2^n} \Big(\mathbb{1}^{\otimes n} + \sum_{j=1}^{n} P_j \Big) \,. \tag{3.2}$$

We denote by $P_j^{(V)}$ a subset of P_j, where V further specifies its support, i.e. its non-trivial terms are located on the subsystems in V. To give an example, a state of three qubits reads

$$\varrho = \frac{1}{2^3} \Big(\mathbb{1}^{\otimes 3} + \sum_{j=1}^{3} P_1^{(j)} + \sum_{1 \le k < l \le 3} P_2^{(kl)} + P_3 \Big) \,, \tag{3.3}$$

where, e.g., $P_2^{(12)} = \sum r_{\alpha_1,\alpha_2,0}\, \sigma_{\alpha_1} \otimes \sigma_{\alpha_2} \otimes \mathbb{1}$ and $\alpha_1, \alpha_2 \neq 0$. When tracing out the third qubit, one drops the terms $P_3, P_2^{(13)}, P_2^{(23)}$, and $P_1^{(3)}$, as they do not contain an identity in the third subsystem. Also, the normalization prefactor is multiplied by the dimension of the parties over which the partial trace was performed, resulting in

$$\mathrm{tr}_{\{3\}}[\varrho] \otimes \mathbb{1} = \frac{1}{2^2} \big(\mathbb{1}^{\otimes 3} + P_1^{(1)} + P_1^{(2)} + P_2^{(12)} \big) \,. \tag{3.4}$$

Accordingly, a three-qubit state having maximally mixed one-body reduced density matrices does not have terms of weight one, the terms $P_1^{(j)}$ are absent. Similarly, in n-qubit AME states all operators P_j with $1 \le j \le \lfloor \frac{n}{2} \rfloor$ vanish.

Our further discussion rests on recognizing what terms may appear in the squared state ϱ^2. For this, consider two terms A and B, both appearing in the Bloch expansion of the state. For computing ϱ^2, the anticommutator $\{A, B\}$ is required, and we state the following observation regarding its weight.

Lemma 1 (parity rule). *Let M, N be Hermitian operators proportional to n-fold tensor products of single-qubit Pauli operators, $M = c_M\, \sigma_{\mu_1} \otimes \cdots \otimes \sigma_{\mu_n}$, $N = c_N\, \sigma_{\nu_1} \otimes \cdots \otimes \sigma_{\nu_n}$, where $c_M, c_N \in \mathbb{R}$. Let us denote their weights, that is, their number of nontrivial Pauli-operators in their tensor expansion, by $|M|$ and $|N|$. Then, if the anticommutator $\{M, N\}$ does not vanish, its weight $|\{M, N\}|$ fulfills*

$$|\{M, N\}| = |M| + |N| \mod 2\,. \tag{3.5}$$

Proof. The product MN, and thus also $\{M, N\}$, has at most weight $|M| + |N|$. This is attained, if the supports of M and N are disjoint. Each pair of equal, but non-zero indices $\mu_j = \nu_j$ corresponds to some overlap of the supports and reduces the maximal weight $|M| + |N|$ by two. In contrast, if a pair of non-zero indices are not equal (e.g., $\mu_j \neq \nu_j$), the product MN contains the term $\sigma_{\mu_j}\sigma_{\nu_j} = i\epsilon_{\mu_j\nu_j\chi}\sigma_\chi$. Consequently for each such pair $|M|+|N|$ is reduced by only one. If an odd number of such pairs exists, the anticommutator has to vanish, as it is Hermitian. So, such pairs have to occur an even number of times, which proves the claim. □

We can summarize the behavior of the weights of M and N and their anticommutator as follows:

$$\begin{aligned} \{\text{even}, \text{even}\} &\longrightarrow \text{even}, \\ \{\text{odd}, \text{odd}\} &\longrightarrow \text{even}, \\ \{\text{even}, \text{odd}\} &\longrightarrow \text{odd}. \end{aligned} \tag{3.6}$$

It follows that an analogous behavior holds for the P_j. If j and k are either both even or both odd, the anticommutator $\{P_j, P_k\}$ can only contribute to the P_l where l is even. Similarly, if j is even and k is odd, it only contributes to the P_l having odd l.

3.2 Properties of AME state reductions

First, recall that for a pure n-party state $|\psi\rangle_{AB}$ consisting of D-level systems, the complementary reduced states of any bipartition share the same spectrum. This follows from its Schmidt decomposition. Hence, if a $(n-k)$-body reduction ϱ_B is maximally mixed, its complementary reduced state ϱ_A of size $k \geq \lfloor \frac{n}{2} \rfloor$ has all $D^{(n-k)}$ nonzero eigenvalues equal to $\lambda = D^{-(n-k)}$. Thus the reduced state is proportional to a projector,

$$\varrho_A^2 = D^{-(n-k)}\varrho_A\,. \tag{3.7}$$

By Schmidt decomposition, one further sees that the full state $|\psi\rangle_{AB}$ is an eigenvector of the reduced state ϱ_A,

$$\varrho_A \otimes \mathbb{1}^{\otimes(n-k)} |\psi\rangle_{AB} = D^{-(n-k)} |\psi\rangle_{AB}\,. \tag{3.8}$$

Accordingly, for an AME state having all $\lfloor \frac{n}{2} \rfloor$-body reduced states maximally mixed, any k-body reduced state $\varrho_{(k)}$ with $\lfloor \frac{n}{2} \rfloor \leq k \leq n$ fulfills relations (3.7) and (3.8).

Let us now consider AME states of n qubits. We decompose Eq. (3.8) in the Bloch representation, using the reduced state $\varrho_{(k)}$ on the first $k = \lfloor \frac{n}{2} \rfloor + 1$ parties of a qubit AME state,

$$\frac{1}{2^k}(\mathbb{1}^{\otimes k} + P_k^{(1\cdots k)}) \otimes \mathbb{1}^{(n-k)} |\psi\rangle = 2^{-(n-k)} |\psi\rangle\,. \tag{3.9}$$

Because all $\lfloor \frac{n}{2} \rfloor$-body marginals are maximally mixed, $P_{j \leq \lfloor \frac{n}{2} \rfloor} = 0$. We obtain the eigenvector relations

$$P_k^{(1\cdots k)} \otimes \mathbb{1}^{\otimes(n-k)} |\psi\rangle = \begin{cases} 3\,|\psi\rangle & n \text{ even}\,, \\ 1\,|\psi\rangle & n \text{ odd}\,. \end{cases} \tag{3.10}$$

By accounting for combinatorial factors, similar relations can be obtained in an iterative way for all $P^{(1\cdots j)}_{j \geq \lfloor \frac{n}{2} \rfloor + 1}$ [1].

3.3 Scott bound

The projector property [Eq. (3.7)] alone is already enough to derive bounds on the existence of AME states. These bounds originate in work by Rains and were applied to AME states by Scott [44, 118]. In the following, I will provide a proof in the Bloch representation.

Proposition 9 (Scott bound)**.** *An AME state of n parties having D levels each fulfills*

$$n \leq \begin{cases} 2(D^2-1) & n \text{ even}, \\ 2D(D+1)-1 & n \text{ odd}. \end{cases} \tag{3.11}$$

Proof. Let $\{\Lambda_\alpha\}$ form an orthonormal basis of Hermitian operators for a qudit system of local dimension D. Because of orthonormality, $\mathrm{tr}[\Lambda_\alpha \Lambda_\beta] = D\delta_{\alpha\beta}$. A k-body reduced state on parties in V can then be written as

$$\varrho_{(k)} = \frac{1}{D^k}(\mathbb{1} + \sum_{\mathrm{supp}(\alpha) \in V} r_{\alpha_1,\ldots,\alpha_n} \Lambda_{\alpha_1} \otimes \cdots \otimes \Lambda_{\alpha_n})\,. \tag{3.12}$$

Here, the sum runs over appropriate α, specifically, over those whose corresponding basis terms have nontrivial support only strictly within the reduced state under discussion, $\mathrm{supp}(\alpha) \in V$, cf. also Eq. (3.4). We recall that any subsystem of an AME state, having size $k \geq \lfloor\, n/2 \,\rfloor + 1$, fulfills the projector property

$$\varrho_{(k)}^2 = D^{-(n-k)} \varrho_{(k)}\,. \tag{3.13}$$

Expanding in the Bloch representation and taking the trace gives

$$\mathrm{tr}[\varrho_{(k)}^2] = \frac{1}{D^k}(1 + \sum_{\mathrm{supp}(\alpha) \in V} r_\alpha^2) = D^{-(n-k)}\,. \tag{3.14}$$

Thus the coefficients r_α are constrained by

$$\sum_{\mathrm{supp}(\alpha) \in V} r_\alpha^2 = \begin{cases} D^{2k-n} - 1 > 0 & k > \lfloor \frac{n}{2} \rfloor\,, \\ 0 & k \leq \lfloor \frac{n}{2} \rfloor\,. \end{cases} \tag{3.15}$$

[1] Also see Sect. 1.2.4 for the weight enumerator of AME states, which is one-to-one related with the eigenvector relations.

For $k > \lfloor \frac{n}{2} \rfloor$, the sum is strictly positive, because reductions of pure states to size $\lfloor \frac{n}{2} \rfloor + 1$ can not be proportional to the identity, as one can see from its Schmidt decomposition.

Let us look at a specific reduced state of size $\lfloor \frac{n}{2} \rfloor + 2$, containing $\lfloor \frac{n}{2} \rfloor + 2$ reduced systems of size $\lfloor \frac{n}{2} \rfloor + 1$. Clearly, all coefficients appearing in the smaller subsystems also appear in the larger subsystem.

To obtain the bound, we require the coefficients corresponding to weight $\lfloor \frac{n}{2} \rfloor + 2$ alone to be non-negative,

$$\begin{aligned} \sum_{\substack{\mathrm{supp}(\alpha)\in V \\ \mathrm{wt}(\alpha)=\alpha+2}} r_\alpha^2 = & \sum_{\substack{\mathrm{supp}(\alpha)\in V \\ \mathrm{wt}(\alpha)\leq\lfloor \frac{n}{2} \rfloor+2}} r_\alpha^2 - (\lfloor \frac{n}{2} \rfloor + 2) \sum_{\substack{\mathrm{supp}(\alpha)\in V \\ \mathrm{wt}(\alpha)=\lfloor \frac{n}{2} \rfloor+1}} r_\alpha^2 \\ & \geq \quad 0\,. \end{aligned} \tag{3.16}$$

This leads to the conditions

$$\begin{aligned} (D^4-1) - (\lfloor \frac{n}{2} \rfloor + 2)(D^2-1) \geq 0 \qquad & n \text{ even}, \\ (D^3-1) - (\lfloor \frac{n}{2} \rfloor + 2)(D-1) \geq 0 \qquad & n \text{ odd}, \end{aligned} \tag{3.17}$$

which can be recast to the bounds of Refs. [44, 118],

$$n \leq \begin{cases} 2(D^2-1) & n \text{ even}, \\ 2D(D+1)-1 & n \text{ odd}. \end{cases} \tag{3.18}$$

This ends the proof. □

3.4 Nonexistence of the seven qubit AME state

With these building blocks in place, we are in the position to solve the last open qubit case — the existence of a seven qubit AME state. In the following, we will combine the projector property of a five qubit reduced state $\varrho_{(5)}$ with the eigenvector relations for $P_4^{(1\cdots5)}$ and $P_5^{(1\cdots5)}$ to obtain a contradiction from the parity rule stated in Lemma 1.

Observation 22. *Consider a pure state of seven qubits. Then not all of its three-body reduced density matrices can be maximally mixed.*

Proof. Assume we have a pure seven-qubit state $\varrho = |\phi\rangle\langle\phi|$, whose three-body marginals are all maximally mixed. Then, its five-party reduced density matrix on systems $\{1, \cdots, 5\}$ is proportional to a projector,

$$\varrho_{(5)}^2 = \frac{1}{4}\varrho_{(5)}\,. \tag{3.19}$$

Note that while the proof requires the projector property only to hold on the first five qubits, Eq. (3.19) actually holds for all possible five-qubit reductions. Regarding

the eigenvector relations, a Schmidt decomposition of the pure state $|\phi\rangle$ across the bipartitions $\{1,2,3,4\,|\,5,6,7\}$ and $\{1,2,3,4,5\,|\,6,7\}$ yields

$$\varrho_{(4)} \otimes \mathbb{1}^{\otimes 3} \, |\phi\rangle = \frac{1}{8} \, |\phi\rangle \ , \tag{3.20}$$

$$\varrho_{(5)} \otimes \mathbb{1}^{\otimes 2} \, |\phi\rangle = \frac{1}{4} \, |\phi\rangle \ . \tag{3.21}$$

Again, analogous equations hold for any possible four- or five-qubit reductions, including for the five different four-party reduced states in $\{1,2,3,4,5\}$.

We will use above three equations to obtain a contradiction: Let us expand $\varrho_{(4)}$ and $\varrho_{(5)}$ in the Bloch basis

$$\varrho_{(4)} = \frac{1}{2^4}(\mathbb{1} + P_4) \, , \tag{3.22}$$

$$\varrho_{(5)} = \frac{1}{2^5}(\mathbb{1} + \sum_{j=1}^{5} P_4^{[j]} \otimes \mathbb{1}^{(j)} + P_5) \, . \tag{3.23}$$

There are five different terms $P_4^{[j]} \otimes \mathbb{1}^{(j)}$, with $[j]$ indexing the five different supports of weight four terms within a five body reduced state, each having an identity on different positions. Inserting Eqs. (3.22, 3.23) into Eqs. (3.20, 3.21) results in the eigenvector relations

$$\begin{aligned} P_4^{[j]} \otimes \mathbb{1}^{\otimes 3} \, |\phi\rangle &= 1 \, |\phi\rangle \ , \\ P_5 \otimes \mathbb{1}^{\otimes 2} \, |\phi\rangle &= 2 \, |\phi\rangle \ . \end{aligned} \tag{3.24}$$

We similarly insert Eq. (3.23) in Eq. (3.19) to obtain

$$\begin{aligned} &\big(\mathbb{1} + \sum_{j=1}^{5} P_4^{[j]} \otimes \mathbb{1}^{(j)} + P_5\big)\big(\mathbb{1} + \sum_{j=1}^{5} P_4^{[j]} \otimes \mathbb{1}^{(j)} + P_5\big) \\ &= 8\big(\mathbb{1} + \sum_{j=1}^{5} P_4^{[j]} \otimes \mathbb{1}^{(j)} + P_5\big) \, . \end{aligned} \tag{3.25}$$

The key observation is now the parity rule stated in Lemma 1: Only certain products occurring on the left-hand side of Eq. (3.25) can contribute to P_5 on the right-hand side. Indeed, P_5^2 on the left-hand side cannot contribute to P_5 on the right-hand side. Similarly, $(\sum_{j=1}^{5} P_4^{[j]} \otimes \mathbb{1}^{(j)})^2$ on the left-hand side cannot contribute to P_5 on the right-hand side. Thus we can collect terms of weight five on both sides of the equation,

$$\{P_5, \sum_{j=1}^{5} P_4^{[j]} \otimes \mathbb{1}^{(j)}\} = 6P_5 \, . \tag{3.26}$$

Tensoring with the identity and multiplying by $|\phi\rangle$ from the right leads to

$$\{P_5, \sum_{j=1}^{5} P_4^{[j]} \otimes \mathbb{1}^{(j)}\} \otimes \mathbb{1}^{\otimes 2} \, |\phi\rangle = 6(P_5 \otimes \mathbb{1}^{\otimes 2}) \, |\phi\rangle \ . \tag{3.27}$$

However, using the eigenvector relations Eqs. (3.20, 3.21), one arrives at a contradiction

$$(2 \cdot 5 \cdot 1 + 5 \cdot 1 \cdot 2) \; |\phi\rangle = 6 \cdot 2 \; |\phi\rangle \; . \tag{3.28}$$

This ends the proof. □

3.5 Upper bound for the number of maximally mixed reductions

Note that in the derivation above not all constraints imposed by the reduced states have been taken into account. In fact, we only needed a single five-qubit reduced state (say, for definiteness, on the qubits $\{1, 2, 3, 4, 5\}$) fulfilling the Eqs. (3.19, 3.21), whose three-body reduced density matrices are all maximally mixed [this was needed for Eq. (3.23)]. In addition, the five four-qubit reduced density matrices corresponding to the possible subsets of $\{1, 2, 3, 4, 5\}$ have to obey Eq. (3.20).

Thus one can try to answer a relaxation of the original question: Given a seven-qubit state whose two-party reduced states are all maximally mixed, how many of its three-party reduced states can then be maximally mixed?

Observation 23. *Let $|\phi\rangle$ be a pure state of seven qubits, where all two-body reduced density matrices are maximally mixed. Then, maximally 32 of the 35 three-body density matrices can be maximally mixed. There exist seven-qubit states for which this bound is reached.*

Proof. Consider a pure seven-qubit state where all two-body marginals are maximally mixed. This implies that any of the $\binom{7}{5} = 21$ possible $\varrho_{(5)}$ obeys Eqs. (3.19, 3.21). There are $\binom{7}{3} = 35$ possible $\varrho_{(3)}$ and corresponding $\varrho_{(4)}$. If a single three-qubit reduced state $\varrho_{(3)}$ (say, $\{1, 2, 3\}$ for definiteness) is not maximally mixed, then nine of the $\varrho_{(5)}$ cannot be used for the proof anymore: First, for six five-qubit subsets (namely, $\{1, 2, 3, 4, 5\}, \ldots, \{1, 2, 3, 6, 7\}$) not all three-qubit density matrices are maximally mixed, implying that Eq. (3.23) is not valid. Furthermore, for three five-qubit subsets (namely, $\{1, 4, 5, 6, 7\}$, $\{2, 4, 5, 6, 7\}$, and $\{3, 4, 5, 6, 7\}$) not all reduced four-qubit subsets obey Eq. (3.20). It follows that if *two* three-qubit reduced states are not maximally mixed then at least $21 - 2 \cdot 9 = 3$ five-qubit sets still obey the conditions required for the proof. This ends the proof. □

We note that the existence of states where 32 of the three-body density matrices are maximally mixed was shown before: Refs. [98, 203] presented such states, which are, up to local unitary transformation, a graph state occurring in Refs. [47, 55]. As a graph state, the state can be described by the graphs in Fig. 3.1. Recall, that graph states are constructed as follows as follows: Each vertex in a graph corresponds to a qubit. One prepares all the qubits in the state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. Then, for any edge connecting the qubits j and k one applies a two-qubit phase gate

$$C_{jk} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \tag{3.29}$$

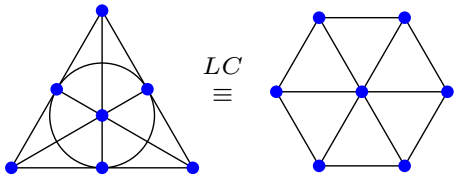


Figure 3.1: The graph of the Fano (or seven-point) plane on the left, which can be transformed by local complementation (corresponding to local Clifford gates) to the wheel graph displayed on the right. The Fano plane plays a role in classical error correction, describing both a balanced block design as well as an error-correcting code [205]. The corresponding graph state saturates the bound of Observation 23, having 32 out of 35 three-body marginals maximally mixed. The states are locally equivalent to the graph state depicted in Figs. 1 in [55], to No. 44 in Table V from Ref. [47], and to the states of Eq. (11) in Ref. [98] and of Eq. (26) in Ref. [203].

to the initial state. The fact that the marginals of this state have the right properties can also directly be checked in the stabilizer formalism, as explained in Ref. [47]. Finally, we add that there exists an AME state for seven *three*-dimensional systems, which is the graph state depicted in Fig. 1.2.1 [48].

3.6 AME states of n qubits

The method presented for seven qubits can also be applied to the general n-qubit case. There, it can *exclude* that an AME state for a given number of qubits exists. It turns out that the qubit numbers n for which no contradiction is found ($n = 2, 3, 5, 6$) are exactly the ones for which AME states are known [91]. Their graph state representations are shown in Fig. 1.2.3.

Observation 24. *Qubit AME states can only exist for $n = 2, 3, 5$ and 6 parties.*

Proof. The general case of determining which n-qubit AME states can possibly exist follows the method which was used in the case of seven qubits: We combine the projector property of the reduced state of the first $\lfloor \frac{n}{2} \rfloor + 2$ parties with the eigenvector relations for the terms $P_{\lfloor \frac{n}{2} \rfloor + 1}$ and $P_{\lfloor \frac{n}{2} \rfloor + 2}$ appearing in its expansion. Collecting terms with either even or odd weight, depending on the case, and applying the parity rule will lead to contradictions except in the cases of $n = 2, 3, 5, 6$ qubits. In the following, we will distinguish four cases, depending on n and $\lfloor \frac{n}{2} \rfloor$ being even or odd.

Case 1 (n even, $\lfloor \frac{n}{2} \rfloor$ even): For n even, one obtains the two eigenvector relations

$$\begin{aligned} P_{\lfloor \frac{n}{2} \rfloor + 1} \otimes \mathbb{1}^{\otimes (\lfloor \frac{n}{2} \rfloor - 1)} \, |\phi\rangle &= 3 \, |\phi\rangle \, , \\ P_{\lfloor \frac{n}{2} \rfloor + 2} \otimes \mathbb{1}^{\otimes (\lfloor \frac{n}{2} \rfloor - 2)} \, |\phi\rangle &= (9 - 3\lfloor \frac{n}{2} \rfloor) \, |\phi\rangle \, . \end{aligned} \tag{3.30}$$

Applying the parity rule, we collect terms of odd weight in $\varrho^2_{(\lfloor \frac{n}{2} \rfloor +2)}$,

$$\{ \sum_{j=1}^{\lfloor \frac{n}{2} \rfloor +2} P^{[j]}_{\lfloor \frac{n}{2} \rfloor +1} \otimes \mathbb{1}^{(j)}, P_{\lfloor \frac{n}{2} \rfloor +2} \} \ |\phi\rangle = 14 \sum_{j=1}^{\lfloor \frac{n}{2} \rfloor +2} P^{[j]}_{\lfloor \frac{n}{2} \rfloor +1} \otimes \mathbb{1}^{(j)} \ |\phi\rangle \ . \tag{3.31}$$

This results in a contradiction, as

$$9 - 3\lfloor \frac{n}{2} \rfloor \neq 7 \, . \tag{3.32}$$

Thus qubit AME states do not exist when n is a multiple of 4.

Case 2 (n even, $\lfloor \frac{n}{2} \rfloor$ odd): The eigenvector relations are as appearing in Case 1, Eq. (3.30). We collect terms of odd weight in $\varrho^2_{(\lfloor \frac{n}{2} \rfloor +2)}$,

$$\{ \sum_{j=1}^{\lfloor \frac{n}{2} \rfloor +2} P^{[j]}_{\lfloor \frac{n}{2} \rfloor +1} \otimes \mathbb{1}^{(j)}, P_{\lfloor \frac{n}{2} \rfloor +2} \} \, |\phi\rangle = 14 P_{\lfloor \frac{n}{2} \rfloor +2} \tag{3.33}$$

If $P_{\lfloor \frac{n}{2} \rfloor +2} \, |\phi\rangle \neq 0$, we obtain a contradiction because

$$(\lfloor \frac{n}{2} \rfloor + 2) \cdot 3 \neq 7 \, . \tag{3.34}$$

Thus $\mathbb{1}^{\otimes (\lfloor \frac{n}{2} \rfloor -2)} \otimes P_{\lfloor \frac{n}{2} \rfloor +2} \, |\phi\rangle = 0$. But from the eigenvector relation in Eq. (3.30) this can only by possible if $n = 6$. Indeed, for this case an AME graph state is known, depicted in Fig. 1.2.3. Note that the Bell state consisting of only two qubits is too small to be excluded by this method.

Case 3 (n odd, $\lfloor \frac{n}{2} \rfloor$ even): For n odd, one obtains the two eigenvector relations

$$\begin{aligned} P_{\lfloor \frac{n}{2} \rfloor +1} \otimes \mathbb{1}^{\otimes (\lfloor \frac{n}{2} \rfloor -1)} \ |\phi\rangle &= \ |\phi\rangle \ , \\ P_{\lfloor \frac{n}{2} \rfloor +2} \otimes \mathbb{1}^{\otimes (\lfloor \frac{n}{2} \rfloor -2)} \ |\phi\rangle &= (5 - \lfloor \frac{n}{2} \rfloor) \ |\phi\rangle \ . \end{aligned} \tag{3.35}$$

We collect terms of odd weight,

$$\{ \sum_{j=1}^{\lfloor \frac{n}{2} \rfloor +2} P^{[j]}_{\lfloor \frac{n}{2} \rfloor +1} \otimes \mathbb{1}^{(j)}, P_{\lfloor \frac{n}{2} \rfloor +2} \} \, |\phi\rangle = 6 \sum_{j=1}^{\lfloor \frac{n}{2} \rfloor +2} P^{[j]}_{\lfloor \frac{n}{2} \rfloor +1} \otimes \mathbb{1}^{(j)} \, |\phi\rangle \ . \tag{3.36}$$

Thus one requires

$$(5 - \lfloor \frac{n}{2} \rfloor) \, |\phi\rangle = 3 \, |\phi\rangle \ , \tag{3.37}$$

whose only solution is $n = 5$. The corresponding AME state is the five-qubit ring-cluster state, depicted in Fig. 1.2.3.

Case 4 (n odd, $\lfloor \frac{n}{2} \rfloor$ odd): This final case is slightly more involved, but the method ultimately succeeds on a larger reduced state of size $\lfloor \frac{n}{2} \rfloor + 4$. The eigenvector relations are as appearing in Case 3, Eq. (3.35). We collect terms of odd weight,

$$\{ \sum_{j=1}^{\lfloor \frac{n}{2} \rfloor + 2} P^j_{\lfloor \frac{n}{2} \rfloor + 1} \otimes \mathbb{1}^{(j)}, P_{\lfloor \frac{n}{2} \rfloor + 2} \} \, |\phi\rangle = 6 P_{\lfloor \frac{n}{2} \rfloor + 2} \, |\phi\rangle \, . \tag{3.38}$$

If $P_{\lfloor \frac{n}{2} \rfloor + 2} |\phi\rangle \neq 0$, it follows that

$$\lfloor \frac{n}{2} \rfloor + 2 = 3 \, . \tag{3.39}$$

The only solution is $n = 3$, corresponding to the GHZ state. If however $P_{\lfloor \frac{n}{2} \rfloor + 2} |\phi\rangle = 0$, that is $n = 11$, we have to make use of further eigenvector relations.

$$\begin{aligned} P_6 \otimes \mathbb{1}^{\otimes 5} \, |\phi\rangle &= 1 \, |\phi\rangle \, , \\ P_7 \otimes \mathbb{1}^{\otimes 4} \, |\phi\rangle &= 0 \, |\phi\rangle \, , \\ P_8 \otimes \mathbb{1}^{\otimes 3} \, |\phi\rangle &= 3 \, |\phi\rangle \, , \\ P_9 \otimes \mathbb{1}^{\otimes 2} \, |\phi\rangle &= 16 \, |\phi\rangle \, . \end{aligned} \tag{3.40}$$

We require $\varrho^2_{(9)} = 2^{-2} \varrho_{(9)}$ and collect terms of odd weight

$$(\{ \sum_{j=1}^{\binom{9}{6}} P_6^{[j]} \otimes \mathbb{1}^{\otimes 3}, P_9 \} + \{ \sum_{j=1}^{9} P_8^{[j]} \otimes \mathbb{1}, P_9 \}) \, |\phi\rangle = 126 P_9 \, |\phi\rangle \, . \tag{3.41}$$

This also leads to a contradiction in the case of $n = 11$,

$$\binom{9}{6} + 9 \cdot 3 \neq 63 \, . \tag{3.42}$$

Therefore, no AME qubit state with both n and $\lfloor \frac{n}{2} \rfloor$ being odd exists. This ends the proof. □

To summarize: the only qubit AME states which are not excluded to exist by this method are the cases of two, three, five, and six parties, all of which are known. Their graph state representations are shown in Fig. 1.2.3.

3.7 Further results

3.7.1 An iterative semidefinite program to find AME states

To find AME states, or more generally, states with maximally mixed k-RDMs, the following algorithm can be used. It is a iterative semidefinite program (c.f. Sect. 1.2.5) with a so-called hard-threshold, as after each iteration step, the state is projected onto the vector corresponding to its largest eigenvalue.

1) Choose a random initial state $|\psi_0\rangle$.

2) Solve the following semidefinite program,

$$\begin{aligned} \underset{\varrho}{\text{maximize}} \quad & \mathrm{Tr}(|\psi_i\rangle\langle\psi_i|\varrho) \\ \text{subject to} \quad & \mathrm{Tr}[\varrho\sigma_{\boldsymbol{\alpha}}] = 0 \quad \forall \sigma_{\boldsymbol{\alpha}} : \mathrm{wt}(\sigma_{\boldsymbol{\alpha}}) \leq k\,, \sigma_{\boldsymbol{\alpha}} \neq \mathbb{1} \\ & \mathrm{Tr}[\varrho] = 1, \quad \varrho = \varrho^\dagger, \quad \varrho \geq 0\,. \end{aligned}$$

3) $|\psi_{i+1}\rangle =$ eigenvector corresponding to maximal eigenvalue of ϱ.

4) Repeat steps 2) & 3) until the desired numerical accuracy is reached.

While the convergence of this algorithm to find AME states is not yet proven, it shows very good results: In the case of five and six qubits, this algorithm typically converges within $5 - 10$ iterations. However, as the complete density matrix has to be represented numerically, it is not yet feasible to search for an four-party AME state with $D = 6$ using a desktop computer only.

3.8 Conclusion

In summary, with my co-authors I have developed a method based on the Bloch representation for characterizing AME states. This allowed to rederive most of the known results for qubits in a very simple manner, but more importantly, it solved the long-standing question whether AME states of seven qubits exist or not. A best approximation to such a state could be determined, which also turned out to be a graph state.

Our treatment highlighted the usefulness of the Bloch representation to not only represent mixed, but also pure states: While the positivity of operators is not obvious from their Bloch decomposition, their marginals can be simply read off. Such an approach can be seen as being complementary to that of representing pure states by normalized vectors. Given a ket, the state is pure and positive by construction, but its marginals are not immediately apparent. Our methodology resonates with other recent developments in this well-established subject [46, 90, 159, 206–208], and it is likely that many other open problems can successfully be approached in this way. Additionally, I developed an iterative semi-definite program to search for highly entangled states.

For future work, it is of interest to apply similar approaches to the question whether or not n-qubit states exist, whose k-body reduced density are all maximally mixed for some $k < \lfloor n/2 \rfloor$. These highly entangled states are central for quantum error correction and secret sharing schemes [102], and many efforts have been devoted to finding them in the last years [209, 210]. It is likely that our methods can contribute also to this problem.

Chapter 4

Ulam's reconstruction problems for quantum states

Provided by a complete set of putative k-body reductions of a quantum state, can one determine the existence of a joint state? Here, we derive necessary criteria for a type of joint state known as graph state to exist. Crucially, these criteria do not require the knowledge of the labeling of the subsystems, in analogy to the Ulam reconstruction problem in graph theory. Interestingly, the non-compatibility of reductions can in some cases already be inferred from the set of marginals having the size of just more than half of the parties. In this Chapter, we consider quantum marginals which are unlabeled, that is, their associated parties are unknown to us, and ask for the existence and uniqueness of a joint state. Such reconstructing amounts to a kind of quantum jigsaw puzzle: One is given overlapping (quantum) parts and is tasked with determining whether or not these can be assembled to one or even many different joint states. This Chapter is based on Project [E].

4.1 Motivation

The relation between the whole and its parts lies at the heart of quantum entanglement. Namely, if a many-party pure quantum state is not the tensor product of its individual parts, the state is said to be entangled. A particularly intriguing consequence is, that given a set of quantum marginals, it is not clear from the outset if and how they can be assembled into a joint pure state. This is the so-called *quantum marginal problem* (QMP) (c.f. Sect. 1.2.6).

These questions are in spirit similar to the Ulam reconstruction problem in graph theory [211, 212]: Given a complete set of vertex-deleted subgraphs, is the original graph the only compatible joint graph they could have been obtained from? Despite of ample research that focused on this question during the last decades, this is still one of the outstanding unresolved problems in graph theory [213–218].

In contrast to previous work on the QMP, we consider here only *unlabeled* marginals, that is, marginals whose corresponding subsystems are unknown to us. Thus, one is free to arrange them as necessary in order to obtain a joint state. Should all reductions to a singly party be different (e.g. when considering reductions of random states), such labels can naturally be restored by comparing the one-body

reductions of the marginals given. However, we are here considering a special type of quantum states that turned out to be immensely useful for certain tasks in quantum information such as quantum error correction [54–56] and measurement-based quantum computation [47, 57, 58], but which can still be described by simple means. The lower-body reductions of these states are often maximally mixed, so above strategy cannot be applied.

4.2 Realizability and uniqueness in graphs

Consider a simple graph $G(V, E)$ on n vertices. Denote by $N(i)$ the neighborhood of vertex j, that is, the vertices connected to vertex i by an edge. By removing a single vertex $j \in V$ and removing all edges e connected to j, one obtains the vertex-deleted subgraph on $(n-1)$ vertices

$$G_j = G\big(V\backslash\{j\}, E\backslash\{e|j \in e\}\big)\,. \tag{4.1}$$

By forming all vertex-deleted subgraphs G_j induced by G, the so-called cards, we obtain its unordered deck, the multi-set

$$D(G) = \{G_1, \ldots, G_n\}\,. \tag{4.2}$$

The *Ulam graph reconstruction problem* states: Given a deck $D(G)$, is there, up to graph isomorphisms, a unique graph corresponding to it? The Ulam graph reconstruction conjecture states that this must indeed be the case for all graphs.

Conjecture 1 (Kelly, Ulam [211, 212])**.** *If $D(G) = D(H)$, then G is isomorph to H.*

However, a deck does not necessarily need to originate from a truly existing graph: Suppose we are given a putative deck containing n cards of size $(n-1)$ each, whose origin is unknown to us. A naturally arising question is: Can this deck indeed be obtained from a graph containing n vertices? This is also called the *legitimate deck problem*, and is a type of realizability problem [213].

Let us state a legitimacy condition originating from Kelly's Lemma [216]:

Theorem 25 (Kelly conditions [216])**.** *Let $D = \{G_i\}$ be a complete deck. Then for any graph F having $\nu(F) < n$ vertices,*

$$\frac{\sum_{i=1}^{n} s'(F, G_i)}{n - \nu(F)} \tag{4.3}$$

must be an integer, where $s'(F, G_i)$ is the number of induced subgraphs of G_i that are isomorphic to F.

Interestingly, for most decks, not all but already a specific set of three cards are sufficient to uniquely reconstruct the original graph [219]. In the following, we aim to treat the Ulam graph reconstruction and the legitimate deck problem for a special type of quantum states called *graph states*. That is, given a collection of graph states marginals, we ask for the existence of a joint state, with which these marginals are compatible. Conversely, if a joint state exist, we are interested in its uniqueness. This motivates the following definition as the analogue of a graph deck for quantum states.

Definition 12. *A quantum k-deck is a collection of quantum marginals, also called quantum cards, having size k each. In particular, the marginals are not associated to any particular parties, thus the cards are unlabeled. The deck is called complete, if it contains $\binom{n}{k}$ cards, and legitimate, if the deck originates from a common joint state.*

Thus given a quantum state $|\psi\rangle$, its corresponding k-deck is given by the collection of all its marginals of size k,

$$D(|\psi\rangle) = \{\varrho_S = \mathrm{Tr}_{S^c}(\varrho) \mid |S| = k\}\,. \tag{4.4}$$

4.3 Graph states

Let us shortly recall how qubit graph states are defined (c.f. Sect. 1.2.1) [47]: Given a graph $G = (V, E)$ of n vertices, its corresponding graph state $|G\rangle$ is defined as the common and unique $(+1)$-eigenstate of the n commuting operators $\{g_i\}$,

$$g_i = X_i \bigotimes_{j \in N(i)} Z_j\,. \tag{4.5}$$

The set $\{g_i\}$ is called the *generator*. The *stabilizer* S is the Abelian group obtained by the multiplication of generator elements,

$$S = \left\{ \prod g_1^{i_1} g_2^{i_2} \dots g_n^{i_n} \;\middle|\; i_1, \dots, i_n \in \{1, \dots, D-1\} \right\}. \tag{4.6}$$

Each of its D^n elements stabilize the state, $g_i\,|G\rangle = |G\rangle$ for all g_i. Then the graph state can be written as

$$|G\rangle\langle G| = \frac{1}{2^n} \sum_{s_a \in S} s_a\,. \tag{4.7}$$

On the other hand, it can be shown that the graph state can also be written as

$$|G\rangle = \prod_{e \in E} C_e\,|+\rangle_V\ , \tag{4.8}$$

where $|+\rangle_V = \bigotimes_{j \in V} (|0\rangle_j + |1\rangle_j)/\sqrt{2}$, and the controlled-$Z$ gate between parties i and j of edge $e = (i, j)$ reads $C_e = \mathrm{diag}(1, 1, 1 - 1)$.

Let us state a first Proposition concerning the reductions of graph states onto $(n-1)$ parties.

Proposition 10 ([220]). *Considering the quantum $(n-1)$-deck of a graph state $|G\rangle$, each of its cards of can be represented by two graphs: a vertex-deleted and a vertex-shrunken graph, each having $(n-1)$ vertices.*

Proof. In Eq. (4.8), let us single out vertex j to be traced over.

$$\begin{aligned} |G\rangle &= \prod_{e \in E} C_e\,|+\rangle_V \\ &= \left(|0\rangle_j + \prod_{e \in E\,|\,j \in e} C_{e \setminus \{j\}}\,|1\rangle_j \right) \otimes \prod_{e' \in E\,|\,j \notin e'} C_{e'}\,|+\rangle_{V \setminus \{j\}}\,. \end{aligned} \tag{4.9}$$

Note that above, if C_e is a controlled two-qubit Z-gate acting on parties i and j, then $C_{e\setminus\{j\}}$ is simply the local Z_i gate acting on party i alone. A partial trace over party j then yields

$$\begin{aligned}\mathrm{tr}_j[|G\rangle\langle G|] &= \langle 0_j|G\rangle\langle G|0_j\rangle + \langle 1_j|G\rangle\langle G|1_j\rangle \\ &= \frac{1}{2}\Big(\underbrace{\prod_{e'\in E\,|\,j\notin e'} C_{e'}|+\rangle\langle +|_{V\setminus\{j\}} \prod_{e'\in E\,|\,j\notin e'} C_{e'}}_{\text{delete}} \\ &+ \underbrace{\prod_{i\in N(j)} Z_i \prod_{e'\in E\,|\,j\notin e'} C_{e'}|+\rangle\langle +|_{V\setminus\{j\}} \prod_{e'\in e\,|\,j\notin e'} C_{e'} \prod_{i\in N(j)} Z_i}_{\text{shrink}} \Big)\,. \end{aligned} \tag{4.10}$$

The reduction of a graph state onto $(n-1)$ parties is thus given by the equal mixture of two graph states: A vertex-deleted graph state $D_j\,|G\rangle$, whose graph is the vertex deleted subgraph of G, and a vertex-shrunken graph state $S_j\,|G\rangle$, whose graph is a vertex deleted subgraph with additional one-edges on $N(j)$ caused by shrinking all edges connected to vertex j. One obtains

$$D_j\,|G\rangle = \prod_{e'\in E\,|\,j\notin e'} C_{e'}\,|+\rangle_{V\setminus\{j\}}\,, \tag{4.11}$$

$$S_j\,|G\rangle = \prod_{i\in N(j)} Z_i \prod_{e'\in E\,|\,j\notin e'} C_{e'}\,|+\rangle_{V\setminus\{j\}}\,, \tag{4.12}$$

and we can write

$$\mathrm{Tr}_j(|G\rangle\langle G|) = \frac{1}{2}(S_j|G\rangle\langle G|S_j + D_j|G\rangle\langle G|D_j)\,. \tag{4.13}$$

This ends the proof. □

If the graph G is fully connected, then $D_j|G\rangle\langle G|S_j = 0$. This follows from the fact that all stabilizer elements corresponding to a fully connected graph must have a weight larger or equal than two. Thus, the one-body reductions are maximally mixed, and the complementary $(n-1)$ body reductions must be proportional to projectors of rank two. When tracing out more than one party, this procedure of substituting each graph by the mixture of its vertex-deleted and vertex-shrunken subgraphs is iteratively repeated. Thus reductions of graph states of size $n-k$ are represented by a collection of 2^k graphs.

Let us now consider a specific formulation of the Ulam graph problem in the quantum setting, where all $(n-1)$-body reductions of a graph state are given in the computational basis. What can one say about the joint state?

Proposition 11. *Given a legitimate $(n-1)$-deck of a graph state $|G\rangle$ in the computational basis, the joint state $|G\rangle$ can be reconstructed up to local Z_j gates from any single card.*

Proof. Let us expand the graph states $D_j\,|G\rangle$ and $S_j\,|G\rangle$ as appearing in (4.13) in the computational basis. Due to our ignorance about the joint state, denote them by $|\alpha\rangle$ and $|\beta\rangle$, where either one could be the vertex-deleted graph state, with the other one

being the vertex-shrunken graph state. From Eq. (4.8) it follows that graph states are real equally weighted states, thus it is possible to expand them as

$$|\alpha\rangle = \sqrt{\frac{1}{N}} \sum \alpha_i |i\rangle \ ,$$
$$|\beta\rangle = \sqrt{\frac{1}{N}} \sum \beta_i |i\rangle \ , \tag{4.14}$$

with $\alpha_i, \beta_i \in \{-1, 1\}$, and $\{|i\rangle\}$ is the computational basis for $V\backslash\{j\}$. We can therefore write the card $C^k = \mathrm{Tr}_k(|G\rangle\langle G|)$ as

$$C^k = \frac{1}{2N} \sum_{i,j=0}^{2^n} (\alpha_i \alpha_j + \beta_i \beta_j) |i\rangle\langle j| \ . \tag{4.15}$$

Because of $\alpha_i, \beta_i \in \{-1, 1\}$, $2NC^k_{ij}$ can only be 0 or ± 1. Because $|0 \ldots 0\rangle$ remains unaffected by any conditional phase gate C_e, we can choose $\alpha_1 = \beta_1 = 1$. Then $\alpha_j = \beta_j = \mathrm{sgn}(C^l_{1j})$ if $C^l_{1j} \neq 0$, and $\alpha_j = -\beta_j$ otherwise. Without loss of generality, set $\alpha_m = -\beta_m = 1$, for the first instance of m where $\varrho_{1m} = 0$. Then the remaining but yet undetermined coefficients α_j and β_j are given from the entries C^k_{1j} and C^k_{mj},

$$\alpha_1\alpha_j + \beta_1\beta_j = \alpha_j + \beta_j = 0 \, , \tag{4.16}$$
$$\alpha_m\alpha_j + \beta_m\beta_j = \alpha_j - \beta_j = 2\alpha_j \, . \tag{4.17}$$

This completely determines the remaining coefficients of $|\alpha\rangle$ and $|\beta\rangle$. Now the task is to reconstruct the graphs corresponding to $|\alpha\rangle$ and $|\beta\rangle$. This can be done by erasing all minus signs in the expansion in the computational basis [221]: first, minus signs in front of terms having a single excitation only, e.g. $|0 \ldots 010 \ldots \ldots 0\rangle$, are removed by local Z_j gates. Then, conditional phase gates are applied to erase minus signs in front of components having two excitations. By this procedure, one obtains the state $|+\rangle^{\otimes n}$ and all the gates necessary to obtain the original graph state, thus determining the graph.

The symmetric difference of the two graphs corresponding to $|\alpha\rangle$ and $|\beta\rangle$ yields all edges which were severed under the partial trace operation,

$$\underbrace{\prod_{j\in e} C_{e\in E\,|\,e\backslash\{j\}} \prod_{e'\in E\,|\,j\notin e'} C_{e'}}_{\text{shrink}} \underbrace{\prod_{e'\in E\,|\,j\notin e'} C_{e'}}_{\text{delete}} = \underbrace{\prod_{e\in E\,|\,j\in e} C_{e\backslash\{j\}}}_{\text{edges connected to } j} = \prod_{i\in N(j)} Z_j \, . \tag{4.18}$$

Then the original graph state can then only be one of the following

$$|G\rangle\langle G| = \prod_{e\in E\,|\,j\in e} C_e |\alpha\rangle \otimes |+\rangle_j \ , \text{ or}$$
$$|G\rangle\langle G| = \prod_{e\in E\,|\,j\in e} C_e |\beta\rangle \otimes |+\rangle_j \ . \tag{4.19}$$

This ends the proof. □

In order to determine whether or not, given a quantum k-deck, a joint graph state could possibly exist, we introduce the weight distribution of quantum states, a tool from the theory of quantum error-correcting codes (c.f. Sect. 5). A partial weight distribution can be obtained from a complete quantum k-deck already, and no knowledge of the labeling of the individual parties is needed, making this tool useful for legitimate deck type problems. With it, it is possible to detect illegitimate decks, that is, marginal sets that are incompatible with any joint pure state.

4.4 Weight distribution

The weight distribution of a quantum state ϱ is given by [118, 128] (c.f. Sect. 1.2.4)

$$A_j(\varrho) = \sum_{\substack{P\in\mathcal{P}\\ \mathrm{wt}(P)=j}} \mathrm{Tr}(P\varrho)\,\mathrm{Tr}(P^\dagger\varrho)\,, \tag{4.20}$$

where the sum is over all elements P of weight j in the n-qubit Pauli basis $\mathcal{P}^n$. Note that for higher dimensional quantum systems, any appropriate orthonormal tensor-product basis can be chosen instead of the Pauli basis, e.g. the Heisenberg-Weyl or Gell-Mann basis. For graph states, the weight distribution is particularly simple: because $\mathrm{Tr}[P|G\rangle\langle G|]$ can only be either 0 or ±1, the weight distribution of $|G\rangle$ is simply given by the number of its stabilizer elements having weight j,

$$A_j(|G\rangle) = |\{s_a \in S(G)|\,\mathrm{wt}(s_a) = j\}|\,. \tag{4.21}$$

Let us give an example.

Example 1. *The three-qubit graph state corresponding to the fully connected graph of three vertices has the generator* $G = \{XZZ, ZXZ, ZZX\}$ [1]*. Its stabilizer reads*

$$S = \{III, IYY, YIY, YYI, XZZ, ZXZ, ZZX, -XXX\}\,. \tag{4.22}$$

Accordingly, the weight distribution is $A = [A_0, A_1, A_2, A_3] = [1, 0, 3, 4]$*. By normalization,* $A_0 = \mathrm{Tr}(\varrho) = 1$ *must hold for all states. Because* ϱ *is pure,* $\mathrm{Tr}(\varrho^2) = 1$*, and* $\sum_{j=0}^n A_j(|\psi\rangle) = 2^n$*.*

As a warm-up, let us derive a result known from quantum error-correcting codes (c.f. Sect. 1.2.4) [44]:

Proposition 12. *Given a graph state, the sum* $A_\mathrm{e} = \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} A_{2j}$ *can only take two possible values,*

$$A_\mathrm{e} = \begin{cases} 2^{(n-1)} & \textit{(type I)}\,, \\ 2^n & \textit{(type II)}\,. \end{cases} \tag{4.23}$$

Proof. Note that the graph state $\varrho = |G\rangle\langle G|$ can be decomposed into

$$\begin{aligned} \varrho &= \frac{1}{2^n}\Big(\sum_{\substack{P\in\mathcal{P}\\ \mathrm{wt}(P)\text{ even}}} \mathrm{tr}[PM]P^\dagger + \sum_{\substack{P\in\mathcal{P}\\ \mathrm{wt}(P)\text{ odd}}} \mathrm{tr}[PM]P^\dagger\Big) \\ &= \frac{1}{2^n}(P_\mathrm{e} + P_\mathrm{o})\,, \end{aligned} \tag{4.24}$$

[1] This is a state LU-equivalent to the GHZ state.

where $P_{\rm e}$ and $P_{\rm o}$ are the sums of all stabilizer elements having even and odd weight respectively. Because of $s\varrho = \varrho$ for all $s \in S$, also $P_{\rm e}$ and $P_{\rm o}$ have ϱ as an eigenvector. We now apply this decomposition to $\varrho^2 = \varrho$, making use of the Lemma 1 from Chpt. 3: The term $\{P_{\rm e}, P_{\rm o}\}$ appearing in ϱ^2 can only contribute to terms of odd weight in ϱ, yielding $\{P_{\rm e}, P_{\rm o}\} = 2^n P_{\rm o}$. From this we obtain

$$\mathrm{Tr}(\{P_{\rm e}, P_{\rm o}\}\varrho) = \mathrm{tr}(2^n P_{\rm o}\varrho)\,. \tag{4.25}$$

Accordingly, $2A_{\rm e}A_{\rm o} = 2^n A_{\rm o}$, where $A_{\rm e}$ and $A_{\rm o}$ are the number even and odd weight terms in the stabilizer respectively. Consider first $A_{\rm o} \neq 0$. Then $A_{\rm e} = 2^{(n-1)}$. Conversely, if $A_{\rm o} = 0$, then $A_{\rm e} = 2^n$, because ϱ is pure and must satisfy $\sum A_j = A_{\rm e} + A_{\rm o} = 2^n$. This ends the proof. □

The same argument can be done for reductions of graph states, that happen to be proportional to projectors of rank 2^q. There, either $A_{\rm e} = 2^{n-q-1}$ or $A_{\rm e} = 2^{n-q}$ holds. These two cases, that is, graph states of type I and II, are also known from the theory of *classical* self-dual additive codes over $GF(4)$ (c.f. Sect. 1.2.4) [44, 108]. If only stabilizer elements of even weight are present, the code is said to be of type II, while codes having both even and odd correlations in equal amount are of type I. It can be shown that all type II codes must have even length, and conversely, self-dual additive codes of odd length n are always of type I. This is also a direct consequence of monogamy relations derived in Ref. [159]: these can be restated in terms of the shadow coefficient S_0 from Chpt. 5, which is known to vanish for an odd number of parties, implying $A_{\rm e} = A_{\rm o} = 2^{n-1}$. Examples of type II codes are the two qubit Bell state and the absolutely maximally entangled state of six qubits of Fig.1.2.3, having only even-body correlations present. Also graph states whose every vertex is connected to an odd number of other vertices, such as e.g. GHZ states of an even number of qubits, are of type II [2].

This result can be used to show that a particular state is LU-inequivalent to any graph state. Let us consider the state depicted in Fig. 4.4. It is a hypergraph state [221], which is obtained by applying the additional gate $C_{138} = \mathrm{diag}(1,1,1,1,1,1,1,-1)$ between particles 1, 3, and 8 to the graph state of a cube, $|H\rangle = C_{138}\,|G_{\rm cube}\rangle$. Its weight distribution reads

$$A = [1,0,0,0,30,48,96,48,33]\,, \tag{4.26}$$

with $A_{\rm e} = \sum_{j\ \mathrm{even}, j\neq 0} = 160$. This is incompatible with being a graph state of type I or type II, these having $A_{\rm e} = 128$ and $A_{\rm e} = 256$ respectively.

One could ask, whether or not the presence of entanglement can be detected from the weight distribution of pure states. This is indeed the case.

Proposition 13. *Let $|\psi\rangle$ be a pure state on n qubits. If $A_j(|\psi\rangle) > \binom{n}{j}$, then $|\psi\rangle$ must be entangled.*

Proof. Take a product state on $m-1$ qubits, having weights denoted by $A_j^{(m-1)}$, and tensor it by a pure state on the last qubit. Then the weight $A_j^{(m)}$ of the resulting state

[2] See Thm. 15 in Ref. [199].

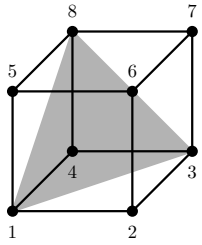


Figure 4.1: A hypergraph state that is LU-inequivalent to graph states. All of its three-body marginals are maximally mixed.

on m qubits is

$$\begin{aligned} A_j^{(m)} &= A_j^{(m-1)} A_0^{(1)} + A_{j-1}^{(m-1)} A_1^{(1)} \\ &= A_j^{(m-1)} + A_{j-1}^{(m-1)} , \end{aligned} \tag{4.27}$$

because of $A_0 = A_1 = 1$ for a pure one-qubit state. But this is exactly the recurrence relation fulfilled by the binomial coefficients, namely

$$\binom{m}{j} = \binom{m-1}{j} + \binom{m-1}{j-1} , \tag{4.28}$$

together with the initial condition $A_j^{(1)} = \binom{1}{j} = 1$. Thus a pure product state on n qubits fulfills $A_j = \binom{n}{j}$. This proofs the claim. □

If $|\psi\rangle$ is entangled across a partition of one party versus the rest, then above relation takes the form of a strict inequality

$$A_j^{(n)} > A_j^{(n-1)} + A_{j-1}^{(n-1)} . \tag{4.29}$$

Considering entanglement across a partition of $m \leq \lfloor \frac{n}{2} \rfloor$ versus $(n-m)$ parties, one obtains in a similar fashion the inequality

$$A_j^{(n)} > A_j^{(n-m)} A_0^{(m)} + A_{j-1}^{(n-m)} A_1^{(m)} + \cdots + A_{j-m}^{(n-m)} A_m^{(m)} . \tag{4.30}$$

4.5 Constraints on the weight distribution

In the following, we derive further relations on the weight distribution of pure states. These are obtained from the Schmidt decomposition along bipartitions having fixes sizes and from monogamy relations. First, let us define the reduced weight distributions.

Definition 13. *Given a quantum state ϱ on n parties and its weight distribution $A_j(\varrho)$, its associated reduced weight distributions $A_j^m(\varrho)$ are defined as*

$$A_j^m(\varrho) = \binom{n}{m}\binom{m}{j} \Big/ \binom{n}{j} A_j(\varrho) = \binom{n-j}{n-m} A_j(\varrho) . \tag{4.31}$$

Proposition 14. *The reduced weight distributions A_j^a of any pure state $|\psi\rangle$ of n qubits satisfy*

$$2^{-a}\sum_{j=0}^{a} A_j^a(|\psi\rangle) = 2^{-(n-a)}\sum_{j=0}^{n-a} A_j^{n-a}(|\psi\rangle)\,. \tag{4.32}$$

Proof. In the following, let us write A_j for $A_j(|\psi\rangle)$. From the Schmidt decomposition of pure states, it follows that the purities of reductions on complementary subsystems must be equal,

$$\mathrm{tr}(\varrho_S^2) = \mathrm{tr}(\varrho_{S^c}^2)\,. \tag{4.33}$$

Define

$$A_j^S = \sum_{\substack{P\in P\\ \mathrm{supp}(P)\subseteq S\\ \mathrm{wt}(S)=j}} \mathrm{Tr}(P\varrho)\,\mathrm{Tr}(P^\dagger\varrho)\,. \tag{4.34}$$

Summing over all bipartitions S, S^c having fixed size $a \leq \lfloor \frac{n}{2} \rfloor$ and $(n-a)$, one then obtains

$$2^{-a}\sum_{|S|=a}\sum_{j=0}^{a} A_j^S = 2^{-(n-a)}\sum_{|S^c|=(n-a)}\sum_{j=0}^{n-a} A_j^{S^c}\,. \tag{4.35}$$

In the case of graph states, A_j^S is just the number of stabilizer elements of weight j having support on S. Note that in Eq. (4.35), the dimensional prefactor results from the difference in normalization of ϱ_S and ϱ_{S^c}. By summing over all subsystem pairs of fixed size, elements of weight j are overcounted by factors of $\binom{n}{a}\binom{a}{j}\binom{n}{j}^{-1} = \binom{n-j}{n-a}$ and $\binom{n-a-j}{n-2a}$ respectively. We arrive at

$$2^{-a}\sum_{j=0}^{a}\binom{n-j}{n-a}A_j = 2^{-(n-a)}\sum_{j=0}^{n-a}\binom{n-a-j}{n-2a}A_j\,. \tag{4.36}$$

In terms of the reduced weight distribution, this reads

$$2^{-a}\sum_{j=0}^{a} A_j^a = 2^{-(n-a)}\sum_{j=0}^{n-a} A_j^{n-a}\,. \tag{4.37}$$

This ends the proof. □

These are $\lfloor (n-1)/2 \rfloor$ independent relations linear equations the weight distributions of pure states have to satisfy. In fact, these relations can seen as a special case of the so-called *quantum MacWilliams* identity for quantum codes, applied to pure quantum states [3].

Let us obtain further constraints on the reduced weight distributions, obtained from the universal state inversion [33–37].

Proposition 15. *The weight distribution of any pure state of n qubits fulfills for all $1 \leq m \leq n$*

$$\sum_{j=0}^{m}(-1)^j A_j^m(|\psi\rangle) \geq 0\,. \tag{4.38}$$

[3] C.f. Eq. (1.177), Ref. [118], and the subsequent Chapter.

Proof. Recall that the universal state inversion for qubits can be written as the spin-flipped state [c.f. Eq. (1.73) and Sects. 2.6.4, 5.11.1]

$$\mathcal{I}[\varrho] = \tilde{\varrho} = Y^{\otimes n} \varrho^T Y^{\otimes n} \,. \tag{4.39}$$

This maps $I \longrightarrow I\,, Y \longrightarrow -Y\,, X \longrightarrow -X$, and $Z \longrightarrow -Z$ in the Bloch decomposition of the state. Because $\tilde{\varrho}$ is positive, it holds that $\mathrm{tr}(\varrho\tilde{\varrho}) \geq 0$. This leads to

$$\begin{aligned}
\mathrm{Tr}(\varrho\tilde{\varrho}) &= \frac{1}{2^{2n}} \mathrm{Tr}\Big[\Big(\sum_{j=0}^{n}(-1)^j \sum_{\substack{P\in\mathcal{P}\\ \mathrm{wt}(P)=j}} \mathrm{Tr}(P\varrho)P^\dagger\Big)\Big(\sum_{j'=0}^{n}\sum_{\substack{P'\in\mathcal{P}\\ \mathrm{wt}(P)=j'}} \mathrm{Tr}(P'^\dagger\varrho)P'\Big)\Big] \\
&= \frac{1}{2^{2n}} \sum_{j=0}^{n}(-1)^j \sum_{\substack{P\in\mathcal{P}\\ \mathrm{wt}(P)=j}} \mathrm{Tr}(P\varrho)\,\mathrm{Tr}(P^\dagger\varrho)\,\mathrm{Tr}(P^\dagger P)\Big] \\
&= \frac{1}{2^n}\sum_{j=0}^{n}(-1)^j A_j \geq 0\,.
\end{aligned} \tag{4.40}$$

Applying the same method to all reductions ϱ_S of fixed size $|S| = m$, one obtains

$$\begin{aligned}
\sum_{|S|=m} \mathrm{tr}[\varrho_S\tilde{\varrho}_S] &= 2^{-2m} \sum_{|S|=m}\sum_{j=0}^{m}(-1)^j A_j^S \\
&= 2^{-m}\sum_{j=0}^{m}(-1)^j \binom{n-j}{n-m} A_j \geq 0\,.
\end{aligned} \tag{4.41}$$

This can be rewritten as $\sum_{j=0}^{m}(-1)^j A_j^m \geq 0$. This ends the proof. □

Th expression $\mathrm{Tr}(\varrho\tilde{\varrho})$ is also known as an entanglement monotone called n-concurrence, and can be converted into a monogamy relation [159, 198]. In light of the subsequent Chapter 5, Eq. (4.38) can also be restated as the requirement that the so-called *shadow coefficient* $S_0 = \mathrm{Tr}(\varrho_S\tilde{\varrho}_S)$ be non-negative when averaged over all m-body marginals ϱ_S. Note that in the case of graph states, this expression must be integer, as it is obtained by counting elements of the stabilizer set with integer prefactors. Similar conditions can be obtained by requiring $S_j(\varrho_S) \geq 0$ for all j and all reductions. This leads to constraints similar to those of the linear program in Eq. (1.182).

4.6 Detecting illegitimate decks

In the following, we use the relations derived in the previous section to detect illegitimate states. This is possible because having access to all reduced states of size m directly yields A_j^m.

Proposition 16. *Given a complete quantum k-deck $D = \{\varrho_S\}$, the weights $A_1, \ldots, A_k$ of the weight distribution of possible joint states can be obtained.*

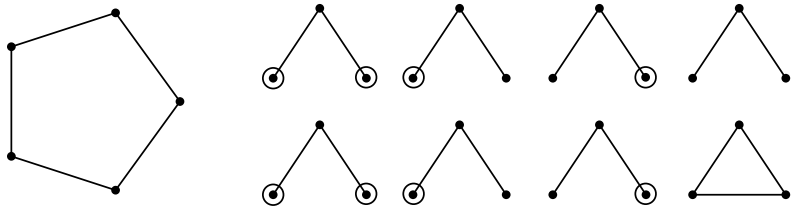


Figure 4.2: Left: Ring cluster state on five qubits. Right, top row: the three-qubit reductions of the five qubit ring cluster state obtained by tracing out nearest neighbors are the equal mixture of these graph states. Right, bottom row: modifying some reductions to be the equal mixture of the graph states shown in the bottom row, no compatible joint state on five qubits exists.

Proof. Given a complete deck D, we obtain

$$\begin{aligned}\sum_{\varrho_S\in D}\sum_{\substack{P\in\mathcal{P}\\ \mathrm{wt}(P)=j}} &= \mathrm{tr}[(\varrho_S\otimes\mathbb{1}_{S^c})P]\,\mathrm{tr}[(\varrho_S\otimes\mathbb{1}_{S^c})P^\dagger]\\ &= 2^{-k}\sum_{S,\,|S|=k} A_j^S = 2^{-k}\binom{n-j}{n-m}A_j = 2^{-k}\sum A_j^k\,. \end{aligned} \tag{4.42}$$

where

$$A_j^S = \sum_{\substack{P\in P\\ \mathrm{supp}(P)\subseteq S\\ \mathrm{wt}(S)=j}} \mathrm{Tr}(P\varrho)\,\mathrm{Tr}(P^\dagger\varrho)\,. \tag{4.43}$$

From A_j^k, the A_j can be obtained from Eq. (4.31). This ends the proof. □

For decks of hypothetical joint graph states, A_j^k is exactly equal to the total number of stabilizer elements of weight j appearing in the quantum k-deck. To see how Prop. 14 can help to decide compatibility of a quantum deck, let us provide some examples.

Example 2. *Consider the case of three qubits. Then, setting $a = 1$ yields the necessary condition on the weight distribution of a pure three-qubit state to be*

$$A_2 = 3\,. \tag{4.44}$$

By normalization, $A_1 + A_3 = 4$ follows. This makes clear that it is not possible to join three Bell states together, as each one has the weights $A = [1, 0, 3]$ already.

Example 3. *Let us consider a more elaborate example, the ring cluster state of five qubits depicted in Fig. 3. Those of its marginals which can be obtained by tracing out nearest neighbors can be described as an equal mixture of the four graph states on three qubits that are shown in Fig. 3, where the circles denote local Z-gates applied to the state. However, modifying the reductions to be equal to the mixture of the states shown in the bottom row, no consistent joint state can exist. This follows from their corresponding weight distribution:*

The ring cluster state has $\binom{5}{3} = 10$ *reductions on three qubits with* $A = [1, 0, 0, 1]$*, consistent with Prop. 14 on five qubits. These read*

$$-2A_1 + A_2 + A_3 = 10 \tag{4.45}$$

$$-4A_1 + 3A_2 + 2A_3 + A_4 = 35\,. \tag{4.46}$$

Slightly modifying some reductions to be an equal mixture of four other states depicted in the lower row of Fig. 3, we obtain an illegitimate deck: These reductions have the weight distribution $A = (1, 0, 3/8, 11/8)$*, together with the rest of the deck, they do not satisfy Prop. 14. Thus, a corresponding joint state on five qubits cannot exist.*

Example 4. *Let us ask whether a pure state* ϱ *on ten qubits could exist that has all reductions on six qubits equal to*

$$\mathrm{Tr}_S(\varrho) = p|GHZ_6\rangle\langle GHZ_6| + (1-p)\mathbb{1}\,, \tag{4.47}$$

for all subsystems S *of size six. Above, the GHZ state on six qubits is defined as* $|GHZ_6\rangle = (|000000\rangle + |111111\rangle)/\sqrt{2}$*, and its weight distribution is* $A(|GHZ_6\rangle) = [1, 0, 15, 0, 15, 0, 33]$*. From it, we can obtain a part of the weight distribution of the full state, namely*

$$A_{j\leq 6}(\varrho) = \binom{10}{j}\binom{6}{j}^{-1} A_j(|GHZ_6\rangle)\,. \tag{4.48}$$

Thus for the putative pure joint state, $[A_0, \ldots, A_6] = [1, 0, 45p, 0, 210p, 0, 6930p]$*. Let us now see what value* p *can have, in order to satisfy Prop. 14. The relation involving* $A_0, \ldots, A_6$ *only requires that*

$$630 = -210A_1 - 42A_2 + 7A_3 + 11A_4 + 5A_5 + A_6\,. \tag{4.49}$$

This can only be fulfilled if $p = 3/35$*.*

Note that in above examples, one does not require to know the labeling of the parties. Despite that, it is possible to make statements whether a joint state might exist, and to already detect illegitimate decks when provided by a deck whose cards have only size $(\lfloor \frac{n}{2} \rfloor + 1)$.

4.7 When is a weight distribution graphical?

Even when given the complete weight distribution $A_0, \ldots, A_n$, one cannot always decide whether or not it can be realized by a graph state, that is, if the weight distribution is *graphical*: While the criteria derived in the previous sections are necessary, they are however not sufficient. One can find weight distributions which satisfy all of the relations derived above, but for which no corresponding quantum states exists. As an example, consider a hypothetical pure state of seven qubits, having all three-body reductions maximally mixed (c.f. Chpt. 3). This a so-called absolutely maximally entangled state, having the code parameters $((7, 1, 4))_2$. Its weights distribution reads [44]

$$A = [1, 0, 0, 0, 35, 42, 28, 22]\,. \tag{4.50}$$

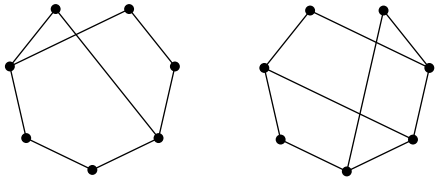


Figure 4.3: Two graph states on seven qubits that share the same weight distribution, but which can be shown to be inequivalent under local unitaries and graph isomorphism. These are the graphs No. 42 and 43 of Table 5 in Ref. [47].

This weight distribution fulfills all of above relations. While it was known by exhaustive search that a realization as a graph state does not exist, we could only recently show that such state can possibly exist with these properties (see Chpt. 3 and Ref. [109]). Interestingly, weight distributions are known for which the existence of corresponding graph states is unknown. As an example, the existence of a graph state on 24 qubits, having all 9-body reductions maximally mixed, is a long-standing open problem [4]. Such state is equivalent to a self-dual additive code over GF_4, and corresponds to a quantum code having the parameters $[[24, 0, 10]]_2$. A putative weight distribution for such a state of type II, having a distribution of even non-vanishing weights, reads

$$[A_{10}, A_{12}, A_{14}, \ldots A_{24}] = \\ [18216, 156492, 1147608, 3736557, 6248088, 4399164, 1038312, 32778]\,, \tag{4.51}$$

This weight distribution can also be found in The On-Line Encyclopedia of Integer Sequences [5].

Finally, note that a weight distribution does not necessarily uniquely identify the corresponding graph state, as states inequivalent under LU-transformations and graph isomorphism can indeed have the same weight distribution. As an example, consider the two graph states on seven qubits that are depicted in Fig. 4.7. These can be shown to be inequivalent under local unitaries and graph isomorphism, but they share the same weight distribution of [6]

$$A = [1, 0, 0, 7, 21, 42, 42, 15]\,. \tag{4.52}$$

Thus a weight distribution does not necessarily uniquely identify a graph state.

4.8 Conclusion

We have introduced the Ulam graph reconstruction problem to the case of quantum graph states. In contrast to classical graph decks, the full graph state can (up to local Z-gates) be reconstructed from a single card in the deck. As in the classical case, the question of detecting illegitimate decks is of interest. Here, consistency equations can be derived which can detect some but not all illegitimate quantum

[4] See Research Problem 13.3.7 in Ref. [106].

[5] See `http://oeis.org/A030331`.

[6] These are graphs No. 42 and 43 of Fig. 5 in Ref. [47]. Also c.f. Eq. (1.176).

decks from their weight distribution; in some cases it is already possible to detect the illegitimacy of decks consisting of marginals of size $\lfloor \frac{n}{2} \rfloor + 1$. It would be interesting to see whether similar relations can also be obtained for decks of classical graphs.

The result by Bollobás [219], namely, that almost every graph can uniquely be reconstructed by a specific set of three cards, has an interesting counterpart in the quantum setting: In Sect. 2.6.3, we have shown that almost all states are already uniquely determined amongst all pure states by three marginals of size $(n-2)$ [184]. It would be desirable to understand if similar results also hold for the special case of graph states.

Chapter 5

Constraints on correlations in QECC and AME states

A pure multipartite quantum state is called absolutely maximally entangled (AME), if all reductions obtained by tracing out at least half of its parties are maximally mixed. However, the existence of such states is in many cases unclear. With the help of the weight enumerator machinery known from quantum error-correcting codes and the generalized shadow inequalities, we obtain new bounds on the existence of AME states in higher dimensions. To complete the treatment on the weight enumerator machinery, the quantum MacWilliams identity is derived in the Bloch representation. This Chapter is based on Project [F].

5.1 Introduction

Recall that a pure state of n parties is called *absolutely maximally entangled* (AME), if all reductions to $\lfloor \frac{n}{2} \rfloor$ parties are maximally mixed. Then maximal possible entanglement is present across each bipartition (c.f. 1.2.3).

As described in Chpt.3, the non-existence of the seven quit AME state solved the AME problem in the case of qubits: Qubit AME states do only exist for $n = 2, 3, 5,$ and 6 parties, all of which can be expressed as graph or stabilizer states [44, 109]. Concerning larger local dimensions however, the existence of such states is only partially resolved. AME states exist for any number of parties, if the dimension of the subsystems is chosen large enough [99]. Furthermore, different constructions for such states have been put forward, based on graph states [47, 48], classical maximum distance separable codes [99, 110], and combinatorial designs [91, 111]. However, for many cases it is still unknown whether or not AME states exist [1].

In this Chapter, we give results on the question of AME state existence when the local dimension is three or higher. Namely, we show that, additionally to the known non-existence bounds, three-level AME states with

$$n = 8, 12, 13, 14, 16, 17, 19, 21, 23\,; \tag{5.1}$$

[1] For the current status of this question, see Problem 35 in Ref. [112]

four-level AME states with

$$n = 12, 16, 20, 24, 25, 26, 28, 29, 30, 33, 37, 39\,; \tag{5.2}$$

and five-level AME states of

$$n = 28, 32, 36, 40, 44, 48 \tag{5.3}$$

parties do not exist.

To this end, we make use of the weight enumerator machinery known from quantum error-correcting codes (QECC). With it, bounds can also be obtained for one-dimensional codes, which are pure quantum states [44]. We will make use of the so-called shadow inequalities, which constrain the admissible correlations of multipartite states, to exclude the existence of the above-mentioned AME states. Along the way, we will prove a central theorem, the quantum MacWilliams identity, originally derived by Shor and Laflamme for qubits [128] and by Rains for arbitrary finite-dimensional systems in Ref. [118]. Thus our aim is twofold: On the one hand, we provide an accessible introduction into the weight enumerator machinery in terms of the Bloch representation, in order to gain physical intuition. On the other hand, we apply this machinery to exclude the existence of certain higher-dimensional AME states by making use of the so-called shadow enumerator.

This Chapter is organized as follows. In the next section, we introduce the shadow inequalities, from which we eventually obtain the bounds mentioned above. In Sect. 5.3, the Bloch representation of quantum states is introduced, followed by a short discussion of QECC and their relation to AME states in Sect. 5.4. In Sect. 5.5, we introduce the shadow enumerator, the Shor-Laflamme enumerators are explained in Sect. 5.6, followed by the derivation of the quantum MacWilliams identity in Sect. 5.7. The shadow enumerator in terms of the Shor-Laflamme enumerator is derived in Sect. 5.8, from which one can obtain bounds on the existence of QECC and of AME states in particular, which is presented in Sect. 5.9. We conclude in Sect. 5.10.

5.2 Motivation

Originally introduced by Shor and Laflamme [128], Rains established the notion of weight enumerators in a series of landmark articles on quantum error-correcting codes [107, 118, 129]. With it, he stated some of the strongest bounds known to date on the existence of QECC [107].

In particular, in his paper on polynomial invariants of quantum codes [129], Rains showed an interesting theorem, which proved to be crucial to obtain those bounds. These are the so-called *generalized shadow inequalities*: For all positive semi-definite Hermitian operators M and N on parties $(1 \dots n)$ and any fixed subset $T \subseteq \{1 \dots n\}$, it holds that

$$\sum_{S \subseteq \{1 \dots n\}} (-1)^{|S \cap T|} \operatorname{Tr}_S[\operatorname{Tr}_{S^c}(M) \operatorname{Tr}_{S^c}(N)] \geq 0\,. \tag{5.4}$$

Here and in what follows, S^c denotes the complement of subsystem S in $\{1 \dots n\}$. Note that if $M = N = \varrho$ is a quantum state, the generalized shadow inequalities

are consistency equations involving the purities of the marginals, i.e. they relate terms of the form $\mathrm{Tr}[\mathrm{Tr}_{S^c}(\varrho)^2]$, which in turn can be expressed in terms of linear entropies. Thus, these inequalities form an exponentially large set of monogamy relations for multipartite quantum states, applicable to any number of parties and local dimensions.

In order to state bounds on the existence of AME states of n parties having local dimension D each, one could in principle just evaluate this expression by inserting the purities of AME state reductions. However, in order to understand the connections to methods from quantum error-correcting codes, let us first recall the quantum weight enumerator machinery, including the so-called shadow enumerator, which is derived from Eq. (5.4). We will then rederive the central theorem, namely the quantum MacWilliams identity. Finally, we obtain new bounds for AME states with the help of the shadow inequalities. In order to remain in a language close to physics, we will work exclusively in the Bloch representation.

5.3 The Bloch representation

Let us recall the Bloch representation (c.f. Sect. 1.1.7). Denote by $\{e_j\}$ an orthonormal basis for operators acting on $\mathbb{C}^D$, such that $\mathrm{Tr}(e_j^\dagger e_k) = \delta_{jk} D$. We require that $\{e_j\}$ contains the identity (e.g. $e_0 = \mathbb{1}$), and therefore all other basis elements are traceless (but not necessarily Hermitian). Then, a local error-basis $\mathcal{E}$ acting on $(\mathbb{C}^D)^{\otimes n}$ can be formed by taking tensor products of elements in $\{e_j\}$. That is, each element $E_\alpha \in \mathcal{E}$ can be written as

$$E_\alpha = e_{\alpha_1} \otimes \ldots \otimes e_{\alpha_n} \,. \tag{5.5}$$

Because the single-party basis $\{e_j\}$ is orthonormal, the relation $\mathrm{Tr}(E_\alpha^\dagger E_\beta) = \delta_{\alpha\beta} D^n$ follows. For qubits, $\mathcal{E}$ can be thought of to contain all tensor products of the Pauli matrices $\sigma_0, \sigma_1, \sigma_2, \sigma_3$; in higher dimensions, a tensor-product basis can be formed from elements of the Heisenberg-Weyl or the generalized Gell-Mann basis [40]. Further, denote by $\mathrm{supp}(E)$ the support of operator E, that is, the set of parties on which E acts non-trivially. The weight of an operator is then size of its support, and we write $\mathrm{wt}(E) = |\mathrm{supp}(E)|$.

Then, every operator on n parties having D levels each can be decomposed in the Bloch representation as

$$M = \frac{1}{D^n} \sum_{E \in \mathcal{E}} \mathrm{Tr}(E^\dagger M) E \,. \tag{5.6}$$

As in the above decomposition, we will often omit the subindex α, writing E for E_α. Also, most equations that follow contain sums over all elements E in $\mathcal{E}$, subject to constraints. In those cases we will often denote the constraints only below the summation symbol.

Given an operator M expanded as in Eq. (5.6), its reduction onto subsystem S^c tensored by the identity on the complement S reads

$$\mathrm{Tr}_S(M) \otimes \mathbb{1}_S = D^{|S|-n} \sum_{\mathrm{supp}(E) \subseteq S^c} \mathrm{Tr}(E^\dagger M) E \,. \tag{5.7}$$

This follows from $\mathrm{Tr}_S(E) = 0$ whenever $\mathrm{supp}(E) \not\subseteq S^c$. Interestingly, this can also be written in terms of a quantum channel, whose Kraus operators also form a unitary 1-design [222].

Observation 26. *The partial trace over subsystem S tensored by the identity on S can also be written as a channel,*

$$\mathrm{Tr}_S(M) \otimes \mathbb{1}_S = D^{-|S|} \sum_{\mathrm{supp}(E) \subseteq S} EME^\dagger \,. \tag{5.8}$$

Proof. Consider a bipartite system with Hilbert space $\mathcal{H} = \mathbb{C}^D \otimes \mathbb{C}^D$ with a local orthonormal operator basis $\{e_j\}$ on $\mathbb{C}^D$. Define the SWAP operator as

$$\mathrm{SWAP} = \sum_{j,k=0}^{D-1} |jk\rangle\langle kj| \,. \tag{5.9}$$

Thus, it acts on pure states as $\mathrm{SWAP}(|\psi\rangle \otimes |\phi\rangle) = |\phi\rangle \otimes |\psi\rangle$. Note that it can also be expressed in terms of any orthonormal basis $\{e_j\}$ as [15]

$$\mathrm{SWAP} = \frac{1}{D} \sum_{j=0}^{D^2-1} e_j^\dagger \otimes e_j \,. \tag{5.10}$$

Therefore we can express $\mathbb{1} \otimes N$ as

$$\begin{aligned} \mathbb{1} \otimes N &= \mathrm{SWAP} \cdot (N \otimes \mathbb{1}) \cdot \mathrm{SWAP} \\ &= (D^{-1} \sum_{j=0}^{D^2-1} e_j \otimes e_j^\dagger)(N \otimes \mathbb{1})(D^{-1} \sum_{k=0}^{D^2-1} e_k^\dagger \otimes e_k) \\ &= D^{-2} \sum_{j,k=0}^{D^2-1} (e_j N e_k^\dagger) \otimes (e_j^\dagger e_k) \,. \end{aligned} \tag{5.11}$$

Tracing over the second party gives

$$\mathrm{Tr}(N)\mathbb{1} = \frac{1}{D} \sum_{j=0}^{D^2-1} e_j N e_j^\dagger \,. \tag{5.12}$$

The claim follows from the linearity of the tensor product. This ends the proof. □

Note that the proof is independent of the local orthonormal operator basis $\{e_j\}$ chosen.

5.4 Quantum error-correcting codes

Let us introduce recall the definition of quantum error-correcting codes (c.f. 1.2.4) and their relation to absolutely maximally entangled states. A quantum error-correcting code with the parameters $((n, K, d))_D$ is a K-dimensional subspace $\mathcal{Q}$ of

$(\mathbb{C}^D)^{\otimes n}$, such that for any orthonormal basis $\{|i_\mathcal{Q}\rangle\}$ of $\mathcal{Q}$ and all errors $E \in \mathcal{E}$ with $\mathrm{wt}(E) < d$ [44, 117],

$$\langle i_\mathcal{Q}| \, E \, |j_\mathcal{Q}\rangle = \delta_{ij} C(E) \, . \tag{5.13}$$

Above, d is called the distance of the code. If $C(E) = \mathrm{Tr}(E)/D^n$, the code is called pure. By convention, codes with $K = 1$ are only considered codes if they are pure. From the definition follows that a one-dimensional code (also called self-dual), described by a projector $|\psi\rangle\langle\psi|$, must fulfill $\mathrm{Tr}(E|\psi\rangle\langle\psi|) = 0$ for all $E \neq \mathbb{1}$ of weight smaller than d. Thus, pure one-dimensional codes of distance d are pure quantum states whose reductions onto $(d-1)$ parties are all maximally mixed. AME states, whose reductions onto $\lfloor \frac{n}{2} \rfloor$ parties are maximally mixed, are QECC having the parameters $((n, 1, \lfloor \frac{n}{2} \rfloor + 1))_D$.

5.5 The shadow enumerator

Let us introduce the shadow enumerator, and point out its usefulness. Following Rains [118], we define

$$\mathcal{A}'_S(M, N) = \mathrm{Tr}_S[\mathrm{Tr}_{S^c}(M) \, \mathrm{Tr}_{S^c}(N)] \, , \tag{5.14}$$

$$\mathcal{B}'_S(M, N) = \mathrm{Tr}_{S^c}[\mathrm{Tr}_S(M) \, \mathrm{Tr}_S(N)] \, . \tag{5.15}$$

Naturally, $\mathcal{A}'_S = \mathcal{B}'_{S^c}$. With this, we define

$$S_j(M, N) = \sum_{|T|=j} \sum_{S \subseteq \{1 \ldots n\}} (-1)^{|S \cap T^c|} \mathcal{A}'_S(M, N) \, , \tag{5.16}$$

where the sum is over all $T \subseteq \{1 \ldots n\}$ of size j. Eq. (5.4) states that all S_j must be non-negative. Note however, that there is the term T^c instead of T in the exponent, compared to Eq. (5.4), but this does not matter, as Eq. (5.4) holds for any T. The *shadow enumerator* then is the polynomial

$$S_{MN}(x, y) = \sum_{j=0}^{n} S_j(M, N) \, x^{n-j} y^j \, . \tag{5.17}$$

The question remains: Given a hypothetical QECC or an AME state in particular, how do we obtain its shadow enumerator in order to check for the non-negativity of its coefficients? Two paths come to mind: First, if we are interested in one-dimensional codes ($K = 1$), the purities of the reductions determine all $\mathcal{A}'_S(\mathcal{Q})$. For AME states of local dimension D, the situation is particularly simple: from the Schmidt decomposition, it can be seen that all reductions to k parties must have the purity

$$\mathrm{Tr}(\varrho^2_{(k)}) = D^{-\min(k, n-k)} \, . \tag{5.18}$$

Second, the coefficients of the so called Shor-Laflamme enumerator $A_j(\mathcal{Q})$ may be known (see also below), from which the shadow enumerator can be obtained. Generally, when dealing with codes whose existence is unknown, putative weight enumerators can often be obtained by stating the relations that follow as a linear program [44, 106, 108]. If, for a set of parameters $((n, K, d))_D$, no solution can be found, a corresponding QECC cannot exist.

In the following three sections, we aim to give a concise introduction as well as intuition to this enumerator theory.

	Coefficient	Enumerator
Shor-Laflamme enum's:	$A_j(M,N) = \sum_{\mathrm{wt}(E)=j} \mathrm{Tr}(EM)\,\mathrm{Tr}(E^\dagger N)$ $B_j(M,N) = \sum_{\mathrm{wt}(E)=j} \mathrm{Tr}(EME^\dagger N)$	$A_{MN}(x,y) = \sum_{j=0}^n A_j(M,N)x^{n-j}y^j$ $B_{MN}(x,y) = \sum_{j=0}^n B_j(M,N)x^{n-j}y^j$
Rain's unitary enum's:	$\mathcal{A}'_S(M,N) = \mathrm{Tr}_S[\mathrm{Tr}_{S^c}(M)\,\mathrm{Tr}_{S^c}(N)]$ $\mathcal{B}'_S(M,N) = \mathrm{Tr}_{S^c}[\mathrm{Tr}_S(M)\,\mathrm{Tr}_S(N)]$ $A'_j(M,N) = \sum_{\lvert S\rvert=j} \mathcal{A}'_S(M,N)$ $B'_j(M,N) = \sum_{\lvert S\rvert=j} \mathcal{B}'_S M,N)$	$A'_{MN}(x,y) = \sum_{j=0}^n A'_j(M,N)x^{n-j}y^j$ $B'_{MN}(x,y) = \sum_{j=0}^n B'_j(M,N)x^{n-j}y^j$
Shadow enumerator:	$S_j(M,N) = \sum_{\lvert T\rvert=j} \sum_S (-1)^{\lvert S\cap T^c\rvert} \mathcal{A}'_S(M,N)$	$S_{MN}(x,y) = \sum_{j=0}^n S_j(M,N)x^{n-j}y^j$

Table 5.1: The weight enumerators and their coefficients, as used in this Chapter.

5.6 Shor-Laflamme enumerators

In this section, we introduce the protagonists of the enumerator machinery, the *Shor-Laflamme (weight) enumerators* [118, 128]. These are defined for any two given Hermitian operators M and N acting on $(\mathbb{C}^D)^{\otimes n}$, and are local unitary invariants. Their (unnormalized) coefficients are given by [2].

$$A_j(M,N) = \sum_{\mathrm{wt}(E)=j} \mathrm{Tr}(EM)\,\mathrm{Tr}(E^\dagger N)\,, \tag{5.19}$$

$$B_j(M,N) = \sum_{\mathrm{wt}(E)=j} \mathrm{Tr}(EME^\dagger N)\,. \tag{5.20}$$

The corresponding enumerator polynomials are

$$A_{MN}(x,y) = \sum_{j=0}^n A_j(M,N)x^{n-j}y^j\,, \tag{5.21}$$

$$B_{MN}(x,y) = \sum_{j=0}^n B_j(M,N)x^{n-j}y^j\,. \tag{5.22}$$

While it might not be obvious from the definition, these enumerators are independent of the local error-basis $\mathcal{E}$ chosen, and are thus local unitary invariants. This follows from the fact that they can expressed as linear combinations of terms having the form of Eq. (5.14). The exact relation will be made clear in Section 5.7.

When dealing with weight enumerators, there is the following pattern, as seen above: First define a set of coefficients [e.g, $A_j(M,N)$], from which the associated polynomial, the enumerator, is constructed [e.g., $A_{MN}(x,y)$]. If $M = N$, we will often write the first argument only, e.g. $A_j(M)$, or leave it out alltogether. In Table 5.1, we give an overview of the coefficients and enumerators used in this Chapter.

Considering a QECC with parameters $((n,K,d))_D$, one sets $M = N$ to be equal to the projector $\mathcal{Q}$ onto the code space. The following results concerning QECC and their Shor-Laflamme enumerators are known [118]: The coefficients $A_j = A_j(\mathcal{Q})$ and $B_j = B_j(\mathcal{Q})$ are non-negative, and

$$KB_0 = A_0 = K^2\,, \tag{5.23}$$

$$KB_j \geq A_j\,, \tag{5.24}$$

[2] In fact, for higher dimensions, we chose a definition that is different, but equivalent, to the original definition as found in Ref. [118].

with equality in the second equation for $j < d$. In fact, these conditions are not only necessary but also sufficient for a projector $\mathcal{Q}$ to be a QECC.

Theorem 27 ([118]). *Let $\mathcal{Q}$ be a projector of rank K. $\mathcal{Q}$ is a code of distance d if and only if*

$$KB_j(\mathcal{Q}) = A_j(\mathcal{Q}) \qquad \forall j < d\,, \tag{5.25}$$

Proof. The equation $KB_0 = A_0 = K^2$ follows by direct computation. Let us show that for a QECC having the parameters $((n, K, d))_D$, the coefficients of the Shor-Laflamme enumerator fulfill [cf. Eq. (5.24)] $A_j(\mathcal{Q}) \leq KB_j(\mathcal{Q})$, where equality holds for $j < d$. Recall that

$$A_j(\mathcal{Q}) = \sum_{\mathrm{wt}(E)=j} \mathrm{Tr}(E\mathcal{Q})\,\mathrm{Tr}(E^\dagger\mathcal{Q})\,, \tag{5.26}$$

$$B_j(\mathcal{Q}) = \sum_{\mathrm{wt}(E)=j} \mathrm{Tr}(E\mathcal{Q}E^\dagger\mathcal{Q})\,. \tag{5.27}$$

Let us check the inequality for each term appearing in the sum, namely for those of the form

$$\mathrm{Tr}(E\mathcal{Q})\,\mathrm{Tr}(E^\dagger\mathcal{Q}) \leq K\,\mathrm{Tr}(E\mathcal{Q}E^\dagger\mathcal{Q})\,, \tag{5.28}$$

where E is a specific error under consideration. For later convenience, let us choose the error-basis $\mathcal{E}$ to be Hermitian, e.g. formed by tensor products of the generalized Gell-Mann matrices (c.f. Sect. 1.1.7) [40]. Decomposing $\mathcal{Q} = \sum_{i=0}^{K} |i_\mathcal{Q}\rangle\langle i_\mathcal{Q}|$, write

$$\begin{aligned}\mathrm{Tr}(E\mathcal{Q})\,\mathrm{Tr}(E^\dagger\mathcal{Q}) &= (\sum_{i=0}^{K} \langle i_\mathcal{Q}|\,E\,|i_\mathcal{Q}\rangle)(\sum_{j=0}^{K} \langle j_\mathcal{Q}|\,E^\dagger\,|j_\mathcal{Q}\rangle)\,,\\ \mathrm{Tr}(E\mathcal{Q}E^\dagger\mathcal{Q}) &= \sum_{i,j=0}^{K} \langle i_\mathcal{Q}|\,E|j_\mathcal{Q}\rangle\langle j_\mathcal{Q}|E^\dagger\,|i_\mathcal{Q}\rangle\ .\end{aligned} \tag{5.29}$$

If $\mathrm{wt}(E) < d$, recall the definition of a QECC [Eq. (5.13)],

$$\langle i_\mathcal{Q}|\,E\,|j_\mathcal{Q}\rangle = \delta_{ij}C(E), \quad \text{if } \mathrm{wt}(E) < d\,. \tag{5.30}$$

From this one obtains for $j < d$

$$\begin{aligned}\mathrm{Tr}(E\mathcal{Q})\,\mathrm{Tr}(E^\dagger\mathcal{Q}) &= K^2C(E)C^*(E)\,,\\ \mathrm{Tr}(E\mathcal{Q}E^\dagger\mathcal{Q}) &= KC(E)C^*(E)\,.\end{aligned} \tag{5.31}$$

Thus for $j < d$, one obtains $A_j(\mathcal{Q}) = KB_j(\mathcal{Q})$. If on the other hand $\mathrm{wt}(E) \geq d$, let us define the matrix $\mathcal{Q}$ with entries $\mathcal{Q}_{ij} = \langle i_\mathcal{Q}|\,E\,|j_\mathcal{Q}\rangle$. Note that $\mathcal{Q}$ is a Hermitian matrix of size $K \times K$. Then

$$\begin{aligned}\mathrm{Tr}(E\mathcal{Q})\,\mathrm{Tr}(E^\dagger\mathcal{Q}) &= [\mathrm{Tr}(\mathcal{Q})]^2\,,\\ \mathrm{Tr}(E\mathcal{Q}E^\dagger\mathcal{Q}) &= \mathrm{Tr}(\mathcal{Q}^2)\,.\end{aligned} \tag{5.32}$$

Consider the diagonalization of $\mathcal{Q}$. By Jensen's inequality, its eigenvalues must fulfill

$$\Big(\sum_{i=1}^{K} \lambda_i\Big)^2 \leq K\sum_{i=1}^{K} \lambda_i^2\,, \tag{5.33}$$

from which the inequality $A_j(\mathcal{Q}) \leq KB_j(\mathcal{Q})$ follows.

Let us now show that a projector $\mathcal{Q}$ of rank K is a QECC of distance d if and only if $A_j(\mathcal{Q}) = KB_j(\mathcal{Q})$ for all $j < d$. This can be seen in the following way:

"$\Rightarrow$": Use the definition of QECC, Eq. (5.13).

"$\Leftarrow$": Note that in order to obtain $A_j(\mathcal{Q}) = KB_j(\mathcal{Q})$, there must be equality in Eq. (5.28) for all E with $\mathrm{wt}(E) = j$. Thus, also equality in Eq. (5.33) is required. However, this is only possible if all eigenvalues λ_i of $\mathcal{Q}$ are equal. Then, $\mathcal{Q}$ is diagonal in any basis, and we can write

$$\langle i_{\mathcal{Q}}| E |j_{\mathcal{Q}}\rangle = \delta_{ij}\lambda(\mathcal{Q})\,. \tag{5.34}$$

Because above equation must hold for all errors E of weight less than d, we obtain Eq. (5.13) defining a quantum error-correcting code:

$$\langle i_{\mathcal{Q}}| E |j_{\mathcal{Q}}\rangle = \delta_{ij}C(E)\,, \tag{5.35}$$

for all E with $\mathrm{wt}(E) < d$. This ends the proof. □

The distance of a code can thus be obtained in the following way: if a projector $\mathcal{Q}$ fulfills the above conditions with equality for all $j < d$, then $\mathcal{Q}$ is a quantum code of distance d [3] For pure codes, additionally $A_j = B_j = 0$ for all $1 < j < d$. In particular, AME states have $A_j = 0$ for all $1 < j < \lfloor \frac{n}{2} \rfloor + 1$; the remaining A_j can be obtained in an iterative way from Eq. (5.18) [44, 109].

In the case of $\mathcal{Q} = |\psi\rangle\langle\psi|$, the weight enumerators have a particularly simple interpretation: The coefficient A_j measures the contribution to the purity of $|\psi\rangle\langle\psi|$ by terms in $|\psi\rangle\langle\psi|$ having weight j only, while the dual enumerator measures the overlap of $|\psi\rangle\langle\psi|$ with itself, given an error-sphere of radius j. Furthermore, we have $A_j = B_j$ for all j, as a direct evaluation shows. In the entanglement literature, $A_j(\varrho)$ is also called the correlation strength, or the two-norm of the j-body correlation tensor [90, 223]. Concerning codes known as stabilizer codes, A_j and B_j count elements of weight j in the stabilizer and in its normalizer respectively [224].

Let us now try to give some intuition for these enumerators for general Hermitian operators M and N. Note that the coefficients of the primary enumerator $A_j(M, N)$ form a decomposition of the inner product $\mathrm{Tr}(MN)$. This can be seen by writing M and N in the Bloch representation [Eq. (5.6)],

$$\begin{aligned}
\mathrm{Tr}(MN) &= D^{-2n}\,\mathrm{Tr}\Big(\sum_E \mathrm{Tr}(EM)E^\dagger \sum_{E'} \mathrm{Tr}(E'^\dagger N)E'\Big) \\
&= D^{-2n}\,\mathrm{Tr}\Big(\sum_E \mathrm{Tr}(EM)\,\mathrm{Tr}(E^\dagger N)\,E^\dagger E\Big) \\
&= D^{-n}\sum_{j=0}^{n} A_j(M,N)\,.
\end{aligned} \tag{5.36}$$

On the other hand, the coefficients of the dual enumerator $B_j(M, N)$ can be seen as a decomposition of $\mathrm{Tr}(M)\,\mathrm{Tr}(N)$. To see this, recall that by definition of the partial trace,

$$\mathrm{Tr}_{S_c}[\mathrm{Tr}_S(M)\,\mathrm{Tr}_S(N)] = \mathrm{Tr}[\mathrm{Tr}_S(M) \otimes \mathbb{1}_S\; N]\,. \tag{5.37}$$

[3] See Theorems 2 and 18 in Ref. [118], and Ref. [128].

As shown in Observation 26, the partial trace over parties in S tensored by the identity on S can also be written as a quantum channel,

$$\mathrm{Tr}_S(M) \otimes \mathbb{1}_S = D^{-|S|} \sum_{\mathrm{supp}(E) \subseteq S} E M E^\dagger \,. \tag{5.38}$$

Thus $B_j(M, N)$ decomposes $\mathrm{Tr}(M)\,\mathrm{Tr}(N)$,

$$\begin{aligned} \mathrm{Tr}(M)\,\mathrm{Tr}(N) &= \mathrm{Tr}[\mathrm{Tr}(M)\mathbb{1}\, N] \\ &= D^{-n}\,\mathrm{Tr}(\sum_E E M E^\dagger N) \\ &= D^{-n} \sum_{j=0}^{n} \sum_{\mathrm{wt}(E)=j} \mathrm{Tr}(E M E^\dagger N) \\ &= D^{-n} \sum_{j=0}^{n} B_j(M, N) \,. \end{aligned} \tag{5.39}$$

The insight gained from writing the partial trace in two different ways, and the decomposition of $\mathrm{Tr}(MN)$ and $\mathrm{Tr}(M)\,\mathrm{Tr}(N)$ in terms of the coefficients of the Shor-Laflamme enumerators will prove to be the essence of the MacWilliams identity, which we rederive in the following section.

5.7 The quantum MacWilliams identity

In this section, we prove the quantum MacWilliams identity. It relates the two Shor-Laflamme enumerators $A_{MN}(x, y)$ and $B_{MN}(x, y)$ for arbitrary Hermitian operators M and N.

Theorem 28 (Rains [106, 118])**.** *Given two Hermitian operators M and N acting on n systems having D levels each, following holds:*

$$A_{MN}(x, y) = B_{MN}\Big(\frac{x + (D^2 - 1)y}{D}, \frac{x - y}{D}\Big) \,. \tag{5.40}$$

Proof. In order to prove this identity, one has to express the trace inner product of reductions in two different ways: given the operator M expanded as in Eq. (5.6), its reduction tensored by the identity reads [cf. Eq. (5.7)]

$$\mathrm{Tr}_{S^c}(M) \otimes \mathbb{1}_{S^c} = D^{|S^c|-n} \sum_{\mathrm{supp}(E) \subseteq S} \mathrm{Tr}(EM) E^\dagger \,. \tag{5.41}$$

Therefore,

$$\begin{aligned} &\mathrm{Tr}[\mathrm{Tr}_{S^c}(M) \otimes \mathbb{1}_{S^c}\, N] \\ &= \mathrm{Tr}\left(D^{|S^c|-2n} \sum_{\mathrm{supp}(E) \subseteq S} \mathrm{Tr}(EM) E^\dagger \sum_{E'} \mathrm{Tr}(E'^\dagger N) E'\right) \\ &= D^{|S^c|-n} \sum_{\mathrm{supp}(E) \subseteq S} \mathrm{Tr}(EM)\,\mathrm{Tr}(E^\dagger N) \,. \end{aligned} \tag{5.42}$$

Summing over all subsystems S of size m, one obtains

$$\begin{aligned}
&\sum_{|S|=m} \mathrm{Tr}[\mathrm{Tr}_{S^c}(M) \otimes \mathbb{1}_{S^c} N] \\
&= D^{|S^c|-n} \sum_{|S|=m} \sum_{\mathrm{supp}(E)\subseteq S} \mathrm{Tr}(EM)\,\mathrm{Tr}(E^\dagger N) \\
&= D^{-m} \sum_{j=0}^{m} \binom{n}{m}\binom{m}{j}\binom{n}{j}^{-1} A_j(M,N) \\
&= D^{-m} \sum_{j=0}^{m} \binom{n-j}{n-m} A_j(M,N)\,. \qquad (5.43)
\end{aligned}$$

Above, the binomial factors account for multiple occurrences of terms having weight j in the sum. Note that Eq. (5.43) forms the coefficients of Rains' *unitary enumerator* [cf. (5.14)] [118], defined as

$$\begin{aligned}
A'_m(M,N) &= \sum_{|S|=m} \mathcal{A}'_S(M,N) \\
&= \sum_{|S|=m} \mathrm{Tr}_S[\mathrm{Tr}_{S^c}(M)\,\mathrm{Tr}_{S^c}(N)]\,. \qquad (5.44)
\end{aligned}$$

On the other hand, by expressing the partial trace as a quantum channel (see Obs. 26) and again summing over subsystems of size m, we can write

$$\begin{aligned}
&\sum_{|S|=m} \mathrm{Tr}[\mathrm{Tr}_S(M) \otimes \mathbb{1}_S\ N] \\
&= \sum_{|S|=m} \mathrm{Tr}(D^{-|S|} \sum_{\mathrm{supp}(E)\subseteq S} EME^\dagger N) \\
&= D^{-m} \sum_{j=0}^{m} \binom{n}{m}\binom{m}{j}\binom{n}{j}^{-1} B_j(M,N) \\
&= D^{-m} \sum_{j=0}^{m} \binom{n-j}{n-m} B_j(M,N)\,. \qquad (5.45)
\end{aligned}$$

Similar to above, Eq. (5.45) forms the coefficients of the unitary enumerator [cf. Eq. (5.14)]

$$\begin{aligned}
B'_m(M,N) &= \sum_{|S|=m} \mathcal{B}'_S(M,N) \\
&= \sum_{|S|=m} \mathrm{Tr}_{S^c}[\mathrm{Tr}_S(M)\,\mathrm{Tr}_S(N)]\,. \qquad (5.46)
\end{aligned}$$

Naturally, the corresponding unitary enumerator polynomials read

$$A'_{MN}(x,y) = \sum_{j=0}^{n} A'_j(M,N) x^{n-j} y^j \qquad (5.47)$$

$$B'_{MN}(x,y) = \sum_{j=0}^{n} B'_j(M,N) x^{n-j} y^j\,. \qquad (5.48)$$

Using relations (5.43) and (5.45), let us relate the unitary enumerators to the Shor-Laflamme enumerators. This is somewhat tedious but straightforward:

$$\begin{aligned}
A'_{MN}(x,y) &= \sum_{m=0}^{n} A'_m(M,N)x^{n-m}y^m \\
&= \sum_{m=0}^{n}\Big[\sum_{j=0}^{m}\binom{n-j}{n-m}A_j(M,N)D^{-m}\Big]x^{n-m}y^m \\
&= \sum_{j=0}^{n}\sum_{m=0}^{n}\binom{n-j}{n-m}A_j(M,N)x^{n-m}(y/D)^m \\
&= \sum_{j=0}^{n}\sum_{m=j}^{n}\binom{n-j}{n-m}A_j(M,N)x^{n-m}(y/D)^m(y/D)^{-j}(y/D)^j \\
&= \sum_{j=0}^{n}\sum_{m=0}^{n-j}\binom{n-j}{n-j-m}A_j(M,N)x^{n-j-m}(y/D)^m(y/D)^j \\
&= \sum_{j=0}^{n} A_j(M,N)(x+y/D)^{n-j}(y/D)^j \\
&= A_{MN}\Big(x+\frac{y}{D},\frac{y}{D}\Big)\,. \qquad (5.49)
\end{aligned}$$

In an analogous fashion (replace A'_m by B'_m, and A_j by B_j), one can relate $B'_{MN}(x,y)$ and $B_{MN}(x,y)$. Thus

$$A'_{MN}(x,y) = A_{MN}\Big(x+\frac{y}{D},\frac{y}{D}\Big)\,, \qquad (5.50)$$

$$B'_{MN}(x,y) = B_{MN}\Big(x+\frac{y}{D},\frac{y}{D}\Big)\,. \qquad (5.51)$$

It remains to use that $\mathcal{B}'_S(M,N) = \mathcal{A}'_{S^c}(M,N)$, from which follows that $B'_k(M,N) = A'_{n-k}(M,N)$, and

$$A'_{MN}(x,y) = B'_{MN}(y,x)\,. \qquad (5.52)$$

Thus the quantum MacWilliams identity is established,

$$\begin{aligned}
A_{MN}(x,y) = A'_{MN}(x-y,Dy) &= B'_{MN}(Dy,x-y) \\
&= B_{MN}\Big(\frac{x+(D^2-1)y}{D},\frac{x-y}{D}\Big)\,. \qquad (5.53)
\end{aligned}$$

This ends the proof. □

For $M = N = |\psi\rangle\langle\psi|$, $A_j(|\psi\rangle) = B_j(|\psi\rangle)$. Therefore the enumerator must stay invariant under the transform

$$\begin{aligned}
x &\longmapsto \frac{x+(D^2-1)y}{D}\,, \\
y &\longmapsto \frac{x-y}{D}\,. \qquad (5.54)
\end{aligned}$$

In this case, a much simpler interpretation of the MacWilliams identity can be given: It ensures that the purities of complementary reductions, averaged over all complementary reductions of fixed sizes, are equal.

As shown above, the quantum MacWilliams identity is in essence a decomposition of the trace inner product of reductions of operators M and N in two different ways. The motivation lies in the decomposition of $\mathrm{Tr}(MN)$ and $\mathrm{Tr}(M)\,\mathrm{Tr}(N)$, using different ways to obtain the partial trace in the Bloch picture [cf. Eqs. (5.7) and Obs. 26]. Finally, note that the derivation of the identity did not require M, N to be positive semi-definite. Therefore the quantum MacWilliams identity holds for all, including non-positive, pairs of Hermitian operators.

5.8 The shadow enumerator in terms of the Shor-Laflamme enumerator

So far, we have introduced the Shor-Laflamme and the shadow enumerator. Let us now see how to express one in terms of the other. The strategy is the following: the shadow inequalities are naturally expressed in terms of $\mathcal{A}'_S$ [cf. Eqs. (5.4) and (5.16)], which we then write as a transformation of $A_{MN}(x, y)$.

Theorem 29 (Rains [4] [106, 107, 118])**.** *Given $A_{MN}(x, y)$, the shadow enumerator is given by*

$$S_{MN}(x, y) = A_{MN}\left(\frac{(D-1)x + (D+1)y}{D}, \frac{y-x}{D}\right). \tag{5.55}$$

Proof. Recall from Eq. (5.16), that for Hermitian operators $M, N \geq 0$, the coefficients of the shadow enumerator are

$$S_j(M, N) = \sum_{|T|=j} \sum_{S} (-1)^{|S\cap T^c|} \mathcal{A}'_S(M, N)\,. \tag{5.56}$$

As a first step, let us understand what combinatorial factor a given $\mathcal{A}'_S(M, N)$ receives from the sum over the subsets $T \subseteq \{1 \ldots n\}$ of size j, or subsets T^c of size $m = n - j$ respectively. For a fixed subsystem S of size k, we can evaluate the partial sum

$$f(m = |T^c|, k = |S|; n) = \sum_{|T^c|=m} (-1)^{|S\cap T^c|}\,. \tag{5.57}$$

By considering what possible subsets T^c of size m have a constant overlap of size α with S, yielding a sign $(-1)^\alpha$, we obtain the expression

$$f(m, k; n) = \sum_{\alpha} \binom{n-k}{m-\alpha}\binom{k}{\alpha}(-1)^\alpha =: K_m(k; n)\,, \tag{5.58}$$

where $K_m(k; n)$ is the so-called Krawtchouk polynomial (see Appendix 5.12). Above, $\binom{k}{\alpha}$ accounts for the different combinatorial possibilities of elements T^c having overlap α with S. Necessarily, T^c must then have a part of size $m - \alpha$ lying outside of S; there are $\binom{n-k}{m-\alpha}$ ways to obtain this. This is illustrated in Fig. 5.1. Therefore,

[4] See Theorem 13.5.1. on p. 383 in Ref. [106] and Theorem 8 in Ref. [107] for $D = 2$. Also Sect. V in Ref. [118] states this result, but contains a sign error in the second argument of A_C.

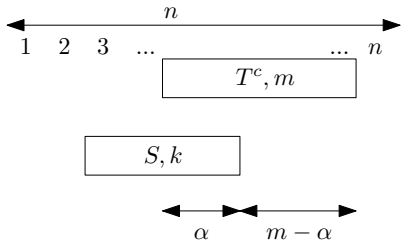


Figure 5.1: Overlap between S and subsets T of size m. The term $\binom{k}{\alpha}$ accounts for the different combinatorial possibilities of elements T^c having overlap α with S. Necessarily, T^c must then have a part of size $m-\alpha$ lying outside of S; there are $\binom{n-k}{m-\alpha}$ ways to obtain this.

one obtains

$$S_j(M,N) = \sum_{k=0}^{n} K_{n-j}(k;n) A'_k(M,N)\,. \tag{5.59}$$

Again, one can write this relation in a more compact form in terms of the unitary enumerator,

$$\begin{aligned}
S_{MN}(x,y) &= \sum_{m=0}^{n} S_m x^{n-m} y^m \\
&= \sum_{m=0}^{n}\sum_{k=0}^{n} K_{n-m}(k;n) A'_k(M,N)\, x^{n-m} y^m \\
&= \sum_{k=0}^{n} A'_k(M,N)\Big[\sum_{m=0}^{n} K_{n-m}(k;n)\, x^{n-m} y^m\Big] \\
&= \sum_{k=0}^{n} A'_k(M,N)\Big[\sum_{m'=0}^{n} K_{m'}(k;n)\, x^{m'} y^{n-m'}\Big] \\
&= \sum_{k=0}^{n} A'_k(M,N)(y+x)^{n-k}(y-x)^k \\
&= A'_{MN}(x+y, y-x)\,.
\end{aligned} \tag{5.60}$$

Above, the second last equality follows from Eq. (118). Thus

$$S_{MN}(x,y) = A'_{MN}(x+y, y-x)\,. \tag{5.61}$$

To obtain the shadow enumerator in terms of the Shor-Laflamme enumerator, we take advantage of Eq. (5.50). Then

$$\begin{aligned}
S_{MN}(x,y) &= A'_{MN}(x+y, y-x) \\
&= A_{MN}\left(\frac{(D-1)x+(D+1)y}{D}, \frac{y-x}{D}\right)\,.
\end{aligned} \tag{5.62}$$

This ends the proof. □

Thus, given the Shor-Laflamme enumerator, one can obtain the shadow enumerator simply by a transform. If any of its coefficients are negative, a corresponding QECC cannot exist.

5.9 New bounds on absolutely maximally entangled states

In this last section, let us return to the question of the existence of absolutely maximally entangled (AME) states. Scott showed in Ref. [44] that a necessary requirement for an AME state of n parties having D levels each to exist, is

$$n \leq \begin{cases} 2(D^2-1) & n \text{ even}, \\ 2D(D+1)-1 & n \text{ odd}. \end{cases} \tag{5.63}$$

We explain now how this bound was obtained by requiring the positivity of the Shor-Laflamme enumerator $A_{\lfloor \frac{n}{2} \rfloor + 2}$. Recall that complementary reductions of pure states share the same spectrum and therefore also the same purity. Thus if $|\phi_{n,D}\rangle$ is a putative AME state of n parties having D levels each, then the coefficients of the unitary enumerator as defined in Eq. (5.44) are given by

$$A'_k(|\phi_{n,D}\rangle) = \binom{n}{k} D^{-\min(k,n-k)} \,. \tag{5.64}$$

Considering the unitary enumerator coefficient $A'_{\lfloor \frac{n}{2} \rfloor + 2}$, only the terms $A_0 = 1$, $A_{\lfloor \frac{n}{2} \rfloor + 1}$, and $A_{\lfloor \frac{n}{2} \rfloor + 2}$ contribute, with appropriate combinatorial prefactors. From Eq. (5.43) [or from the transform in Eq. (5.50)], one obtains

$$\begin{aligned} A'_{\lfloor \frac{n}{2} \rfloor + 2} = D^{-(\lfloor \frac{n}{2} \rfloor + 2)} \Bigg[& \binom{n}{\lfloor \frac{n}{2} \rfloor + 2} A_0 \\ & + \binom{n-(\lfloor \frac{n}{2} \rfloor + 1)}{n-(\lfloor \frac{n}{2} \rfloor + 2)} A_{\lfloor \frac{n}{2} \rfloor + 1} + A_{\lfloor \frac{n}{2} \rfloor + 2} \Bigg] . \end{aligned} \tag{5.65}$$

The term $A_{\lfloor \frac{n}{2} \rfloor + 1}$ in above equation is fixed by the knowledge of $A'_{\lfloor \frac{n}{2} \rfloor + 1}$,

$$A'_{\lfloor \frac{n}{2} \rfloor + 1} = D^{-(\lfloor \frac{n}{2} \rfloor + 1)} \Bigg[\binom{n}{\lfloor \frac{n}{2} \rfloor + 1} A_0 + A_{\lfloor \frac{n}{2} \rfloor + 1} \Bigg] . \tag{5.66}$$

Combining Eqs. (5.64), (5.65), and (5.66), solving for $A_{\lfloor \frac{n}{2} \rfloor + 2}$, and requiring its non-negativity yields then the bound of Eq. (5.63).

Let us now see what the additional constraints from the shadow enumerator yield. Having knowledge of all the unitary enumerator coefficients [Eq. (5.64)], all that is left is to evaluate Eq. (5.59) [or Eq. (5.61) respectively], which relates the shadow enumerator to the unitary enumerator. If any coefficient $S_j(|\phi_{n,D}\rangle)$ happens to be negative, a AME state on n parties having D levels each cannot exist. We should mention that one could also evaluate Eq. (5.4) directly, for a suitable choice of $T \subseteq \{1 \ldots n\}$. To give an example, consider a putative AME state on four qubits, whose non-existence proven by Ref. [86]. Then

$$S_0(|\phi_{4,2}\rangle) = A'_0 - A'_1 + A'_2 - A'_3 + A'_4 = -\frac{1}{2} \,, \tag{5.67}$$

in contradiction to the requirement that all S_j be non-negative.

In Fig. 5.2, the parameters of hypothetical AME states are shown: In dark blue, AME states which are already excluded by the bound from Scott are marked; in

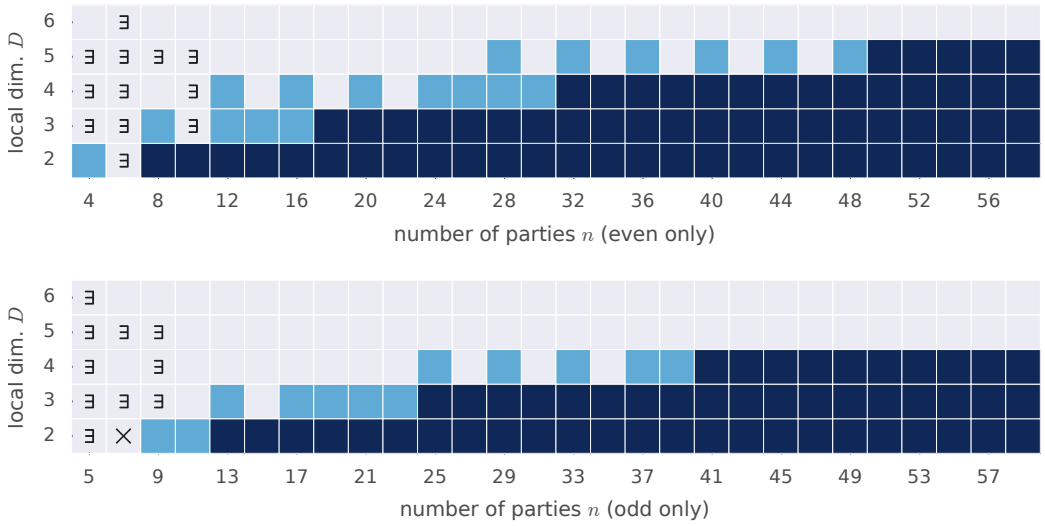


Figure 5.2: In dark blue, AME states which are already excluded by the bound from Scott are marked; in light blue, those AME states for which the negativity of the shadow enumerator coefficients $S_j(|\phi_{n,D}\rangle)$ gives stronger bounds. The non-existence of an AME state having parameters $n = 4$ and $D = 2$ is already known [86]. The AME state with $n = 7$ and $D = 2$ (also marked in blue) is neither exluded by the Scott bound nor by the shadow enumerator, but by Ref. [109]. The symbol $\exists$ marks states which are known to exist, constructions can be found in Refs. [48, 91, 110, 111, 123, 203, 204, 225, 226].

light blue, those AME states for which the negativity of the shadow enumerator coefficients $S_j(|\phi_{n,D}\rangle)$ gives stronger bounds. For Fig. 5.2, all shadow coefficients of hypothetical AME states with local dimension $D \leq 9$ and n not violating the Scott bound have been evaluated. The non-existence of an AME state having parameters $n = 4$ and $D = 2$ is already known [86]. The AME state with $n = 7$ and $D = 2$ (also marked in blue) is neither exluded by the Scott bound nor by the shadow enumerator, but by Ref. [109]. The symbol $\exists$ marks states which are known to exist, constructions can be found in Refs. [48, 91, 110, 111, 123, 203, 204, 225, 226].

We conclude, that additionally to the known non-existence bounds, three-level AME states with

$$n = 8, 12, 13, 14, 16, 17, 19, 21, 23\,; \tag{5.68}$$

four-level AME states with

$$n = 12, 16, 20, 24, 25, 26, 28, 29, 30, 33, 37, 39\,; \tag{5.69}$$

and five-level AME states of

$$n = 28, 32, 36, 40, 44, 48 \tag{5.70}$$

parties do not exist.

5.10 Discussion

Using the quantum weight enumerator machinery originally derived by Shor, Laflamme and Rains, we obtained bounds on the existence of absolutely maximally entangled states in higher dimensions. For this, we used the so-called shadow inequalities, which constrain the possible correlations arising from quantum states (also see Sect. 5.11.1). Additionally, we provided a proof of the quantum MacWilliams transform in the Bloch representation, clarifying its physical interpretation. It should be possible to apply the shadow inequalities also to investigate the existence of maximally entangled states whose subsystems have differing local dimensions.

For future work, it would be interesting to see what the generalized shadow inequalities involving higher-order invariants [129] imply for the distribution of correlations in QECC and multipartite quantum states.

5.11 Further results

5.11.1 A generalization of the universal state inversion from the shadow inequalities

Here, I introduce a generalization of the universal state inversion that naturally arises from the shadow inequality. It also incorporates an extension of the Breuer-Hall map to many particles, and can, similar to the reduction criterion, be used to detect entanglement. Recall that the *universal state inversion* already generalizes the *reduction map* and the *reduction criterion* (c.f. Sect. 1.1.6). It is given by [35–37] [5]

$$\mathcal{I}[\varrho] = \sum_{S\subseteq\{1\dots n\}} (-1)^{|S|} \varrho_S \otimes \mathbb{1}_{S^c}\,, \tag{5.71}$$

where $\varrho_S = \mathrm{Tr}_{S^c}\,\varrho$. Note that it can also be written as

$$\mathcal{I}[\varrho] = \bigotimes_j (\mathbb{1}_j\,\mathrm{Tr}_j - \mathbb{1})[\varrho]\,. \tag{5.72}$$

As with the reduction criterion, the universal state inversion can detect entanglement: If $(\mathcal{I}_A \otimes \mathbb{1}_B)[\varrho] < 0$, then ϱ must be entangled across the bipartition $A|B$.

In Sect. 5.5, I introduced the shadow inequality as established by Rains: For any two positive semi-definite operators M and N, and a fixed subset $T \subseteq \{1\dots n\}$, the following expression is non-negative

$$\sum_{S\subseteq\{1\dots n\}} (-1)^{|S\cap T|}\,\mathrm{Tr}[\mathrm{Tr}_{S^c}(M)\,\mathrm{Tr}_{S^c}(N)] \geq 0\,. \tag{5.73}$$

Naturally, if $M = N = \varrho$, the above inequality takes the form of

$$\sum_{S\subseteq\{1\dots n\}} (-1)^{|S\cap T|}\,\mathrm{Tr}[\varrho_S^2] \geq 0\,. \tag{5.74}$$

Thus the shadow inequality represents an exponentially large family of relations that constrain the distribution of entanglement of multipartite states in terms of purities of its reductions [6]. A analogous relation in terms of Von Neumann entropies instead of purities has shown to not hold, as the expression generally can take either sign [227].

Interestingly, the shadow inequality can also be seen as a generalization of the universal state inversion. Let us define the *T-inversion map*:

Definition 14. *Let $T \subseteq \{1\dots n\}$. The T-inversion map $\mathcal{I}_T$ on a system of n parties is given by*

$$\mathcal{I}_T[\cdot] = \sum_{S\subseteq\{1\dots n\}} (-1)^{|S\cap T|}\,\mathrm{Tr}_{S^c}[\cdot] \otimes \mathbb{1}_{S^c}\,. \tag{5.75}$$

If M is an operator, denote by $\tilde{M}_{(T)} = \mathcal{I}_T[M]$ its T-inversion.

[5] A two-partite version of the universal state inversion already appeared in Refs. [33, 34].

[6] This is why it can be used to investigate the existence of QECC and AME states, as shown in the main part of this Chapter.

Similar to the universal state inversion, the T-inversion $\mathcal{I}_T$ is a positive map.

Corollary 4. *The map $\mathcal{I}_T$ is positive for all $T \subseteq \{1 \dots n\}$.*

Proof. Let M be a positive semi-definite operator, $M \geq 0$. Consider Eq. (5.73): Note that given a specific operator M, one can choose $N \geq 0$ freely. In particular, consider $N = |\phi\rangle\langle\phi|$ to be a random unit vector. Then

$$\begin{aligned} \mathrm{Tr}[\mathrm{Tr}_{S^c}(M)\,\mathrm{Tr}_{S^c}(|\phi\rangle\langle\phi|)] &= \mathrm{Tr}[(\mathrm{Tr}_{S^c}(M) \otimes \mathbb{1}_{S^c})|\phi\rangle\langle\phi|] \\ &= \langle\phi|\,(\mathrm{Tr}_{S^c}(M) \otimes \mathbb{1}_{S^c})\,|\phi\rangle\ . \end{aligned} \tag{5.76}$$

Inserting this into the definition of $\mathcal{I}_T$ in Eq. (5.75) yields

$$\mathcal{I}_T[M] = \langle\phi|\Big(\sum_{S\subseteq\{1\dots n\}} (-1)^{|S\cap T|}\,\mathrm{Tr}_{S^c}[M] \otimes \mathbb{1}_{S^c}\Big)\,|\phi\rangle \geq 0 \qquad \forall\,|\phi\rangle\ . \tag{5.77}$$

Therefore, given a positive operator M, its T-inversions $\mathcal{I}_T[M]$ are positive for all $T \subseteq \{1 \dots n\}$. This ends the proof. □

Choosing $T = \{1 \dots n\}$, one recovers the universal state inversion from Eq. (5.71), $\mathcal{I}_{\{1\dots n\}}[M] = \mathcal{I}[M]$. While $\mathcal{I}_T$ is positive map, it is however not completely positive. Thus if $(\mathcal{I}_T \otimes \mathbb{1})[\varrho] < 0$, then ϱ must be entangled.

The T-inversion as a fine-graining of the reduction map.

The T-inversions with $|T|$ odd form a kind of fine-graining of the reduction map $\mathcal{R}[\varrho] = \mathbb{1} - \varrho$, in the sense made precise below.

Proposition 17. *For any operator ϱ,*

$$\sum_{\substack{T\subseteq\{1\dots n\}\\ |T|\ odd}} \mathcal{I}_T[\varrho] = 2^{n-1}(\mathbb{1} - \varrho)\,. \tag{5.78}$$

Proof. We have to evaluate

$$\sum_{\substack{T\subseteq\{1\dots n\}\\ |T|\ \mathrm{odd}}} \mathcal{I}_T[\varrho] = \sum_{\substack{T\subseteq\{1\dots n\}\\ |T|\ \mathrm{odd}}} \sum_{S\subseteq\{1\dots n\}} (-1)^{|S\cap T|}\varrho_S \otimes \mathbb{1}_{S^c}\,. \tag{5.79}$$

Let us now examine the contribution of these sums to a single term of the form $\varrho_S \otimes \mathbb{1}_{S^c}$. Let S be of size k with $0 < k < n$, and consider those subsets T of size m that have an overlap of size α with S. Then T must have an overlap of size $\beta = m - \alpha$ with S^c. If α is odd, then β must be even, and vice versa; this follows from T being odd. Then there are

$$\Big[\sum_{\alpha\ \mathrm{odd}} \binom{k}{\alpha}\Big]\Big[\sum_{\beta\ \mathrm{even}} \binom{n-k}{\beta}\Big] \tag{5.80}$$

terms acquiring a negative sign from $(-1)^{|T\cap S|}$, and

$$\Big[\sum_{\alpha\ \mathrm{even}} \binom{k}{\alpha}\Big]\Big[\sum_{\beta\ \mathrm{odd}} \binom{n-k}{\beta}\Big] \tag{5.81}$$

yielding a positive sign. But

$$\sum_{\alpha \text{ odd}} \binom{k}{\alpha} = \sum_{\alpha \text{ even}} \binom{k}{\alpha} = 2^{k-1}\,, \tag{5.82}$$

and

$$\sum_{\beta \text{ even}} \binom{n-k}{\beta} = \sum_{\beta \text{ odd}} \binom{n-k}{\beta} = 2^{n-k-1}\,. \tag{5.83}$$

Thus, all positive and all negative terms cancel. However, if $|S| = 0$, no odd overlap α can possibly exist. Similarly, if $|S| = n$, no odd overlap β exists. Therefore, these terms do not cancel: In the case of S being the empty set, 2^{n-1} terms acquire a positive sign from $(-1)^{|S\cap T|}$; and conversely, 2^{n-1} terms acquire a negative sign in the case of $S = \{1 \dots n\}$. We are left with

$$\sum_{\substack{T\subseteq\{1\dots n\}\\ |T| \text{ odd}}} \mathcal{I}_T[\varrho] = 2^{n-1}(\mathbb{1} - \varrho)\,. \tag{5.84}$$

This ends the proof.

□

Thus the odd T-inversions form a *fine-graining* of the reduction map,

$$\mathcal{R}[\cdot] = \frac{1}{2^{n-1}} \sum_{|T| \text{ odd}} \mathcal{I}_T[\cdot]\,. \tag{5.85}$$

Consequently, ϱ and all its odd inversions form a POVM (c.f. Sect. 1.1.3),

$$\varrho + \frac{1}{2^{n-1}} \sum_{|T| \text{ odd}} \mathcal{I}_T[\varrho] = \mathbb{1}\,. \tag{5.86}$$

Let us explain the connections of the T-inversion to the weight enumerator theory introduced earlier in this Chapter: Note that the coefficients of the shadow enumerator [c.f. Eq. (5.16)] are given by [7]

$$S_j(\mathcal{Q}) = \sum_{|T^c|=j} \mathrm{Tr}(\mathcal{I}_T[\mathcal{Q}]\mathcal{Q})\,. \tag{5.87}$$

Additionally, for pure states $\varrho = |\phi\rangle\langle\phi|$ and $|T|$ odd it holds that

$$\mathrm{Tr}(\mathcal{I}_T[\varrho]\varrho) = 0\,. \tag{5.88}$$

This follows from the fact that for pure states,

$$(\varrho_A \otimes \mathbb{1}_B)\varrho_{AB} = (\mathbb{1}_A \otimes \varrho_B)\varrho_{AB}\,. \tag{5.89}$$

Thus when expanding $\mathcal{I}_T[\varrho]$, if ϱ_S happens to have a positive sign, ϱ_{S^c} will obtain a negative sign, and vice versa. Thus all terms in $\mathrm{Tr}(\mathcal{I}_T[\varrho]\varrho)$ cancel pairwise. We conclude that $S_j(\mathcal{Q}) = 0$ if $(n-j)$ is odd in the case of pure quantum states or self-dual codes. Also note that in the case of qubits, $S_0(\mathcal{Q})$ is the n-concurrence [198], vanishing for an odd number of parties.

[7] Note that $S_0(\mathcal{Q})$ corresponds to $T = \{1 \dots n\}$, and S_j corresponds to having $(n-j)$ minus signs appearing in the inversions. This originates from the definition of the shadow enumerator [107, 118].

A further extension of the T-inversion

One can further generalize the shadow inequalities, and with it, the T-inversion. This is done by introducing additional parameters, and by incorporating terms similar to those which appear in the Breuer-Hall map (c.f. Sect. 1.1.5).

Theorem 30. *For $0 \leq \alpha, \beta \leq 1$, the following map is positive,*

$$\mathcal{I}_T(\alpha,\beta)[\cdot] = \sum_S (-1)^{|S\cap T|}\, \alpha^{|S\cap T|}\, \beta^{|S\cap T^c|}\, \mathrm{Tr}_{S^c}[\cdot] \otimes \mathbb{1}_{S^c}\,. \tag{5.90}$$

Proof. We generalize the proof from Ref. [46] in a straightforward way. Note that Eq. (5.90) can be expressed as

$$\mathcal{I}_T(\alpha,\beta)[\cdot] = \bigotimes_{j\in T} \Big(\mathbb{1}_j \,\mathrm{tr}_j \,-\alpha \mathbb{1}_j\Big) \bigotimes_{j'\notin T} \Big(\mathbb{1}_{j'}\,\mathrm{tr}_{j'} \,+\beta \mathbb{1}_{j'}\Big)[\cdot]\,. \tag{5.91}$$

We need following useful formulae, as shown in Observation 26 and in Ref. [46]: Denote by $\{h_i\}$ an orthonormal operator basis. Then

$$\mathrm{tr}[\varrho]\mathbb{1} = \frac{1}{D}\sum_{i=0}^{D^2-1} h_i \varrho h_i^\dagger\,, \tag{5.92}$$

$$\varrho^T = \frac{1}{D}\sum_{i=0}^{D^2-1} h_i^T \varrho h_i^\dagger\,. \tag{5.93}$$

Denote by $\{k_i\}$ the real generalized Gell-Mann matrices (consisting of $\{x_{jk}\}$ and $\{z_l\}$) and by $\{y_i\}$ the imaginary generalized Gell-Mann matrices [c.f. Eq. (1.102) in Sect. 1.1.7]. They form an orthonormal Hermitian basis, with $k_i^T = k_i^* = k_i$, and $y_i^T = y_i^* = -y_i$. Then

$$\begin{aligned}
\Big[\mathbb{1}\,\mathrm{tr}[\varrho] \,-\, \alpha\varrho\Big] &= \Big[\mathbb{1}\,\mathrm{tr}[\varrho^T] \,-\, \alpha\varrho^T\Big]^* \\
&= \Big[\frac{1}{D}\sum_i (h_i\varrho h_i^\dagger \,-\, \alpha h_i^T \varrho h_i^\dagger)\Big]^* \\
&= \frac{1}{D}\Big[(1+\alpha)\sum_i y_i\varrho y_i \,+\, (1-\alpha)\sum_i k_i\varrho k_i\Big]^* \\
&= \frac{1}{D}\Big[(1+\alpha)\sum_i y_i\varrho^* y_i \,+\, (1-\alpha)\sum_i k_i\varrho^* k_i\Big] \\
&= \frac{1}{D}\Big[(1+\alpha)\sum_i y_i\varrho^T y_i \,+\, (1-\alpha)\sum_i k_i\varrho^T k_i\Big]\,.
\end{aligned} \tag{5.94}$$

Similarly,

$$\Big[\mathbb{1}\,\mathrm{tr}[\varrho] \,+\, \beta\varrho\Big] = \frac{1}{D}\Big[(1-\beta)\sum_i y_i\varrho^T y_i \,+\, (1+\beta)\sum_i k_i\varrho^T k_i\Big]\,. \tag{5.95}$$

Denote by $y_i^{(j)}$ and $k_i^{(j)}$ Gell-Mann matrices acting on subsystem j, and by $[\cdot]^{T_j}$ the partial transpose on subsystem j. Then, Eq. (5.91) can be written as

$$\begin{aligned}\mathcal{I}_T(\alpha,\beta)[\cdot] &= \bigotimes_{j\in T}\Big(\mathbb{1}_j\,\mathrm{tr}_j - \alpha\mathbb{1}_j\Big)\bigotimes_{j'\notin T}\Big(\mathbb{1}_{j'}\,\mathrm{tr}_{j'} + \beta\mathbb{1}_{j'}\Big)[\cdot]\\ &= D^{-n}\bigotimes_{j\in T}\Big[(1+\alpha)\sum_i y_i^{(j)}[\cdot]^{T_j}y_i^{(j)} + (1-\alpha)\sum_i k_i^{(j)}[\cdot]^{T_j}k_i^{(j)}\Big]\\ &\quad\bigotimes_{j'\notin T}\Big[(1-\beta)\sum_i y_i^{(j')}[\cdot]^{T_{j'}}y_i^{(j')} + (1+\beta)\sum_i k_i^{(j')}[\cdot]^{T_{j'}}k_i^{(j')}\Big]. \qquad (5.96)\end{aligned}$$

Note that the partial transposition of all subsystems yields a global transposition. Therefore $\mathcal{I}_T(\alpha,\beta)$ is for $0\leq\alpha,\beta\leq 1$ a *co-positive*, but not completely positive, map. This means it can be written as

$$\mathcal{I}_T(\alpha,\beta) = \mathcal{L}\circ\mathcal{T}\,, \qquad (5.97)$$

where $\mathcal{L}$ is a positive map that can be written in Kraus form [8]. This ends the proof. □

If $(\mathcal{I}_{T,A_1\ldots A_k}(\alpha,\beta)\otimes\mathbb{1}_{B_1\ldots B_l})[\varrho] < 0$, then ϱ must be entangled. Note that for $\beta = 0$, Eq. (5.91) yields the universal inversion on the reduced state tensored by the identity,

$$\mathcal{I}_T(\alpha,\beta=0) = \mathcal{I}[\mathrm{Tr}_{T^c}(\varrho)]\otimes\mathbb{1}_{T^c}\,. \qquad (5.98)$$

Note that for $\alpha=\beta=1$, this map equals the T-inversion. Thus the above derivation represents an alternative proof of the shadow inequality in Eq. (5.73). A natural extension of this map follows by associating individual coefficients $0\leq\alpha_j,\beta_{j'}\leq 1$ to each subsystem.

Furthermore, it is possible to incorporate the features of the *Breuer-Hall map*: Recall from Sect. 1.1.6 that this is the map given by [31, 32]

$$\mathcal{R}_{BH}[X] = \mathrm{Tr}(X)\mathbb{1} - X - UX^TU^\dagger. \qquad (5.99)$$

for any U with $U^T=-U$ and $U^\dagger U\leq\mathbb{1}$. The map $\mathcal{R}_{BH}$ is non-decomposable if U is additionally unitary for $D>2$ [9]. This ingredient can be incorporated in Eq.(5.96) by replacing the following terms

$$\sum_i y_i^{(j)}[\cdot]^{T_j}y_i^{(j)} \qquad\longrightarrow\qquad \sum_i y_i^{(j)}[\cdot]^{T_j}y_i^{(j)} - U^{(j)}[\cdot]^{T_j}U^{(j)\dagger}\,, \qquad (5.100)$$

where $U^{(j)^T} = -U^{(j)}$ and $U^{(j)^\dagger}U^{(j)}\leq\mathbb{1}$. Note that $\mathcal{I}_T(\alpha,\beta)$ and its Breuer-Hall modified form are positive but not completely positive maps that generalize the reduction criterion. Thus they can be used for entanglement detection. One could ask under what conditions the Breuer-Hall modified map may also be non-decomposable. While I did not check this, one could expect this to be the case if the antisymmetric $U^{(j)}$ are unitary.

[8] Recall that a map is positive if and only if it is of the form $\varrho\to\varrho' = \sum_i A_i\varrho A_i^\dagger$. Because the Gell-Mann matrices are Hermitian, the above map is indeed co-positive.

[9] Note that in case of $D=2$, one could simply choose U to be the Pauli matrix Y. However, $\mathcal{R}_{BH}[\cdot]$ is then a trivial mapping to the zero matrix, as can be seen from Eq. (5.94).

5.11.2 An application to the quantum marginal problem

As presented in Sect. 1.2.6, Butterley et al. derived a condition for the subsystems $\varrho_{12}, \varrho_{13}, \varrho_{23}$ to be reductions of a joint three-qubit state ϱ_{123} [36]. Defining

$$\Delta = \mathbb{1} - \varrho_1 - \varrho_2 - \varrho_3 + \varrho_{12} + \varrho_{13} + \varrho_{23}\,, \tag{5.101}$$

then for $\varrho_{12}, \varrho_{23}, \varrho_{13}$ to be compatible with a joint state ϱ_{123}, the quantum Bell-Wigner inequality must hold

$$0 \leq \Delta \leq \mathbb{1}\,. \tag{5.102}$$

While this condition is necessary, it is not sufficient for a joint state to exist [37]. With the T-inversion $\mathcal{I}_T$ defined in Eq. (5.75), one can extend this to multiple conditions valid for all finite dimensions.

Proposition 18 (Extended quantum Bell-Wigner inequalities)**.** *Consider the putative reductions $\varrho_{12}, \varrho_{13}, \varrho_{23}$ of a three-partite state of arbitrary finite local dimensions having compatible one-body marginals. If a compatible join state ϱ_{123} exists, then*

$$\begin{aligned}
&\mathbb{1} - \varrho_1 - \varrho_2 - \varrho_3 + \varrho_{12} + \varrho_{13} + \varrho_{23} \geq 0\,,\\
&\mathbb{1} - \varrho_1 + \varrho_2 + \varrho_3 - \varrho_{12} - \varrho_{13} + \varrho_{23} \geq 0\,,\\
&\mathbb{1} + \varrho_1 - \varrho_2 + \varrho_3 - \varrho_{12} + \varrho_{13} - \varrho_{23} \geq 0\,,\\
&\mathbb{1} + \varrho_1 + \varrho_2 - \varrho_3 + \varrho_{12} - \varrho_{13} - \varrho_{23} \geq 0\,,
\end{aligned} \tag{5.103}$$

where we wrote ϱ_1 for $\mathrm{Tr}_{23}(\varrho) \otimes \mathbb{1}_{23}$.

Proof. Consider those T-inversions where $|T|$ is odd. Then the expression $\mathcal{I}_T(\varrho) + \varrho$ yields the four inequalities above. □

Similar compatibility equations can be obtained for an arbitrary number n of parties and local dimensions by noting that the expression $\mathcal{I}_T[\varrho] + \varrho$ is positive and will only ever contain marginals of size smaller or equal than $(n-1)$ if $|T|$ is chosen to be odd. Let us state this more formally.

Proposition 19. *Let $\varrho_{1^c}, \ldots \varrho_{n^c}$ be putative marginals of size $(n-1)$ with compatible reductions. A necessary condition for a compatible joint state on n parties to exist, is*

$$\sum_{S \subsetneq \{1 \ldots n\}} (-1)^{|S \cap T|} \varrho_S \geq 0\,, \tag{5.104}$$

for all T with $|T|$ odd. Note that the sum above runs over all proper subsets of $\{1 \ldots n\}$.

As an example, Prop. 19 yields with choosing $T = \{1\}$ the following QMP-criterion three-party marginals ϱ_{ijk} to be compatible with a joint four-party state ϱ_{1234},

$$\begin{aligned}
&\mathbb{1} - \varrho_1 + \varrho_2 + \varrho_3 + \varrho_4 - \varrho_{12} - \varrho_{13} - \varrho_{14} + \varrho_{23} + \varrho_{24} + \varrho_{34}\\
&- \varrho_{123} - \varrho_{124} - \varrho_{134} + \varrho_{234} \geq 0\,.
\end{aligned} \tag{5.105}$$

Interestingly, a condition analogous to Eq. (5.104) is in the classical case both necessary *and* sufficient for a joint state to exist [36].

Lastly, in order for a *pure* joint state to exist in the case of qubits, Δ in Eq. (5.101) must necessarily be a projector of rank two. This follows from the fact that in the case of qubits, a pure state stays pure under the state inversion,

$$\mathcal{I}_{123}[|\phi\rangle\langle\phi|] = \sigma_y^{\otimes 3}(|\phi\rangle\langle\phi|)^T\sigma_y^{\otimes 3}\,, \tag{5.106}$$

and is, according to Eq. (5.88), also orthogonal to $|\phi\rangle$. Therefore $\Delta = \mathcal{I}_{123}[|\phi\rangle\langle\phi|] + |\phi\rangle\langle\phi|$ must be of rank two.

5.11.3 A strong subadditivity - like expression for the linear entropy

In Sect. 1.1.5, I introduced the von Neumann entropy, $S(\varrho) = -\operatorname{Tr}\varrho\log(\varrho)$. Recall that the strong subadditivity (SSA) holds, which requires for any tripartite state that [20]

$$S(\varrho_{123}) + S(\varrho_2) \leq S(\varrho_{12}) + S(\varrho_{23})\,. \tag{5.107}$$

This can be restated in a different way: purify ϱ_{123} by a fourth party. Then, $S(\varrho_{123}) = S(\varrho_4)$ and $S(\varrho_{12}) = S(\varrho_{34})$, and Eq. (5.107) yields $S(\varrho_4) + S(\varrho_2) \leq S(\varrho_{34}) + S(\varrho_{23})$. By a relabeling of the parties, one obtains

$$S(\varrho_1) + S(\varrho_3) \leq S(\varrho_{12}) + S(\varrho_{23})\,. \tag{5.108}$$

Let us now state a remarkably similar relation for the linear entropies of reductions, which are defined as

$$S_L(\varrho_S) = \frac{D}{D-1}[1 - \operatorname{tr}(\varrho_S^2)]\,. \tag{5.109}$$

Proposition 20. *Let ϱ_{123} be a tripartite state of arbitrary local dimensions. Then, it must fulfill*

$$S_L(\varrho_1) + S_L(\varrho_3) \leq S_L(\varrho_{12}) + S_L(\varrho_{23}) + 2S_L(\varrho_{123})\,. \tag{5.110}$$

Proof. Let us regard the inversions $\mathcal{I}_{(12)}$ and $\mathcal{I}_{(23)}$ of ϱ_{123}, where the parties $1\,\&\,2$ and $2\,\&\,3$ respectively are grouped together.

$$\begin{aligned}\mathcal{I}_{(12)}[\varrho] &= \mathbb{1} - \varrho_{12} + \varrho_3 - \varrho_{123} \geq 0\,,\\ \mathcal{I}_{(23)}[\varrho] &= \mathbb{1} + \varrho_1 - \varrho_{23} - \varrho_{123} \geq 0\,.\end{aligned} \tag{5.111}$$

Adding the two equations, we obtain

$$2\mathbb{1} + \varrho_1 + \varrho_3 - \varrho_{23} - \varrho_{12} - 2\varrho_{123} \geq 0\,. \tag{5.112}$$

Multiplying by ϱ_{123} and taking the trace, we obtain the following constraint

$$2 + \operatorname{tr}(\varrho_1^2) + \operatorname{tr}(\varrho_3^2) \geq \operatorname{tr}(\varrho_{12}^2) + \operatorname{tr}(\varrho_{23}^2) + 2\operatorname{tr}(\varrho_{123}^2)\,, \tag{5.113}$$

which can brought to the form of

$$S_L(\varrho_1) + S_L(\varrho_3) \leq S_L(\varrho_{12}) + S_L(\varrho_{23}) + 2S_L(\varrho_{123})\,. \tag{5.114}$$

This ends the proof. □

For pure states, $S_L(\varrho_{123}) = 0$, and equality holds in Prop. 20.

5.11.4 Further non-existence results of qubit-codes

Recall new codes can be obtained from reductions of pure codes (c.f. Sect. 1.2.4):

Theorem 31 (Rains [118], Theorem 20)**.** *Suppose $\mathcal{Q}$ is a pure $((n, K, d))_D$ code with $n, d \geq 2$. Then there exists a pure $((n-1, DK, d-1))_D$.*

This excludes the existence of a $((13, 1, 6))_2$, $((25, 1, 10))_2$, and $((31, 1, 12))_2$ as only *impure* $((12, 2, 5))_2$, $((24, 2, 9))_2$, and $((30, 2, 11))_2$ codes could possibly exist from the linear programming bound in Eq. (1.182) [209].

5.11.5 Weight distributions of hypothetical codes

Here, I list hypothetical weight distributions of self-dual codes having distance $d = \lfloor \frac{n}{2} \rfloor$. That is, these are hypothetical states which are almost $\lfloor \frac{n}{2} \rfloor$-uniform, approximating AME states. The weight distributions below were obtained by the linear program as described in Eq. (1.182). Only non-negative weights with $j \geq d$ are listed, because $A_0 = 1$ and $A_{j<d} = 0$ for all self-dual codes.

$$
\begin{aligned}
((8,1,4))_3: &\quad [32, 320, 1088, 2560, 2560] \\
((12,1,6))_3: &\quad [480, 3456, 15120, 55520, 133920, 193536, 129408] \\
((16,1,8))_3: &\quad [6720, 37760, 188160, 881664, 2916480, 7123200, \\
&\quad 12284160, 13068288, 6540288] \\
((20,1,10))_3: &\quad [95840, 385280, 2297280, 12685440, 48653760, 155818752, \\
&\quad 392454960, 734998560, 982256480, 826462720, 330675328] \\
((24,1,12))_3: &\quad [1394624, 3233664, 29284992, 174344192, 713873952, \\
&\quad 2763516096, 8619269120, 21623196672, 43440522048, \\
&\quad 66060142720, 72121509504, 50158439424, 16720809472] \\
((12,1,6))_4: &\quad [324, 9936, 71685, 508320, 2266020, 6187536, 7733394]
\end{aligned} \tag{5.115}
$$

5.12 Conclusion

From this work it emerges that certain methods in quantum error correction and multipartite entanglement are strongly connected: The shadow enumerator as known from QECC represents an exponentially large family of inequalities that constrain the distribution of entanglement in multipartite systems. It thus can be used to investigate the existence of multipartite states and QECC. It is furthermore naturally related to a fine-graining of the well-known reduction map, and can be used for entanglement detection.

Nevertheless, many questions still remain: In the case of stabilizer states, the dual code corresponds to the normalizer of the stabilizer. However, this dual code is a proper code only in the classical theory, what is its nature in the quantum domain? Can a natural extension of this notion also be found for non-stabilizer codes? Can stronger conditions on code existence be obtained from the shadow enumerator of the dual code? As shown, all odd T-inversions of a given QECC form a projector onto its orthogonal subspace. What is the nature of these odd T-inversions, do

they form interesting QECC themselves? A higher dimensional system can be split into smaller subsystems, thus the shadow enumerator and the corresponding T-inversions can further be refined. Can this be applied to solve higher dimensional existence problems of AME states and QECC [10]?

As already noted by Rains, it would be interesting to see what the generalized shadow inequalities imply for the distribution of correlations in QECC and multipartite quantum states [129]. These relate higher-order invariants of quantum states and codes in a monogamy-like ways. It would be desirable to incorporate these higher-order invariants in terms of higher-order weight enumerators to strengthen the linear programming approach as introduced by Calderbank et al. [108].

[10] As an example, the hitherto unresolved case of a four-partite AME state with $D = 6$ could be approached by decomposing the state into four qubits and four qutrits. Then a semidefinite program similar to Eq. (1.182) can be used to test for the existence of such state. While the approach is promising, the currently known relations are yet insufficient to yield a contradiction.

Summary and outlook

In this thesis, I explored the relation between the whole and its parts in quantum states. For this, methods borrowed from statistics, graph theory, and from the theory of quantum error correction turned out to be fruitful.

Together with my co-author, I developed methods to detect states that can neither be obtained as ground or thermal states of Hamiltonians, nor as convex combinations thereof [A]. Such states can be regarded as being more complex, because they cannot be reconstructed from few-body measurements and from the maximum entropy method alone. The approach can be seen as an extension of the concept of entangled states, which likewise cannot be obtained as convex combinations from states that are reconstructable by their one-body marginals. Our results allow to experimentally test with a witness whether three-body or higher-order interactions are present. For future work, it would be of interest to characterize the entanglement properties of the set of ground and thermal states of few-body Hamiltonians; e.g. to determine whether the entanglement in these states is bounded, or whether they can be simulated classically in any efficient manner.

A question that arose during this project was concerned with states of four qubits: namely, whether or not pure four-qubit states are already determined by their two-body reductions. We could successfully address this problem, and showed that in fact generic pure four-*qudit* states are uniquely determined amongst all pure states by already three of their six different two-party marginals [B]. Moreover, from this follows that almost all pure states of an arbitrary number of qudits are determined by a set of three marginals having size $(n-2)$.

We subsequently analyzed pure qubit states in terms of their even- and odd-body correlations [C]. We found intricate relations between these sets of correlations, either set of correlations often completely determining the state up to a few parameters. This led to explicit reconstruction formulae for the missing correlations. Our results are applicable to deduce certain properties of ground states, to obtain invariants under unitary time evolution, and to simplify specific tasks in entanglement detection. Naturally, one may ask if similar relations also hold for states whose parties have higher dimensions; we think this would be an interesting question to consider for future research.

Let us turn to the possible correlations that quantum states can exhibit. We made significant progress on the question of the existence of certain highly entangled states known as absolutely maximally entangled (AME). In particular, we solved the last open case concerning qubits by proving the non-existence of an absolutely maximally entangled state of seven parties [D]. For this, we developed new methods to understand the algebraic structure of quantum states, using the Bloch representa-

tion as a mean to investigate pure states. At first sight, this may seem to complicate the analysis of the question at hand, as guaranteeing the positivity of an operator by its Bloch coefficients is generally difficult. On closer inspection however, this requirement was already satisfied by assumption, and the Bloch representation allowed us to take advantage of certain signature properties of these states, such as the uniform spectrum of its marginals, in a straightforward way. Such an approach can be seen as being complementary to that of representing pure states by kets, where positivity is guaranteed by construction. This allowed us to solve the case of seven qubits, and to rederive all known results concerning qubits in a very simple manner. We could also identify a best approximation to a seven qubit AME state, and developed an iterative semi-definite program to numerically search for such highly entangled states. As all presently known AME states are of the stabilizer state type, this leaves the question open whether or not this is the case for all absolutely maximally entangled states. The next "small" candidate for an AME state is one of four parties, having six levels each, and settling the question of its existence would provide new insights into AME states of non-prime dimensional systems.

We have introduced the Ulam graph reconstruction problem for graph states to examine the quantum marginal problem when having access to unlabeled marginals only [E]. In contrast to classical collections (so-called graph decks) of vertex-deleted subgraphs, the full quantum graph state can already be reconstructed, up to local unitaries, from a single marginal in the deck. As for the classical case, the question of detecting illegitimate decks, which do not originate from joint states, is of interest. Indeed it is possible to state conditions on the weight distribution for a deck to originate from a joint state. This already allows to detect illegitimate decks consisting of marginals having size $\lfloor \frac{n}{2} \rfloor + 1$. It would be interesting to understand if similar constraints can also be obtained for classical decks.

Lastly, we provided a systematic method to investigate the existence of absolutely maximally entangled states in higher dimensions: with the help of the weight enumerator machinery known from quantum error correction, we could disprove the existence of an additional 27 higher-dimensional AME states [F]. Moreover, we presented a proof of a remarkable relation known as the quantum MacWillams identity in the Bloch representation, and could interpret the shadow inequalities as an exponentially large family of monogamy-like relations that constrain the distribution of entanglement in all finite dimensions. With the shadow inequalities, one furthermore obtains a generalization and fine-graining of the reduction map. In the light of these results, a possibly fruitful line of research would consist of investigating the generalized shadow inequalities as derived by Rains [129]: these could likely be used to obtain monogamy relations involving higher-order polynomial invariants. Also, a more thorough understanding of the nature of the dual code and of the state inversions seem to be promising avenues of research, and may allow to obtain stronger bounds on the existence of quantum error-correcting codes and highly entangled quantum states.

Acknowledgments

I first and foremost want to thank my supervisor Otfried Gühne for his guidance, patience, and encouragement. As I started with little to no knowledge of quantum information, his easy-to-understand explanations were key for my contribution to this field. A special thank goes to Jens Siewert for inofficially co-supervising me, and for inviting me to Bilbao for work and excellent fish dishes. I am indebted to my co-authors Christopher Eltschka, Simone Severini, and Nikolai Wyderka for their efforts in our joint works and for sharing their valuable insights.

A particular thank goes to my office mate Marius Paraschiv and the whole ET crew which helped to transform our after-lunch time into a window of productivity, and to Nikolai Wyderka for his tireless and always good-humored efforts in programming and calculations. I want to thank Tristan Kraft for brewing excellent beer and for proof-reading large parts of this work. Special thanks also goes to my climbing partner Gael Sentís for sharing his enthusiasm in research and on the wall.

I want to thank all my friends and colleagues in the TQO group, Sanah Altenburg, Atul Singh Arora, Ali Asadian, Fabian Bernards, Costandino Budroni, Shin-Liang Chen, Ana Cristina Sprotte Costa, Mariami Gachechiladze, Martin Hofmann, Jannik Hoffmann, Fabiano Lever, Andreas Ketterer, Matthias Kleinmann, Nikolai Miklin, Tobias Moroder, Christina Ritz, Roope Uola, Ritabrata Sengupta, Cornelia Spee, Jiangwei Shang, Frank E. S. Steinhoff, Timo Simnacher, Sabine Wölk, and Xiao-Dong Yu. A special thanks goes to our kind secretary Daniela Lehmann, taking care of any bureaucratic obstacles.

I am particularly glad for many productive exchanges with Dardo Goyeneche about AME states, equiangular tight frames, and the Hadamard Conjecture. I would like to thank Markus Grassl for visiting our group and for introducing me to the theory of quantum error-correcting codes. I am indebted to Hans-Jörg Briegel, Jens Eisert, Marcus Huber, Andreas Osterloh, Jens Siewert, Simone Severini, and Karol Życzkowski for their invitations to visit their groups. I thank Daniel Alsina, Sönke Niekamp, Sara Di Martino, Jens Eisert, Nikolai Friis, Tobias Galla, Dardo Goyeneche, Marcus Huber, Joshua Lockhart, Christian Majenz, Marcin Pawłowski, Marco Piani, Zahra Raissi, Ingo Roth, David Sauerwein, Christian Schilling, Albert Werner, and Karol Życzkowski for fruitful discussions regarding the topics I present in this thesis.

This work was generously supported by the German Research Foundation ("Characterizing multiparticle correlations with exponential families"), the COST Action MP1209, and the Swiss National Science Foundation (Doc.Mobility grant 165024, "Thermal and ground states of local Hamiltonians").

Finally, I want to thank my family and friends at home, and Lisa for her steadfast support and love.

Appendix: Krawtchouk polynomials

The Krawtchouk (also Kravchuk) polynomials are, for $n, k \in \mathbb{N}_0$ and $n - k \geq 0$, defined as [11]

$$K_m(k;n) = \sum_\alpha (-1)^\alpha \binom{n-k}{m-\alpha}\binom{k}{\alpha}. \tag{116}$$

If $m < 0$, $K_m(k;n) = 0$. The generating function of the Krawtchouk polynomial is

$$\sum_m K_m(k;n) z^m = (1+z)^{n-k}(1-z)^k. \tag{117}$$

In this work, we need a closely related expression,

$$\sum_m K_m(k;n) x^{n-m} y^m = (x+y)^{n-k}(x-y)^k. \tag{118}$$

That above equation holds, can be seen in the following way.

$$\begin{aligned}
&(x+y)^{n-k}(x-y)^k \\
&= \sum_\alpha \binom{n-k}{\alpha} x^{n-k-\alpha}(y)^\alpha \sum_\beta \binom{k}{\beta} x^{k-\beta} y^\beta (-1)^\beta \\
&= \sum_\alpha \sum_\beta \binom{n-k}{\alpha}\binom{k}{\beta} x^{n-(\alpha+\beta)} y^{(\alpha+\beta)} (-1)^\beta \\
&= \sum_m \Big[\sum_\beta \binom{n-k}{m-\beta}\binom{k}{\beta}(-1)^\beta \Big] x^{n-m} y^m \\
&= \sum_m K_m(k;n) x^{n-m} y^m,
\end{aligned} \tag{119}$$

where we set $m = \alpha + \beta$ in the third line. Of course, setting $x = 1$ recovers Eq. (117).

This can be generalized to the Krawtchouk-like polynomial

$$K_m(k;n,E,F) = \sum_\alpha (-1)^\alpha \binom{n-k}{m-\alpha}\binom{k}{\alpha} E^{[(n-k)-(m-\alpha)]} F^{m-\alpha}, \tag{120}$$

[11] See p. 42 in Ref. [106] or Chpt. 5, §7 in Ref. [228].

which are the coefficients of

$$
\begin{aligned}
(Ex+Fy)^{n-k}(x-y)^k &= \sum_\alpha \binom{n-k}{\alpha}(Ex)^{n-k-\alpha}(Fy)^\alpha \sum_\beta \binom{k}{\beta} x^{k-\beta}y^\beta(-1)^\beta \\
&= \sum_\alpha \sum_\beta \binom{n-k}{\alpha}\binom{k}{\beta} x^{n-(\alpha+\beta)}y^{(\alpha+\beta)}E^{n-k-\alpha}F^\alpha(-1)^\beta \\
&= \sum_m \Big[\sum_\beta \binom{n-k}{m-\beta}\binom{k}{\beta}(-1)^\beta E^{(n-k)-(m-\beta)}F^{m-\beta}\Big] x^{n-m}y^m \\
&= \sum_m K_m(k;n,E,F)x^{n-m}y^m\,. \qquad (121)
\end{aligned}
$$

Bibliography

[1] E. Schrödinger, "Discussion of Probability Relations between Separated Systems," Math. Proc. Cambridge Phil. Soc. **31**, 555 (1935).

[2] L. Gurvits, "Classical complexity and quantum entanglement," J. Comp. Syst. Sci. **69**, 448 (2004), special Issue on STOC 2003.

[3] S. Gharibian, "Strong NP-hardness of the Quantum Separability Problem," Quant. Inf. Comp. **10**, 343 (2010).

[4] J. J. Sakurai, *Modern Quantum Mechanics*, Revised ed. (Addison-Wesley, New York, 1994).

[5] R. Bhatia, *Matrix Analysis*, Graduate Texts in Mathematics (Springer (New York), 1997).

[6] W. F. Stinespring, "Positive Functions on C*-Algebras," Proc. Americ. Math. Soc. **6**, 211 (1955).

[7] E. C. G. Sudarshan, P. M. Mathews, and J. Rau, "Stochastic Dynamics of Quantum-Mechanical Systems," Phys. Rev. **121**, 920 (1961).

[8] K. Kraus, "General state changes in quantum theory," Ann. Phys. **64**, 311 (1971).

[9] M. A. Nielsen, "Conditions for a Class of Entanglement Transformations," Phys. Rev. Lett. **83**, 436 (1999).

[10] M. Horodecki, P. Horodecki, and R. Horodecki, "Mixed-State Entanglement and Distillation: Is there a "Bound" Entanglement in Nature?" Phys. Rev. Lett. **80**, 5239 (1998).

[11] M. Horodecki and P. Horodecki, "Reduction criterion of separability and limits for a class of distillation protocols," Phys. Rev. A **59**, 4206 (1999).

[12] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," Nature **299**, 802 (1982).

[13] D. Dieks, "Communication by EPR devices," Phys. Lett. A **92**, 271 (1982).

[14] O. Gühne and G. Tóth, "Entanglement detection," Phys. Rep. **474**, 1 (2009).

[15] M. M. Wolf, "Lecture Notes: Quantum Channels & Operations, a Guided Tour," Online available at `http://www-m5.ma.tum.de/foswiki/pub/M5/Allgemeines/MichaelWolf/QChannelLecture.pdf` (2012).

[16] J. S. Bell, "On the Einstein Podolsky Rosen paradox," Physics **1**, 195 (1964).

[17] I. Bengtsson and K. Życzkowski, *Geometry of Quantum States: An Introduction to Quantum Entanglement* (Cambridge University Press, 2006).

[18] R. Jozsa, "Fidelity for Mixed Quantum States," J. Mod. Opt. **41**, 2315 (1994).

[19] A. Capel, A. Lucia, and D. Pérez-García, "Superadditivity of quantum relative entropy for general states," (2017), arXiv:1705.03521v3 .

[20] M. B. Ruskai, "Inequalities for quantum entropy: A review with conditions for equality," J. Math. Phys. **43**, 4358 (2002).

[21] B. Schumacher, "Quantum coding," Phys. Rev. A **51**, 2738 (1995).

[22] C. A. Fuchs and J. van de Graaf, "Cryptographic Distinguishability Measures for Quantum-Mechanical States." IEEE Trans. Inf. Theory **45**, 1216 (1999).

[23] K. M. R. Audenaert, "Comparisons between quantum state distinguishability measures." Quant. Inf. Comp. **14**, 31 (2014).

[24] K. M. R. Audenaert and J. Eisert, "Continuity bounds on the quantum relative entropy — II," J. Math. Phys. **52**, 112201 (2011).

[25] K. M. R. Audenaert, "A sharp continuity estimate for the von Neumann entropy," J. Phys. A: Math. Theor. **40**, 8127 (2007).

[26] A. Winter, "Tight Uniform Continuity Bounds for Quantum Entropies: Conditional Entropy, Relative Entropy Distance and Energy Constraints," Comm. Math. Phys. **347**, 291 (2016).

[27] M. M. Wilde, *Quantum Information Theory* (Cambridge University Press, 2013).

[28] M. Horodecki, P. Horodecki, and R. Horodecki, "Separability of mixed states: necessary and sufficient conditions," Phys. Lett. A **223**, 1 (1996).

[29] O. Gühne, P. Hyllus, D. Bruß, A. Ekert, M. Lewenstein, C. Macchiavello, and A. Sanpera, "Detection of entanglement with few local measurements," Phys. Rev. A **66**, 062305 (2002).

[30] O. Gühne and P. Hyllus, "Investigating Three Qubit Entanglement with Local Measurements," Int. J. Theor. Phys. **42**, 1001 (2003).

[31] H.-P. Breuer, "Optimal Entanglement Criterion for Mixed Quantum States," Phys. Rev. Lett. **97**, 080501 (2006).

[32] W. Hall, "A new criterion for indecomposability of positive maps," J. Phys. A **39**, 14119 (2006).

[33] 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).

[34] S. Albeverio, K. Chen, and S.-M. Fei, "Generalized reduction criterion for separability of quantum states," Phys. Rev. A **68**, 062313 (2003).

[35] W. Hall, "Multipartite reduction criteria for separability," Phys. Rev. A **72**, 022311 (2005).

[36] P. Butterley, A. Sudbery, and J. Szulc, "Compatibility of Subsystem States," Found. Phys. **36**, 83 (2006).

[37] W. Hall, "Compatibility of subsystem states and convex geometry," Phys. Rev. A **75**, 032102 (2007).

[38] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," Phys. Rev. A **54**, 3824 (1996).

[39] U. Fano, "Description of States in Quantum Mechanics by Density Matrix and Operator Techniques," Rev. Mod. Phys. **29**, 74 (1957).

[40] R. A. Bertlmann and P. Krammer, "Bloch vectors for qudits and geometry of entanglement," (2007), arXiv:0706.1743v1 .

[41] E. Knill, "Non-binary Unitary Error Bases and Quantum Codes," (1996), arXiv:quant-ph/9608048v2 .

[42] A. A. Klappenecker and M. Rotteler, "Beyond stabilizer codes .I. Nice error bases," IEEE Trans. Inf. Theory **48**, 2392 (2002).

[43] A. Vourdas, "Quantum systems with finite Hilbert space," Rep. Prog. Phys. **67**, 267 (2004).

[44] A. J. Scott, "Multipartite entanglement, quantum-error-correcting codes, and entangling power of quantum evolutions," Phys. Rev. A **69**, 052330 (2004).

[45] D. Gottesman, "Fault-Tolerant Quantum Computation with Higher-Dimensional Systems," Chaos Solit. Fract. **10**, 1749 (1999).

[46] C. Eltschka and J. Siewert, "Distribution of entanglement and correlations in all finite dimensions," (2017), arXiv:1708.09639v1 .

[47] M. Hein, J. Eisert, and H. J. Briegel, "Multiparty entanglement in graph states," Phys. Rev. A **69**, 062311 (2004).

[48] W. Helwig, "Absolutely Maximally Entangled Qudit Graph States," (2013), arXiv:1306.2879v1 .

[49] T. A. Gulliver and M. Harada, "Weight Enumerators of Double Circulant Codes and New Extremal Self-Dual Codes," Des. Codes Cryptogr. **11**, 141 (1997).

[50] Z. Varbanov, "Additive circulant graph codes over GF (4)," Sixth International Workshop on Optimal Codes and Related Topics , 189 (2009).

[51] M. Grassl and M. Harada, "New self-dual additive F4-codes constructed from circulant graphs," Discrete Math. **340**, 399 (2017).

[52] M. Grassl and T. A. Gulliver, "On circulant self-dual codes over small fields," Des. Codes Cryptogr. **52**, 57 (2009).

[53] L. E. Danielsen, "Database of Self-Dual Quantum Codes and Entanglement in Graph States," Online available at `http://www.ii.uib.no/~larsed/`.

[54] D. Schlingemann and R. F. Werner, "Quantum error-correcting codes associated with graphs," Phys. Rev. A **65**, 012308 (2001).

[55] M. Grassl, A. Klappenecker, and M. Rotteler, "Graphs, quadratic forms, and quantum codes," in *Proc. IEEE Int. Symp. Inf. Theory* (2002) p. 45.

[56] S. Y. Looi, L. Yu, V. Gheorghiu, and R. B. Griffiths, "Quantum-error-correcting codes using qudit graph states," Phys. Rev. A **78**, 042303 (2008).

[57] R. Raussendorf and H. J. Briegel, "A One-Way Quantum Computer," Phys. Rev. Lett. **86**, 5188 (2001).

[58] R. Raussendorf, D. E. Browne, and H. J. Briegel, "Measurement-based quantum computation on cluster states," Phys. Rev. A **68**, 022312 (2003).

[59] M. Van den Nest, J. Dehaene, and B. De Moor, "Graphical description of the action of local Clifford transformations on graph states," Phys. Rev. A **69**, 022316 (2004).

[60] Z.-F. Ji, J. Chen, Z. Wei, and M. Ying, "The LU-LC conjecture is false." Quant. Inf. Comp. **10**, 97 (2010).

[61] N. Tsimakuridze and O. Gühne, "Graph states and local unitary transformations beyond local Clifford operations," J. Phys. A **50**, 195302 (2017).

[62] C. Gogolin and J. Eisert, "Equilibration, thermalisation, and the emergence of statistical mechanics in closed quantum systems," Rep. Prog. Phys. **79**, 056001 (2016).

[63] E. T. Jaynes, "Information Theory and Statistical Mechanics," Phys. Rev. **106**, 620 (1957).

[64] E. T. Jaynes, "Lectures in Theoretical Physics: Information Theory and Statistical Mechanics," (1962).

[65] E. T. Jaynes, "Information Theory and Statistical Mechanics. II," Phys. Rev. **108**, 171 (1957).

[66] S.-I. Amari, "Information geometry on hierarchy of probability distributions," IEEE Trans. Inf. Theory **47**, 1701 (2001).

[67] S.-I. Amari, *Information Geometry and Its Applications*, Applied Mathematical Sciences (Springer Japan, 2016).

[68] C. Moler and C. Van Loan, "Nineteen Dubious Ways to Compute the Exponential of a Matrix, Twenty-Five Years Later," SIAM Rev. **45**, 3.

[69] J. Kempe, A. Kitaev, and O. Regev, "The Complexity of the Local Hamiltonian Problem," SIAM J. Comput. **35**, 1070 (2006).

[70] T. Cubitt and A. Montanaro, "Complexity Classification of Local Hamiltonian Problems," SIAM J. Comput. **45**, 268 (2016).

[71] W. Brown and D. Poulin, "Quantum Markov Networks and Commuting Hamiltonians," (2012), arXiv:1206.0755v1 .

[72] K. Kato and F. G. S. L. Brandao, "Quantum Approximate Markov Chains are Thermal," (2016), arXiv:1609.06636v1 .

[73] A. Molnar, N. Schuch, F. Verstraete, and J. I. Cirac, "Approximating Gibbs states of local Hamiltonians efficiently with projected entangled pair states," Phys. Rev. B **91**, 045138 (2015).

[74] O. Fawzi and R. Renner, "Quantum Conditional Mutual Information and Approximate Markov Chains," Comm. Math. Phys. **340**, 575 (2015).

[75] M. B. Hastings, "Locality in Quantum Systems," (2010), arXiv:1008.5137v1 .

[76] J. M. Hammersley and P. E. Clifford, "Markov random fields on finite graphs and lattices," *Unpublished manuscript* (1971), online available at `http://www.statslab.cam.ac.uk/~grg/books/hammfest/hamm-cliff.pdf`.

[77] C. J. Preston, "Generalized Gibbs States and Markov Random Fields," Advances in Applied Probability **5**, 242 (1973).

[78] D. L. Zhou, "Irreducible multiparty correlations can be created by local operations," Phys. Rev. A **80**, 022113 (2009).

[79] S. Niekamp, T. Galla, M. Kleinmann, and O. Gühne, "Computing complexity measures for quantum states based on exponential families," J. Phys. A: Math. Theor. **46**, 125301 (2013).

[80] Y. S. Teo, H. Zhu, B.-G. Englert, J. Řeháček, and Z. c. v. Hradil, "Quantum-State Reconstruction by Maximizing Likelihood and Entropy," Phys. Rev. Lett. **107**, 020404 (2011).

[81] S. Weis and A. Knauf, "Entropy distance: New quantum phenomena," J. Math. Phys. **53**, 102206 (2012).

[82] D. L. Zhou, "Irreducible Multiparty Correlations in Quantum States without Maximal Rank," Phys. Rev. Lett. **101**, 180505 (2008).

[83] H. Hasegawa, "Exponential and mixture families in quantum statistics: Dual structure and unbiased parameter estimation," Rep. Math. Phys. **39**, 49 (1997).

[84] N. Linden, S. Popescu, and W. K. Wootters, "Almost Every Pure State of Three Qubits Is Completely Determined by Its Two-Particle Reduced Density Matrices," Phys. Rev. Lett. **89**, 207901 (2002).

[85] N. Gisin and H. Bechmann-Pasquinucci, "Bell inequality, Bell states and maximally entangled states for n qubits," Phys. Lett. A **246**, 1 (1998).

[86] A. Higuchi and A. Sudbery, "How entangled can two couples get?" Phys. Lett. A **273**, 213 (2000).

[87] I. D. K. Brown, S. Stepney, A. Sudbery, and S. L. Braunstein, "Searching for highly entangled multi-qubit states," J. Phys. A **38**, 1119 (2005).

[88] W. Helwig, W. Cui, J. I. Latorre, A. Riera, and H.-K. Lo, "Absolute maximal entanglement and quantum secret sharing," Phys. Rev. A **86**, 052335 (2012).

[89] L. Arnaud and N. J. Cerf, "Exploring pure quantum states with maximally mixed reductions," Phys. Rev. A **87**, 012319 (2013).

[90] C. Klöckl and M. Huber, "Characterizing multipartite entanglement without shared reference frames," Phys. Rev. A **91**, 042339 (2015).

[91] D. Goyeneche, D. Alsina, J. I. Latorre, A. Riera, and K. Życzkowski, "Absolutely maximally entangled states, combinatorial designs, and multiunitary matrices," Phys. Rev. A **92**, 032316 (2015).

[92] A. Bernal, "On the Existence of Absolutely Maximally Entangled States of Minimal Support," Quant. Phys. Lett. **6**, 1 (2017), arXiv:1603.06082v2 .

[93] J. E. Tapiador, J. C. Hernandez-Castro, J. A. Clark, and S. Stepney, "Highly entangled multi-qubit states with simple algebraic structure," J. Phys. A: Math. Theor. **42**, 415301 (2009).

[94] P. Facchi, G. Florio, G. Parisi, and S. Pascazio, "Maximally multipartite entangled states," Phys. Rev. A **77**, 060304 (2008).

[95] P. Facchi, G. Florio, U. Marzolino, G. Parisi, and S. Pascazio, "Classical statistical mechanics approach to multipartite entanglement," J. Phys. A: Math. Theor. **43**, 225303 (2010).

[96] G. Gour and N. R. Wallach, "All maximally entangled four-qubit states," J. Math. Phys. **51**, 112201 (2010).

[97] M. Enríquez, I. Wintrowicz, and K. Życzkowski, "Maximally Entangled Multipartite States: A Brief Survey," J. Phys: Conf. **698**, 012003 (2016).

[98] X.-w. Zha, H.-y. Song, J.-x. Qi, D. Wang, and Q. Lan, "A maximally entangled seven-qubit state," J. Phys. A: Math. Theor. **45**, 255302 (2012).

[99] W. Helwig and W. Cui, "Absolutely Maximally Entangled States: Existence and Applications," (2013), arXiv:1306.2536v1 .

[100] L. Chen and D. L. Zhou, "Graph states of prime-power dimension from generalized CNOT quantum circuit," Sci. Rep. **6**, 27135 (2016).

[101] J. H. Quick, "The turbo-encabulator in industry," Students' Quarterly Journal **15**, 22 (1944).

[102] R. Cleve, D. Gottesman, and H.-K. Lo, "How to Share a Quantum Secret," Phys. Rev. Lett. **83**, 648 (1999).

[103] J. I. Latorre and G. Sierra, "Holographic codes," (2015), arXiv:1502.06618v1 .

[104] F. Pastawski, B. Yoshida, D. Harlow, and J. Preskill, "Holographic quantum error-correcting codes: toy models for the bulk/boundary correspondence," J. High Energy Phys. **2015**, 149 (2015).

[105] Y. Li, M. Han, M. Grassl, and B. Zeng, "Invariant perfect tensors," N. J. Phys. **19**, 063029 (2017).

[106] G. Nebe, E. M. Rains, and N. J. A. Sloane, *Self-Dual Codes and Invariant Theory* (Springer Berlin-Heidelberg, 2006).

[107] E. M. Rains, "Quantum shadow enumerators," IEEE Trans. Inf. Theory **45**, 2361 (1999).

[108] A. R. Calderbank, E. M. Rains, P. M. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," IEEE Trans. Inf. Theory **44**, 1369 (1998).

[109] F. Huber, O. Gühne, and J. Siewert, "Absolutely Maximally Entangled States of Seven Qubits Do Not Exist," Phys. Rev. Lett. **118**, 200502 (2017).

[110] M. Grassl, T. Beth, and M. Rötteler, "On optimal quantum codes," Int. J. Quant. Inf. **2**, 55 (2004).

[111] D. Goyeneche, Z. Raissi, S. D. Martino, and K. Życzkowski, "Entanglement and quantum combinatorial designs," (2017), arXiv:1708.05946v1 .

[112] "QOQI List of Open Quantum Problems," IQOQI Vienna (2017), online accessible at `http://oqp.iqoqi.univie.ac.at/existence-of-absolutely-maximally-entangled-pure-states`.

[113] J. Kempe, "Approaches to Quantum Error Correction," (2005), arXiv:quant-ph/0612185v1 .

[114] T. A. Brun and D. E. Lidar, *Quantum Error Correction* (Cambridge University Press, 2013).

[115] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," Phys. Rev. A **52**, 2493(R) (1995).

[116] E. Knill, R. Laflamme, and L. Viola, "Theory of Quantum Error Correction for General Noise," Phys. Rev. Lett. **84**, 2525 (2000).

[117] D. Gottesman, "An Introduction to Quantum Error Correction," (American Mathematical Society, 2002) p. 221, arXiv:quant-ph/0004072v1 .

[118] E. M. Rains, "Quantum weight enumerators," IEEE Trans. Inf. Theory **44**, 1388 (1998).

[119] M. Grassl, P. Shor, G. Smith, J. Smolin, and B. Zeng, "Generalized concatenated quantum codes," Phys. Rev. A **79**, 050306 (2009).

[120] E. Knill and R. Laflamme, "Concatenated Quantum Codes," (1996), arXiv:quant-ph/9608012v1 .

[121] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, "Nonbinary Stabilizer Codes Over Finite Fields," IEEE Trans. Inf. Theory **52**, 4892 (2006).

[122] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," IEEE Trans. Inf. Theory **47**, 3065 (2001).

[123] E. M. Rains, "Nonbinary quantum codes," IEEE Trans. Inf. Theory **45**, 1827 (1999).

[124] E. M. Rains, "Shadow bounds for self-dual codes," IEEE Trans. Inf. Theory **44**, 134 (1998).

[125] E. Rains and N. Sloane, "Self-Dual Codes," in *Handbook of Coding Theory*, edited by V. S. Pless and W. C. Huffman (1998) p. 177.

[126] A. Ekert and C. Macchiavello, "Error Correction in Quantum Communication," (1996), arXiv:quant-ph/9602022v1 .

[127] P. Sarvepalli and A. Klappenecker, "Degenerate quantum codes and the quantum Hamming bound," Phys. Rev. A **81**, 032318 (2010).

[128] P. Shor and R. Laflamme, "Quantum Analog of the MacWilliams Identities for Classical Coding Theory," Phys. Rev. Lett. **78**, 1600 (1997).

[129] E. M. Rains, "Polynomial invariants of quantum codes," IEEE Trans. Inf. Theory **46**, 54 (2000).

[130] L. Vandenberghe and S. Boyd, "Semidefinite Programming," SIAM Rev. **38**, 49 (1996).

[131] H. Wolkowicz, R. Saigal, and L. Vandenberghe, *Handbook of Semidefinite Programming: Theory, Algorithms, and Applications* (Springer US, 2000).

[132] P. A. Parrilo and S. Lall, "Semidefinite Programming Relaxations and Algebraic Optimization in Control," Eur. J. Contr. **9**, 307 (2003).

[133] G. Blekherman, P. A. Parrilo, and R. R. Thomas, eds., *Semidefinite Optimization and Convex Algebraic Geometry* (Society for Industrial and Applied Mathematics, 2013).

[134] E. M. Rains, "A semidefinite program for distillable entanglement," IEEE Trans. Inf. Theory **47**, 2921 (2001).

[135] B. M. Terhal, A. C. Doherty, and D. Schwab, "Symmetric Extensions of Quantum States and Local Hidden Variable Theories," Phys. Rev. Lett. **90**, 157903 (2003).

[136] M. Navascués, S. Pironio, and A. Acín, "A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations," N. J. Phys. **10**, 073013 (2008).

[137] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, "Complete family of separability criteria," Phys. Rev. A **69**, 022308 (2004).

[138] D. Cavalcanti and P. Skrzypczyk, "Quantum steering: a review with focus on semidefinite programming," Rep. Prog. Phys. **80**, 024001 (2017).

[139] T. Heinosaari and M. M. Wolf, "Nondisturbing quantum measurements," J. Math. Phys. **51**, 092201 (2010).

[140] J. Watrous, "Lecture Notes: Theory of Quantum Information," Online available at `http://cs.uwaterloo.ca/~watrous/TQI` (2017).

[141] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, "Distinguishing Separable and Entangled States," Phys. Rev. Lett. **88**, 187904 (2002).

[142] N. Miklin, T. Moroder, and O. Gühne, "Multiparticle entanglement as an emergent phenomenon," Phys. Rev. A **93**, 020104 (2016).

[143] A. J. Coleman, "Structure of Fermion Density Matrices," Rev. Mod. Phys. **35**, 668 (1963).

[144] National Research Council, *Mathematical Challenges from Theoretical/Computational Chemistry* (Washington DC: The National Academies Press, 2005).

[145] 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).

[146] S. Bravyi, "Requirements for compatibility between local and multipartite quantum states." Quant. Inf. Comp. **4**, 12 (2004).

[147] A. Higuchi, "On the one-particle reduced density matrices of a pure three-qutrit quantum state," (2003), arXiv:quant-ph/0309186v2 .

[148] A. Klyachko, "Quantum marginal problem and representations of the symmetric group," (2004), arXiv:quant-ph/0409113v1 .

[149] A. A. Klyachko, "Quantum marginal problem and N-representability," J. Phys: Conf. **36**, 72 (2006).

[150] J. Eisert, T. Tyc, T. Rudolph, and B. C. Sanders, "Gaussian Quantum Marginal Problem," Comm. Math. Phys. **280**, 263 (2008).

[151] T. J. Osborne, "Entropic bounds for the quantum marginal problem," (2008), arXiv:0806.2962v1 .

[152] E. A. Carlen, J. L. Lebowitz, and E. H. Lieb, "On an extension problem for density matrices," J. Math. Phys. **54**, 062103 (2013).

[153] J. Chen, Z. Ji, N. Yu, and B. Zeng, "Detecting consistency of overlapping quantum marginals by separability," Phys. Rev. A **93**, 032105 (2016).

[154] J. Chen, Z. Ji, D. Kribs, N. Lütkenhaus, and B. Zeng, "Symmetric extension of two-qubit states," Phys. Rev. A **90**, 032318 (2014).

[155] B. M. Terhal, "Is entanglement monogamous?" IBM J. Res. Dev. **48**, 71 (2004).

[156] V. Coffman, J. Kundu, and W. K. Wootters, "Distributed entanglement," Phys. Rev. A **61**, 052306 (2000).

[157] T. J. Osborne and F. Verstraete, "General Monogamy Inequality for Bipartite Qubit Entanglement," Phys. Rev. Lett. **96**, 220503 (2006).

[158] M. Koashi and A. Winter, "Monogamy of quantum entanglement and other correlations," Phys. Rev. A **69**, 022309 (2004).

[159] C. Eltschka and J. Siewert, "Monogamy Equalities for Qubit Entanglement from Lorentz Invariance," Phys. Rev. Lett. **114**, 140402 (2015).

[160] B. Toner, "Monogamy of non-local quantum correlations," Proc. Roy. Soc. A **465**, 59 (2009).

[161] C. Eltschka, T. Bastin, A. Osterloh, and J. Siewert, "Multipartite-entanglement monotones and polynomial invariants," Phys. Rev. A **85**, 022301 (2012).

[162] H. S. Dhar, A. K. Pal, D. Rakshit, A. S. De, and U. Sen, "Monogamy of quantum correlations - a review," *Lectures on General Quantum Correlations and their Applications*, Quantum Science and Technology, 23 (2017).

[163] L. Diósi, "Three-party pure quantum states are determined by two two-party reduced states," Phys. Rev. A **70**, 010302 (2004).

[164] N. S. Jones and N. Linden, "Parts of quantum states," Phys. Rev. A **71**, 012324 (2005).

[165] M. Fukuda, B. J. Braams, M. Nakata, M. L. Overton, J. K. Percus, M. Yamashita, and Z. Zhao, "Large-scale semidefinite programs in electronic structure calculation," Math. Prog. **109**, 553 (2007).

[166] Y.-K. Liu, "Consistency of Local Density Matrices Is QMA-Complete," in *Approximation, Randomization, and Combinatorial Optimization*, edited by J. Díaz, K. Jansen, J. D. P. Rolim, and U. Zwick (Springer Berlin Heidelberg, 2006) p. 438.

[167] Y.-K. Liu, M. Christandl, and F. Verstraete, "Quantum Computational Complexity of the N-Representability Problem: QMA Complete," Phys. Rev. Lett. **98**, 110503 (2007).

[168] S. Diehl, A. Micheli, A. Kantian, B. Kraus, H. P. Büchler, and P. Zoller, "Quantum states and phases in driven open quantum systems with cold atoms," Nat. Phys. **4**, 878 (2008).

[169] B. Röthlisberger, J. Lehmann, D. S. Saraga, P. Traber, and D. Loss, "Highly Entangled Ground States in Tripartite Qubit Systems," Phys. Rev. Lett. **100**, 100502 (2008).

[170] R. Oliveira and B. M. Terhal, "The complexity of quantum spin systems on a two-dimensional square lattice," Quant. Inf. Comp. **8**, 0900 (2008).

[171] F. Verstraete, M. M. Wolf, and C. J. Ignacio, "Quantum computation and quantum-state engineering driven by dissipation," Nat. Phys. **5**, 633 (2009), 10.1038/nphys1342.

[172] P. Facchi, G. Florio, S. Pascazio, and F. V. Pepe, "Greenberger-Horne-Zeilinger States and Few-Body Hamiltonians," Phys. Rev. Lett. **107**, 260502 (2011).

[173] J. Chen, Z. Ji, Z. Wei, and B. Zeng, "Correlations in excited states of local Hamiltonians," Phys. Rev. A **85**, 040303 (2012).

[174] F. Ticozzi and L. Viola, "Stabilizing entangled states with quasi-local quantum dynamical semigroups," Phil. Trans. A **370**, 5259 (2012).

[175] M. Van den Nest, K. Luttmer, W. Dür, and H. J. Briegel, "Graph states as ground states of many-body spin-12 Hamiltonians," Phys. Rev. A **77**, 012301 (2008).

[176] G. Tóth, "Entanglement witnesses in spin models," Phys. Rev. A **71**, 010301 (2005).

[177] J. Tura, R. Augusiak, A. B. Sainz, T. Vértesi, M. Lewenstein, and A. Acín, "Detecting nonlocality in many-body quantum states," Science **344**, 1256 (2014).

[178] H. L. Haselgrove, M. A. Nielsen, and T. J. Osborne, "Quantum States far from the Energy Eigenstates of Any Local Hamiltonian," Phys. Rev. Lett. **91**, 210401 (2003).

[179] S. Boyd and L. Vandenberghe, *Convex optimization* (Cambridge University Press, 2004).

[180] F. Mezzadri, "How to generate random matrices from the classical compact groups," Notices of the AMS **54**, 592 (2007).

[181] O. Gühne, M. Cuquet, F. E. S. Steinhoff, T. Moroder, M. Rossi, D. Bruß, B. Kraus, and C. Macchiavello, "Entanglement and nonclassical properties of hypergraph states," J. Phys. A: Math. Theor. **47**, 335303 (2014).

[182] B. Kraus, *Entanglement Properties of Quantum States and Quantum Operations*, Ph.D. thesis, Universität Innsbruck (2003), online available at `ftp://ftp.ipp-garching.mpg.de/pub/mpq/MPQ282.pdf`.

[183] A. Osterloh and J. Siewert, "Constructing N-qubit entanglement monotones from antilinear operators," Phys. Rev. A **72**, 012337 (2005).

[184] N. Wyderka, F. Huber, and O. Gühne, "Almost all four-particle pure states are determined by their two-body marginals," Phys. Rev. A **96**, 010102 (2017).

[185] S. Niekamp, *Characterizing quantum correlations: entanglement, uncertainty relations and exponential families*, Ph.D. thesis, Universität Siegen (2012), online available at `http://d-nb.info/1023156733/34`.

[186] M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel, "On quantum Rényi entropies: A new generalization and some properties," J. Math. Phys. **54**, 122203 (2013).

[187] Büchler H. P., Micheli A., and Zoller P., "Three-body interactions with cold polar molecules," Nat. Phys. **3**, 726 (2007), 10.1038/nphys678.

[188] A. Bermudez, D. Porras, and M. A. Martin-Delgado, "Competing many-body interactions in systems of trapped ions," Phys. Rev. A **79**, 060303 (2009).

[189] J. K. Pachos and M. B. Plenio, "Three-Spin Interactions in Optical Lattices and Criticality in Cluster Hamiltonians," Phys. Rev. Lett. **93**, 056402 (2004).

[190] H. Weimer, M. Müller, I. Lesanovsky, P. Zoller, and H. P. Büchler, "A Rydberg quantum simulator," Nat. Phys. **6**, 382 (2010).

[191] M. Hafezi, P. Adhikari, and J. M. Taylor, "Engineering three-body interaction and Pfaffian states in circuit QED systems," Phys. Rev. B **90**, 060503 (2014).

[192] B. P. Lanyon, C. Hempel, D. Nigg, M. Müller, R. Gerritsma, F. Zähringer, P. Schindler, J. T. Barreiro, M. Rambach, G. Kirchmair, M. Hennrich, P. Zoller, R. Blatt, and C. F. Roos, "Universal Digital Quantum Simulation with Trapped Ions," Science **334**, 57 (2011).

[193] E. Carlen, "Trace Inequalities and Quantum Entropy: An Introductory Course," Contemp. Math. **529** (2009).

[194] 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).

[195] 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).

[196] S. Hill and W. K. Wootters, "Entanglement of a Pair of Quantum Bits," Phys. Rev. Lett. **78**, 5022 (1997).

[197] W. K. Wootters, "Entanglement of Formation of an Arbitrary State of Two Qubits," Phys. Rev. Lett. **80**, 2245 (1998).

[198] A. Uhlmann, "Fidelity and concurrence of conjugated states," Phys. Rev. A **62**, 032307 (2000).

[199] L. E. Danielsen and M. G. Parker, "On the classification of all self-dual additive codes over GF(4) of length up to 12," J. Comb. Theory A **113**, 1351 (2006).

[200] H. A. Kramers, "Théorie générale de la rotation paramagnétique dans les cristaux," Proc. Amsterdam Acad. **33** (1930).

[201] S. S. Bullock, G. K. Brennen, and D. P. O'Leary, "Time reversal and n-qubit canonical decompositions," J. Math. Phys. **46**, 062104 (2005).

[202] J. K. Pachos and E. Rico, "Effective three-body interactions in triangular optical lattices," Phys. Rev. A **70**, 053620 (2004).

[203] D. Goyeneche and K. Życzkowski, "Genuinely multipartite entangled states and orthogonal arrays," Phys. Rev. A **90**, 022316 (2014).

[204] M. Grassl and M. Rötteler, "Quantum MDS codes over small fields," in *2015 IEEE Int. Symp. Inf. Theory (ISIT)* (2015) p. 1104.

[205] J. H. F. Mattson, "A First Course in Coding Theory (Raymond Hill)," SIAM Review **30**, 148 (1988).

[206] A. Asadian, P. Erker, M. Huber, and C. Klöckl, "Heisenberg-Weyl Observables: Bloch vectors in phase space," Phys. Rev. A **94**, 010301 (2016).

[207] N. Friis, M. Huber, and M. Perarnau-Llobet, "Energetics of correlations in interacting systems," Phys. Rev. E **93**, 042135 (2016).

[208] P. Appel, M. Huber, and C. Klöckl, "Monogamy of correlations and entropy inequalities in the Bloch picture," (2017), arXiv:1710.02473v1 .

[209] M. Grassl, "Bounds on the minimum distance of linear codes and quantum codes," Online available at `http://www.codetables.de` (2007).

[210] K. Feng, L. Jin, C. Xing, and C. Yuan, "Multipartite Entangled States, Symmetric Matrices, and Error-Correcting Codes," IEEE Trans. Inf. Theory **63**, 5618 (2017).

[211] P. J. Kelly, "A congruence theorem for trees." Pacific J. Math. **7**, 961 (1957).

[212] S. M. Ulam, "A collection of mathematical problems," (1960).

[213] M. Aigner and E. Triesch, "Realizability and uniqueness in graphs," Discrete Math. **136**, 3 (1994).

[214] P. V. O'Neil, "Ulam's Conjecture and Graph Reconstructions," Americ. Math. Month. **77**, 35 (1970).

[215] J. A. Bondy and R. L. Hemminger, "Graph reconstruction—a survey," J. Graph Theory **1**, 227 (1977).

[216] J. A. Bondy, "Reflections on the legitimate deck problem," in *Comb. Math.: Proc. Int. Conf. Comb. Theory*, edited by D. A. Holton and J. Seberry (Springer Berlin Heidelberg, 1978) p. 1.

[217] T. G. Seierstad, *Ulam's reconstruction problem for graphs*, Ph.D. thesis, University of Bergen (2002), online available at `https://folk.uio.no/taralgs/artikler/hovedfag.pdf`.

[218] M. Bilinski, Y. S. Kwon, and X. Yu, "On the reconstruction of planar graphs," J. Comb. Theory B **97**, 745 (2007).

[219] B. Bollobás, "Almost every graph has reconstruction number three," Journal of Graph Theory **14**, 1 (1990).

[220] D. W. Lyons, D. J. Upchurch, S. N. Walck, and C. D. Yetter, "Local unitary symmetries of hypergraph states," J. Phys. A **48**, 095301 (2015).

[221] M. Rossi, M. Huber, D. Bruß, and C. Macchiavello, "Quantum hypergraph states," N. J. Phys. **15**, 113022 (2013).

[222] D. Gross, K. Audenaert, and J. Eisert, "Evenly distributed unitaries: On the structure of unitary designs," J. Math. Phys. **48**, 052104 (2007).

[223] 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** (2004).

[224] D. Gottesman, *Stabilizer Codes and Quantum Error Correction*, Ph.D. thesis, Caltech (1997), arXiv:quant-ph/9705052v1 .

[225] L. E. Danielsen, "On the Classification of Hermitian Self-Dual Additive Codes Over GF(9)," IEEE Trans. Inf. Theory **58**, 5500 (2012).

[226] L. E. Danielsen, "Graph-based classification of self-dual additive codes over finite fields," Adv. Math. Comm. **3**, 329 (2009).

[227] P. Hayden, M. Headrick, and A. Maloney, "Holographic mutual information is monogamous," Phys. Rev. D **87**, 046003 (2013).

[228] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (North Holland, 1981).

$$\begin{bmatrix} X & I & I & X & Y & Y \\ I & X & I & Y & X & Y \\ I & I & X & Y & Y & X \\ Y & I & I & Y & Z & Z \\ I & Y & I & Z & Y & Z \\ I & I & Y & Z & Z & Y \end{bmatrix}$$