Quantum correlations: entanglement detection with second moments and the classical simulation of disordered systems

Dissertation

zur Erlangung des akademischen Grades
Doktor der Naturwissenschaften

eingereicht an der
Fakultät für Mathematik, Informatik und Physik der Universität zu Innsbruck

von

Dipl.-Phys. Oleg Gittsovich

geboren am 8. Dezember 1981 in Sankt-Petersburg, Rußland

Betreuer der Dissertation: Prof. Hans J. Briegel, Institut für Theoretische Physik

Innsbruck, 5. Oktober, 2010

ABSTRACT

This thesis is devoted to two main questions. Firstly, the problem of entanglement detection and quantification is addressed. Secondly, the influence of disorder of internal parameters (e.g. coupling constants) on the ground state properties of many-body quantum systems is investigated.

As a tool to investigate the first question I consider the covariance matrix of a quantum state. Using covariance matrices, one can in many cases efficiently answer whether a given state (pure or mixed) is entangled or separable in the first place. The answer is formulated in form of a easily computable separability criterion, which is called covariance matrix criterion (CMC).The criterion provides a strong condition on a covariance matrix of separable quantum states and detects many bound entangled states in case of bipartite and multipartite setting. Further it is shown that several other criteria detecting bound entangled states are corollaries of the CMC. Apart from it, it is proved that physical observables used for the construction of a covariance matrix of the state, which is detected by the CMC, can be used to show a violation of a criterion based on local uncertainty relations (LURs). The converse is also true: If LURs criterion is violated for some observables, then the CMC cannot be fulfilled. Then I discuss extensions of the CMC to the multipartite case and show that such extensions are able to detect multipartite entangled states.

Furthermore, it turns out that one can use covariance matrices to estimate the amount of entanglement in a quantum state. To this end I define a quantity $\mathcal{E}(\rho)$, which quantifies the violation of the CMC, and study its general properties from the point of view of entanglement monotones. In addition this quantity is compared with the concurrence. It is shown that $\mathcal{E}(\rho)$ coincides with the concurrence on two qubit pure states and provides a lower bound on it for mixed states of bipartite d-level systems with $d \leq 4$.

Then I address the question of influence of disorder on quantum many-body systems. The description of these systems is carried out in terms of Hamiltonians. The Hamiltonians considered in this thesis contain only nearest neighbor interaction terms and are defined on a rectangular two dimensional lattice. The main goal is to investigate the influence of the stochastic nature of Hamiltonian's terms on the ground state of the whole Hamiltonian. To this end I introduce a method for achieving ground states of these Hamiltonians. The idea of the method is based on the local real space renormalizations and can be efficiently performed on the classical computer. The part of the lattice and hence of the Hamiltonian, which is to be renormalized is chosen according to the strength of disorder, which is reminiscent of the strong disorder renormalization technique originally developed for one dimensional systems.

ZUSAMMENFASSUNG

Diese Dissertation beschäftigt sich hauptsächlich mit zwei Fragen. Erstens wird von dem Problem der Verschränkungsdetektion und Verschränkungsquantifizierung die Rede sein. Zweitens wird der Einfluss der Unordnung in internen Systemparametern, wie z.B. in Kopplungskonstanten, auf Grundzustandseigenschaften von Mehrteilchenquantensystemen untersucht.

Die Untersuchung der ersten Frage wird mittels Kovarianzmatrizen erfolgen. Die Frage ob ein Quantenzustand verschränkt oder separabel ist lässt sich mit Hilfe von Kovarianzmatrizen in vielen Fällen beantworten. Die Antwort auf diese Frage ist in Form eines leicht verifizierbaren Verschränkungskriteriums formuliert, das Kovarianzmatrizenkriterium genannt wird (CMC). Das CMC stellt eine starke Bedingung an separable Zustände und detektiert viele gebunden verschränkte Zustände im bipartiten und im multipartiten Fall. Ferner wird gezeigt, dass einige andere Kriterien, die gebundene Verschränkung detektieren, Korollare des CMC sind. Außerdem wird bewiesen, dass die physikalischen Observablen, die zur Konstruktion der Kovarianzmatrix eines mit dem CMC detektierbaren Zustandes benutzt werden, auch für die Verletzung einer lokalen Unschärferelation (LUR) verwendet werden können. Die Umkehrung dieser Aussage wird ebenfalls bestätigt: Wenn das LUR Kriterium verletzt ist, wird das CMC ebenso verletzt. Weiterhin werden die Erweiterungen des CMC auf multipartite Systeme betrachtet. Es wird gezeigt, dass man mit solchen Erweiterungen multipartite Verschränkung detektieren kann.

Darüber hinaus werden Kovarianzmatrizen zur Verschränkungquantifizierung in einem Quantenzustand verwendet. Zu diesem Zweck definiere ich eine Größe $\mathcal{E}(\rho)$, die die Verletzung des CMC quantifiziert, und untersuche ihre allgemeinen Eigenschaften aus der Perspektive der Verschränkungsmonotone. Zudem wird diese Größe mit der Concurrence verglichen. Es wird gezeigt, dass $\mathcal{E}(\rho)$ mit der Concurrence für reine Zweiqubitzustände übereinstimmt und eine untere Schranke für die Concurrence für gemischte Zustände von bipartiten d-Niveau Systemen mit $d \leq 4$ darstellt.

Im Weiteren wende ich mich der oben erwähnten Frage der Unordnung in quantenmechanischen Vielteilchensystemen zu. Beschreibung dieser Systeme erfolgt mittels eines Hamiltonoperators. In dieser Doktorarbeit werden Hamiltonians betrachtet, die nur Nächst-Nachbar-Wechselwirkung enthalten und auf einem rechteckigen Gitter in zwei räumlichen Dimensionen definiert sind. Das Hauptaugenmerk ist auf die Untersuchung des Einflusses der stochastischen Natur der einzelnen Hamiltonianterme auf den Grundzustand des ganzen Hamiltonians ausgerichtet. Zu diesem Zweck wird eine Renormierungsmethode definiert und angewandt. Die Idee der Methode basiert auf lokalen Renormierungen im Ortsraum und kann auf einem klassischen Rechner effizient durchgeführt werden. Der Teil des Hamiltonians, der zu renormieren ist, wird nach Regeln gewählt, die einen an das Verfahren des Strong Disorder Renormalization Technique erinnern, das ursprünglich für eindimensionale Systeme entwickelt wurde.

Contents

Introduction

Entanglement is one of the most mysterious phenomena of nature discovered in the last century. Albert Einstein, Boris Podolsky and Nathan Rosen were the first who mentioned this peculiar property of quantum mechanical correlations of composite systems [1]. The term entanglement was chosen by Erwin Schrödinger to describe these correlations [2]. As a rather counter-intuitive property of quantum mechanics, entanglement was considered by Einstein, Podolsky and Rosen as a proof for the incompleteness of quantum mechanics.

For several decades entanglement did not receive much attention. It was known to be a bizarre phenomenon, but mainly due to the lacking of experimental implementation had not been intensively investigated. This situation started to change in the beginning of 80's. At that time an idea to use principles of quantum mechanics for tasks in classical information theory were discussed by several authors [3, 4, 5, 6, 7]. Later on it was proved that quantum mechanics allows to perform tasks inconceivable within the framework of classical mechanics. The newborn theory received the name *Quantum Information Theory*. This new promising theory opened new branches in computer science [4, 8, 9] and in communication theory [5, 6, 7], which found already certain commercial implementation [10]. Substantiated by several experiments [11, 12, 13, 14] quantum information theory rapidly became one of the most prospered fields of modern physics. Entanglement plays a crucial role there.

As it has been realized in the above theoretical works and confirmed by several experimental groups, entanglement serves as a resource to perform quantum information tasks. In some cases entanglement turned out to be not only useful but also a necessary property of a quantum state in order to be useful for realization of quantum informational tasks. The most simple example is quantum teleportation of an unknown quantum state [7], which is impossible to perform without having an entangled state. Although examples of quantum algorithms exist [4, 8, 9] that theoretically outperform their classical analogues, their relation to entanglement is not so clear. In Ref. [15] it was shown that quantum computer, which operates with quasipure quantum states (pure states contaminated by white noise), is not able to outperform the classical factorization algorithm when the state stays separable throughout the computation. For pure states it was shown that in order to be able to outperform classical computation, quantum computing should be carried out on the states with sufficiently large amount of entanglement [16]. For quantum computation with pure states entanglement is proved to be a necessary resource, meaning

that if the amount of entanglement in a system, measured as a maximal Schmidt rank over all possible bipartitions, of n qubits scales at most logarithmically with the system size, then the classical simulation of n qubit computation can be done with only $poly(n)$ classical resources [16]. The general case of quantum computation with mixed states is more subtle and only partial answers are known. Certain computational schemes, e.g. deterministic quantum computation with one qubit (DQC1) [17] involving highly mixed state that does not contain much entanglement, are able to perform certain tasks (for DQC1 it is a computation of the normalized trace of a unitary matrix) with fixed accuracy exponentially faster than any known classical algorithm. Concerning this it was recently shown that the amount of correlations in a mixed state of a quantum computer implementing DQC1 is exponentially large [18]. These correlations do not need to be of quantum nature and the state contains only small amount of entanglement. It is important to note that there is no proof that no classical algorithm simulating DQC1 exists and the question of the classical simulatability of DQC1 is still open. Summarizing this paragraph one can say that entanglement is proved to be necessary for quantum teleportation and quantum computing with pure states.

During the last decade there has been a lot of effort to understand properties of entanglement. Yet there are still a number of entanglement's facets, which are not completely investigated. Which states are entangled, what type of entanglement is present in a particular entangled state, how can it be characterized and detected? These are only few of many [19] questions in quantum information theory that have no general answer.

In this thesis I address mainly two tasks. Firstly, I will attempt to answer the question: *How to decide whether a given physical state entangled or not?* The results will be formulated in a form of entanglement criteria that can be used to detect entanglement. Obviously in order to decide whether a given state is separable or entangled one needs some information about the state. Some of entanglement criteria need the full information about the state, i.e. use the density matrix for decision. Other criteria use only partial information about the state. The criteria formulated in this thesis belong to latter class entanglement criteria and are formulated in terms of second moments (covariances) of certain observables. Then, I will elaborate on the connection between entanglement detection and entanglement quantification. In particular, I will show that the entanglement criteria, which will be formulated in the main part of this thesis, can be used to estimate (in some cases even to calculate exactly) the amount of entanglement in a given quantum state. Secondly, I will consider Hamiltonians of disordered quantum spin models. Investigations of systems that are also a subject of intensive studies in condensed matter physics are motivated by the following question: *What properties of a quantum mechanical system are responsible for the existence of entanglement in it?* As it was shown by several authors, the ground states of many-body Hamiltonians must be highly entangled. It is therefore natural to consider disordered quantum system and analyze to which extent the disorder can affect the quantumness of initially highly entangled ground state of a many-body Hamiltonian. I will introduce a method that allows to investigate disordered quantum spin systems on two dimensional rectangular lattices

by renormalizing their Hamiltonian. The renormalization is carried out locally in the real space and therefore addresses the question of locality of correlations in these systems. On the one hand these investigations confirm the conjecture that the locality of correlations depends on the strength of disorder, which was proven rigorously for one dimensional systems and was indicated numerically for some two dimensional models. On the other hand I consider a new and more general framework for analyzing quantum Hamiltonians with arbitrary nearest neighbor interactions on rectangular lattices.

This thesis is organized as follows. Chapter 1 is thought to be a warm-up for upcoming sections and contains a short overview about topics related to the main subjects of the thesis. In the second Chapter of this thesis I introduce covariance matrices as a framework, which is used as a main tool in Chapters 3, 4, 5 and 6, where I investigate the questions of entanglement detection and quantification. In particular, Chapter 3 is devoted to the bipartite entanglement criterion, which is formulated in terms of the covariance matrix of a given quantum state. In Chapter 4 several ways of evaluation of this criterion are discussed. The generalization of the criterion on more than two parties is the subject of Chapter 5. In Chapter 6 the question of entanglement quantification with covariance matrices in bipartite case is investigated. The seventh chapter is devoted to the investigation of the influence of disorder on many body quantum systems.

Chapter 1

Preliminaries

In this chapter I will briefly discuss notions of entanglement and its role in solid state systems.

1.1 Entanglement: general notions, bipartite case

1.1.1 Bipartite pure states

Let us begin our discussion with the bipartite pure case. Assume we have a task to describe two physical systems A and B simultaneously. In quantum mechanics one associates to each system a Hilbert space and to each physical state a normalized vector in this particular space. The composite system AB is then associated with a Hilbert space, which is the tensor product of the individual Hilbert spaces $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ with $d_A = \dim \mathcal{H}_A < \infty$ and $d_B = \dim \mathcal{H}_B < \infty$ their dimensions. The states of the composite system are then again normalized vectors that can be written in the form

$$|\psi_{AB}\rangle = \sum_{i=1}^{n} \sum_{j=1}^{m} c_{ij} |\psi_i^A\rangle \otimes |\psi_j^B\rangle, \tag{1.1}$$

where $n = dim\mathcal{H}_A$ and $m = dim\mathcal{H}_B$ respectively. In this case one speaks of *bipartite* pure states.

All states of the composite system can be now naturally divided into two groups: *entangled* and *separable*.

Definition 1.1. *A given pure state $|\psi_{AB}\rangle$ is called* **separable** *iff it can be written as a tensor product of the form*

$$|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle. \tag{1.2}$$

It is called **entangled** *otherwise.*

To pick an example, let us consider a system, that consists of only two spin-$\frac{1}{2}$ particles. Denote by $|0\rangle$ and $|1\rangle$ the spin up and spin down polarizations of the particle, then the state $|00\rangle$ is an example of a separable pure state, whereas a singlet $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ is an example of an entangled state.

Physically one can perceive the product states as completely uncorrelated states. Two experimentalists can prepare their states locally in their labs independently of each other. The resulting state of the composite system will be always a product state. There is however no chance to prepare a state $|\psi^-\rangle$ in such a way [1, 11].

The question how to distinguish between separable and entangled states is rather easy to answer. Indeed, the state $|\psi_{AB}\rangle$ is a product state if and only if the rank of the matrix of the coefficients $C = \{c_{ij}\}$ in (1.1) is equal to one. It turns out that for the description of entangled states it is useful to represent the state $|\psi_{AB}\rangle$ in a particular form

$$|\psi_{AB}\rangle = \sum_{i=1}^{r} \lambda_i |\psi_i^A\rangle \otimes |\psi_i^B\rangle. \tag{1.3}$$

Such a representation always exists and is called *Schmidt decomposition*. The coefficients $\lambda_i > 0$ are the singular values of the matrix C [20, 21] and the number r is called *Schmidt rank*. Therefore, in terms of the Schmidt decomposition we come to the following conclusion:

Remark 1.2. *A given pure state $|\psi_{AB}\rangle$ of a composite system associated with the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ is entangled iff its Schmidt rank r is strictly larger than one.*

1.1.2 Bipartite mixed states

Now imagine that we are not provided with the information which state describes the composite system AB in a faithful way. However, we do know that the system is in one of the states $|\psi_\alpha^{AB}\rangle$, where α can take values from 1 to some P. In this case we say that the system is in a mixed state and describe it in terms of linear[1]. positive semidefinite operators with unit trace

$$\rho^{AB} = \sum_{\alpha=1}^{P} p_\alpha |\psi_\alpha^{AB}\rangle\langle\psi_\alpha^{AB}|, \tag{1.4}$$

with probabilities $p_\alpha > 0$ and $\sum_{\alpha=1}^{P} p_\alpha = 1$. Mixed states can be classified as follows:

Definition 1.3. *(Mixed states) A given mixed state ρ^{AB} is a* **product state** *iff it can be written as*

$$\rho^{AB} = \rho^A \otimes \rho^B. \tag{1.5}$$

The state is called **separable** *iff it belongs to the convex hull of product states*

$$\rho = \sum_{\alpha} p_\alpha \rho_\alpha^A \otimes \rho_\alpha^B. \tag{1.6}$$

It is called **entangled** *otherwise.*

[1]The set of Hermitian linear operators is denoted by $\mathcal{B}(\mathcal{H})$

Separable states contain a certain amount of correlations. However, for preparing these states no non-local apparatus is necessary. Indeed if we would like to prepare such a state we would need again two experimentalists in two distinct labs, a couple of dice and a telegraphic channel between the labs. For every outcome α of a die throw that occurs with a certain probability p_α the experimentalists agree to prepare a state $\rho_\alpha^A \otimes \rho_\alpha^B$ locally. By this procedure they produce a state of the type (1.6) in Definition 1.3. This state will be separable and the preparation procedure, which led to that state, does not need quantum mechanical correlations, which can be in principle established between two distinct labs.

The described process can be cast in a mathematical strict framework. The general statement in quantum information theory reads *entanglement can not be produced by local operations and classical communication (LOCC)*. The outstanding importance of this statement will start to become clear in the next chapter, where we discuss entanglement measures.

For the time being we note that to decide whether the given bipartite mixed state is entangled or not is a computationally hard task. This problem is known under the name *separability problem*. The difficulty of this problem can be illustrated by the following example. Imagine we are given a bipartite state ρ and would like to know whether know, whether it is entangled or separable. Then naively one could solve the problem by minimizing distance between the state and the convex set of the separable states

$$D(\rho) = \min_{\pi \in \mathcal{S}} ||\rho - \sigma||, \tag{1.7}$$

where $||.||$ is some operator norm. In order to calculate this distance one has to minimize over all separable states, which is in general very hard. We will come back to the separability problem later and demonstrate that in some special cases this problem yet can be solved exactly.

1.1.3 Bipartite states in infinite dimensional Hilbert spaces

The general notion of a pure or mixed state as well as the definition of separability does not depend on the dimensionality of the underlying Hilbert spaces. However the forthcoming analysis of the properties of the quantum states and their description relies heavily on the fact, whether the underlying Hilbert space is finite dimensional or not.

In this part we discuss several specific issues of quantum states in infinite dimensional Hilbert spaces. To motivate this discussion we point out that many experiments in quantum information are carried out in the quantum optical setting. The observables in this setting are quadratures of the field modes that satisfy canonical commutation relations and have no finite-dimensional realizations

$$[X_\alpha, P_\beta] = i\delta_{\alpha\beta}\mathbb{1},\ [X_\alpha, X_\beta] = [P_\alpha, P_\beta] = 0, \tag{1.8}$$

where $\alpha, \beta = 1, \ldots, n$ is the number of field modes in a wave packet, generally these are canonical coordinates. Very often it is useful to describe the system in the phase

space. To this end one can rewrite the commutation relations in a more compact form

$$[R_\alpha, R_\beta] = i\sigma_{\alpha\beta}\mathbb{1},\ \sigma = \begin{pmatrix} \mathbb{O} & \mathbb{1} \\ -\mathbb{1} & \mathbb{O} \end{pmatrix}. \tag{1.9}$$

σ is called the *symplectic matrix* and $R_\alpha \in \{X_1, \ldots, X_n, P_1, \ldots, P_n\}$ is one of the $2n$ canonical observables.

Using these notions one defines the so-called *Weyl operators*

$$\mathbf{W}\left(\overrightarrow{\xi}\right) = \exp\left(i\overrightarrow{\xi}\sigma\overrightarrow{R}\right), \tag{1.10}$$

where we used the shorthand notation $\overrightarrow{\xi}\sigma\overrightarrow{R} = \sum_{\alpha,\beta}\xi_\alpha\sigma_{\alpha\beta}R_\beta$ and denoted by $\overrightarrow{\xi}$ vectors in the phase space. Weyl operators act as translation operators on the phase space. Often in quantum optics these operators are written in terms of creation and annihilation operators of particular optical modes and called *displacement operators*.

To reveal the important role of Weyl operators in quantum mechanics we note, under the assumption that there are no further degrees of freedom in the system, that $W(\overrightarrow{\xi})$ contains all possible products of operators of the type $R_1^{m_1}R_2^{m_2}\cdots R_{2n}^{m_{2n}}$. Therefore taking the expectation values of these operators in some state ρ will provide complete information about the state. Formally, one says that the state ρ *is determined by its characteristic function* and writes

$$C\left(\overrightarrow{\xi}\right) = \mathrm{Tr}\left(\rho\mathbf{W}\left(\overrightarrow{\xi}\right)\right). \tag{1.11}$$

The characteristic function (1.11) can be interpreted as a *quantum Fourier transformation* of the density operator ρ [22].

In quantum optics one frequently uses the notion of *Wigner function* [23, 24]. This function is defined as inverse classical Fourier transform of the characteristic function [25]

$$W\left(\overrightarrow{\eta}\right) = \mathcal{F}_c^{-1}\left(C\left(\overrightarrow{\xi}\right)\right) \tag{1.12}$$

To gain ground a bit we calculate the Wigner function of one mode. In this case $\overrightarrow{R} = (\mathbf{q}, \mathbf{p})$ and the Weyl operator takes the form

$$\mathbf{W}\left(q_0, p_0\right) = \mathrm{e}^{i(q_0\mathbf{p} - p_0\mathbf{q})} = \mathrm{e}^{-ip_0\mathbf{q}}\mathrm{e}^{iq_0\mathbf{p}}\mathrm{e}^{\frac{1}{2}[-p_0\mathbf{q}, q_0\mathbf{p}]} = \mathrm{e}^{-ip_0\mathbf{q}}\mathrm{e}^{iq_0\mathbf{p}}\mathrm{e}^{-\frac{i}{2}p_0q_0}, \tag{1.13}$$

where we used the Baker-Campbell-Hausdorff formula and the fact that $[\mathbf{q}, \mathbf{p}] = i\mathbb{1}$. In order to express the characteristic function in notation common in quantum optics literature it is convenient to rewrite the Weyl operator in the following form

$$\mathbf{W}\left(q_0, p_0\right) = \mathrm{e}^{i\frac{q_0}{2}\mathbf{p}}\mathrm{e}^{-i\frac{q_0}{2}\mathbf{p}}\mathrm{e}^{-ip_0\mathbf{q}}\mathrm{e}^{i\frac{q_0}{2}\mathbf{p}}\mathrm{e}^{i\frac{q_0}{2}\mathbf{p}}\mathrm{e}^{-\frac{i}{2}p_0q_0}. \tag{1.14}$$

For further simplification it is worth to use following relations

$$\begin{aligned}
&\mathrm{e}^A F(B)\mathrm{e}^{-A} = F\left(\mathrm{e}^A B\mathrm{e}^{-A}\right), \text{ with } F \text{ some analytic function} \\
&\mathrm{e}^A B\mathrm{e}^{-A} = B + [A, B], \text{ if } [A, [A, B]] = 0 \\
&\mathrm{e}^{-iu\mathbf{p}}|\psi(q,p)\rangle = |\psi(q+u,p)\rangle,\ \mathbf{q}|\psi(q,p)\rangle = q|\psi(q,p)\rangle, \text{ in } q\text{-representation.}
\end{aligned} \tag{1.15}$$

Putting together (1.14) and (1.15) we arrive at

$$\begin{aligned} C(q_0,p_0) &= \mathrm{Tr}\left(\rho \mathrm{e}^{i\frac{q_0}{2}\mathbf{p}}\mathrm{e}^{-ip_0\mathbf{q}+\frac{i}{2}p_0q_0}\mathrm{e}^{i\frac{q_0}{2}\mathbf{p}}\mathrm{e}^{-\frac{i}{2}p_0q_0}\right) \\ &= \mathrm{Tr}\left(\mathrm{e}^{i\frac{q_0}{2}\mathbf{p}}\rho \mathrm{e}^{i\frac{q_0}{2}\mathbf{p}}\mathrm{e}^{-ip_0\mathbf{q}}\right) \\ &= \int dq \langle q|\mathrm{e}^{i\frac{q_0}{2}\mathbf{p}}\rho \mathrm{e}^{i\frac{q_0}{2}\mathbf{p}}\mathrm{e}^{-ip_0\mathbf{q}}|q\rangle \\ &= \int dq \langle q+\frac{q_0}{2}|\rho|q-\frac{q_0}{2}\rangle \mathrm{e}^{-ip_0q}. \end{aligned} \tag{1.16}$$

Finally we calculate the Wigner function

$$\begin{aligned} W(q',p') &= \frac{1}{4\pi^2}\iint dqdpC(q,p)\mathrm{e}^{i(q'p+p'q)} \\ &= \frac{1}{4\pi^2}\iiint dqdq_0dp\langle q_0+\frac{q}{2}|\rho|q_0-\frac{q}{2}\rangle \mathrm{e}^{ip(q'-q_0)}\mathrm{e}^{ip'q} \qquad (1.17) \\ &= \frac{1}{2\pi}\int dq\langle q'+\frac{q}{2}|\rho|q'-\frac{q}{2}\rangle \mathrm{e}^{ip'q}, \qquad (1.18) \end{aligned}$$

where we used $\int dp \mathrm{e}^{ip(q'-q_0)} = 2\pi\delta(q_0-q')$. This is the common form of the Wigner function. Rather often the Wigner function is just defined in this way without any further explanation and discussion of its origins. Integrating $W(q',p')$ over q' (p') gives the probability distribution of momentum (coordinate):

$$\begin{aligned} \int_{q'} W(q',p') &= \langle p'|\rho|p'\rangle \\ \int_{p'} W(q',p') &= \langle q'|\rho|q'\rangle. \end{aligned} \tag{1.19}$$

The Wigner function is a *quasi-probability distribution*, since it can be negative. There are important examples of states, however, for which the Wigner function is positive, these are mixtures of *coherent states* or *squeezed vacuum states*. The positivity of the Wigner function was believed to be connected to the existence of a local realistic model. Bell conjectured that a positive Wigner function can not violate certain inequalities that cannot be violated by a local realistic models. Later these type of locality tests became his name and now are called *Bell inequalities*. Recently, however, one was able to provide an example of a positive Wigner function that does violate a Bell inequality [26].

In this framework it is easy to define a special class of states, which play an important role in quantum optics and quantum information theory.

Definition 1.4. *A state ρ is called* **Gaussian** *if its characteristic function has a Gaussian form*

$$G\left(\overrightarrow{\xi}\right) = Tr\left(\rho \mathbf{W}\left(\overrightarrow{\xi}\right)\right) = \exp\left(i\overrightarrow{E}\cdot\overrightarrow{\xi} - \frac{1}{2}\overrightarrow{\xi}^T\gamma\overrightarrow{\xi}\right), \tag{1.20}$$

where

$$\overrightarrow{E} = (\langle R_1 \rangle, \ldots, \langle R_{2n} \rangle) \tag{1.21}$$

denotes the vector of mean values of observables R_α *and*

$$\gamma_{\alpha\beta} = \frac{1}{2}\langle \{R_\alpha, R_\beta\} \rangle - \langle R_\alpha \rangle \langle R_\beta \rangle \tag{1.22}$$

is the matrix of second moments or the **covariance matrix**.

The covariance matrix γ exists for every state. However, for Gaussian states, all higher moments disappear and the covariance matrix fully characterize the properties of the state.

The covariance matrix is a real, symmetric and positive semidefinite. Note that the covariance matrix and the symplectic matrix σ are related via

$$\gamma + \frac{i}{2}\sigma \geq 0. \tag{1.23}$$

It is important to point out that the latter relation is a matrix form of the quantum mechanical uncertainty relations. Interestingly the opposite is also true, i.e. if a matrix fulfills (1.23) then it is a covariance matrix of a valid state.

An important example of Gaussian states are coherent states, which were introduced by Schrödinger in order to achieve an equality in Heisenberg's uncertainty relation. Nowadays coherent states are used in various branches of physics. For example squeezed states of the light field can be used to generate continuous variable cluster states, which are universal resource for one-way quantum computation [27, 28, 29, 30, 31].

Gaussian states can be generalized to any number of parties. The composite phase space will be given by a orthogonal sum of its components and Weyl operators can be identified with tensor products [32]

$$\mathbf{W}\left(\overrightarrow{\xi}_A \oplus \overrightarrow{\xi}_B\right) \sim \mathbf{W}\left(\overrightarrow{\xi}_A\right) \otimes \mathbf{W}\left(\overrightarrow{\xi}_B\right). \tag{1.24}$$

Entanglement properties of Gaussian states are rather well understood. There is a necessary and sufficient criterion for these states to be separable [32, 33].

1.2 Multipartite entanglement

In the case of more than two systems the notion of entanglement becomes more complicated. There are different classes of entangled states depending on the fact how many parties are entangled with each other. We begin with the case of three qubits.

1.2.1 Three qubits

As usual we start our discussion with pure states.

Definition 1.5. *A pure three qubit state is called* **fully separable** *iff it can be written in the form*

$$|\psi_{fs}^{ABC}\rangle = |\psi^A\rangle \otimes |\psi^B\rangle \otimes |\psi^C\rangle. \tag{1.25}$$

Another possible situation, which arises, when we go beyond the bipartite setting, is that two of three parties share some entanglement and no entanglement with the third party.

Definition 1.6. *A pure three qubit state is called* **bi-separable** *with respect to the bipartition $AB|C$ iff it can be written in the form*

$$|\psi_{bs}^{AB|C}\rangle = |\psi^{AB}\rangle \otimes |\psi^C\rangle, \tag{1.26}$$

where $|\psi^{AB}\rangle$ is an entangled state in $\mathcal{H}_A \otimes \mathcal{H}_B$.

The last class of entanglement in the case of pure tripartite states is the class of *genuine tripartite entangled* states.

Definition 1.7. *A pure three qubit state is called* **genuinely tripartite entangled** *iff it is neither fully separable nor bi-separable with respect to any bipartition.*

From Definitions 1.6 and 1.7 one can immediately conclude that the states from the one class can not be transformed into the states from the other class by using LOCC operations.

It turns out that a reasonable classification of tripartite (and actually multipartite) entangled states is done in terms of stochastic LOCC operations (SLOCC), i.e. LOCC operations without demanding that the result is achieved with unit probability [41]. Such operations are termed *SLOCC* or *Local Filtering Operations*. Formally, the equivalence is defined in the following way:

Definition 1.8. *Two states $|\psi\rangle$ and $|\phi\rangle$ are equivalent $|\psi\rangle \sim |\phi\rangle$ iff there exist invertible local operations O_A, O_B and O_C such that*

$$|\psi\rangle = O_A \otimes O_B \otimes O_C |\phi\rangle. \tag{1.27}$$

The definition of such an equivalence relation is reasonable, since one can prove that the equivalent states can be used to implement the same tasks of quantum information theory. Note however that the success probability of performing a task may differ in this case. As it was proved in Ref. [41], there are two different equivalence classes of genuinely three qubit entangled states called *GHZ-* and *W-class*. In this sense the GHZ-state

$$|GHZ_3\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right) \tag{1.28}$$

cannot be transformed by SLOCC operations into a W-state

$$|W_3\rangle = \frac{1}{\sqrt{3}}\left(|001\rangle + |010\rangle + |100\rangle\right). \tag{1.29}$$

The parametrization of pure three qubit states has been done in [42] by proving that every pure three qubit state can be transformed into

$$|\psi\rangle = \lambda_0|000\rangle + \lambda_1 e^{i\theta}|100\rangle + \lambda_2|101\rangle + \lambda_3|110\rangle + \lambda_4|111\rangle \tag{1.30}$$

by local unitary operations. The coefficients in (1.30) fulfill $\lambda_i \geq 0$, $\sum_i \lambda_i^2 = 1$ and $\theta \in [0, \pi]$. Therefore there are six parameters, which characterize non-local properties of the three qubit states. It is noteworthy that for the W-class of states $\theta = \lambda_4 = 0$ holds. Thus the states from the W-class form a set of measure zero in the set of all pure states.

Physically, the GHZ-states are generalization of maximally entangled Bell states for two qubits. However, the GHZ-states are extremely sensitive to the loss of qubits: if one qubit is gone, no entanglement is left at all. The W-states in contrast are more robust in this sense. Indeed, the reduced state $\rho_{AB} = \mathrm{Tr}\left(|W_3\rangle\langle W_3|\right)_C$ is still entangled.

1.2.2 Multipartite pure states

The number of different entanglement classes grows with the number of parties and the classification of the pure multipartite states becomes a rather difficult task. One straightforward way to achieve the task is to generalize the method for three parties and define classes according to SLOCC operations. One way of doing it was presented in [43, 44]. There, each class was assigned to its *normal form*. States, which belong to different classes cannot be transformed into each other by SLOCC. The main problem in such a classification is the fact that already for four qubits one derives nine different families of states. Each family is parametrized by certain complex numbers, which leads us to the conclusion that there are actually infinitely many SLOCC equivalence classes for four qubits. Another approach to classify pure states under SLOCC operations based on analysis of the tensor of the coefficients of a pure state in an arbitrary product basis $C_{i_1,i_2,\ldots,i_N}$ [45, 46]. There the authors provide a recursive (in the number of parties) method of classification of entangled states. For two parties the answer is given by the Schmidt decomposition, i.e. if the matrix C_{i_1,i_2} has only one non-zero singular value, then the state is a product state. For three parties three different decompositions must be considered. For every bipartition C can be seen as a $d^2 \times d^2$ matrix. Then the characterization of entanglement classes can be done by considering singular values of the matrix C and its right singular vectors. Furthermore one can prove that knowing the characterization for N parties one also knows the characterization for $N+1$ parties, which is proven by induction in [45].

Besides the question of which states can be converted into each other by SLOCC operations and therefore share the same entanglement properties and can be in

principle used to carry out the same quantum informational tasks, an important question of interconvertability of the pure states under local unitary (LU) operations was open until recently [47]. Two states, which can be converted into each other by LU-operations are completely equivalent from the point of view of quantum information theory. Obviously such states belong to the same equivalence class under SLOCC and possess the same type of entanglement. Moreover they do possess precisely the same amount of entanglement. Indeed one can provide a criterion of interconvertability of the pure states by LU operations. The idea consists of introducing the *LU standard form*, which can be easily computed. The necessary and sufficient condition of two pure states to be LU equivalent is coincidence of their standard forms [47].

1.2.3 Multipartite mixed states

The classification for mixed state is done in the same manner as for pure states. One can associate with a class of pure states a class of mixed states that will be just a convex sum of the former. For example for three qubits one can use the following classification:

Definition 1.9. *A mixed three qubit state is called* **fully separable**, *iff*

$$\rho_{fs} = \sum_i p_i |\psi_i^{fs}\rangle\langle\psi_i^{fs}| \tag{1.31}$$

bi-separable, *iff*

$$\rho_{bs} = \sum_i p_i |\psi_i^{bs}\rangle\langle\psi_i^{bs}|, \tag{1.32}$$

where $|\psi_i^{bs}\rangle$ *is separable with respect to some bipartition.*
The state belongs to the **W-class**, *iff*

$$\rho_W = \sum_i p_i |\psi_i^{W}\rangle\langle\psi_i^{W}|, \tag{1.33}$$

and to the **GHZ-class**, *iff*

$$\rho_{GHZ} = \sum_i p_i |\psi_i^{GHZ}\rangle\langle\psi_i^{GHZ}|. \tag{1.34}$$

Two facts should be mentioned about the GHZ- and W-class of mixed states. First of all one can show that the set of W states lies in the set of GHZ states, the GHZ states in this sense form a bigger set. Secondly, in contrast to the case of pure states, the W mixed states are not a set of measure zero anymore [48]. Interestingly, for mixed states there are examples of states that are biseparable with respect to any bipartition and yet entangled [49]. Furthermore, such states appear naturally as thermal states in quantum spin chains [50, 51] and will be one of the objects of study in this thesis.

1.3 Entanglement detection

1.3.1 Separability criteria and bound entanglement

Although the separability problem mentioned in Section 1.1.2 is generally very hard to solve some partial answers are already known. Usually these answers are formulated in the form of criteria that impose some conditions on separable or entangled states.

Historically one of the first separability criteria is called *partially positive transpose* criterion or PPT criterion, was introduced for finite-dimensional systems in [52].

Before we formulate the criterion we shall dwell on the term partial transpose. A mixed state can be represented by a density matrix that we can expand in a chosen basis

$$\rho_{AB} = \sum_{i,j=1}^{n} \sum_{k,l=1}^{m} \rho_{ij,kl} |i\rangle\langle j| \otimes |k\rangle\langle l|. \tag{1.35}$$

The partial transposition of a matrix is a transposition with respect to one of the subsystems. Hence there are two possibilities for to give a partial transposition: (i) with respect to subsystem A: $\rho_{AB}^{T_A} = \sum_{i,j=1}^{n} \sum_{k,l=1}^{m} \rho_{ji,kl} |i\rangle\langle j| \otimes |k\rangle\langle l|$ and (ii) with respect to subsystem B: $\rho_{AB}^{T_B} = \sum_{i,j=1}^{n} \sum_{k,l=1}^{m} \rho_{ij,lk} |i\rangle\langle j| \otimes |k\rangle\langle l|$.

Note that although the partial transposition depends on the basis choice, the spectrum of the matrix before and after the partial transposition does not.

Definition 1.10. *We say that the matrix ρ_{AB} has a positive partial transpose (or it is a PPT matrix) iff*

$$\rho_{AB}^{T_A} \geq 0 \;\Leftrightarrow\; \rho_{AB}^{T_B} \geq 0. \tag{1.36}$$

If the matrix is not PPT we call it a negative partial transpose (NPT) matrix.

Now we are ready to formulate the PPT criterion.

Theorem 1.11. *If a given bipartite state ρ_{AB} is separable, then it has a positive partial transpose.*

Proof: The claim follows immediately from the definition 1.3 of separable mixed states.

$$\rho^{T_B} = \sum_{\alpha} p_\alpha \rho_\alpha^A \otimes \left(\rho_\alpha^B\right)^T, \tag{1.37}$$

since for all α ρ_α^B is a density matrix its transpose is also positive.
■

The last theorem provides us with a very strong criterion. For a given density matrix one can easily calculate the partial transpose and decide whether the result is still positive semidefinite or not. The PPT criterion provides a complete solution for the separability problem for the case of small dimensions of the Hilbert spaces:

Theorem 1.12. *For $n = 2$ and $m = 2, 3$ a given bipartite state ρ_{AB} is separable, iff it has a positive partial transpose.*

Proof: The proof of the claim is given in [59].
■

The first counterexample of a state in a 2×4 system that has a positive partial transpose yet cannot be decomposed as in the definition 1.3 was given in Ref. [60]. These type of states is called *bound entangled states* as the opposite to *free entanglement* contained in states with negative partial transpose (NPT states).

Bound entangled states contain a relatively small amount of entanglement. At this point one faces the following dilemma: on the one hand, to perform many quantum informational tasks one needs maximally entangled states, e.g. for quantum teleportation or for quantum dense coding. On the other hand, maximally entangled states are hardly achievable experimentally because of the presence of noise. In principle the noise can be so strong that the prepared quantum state would be bound entangled. The question whether one can use noisy or bound entangled states for quantum information processing is therefore of a great importance.

The answer on this question is following. First of all it is possible to distill some of the noisy entangled states. Under distillation we understand a LOCC protocol, which is able to produce some singlets out of many copies of the noisy entangled states [53, 54]. Secondly, although such distillation is not possible for bound entangled states [55], bound entangled states can be used to establish a secret key in quantum cryptography [56] or to increase the fidelity of the state teleportation [57]. The last phenomenon is known as *activation of the bound entanglement*. Furthermore, it has been shown that bound entangled states can maximally violate Bell inequalities [58].

Continuing the discussion of the separability criteria we point out that the separability problem can be formulated in terms of positive maps. Note that a linear map is called positive if it maps positive operators into a set of positive operators, i.e. if $O \geq 0$, then $\Lambda(O) \geq 0$ (a linear map Λ is called completely positive if and only if $\Lambda \otimes \mathbb{1}_n$ is positive for all n). In this framework the following statement is true [59]:

Theorem 1.13. *A given bipartite state ρ_{AB} is separable, iff $(\mathbb{1} \otimes \Lambda_B)\rho$ is positive for any positive map $\Lambda_B : \mathcal{B}(\mathcal{H}_B) \to \mathcal{B}(\mathcal{H}_B)$.*

Note that the choice of the subspace, to which the map Λ is applied, in the theorem 1.13 is arbitrary. Indeed, the result also holds if one takes maps $\Lambda_A \otimes \Lambda_B$ or $\Lambda_A \otimes \mathbb{1}$, where Λ_A is positive.

The connection of the separability problem to the positive maps turns out to be very fruitful. Several other criteria formulated later, such as the *reduction criterion* [61] or the *majorization criterion* [62] can be brought in connection with positive maps and do not detect PPT entangled states. One has however to mention that the

connection of the majorization criterion to the positive maps has been only a conjecture for several years. In fact the majorization criterion is implied by the reduction criterion, which was proved in [63]. We state here the majorization criterion, since it provides the answer to the question of distillability and bound entanglement:

Theorem 1.14. *If ρ_{AB} is separable then the eigenvalues of either reduced states ρ_A and ρ_B are* **majorized** *by the eigenvalues of ρ_{AB}*

$$\lambda(\rho_{AB}) \prec \lambda(\rho_A),\ \lambda(\rho_{AB}) \prec \lambda(\rho_B), \tag{1.38}$$

where the eigenvalues are arranged in descending order and $\lambda(\rho_{AB}) \prec \lambda(\rho_A)$ means that for every $m < rank(\rho_{AB})$

$$\sum_{k=1}^{m} \lambda_k^{\downarrow}(\rho_{AB}) \leq \sum_{k=1}^{m} \lambda_k^{\downarrow}(\rho_A) \tag{1.39}$$

holds.

Proof: The proof of the theorem can be found in [62]. ■

The majorization criterion has an intuitive physical interpretation that separable states are more disordered globally than locally. This intuition follows from the fact that the majorization can be quantified in terms of the von Neumann entropy [62].

The following statement characterizes the distillability property of quantum states and connects it with the positivity of partial transpose.

Theorem 1.15. *If a bipartite state is PPT or bound entangled, then the state is undistillable. If a state violates the majorization criterion, then the state is distillable.*

Proof: The first part of the proof can be found in [55], for the proof of the second part we refer the reader to [63]. ■

Apart from the criteria that can be connected to the positive maps there are criteria where such connection seemingly does not exist.

The most prominent criterion of this type is the computable cross-norm or realignment criterion [64, 65, 66] (CCNR). The simplest way to formulate this criterion is to consider the Schmidt decomposition for density matrices

$$\rho_{AB} = \sum_{k=1}^{\min\{n,m\}^2-1} \sigma_k G_k^A \otimes G_k^B, \tag{1.40}$$

where the operators $G_k^{A/B}$ form an orthonormal basis in $\mathcal{B}(\mathcal{H}_{A/B})$ with respect to the scalar product $\mathrm{Tr}\left(A^{\dagger}B\right)$. Then the following statement is true [67]

Theorem 1.16. *If a given state ρ_{AB} is separable, then $\sum_{k=1}^{\min\{n,m\}^2-1} \sigma_k \leq 1$. If $\sum_{k=1}^{\min\{n,m\}^2-1} \sigma_k > 1$ then the state ρ_{AB} must be entangled.*

This criterion can be seen as the complement to the PPT criterion in the following sense: it detects states, which the PPT criterion fails to detect, i.e. it detects bound entangled states. One can interpret the detection of bound entangled states as a measure of performance of separability criteria that go beyond the usual PPT or positive maps scenario.

Up to now we have been discussing entanglement criteria that need a state as an input to answer (albeit in most cases partially) the separability question. However the full knowledge of the state is a rare event in the real world. For example we can give an existent state to an experimentalist and ask him/her to determine whether the state is entangled or not but we do not say how the state looks like, so the experimentalist is left without any knowledge about the state. Even if the experimentalist prepares some state for him/herself with a good precision the interaction with the environment is unavoidable and will cause decoherence and hence a certain deviation from the initial state. These kind of situation leads us to a natural question: *What kind of information about the state will suffice to answer the separability question?* We have already learned that entanglement is a resource of purely quantum mechanical correlations. Correlations can be measured and to do this we need to pick up certain observables. As it can be guessed from the EPR paradox the observables that one should choose to detect the quantum mechanical correlations should not commute. The EPR type of correlations was then predicted theoretically for quantum optical systems [68]. It turned out that it is possible to formulate a separability criterion in terms of non-commuting observables (also called EPR-operators) for continuous variable systems [69, 70]. This criterion established a connection between uncertainty relations and entanglement for infinite-dimensional systems. For finite-dimensional systems this connection was established in [71, 72] and resulted in the so-called *entanglement criterion based on local uncertainty relations* (LUR-criterion).

Proposition 1.17. *Let ρ be a separable state and let A_i, B_i, $i = 1, \ldots, n$ be observables on $\mathcal{H}_A$, $\mathcal{H}_B$ respectively, such that $\sum_{i=1}^{n} \delta^2 (A_i)_{\rho_A} \geq C_A$ and $\sum_{i=1}^{n} \delta^2 (B_i)_{\rho_B} \geq C_B$. Then*

$$\sum_{i=1}^{n} \delta^2 (A_i \otimes \mathbb{1} + \mathbb{1} \otimes B_i)_{\rho} \geq C_A + C_B \tag{1.41}$$

holds.

Although the LURs provide very strong criterion, it is not *a priori* clear which local observables should be chosen in order to detect a given entangled state. This is one of the disadvantages of the LURs, which one can overcome.

1.3.2 Separability criteria for Gaussian states

To close the part dedicated to entanglement criteria we discuss the case of infinite-dimensional Hilbert spaces. The scope of our discussion here will be the special class of states, namely Gaussian states, which were defined in Section 1.1.3. Separability

properties of the Gaussian states were discussed first in [69, 70] in the simplest case of two modes.

One way to characterize entanglement in continuous variable systems is to generalize the PPT criterion (Theorem 1.11) to the case of infinite dimensional Hilbert spaces. Note that transposition operation corresponds to the sign flip of the momenta of the system:

$$\begin{aligned} \rho \to \rho^T \;\Leftrightarrow\; \mathrm{Tr}\left(\rho \mathbf{W}\left(\overrightarrow{\xi}\right)\right) \to \mathrm{Tr}\left(\rho^T \mathbf{W}\left(\overrightarrow{\xi}\right)\right) \\ \mathrm{Tr}\left(\rho^T \mathbf{W}\left(\overrightarrow{\xi}\right)\right) = \mathrm{Tr}\left(\rho \mathrm{e}^{i\overrightarrow{\xi}\sigma^T\overrightarrow{R}}\right), \end{aligned} \tag{1.42}$$

where we used the the definition of the Weyl operators Eq. (1.10). The transposition of the symplectic matrix σ is equivalent to the sign flip of the canonical commutation relations (1.8) or to the sign change of all P_α, which is again is the same as the sign change of p_α in $\overrightarrow{\xi}$.

Therefore, the operation of partial transposition for a system consisting of two modes can be written as the following map on the phase space:

$$\Lambda \;:\; \overrightarrow{\xi} = (x1, p1, x2, p2) \mapsto \overrightarrow{\xi}' = (x1, p1, x2, -p2). \tag{1.43}$$

Therefore the PPT criterion for separability for a two mode state ρ can be formulated as

Theorem 1.18. *If a given two mode state ρ is separable, then its characteristic function $C\left(\overrightarrow{\xi}\right)$ necessarily goes over into a characteristic function of a valid state under the transformation $\Lambda = diag\{1, 1, 1, -1\}$*

$$C\left(\Lambda\overrightarrow{\xi}\right) \to C\left(\overrightarrow{\xi}\right) \tag{1.44}$$

Physically, it means that local time reversal Λ is a symmetry on the subspace of all separable states [70].

The covariance matrix, defined in Eqs. (1.20,1.22) transforms according to

$$\gamma' = \Lambda\gamma\Lambda. \tag{1.45}$$

For all separable states the symmetry (1.44) implies that the corresponding covariance matrix γ' after the partial transpose operation is still a covariance matrix of a physical state. Then the uncertainty condition (1.23) holds

$$\gamma' + \frac{i}{2}\sigma \geq 0 \tag{1.46}$$

or equivalently

$$\gamma + \frac{i}{2}\sigma' \geq 0, \text{ with } \sigma' = \Lambda\sigma\Lambda = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{1.47}$$

Hence the necessary condition for separability for continuous variable states can be formulated in terms of covariance matrices:

Corollary 1.19. *Let be ρ a two mode state with covariance matrix*

$$\gamma(\rho) = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix}. \tag{1.48}$$

If ρ is separable then

$$\det A \det B - \left(\frac{1}{4} - |\det C|\right)^2 - \mathrm{Tr}\left(A\sigma C\sigma B\sigma C^T\sigma\right) \geq \frac{1}{4}(\det A + \det B) \tag{1.49}$$

must hold.

Proof: The first step of the proof is to put the conditions (1.23) and (1.47) together and to realize that Eqs. (1.49), (1.23) and (1.47) are equivalent if the covariance matrix $\gamma(\rho)$ has a special form, namely

$$\gamma(\rho) = \begin{pmatrix} a & 0 & c_1 & 0 \\ 0 & a & 0 & c_2 \\ c_1 & 0 & b & 0 \\ 0 & c_2 & 0 & b \end{pmatrix}. \tag{1.50}$$

Secondly, any covariance matrix can be transformed in this form by the local transformations $Sp(2,\mathbb{R}) \otimes Sp(2,\mathbb{R})$ that do not affect separability of a given state. The technical details of the proof can be found in [70]. ■

The condition in Eq. (1.47) is in fact the PPT criterion for continuous variable states in terms of covariance matrices. Being closely related to the uncertainty principle this condition must be seen as an additional condition on the uncertainties for all separable states.

This fact can be directly seen on a simple example of two mode squeezed states. Consider operators of EPR type [69]

$$S_x(a) = |a|X_1 + \frac{1}{a}X_2, \tag{1.51}$$

$$S_p(a) = |a|P_1 + \frac{1}{a}P_2. \tag{1.52}$$

Operators S_x and S_p commute if $a = 1$ and can therefore be measured simultaneously in this case. The state where the uncertainty of the measurement of these two operators is zero is a maximally entangled state. Conversely, for all separable states there exists a lower bound for uncertainty:

Theorem 1.20. *([69]) For any two mode separable state ρ*

$$\delta^2\left(S_x(a)\right)_\rho + \delta^2\left(S_p(a)\right)_\rho \geq a^2 + \frac{1}{a^2}. \tag{1.53}$$

Proof: First of all let us note that the Heisenberg uncertainty relation can be written as

$$\delta^2(X)\,\delta^2(P) \geq \frac{1}{4}|[X,P]|^2 \;\Rightarrow\; \delta^2(X) + \delta^2(P) \geq |[X,P]| = 1. \tag{1.54}$$

This follows from the fact that $ab \geq |c|^2/4$ implies $a+b \geq |c|$. Then for all separable states we have

$$\begin{aligned} &\delta^2\left(S_x(a)\right)_\rho + \delta^2\left(S_p(a)\right)_\rho \geq \\ &\sum_i p_i \left(a^2\delta^2\left(X_1\right)_{\rho_i^A} + \frac{1}{a^2}\delta^2\left(X_2\right)_{\rho_i^B} + a^2\delta^2\left(P_1\right)_{\rho_i^A} + \frac{1}{a^2}\delta^2\left(P_2\right)_{\rho_i^B} \right) \geq \\ &a^2 + \frac{1}{a^2}, \end{aligned} \tag{1.55}$$

where the last inequality is implied by Eq. (1.54). ■

In the case of two mode Gaussian states Eqs. (1.49) and (1.53) provide a necessary and sufficient entanglement criterion for separability [70, 69]. These relations must be seen as generalizations of the PPT condition to the case of infinite dimensional Hilbert spaces.

The uncertainty relation (1.23) and Gaussianity of a state augmented with the additional uncertainty relation (1.47) provides full characterization of a covariance matrix of a two mode Gaussian state, which results in a necessary and sufficient criterion. However, if a bipartite Gaussian state consists of more than two modes, examples of bound entangled states are known [32]. Nonetheless a necessary and sufficient criterion for separability for Gaussian states can be formulated [32].

Theorem 1.21. *A given bipartite $n \times m$ mode Gaussian state is entangled iff there exist two CMs γ_A and γ_B such that*

$$\gamma \geq \gamma_A \oplus \gamma_B \tag{1.56}$$

is satisfied, where γ is the CM of the state, defined on the whole phase space, and γ_A and γ_B are CMs on the Alice's and Bob's phase space respectively.

Proof: The easy proof of the first part of the Theorem can be found in [37]. Later on in Chapter 2 we will provide an alternative proof of the first part, which holds for all systems, and is independent of the dimension of the underlying Hilbert space.

The prove of the second part uses the definition of quantum Fourier transformation and its properties and can be found in [32, 22]. ■

This important result provides a complete characterization of separable states in continuous variables setting. However, the proof of the theorem is an existence proof and is by no means constructive. Therefore the condition (1.56) is hard to implement in practice. Surprisingly, it can be shown that the uncertainty relation (1.23) can be used to find an explicit decomposition of ρ as a convex combination of product states, if ρ is separable [33]. The method consists of constructing a sequence of matrices

$$\{\gamma_N\}_{N=0}^{\infty}, \text{ where } \gamma_N = \begin{pmatrix} A_N & C_N \\ C_N^T & B_N \end{pmatrix}. \tag{1.57}$$

The matrix γ_0 is the CM of a given Gaussian state ρ. The sequence is defined recursively

$$\begin{aligned} A_{N+1} &\equiv B_{N+1} \equiv A_N - \mathfrak{Re}\,(X_N)\,, \\ C_{N+1} &\equiv -\mathfrak{Im}\,(X_N)\,, \\ X_N &\equiv C_N (B_N - i\sigma)^{-1} C_N^T. \end{aligned} \tag{1.58}$$

Using this recursion one can determine whether a given state is separable or not. To this end one can prove the following theorem [33]:

Theorem 1.22.
A. *If for some $N \geq 1$ one finds $A_N \ngeq i\sigma$ then $\gamma_0(\rho)$ corresponds to a non-separable state.*
B. *If for some $N \geq 1$ one finds*

$$A_N - ||C_N||_{op} \mathbb{1} \geq i\sigma, \tag{1.59}$$

where $||C_N||_{op}$ denotes the maximal singular value of the C_N, then the state ρ must be separable.

Proof: The detailed proof of this theorem as well as construction of the corresponding matrices is originally discussed in [33]. ■

This theorem is constructive and basically consists of testing the uncertainty relation (1.23) for the sequence of CMs.

The algorithm of deciding whether a bipartite Gaussian state is separable or not and finding a decomposition (1.56) for its covariance matrix, if it is separable, is very practical. It converges surprisingly fast and even for entangled states that lie near the core of separable states the algorithm needs less than 30 iterations. Note, however, that the separability criterion presented in Theorem 1.21 can be written as a semi-definite program (SDP) [34, 35, 36], which effectively finds the decomposition $\gamma_A \oplus \gamma_B$ for separable states. Semi-definite programs turn out to be very useful to detect entanglement in the case of non-Gaussian states, where a violation of the condition (1.56) becomes only a sufficient condition for entanglement.

Nevertheless, Theorem 1.21 presents a strong and computable separability criterion for Gaussian states. In contrast, for finite-dimensional systems, the theory is hardly developed [37, 38, 39, 40].

In Chapter 3 of this thesis we formulate a separability criterion for finite-dimensional systems in terms of covariance matrices. As we will show later this criterion presents also a strong and computable criterion for separability, which is necessary and sufficient for two qubits.

1.3.3 Entanglement witnesses

The idea of measuring certain observables in order to detect entanglement resulted in a very powerful experimental method. Directly measurable observables, which can be used for entanglement detection are called *entanglement witnesses*.

Definition 1.23. *An observable $\mathcal{W}$ is called an* **entanglement witness** *if*

$$Tr(\mathcal{W}\rho_s) \geq 0, \text{ for all separable states } \rho_s$$
$$Tr(\mathcal{W}\rho_e) < 0, \text{ for at least one entangled state } \rho_e.$$

Therefore if one measures the observable $\mathcal{W}$ in some state ρ and the result is a negative number, then one knows with certainty that the state is entangled.

For every entangled state there exists a witness, which detects it. This condition is called completeness of witnesses and was proved in [59]. This existence theorem does not provide, however, any information about how to construct the witness. In order to shed some light on witnesses' construction it is useful to discuss witnesses from the geometrical point of view. Indeed, witnesses have a clear geometrical meaning. Since the mean value of an observable is linear in the state, the equation $\mathrm{Tr}\,(\mathcal{W}\rho) = 0$ defines a hyperplane in the space of all states and divides it into two parts: the states that are detected by the witness (all states fulfilling $\mathrm{Tr}\,(\mathcal{W}\rho) < 0$) and the states that are not detected ($\mathrm{Tr}\,(\mathcal{W}\rho) \geq 0$). All separable states belongs to the second subspace. From Figure 1.1 one can see that some witnesses detect more entangled states than the others. For example the witness $\mathcal{W}_1$ detects more states that the witness $\mathcal{W}_2$. One calls the witness $\mathcal{W}_1$ a *finer* witness than $\mathcal{W}_2$. Beginning with some witness one can always look for a finer witness. In other words one can always try to *optimize* a given witness. The *optimal* witness is a witness, which cannot be optimized further. A necessary condition for a witness to be optimal is to tangent the set of separable states. In the Figure 1.1 the witness $\mathcal{W}_1$ satisfies this condition.

Therefore one might deduce that the construction of witnesses might be connected to separability criteria. In fact, there is such connection. To give an example, consider all states that violate the CCNR criterion (Theorem 1.16). Let us now choose observables, which occur in the Schmidt decomposition (1.40), and construct a witness

$$\mathcal{W}_{CCNR} = \mathbb{1} - \sum_{k=1}^{\min\{n,m\}^2-1} G_k^A \otimes G_k^B. \tag{1.60}$$

Clearly, $\mathrm{Tr}\,(\mathcal{W}_{CCNR}\rho^e_{CCNR}) < 0$, where ρ^e_{CCNR} is such that ρ^e_{CCNR} is detected by the CCNR criterion and hence $\sum_k \lambda_k(\rho^e_{CCNR}) < 1$. Since any state can be written in the Schmidt form $\rho = \sum_{kl} \mu_{kl} G_k^A \otimes G_l^B$, for all separable states $\mathrm{Tr}\,(\mathcal{W}_{CCNR}\rho) = 1 - \sum_k \mu_{kk} > 1 - \sum_k \lambda_k(\rho) > 0$ holds. In the first estimation we used the fact that the trace of a matrix is always upper bounded by the sum of the matrix's singular values. The second inequality is the CCNR criterion. Note that the constructed witness can detect bound entangled states.

In the way demonstrated one can construct a whole variety of witnesses. To detect a particular pure state $|\psi\rangle$ one can construct a projector-based witness of the form $\mathcal{W} = a\mathbb{1} - |\psi\rangle\langle\psi|$. However, from the experimental point of view, one prefers to expand the projector into a form of observables, which can be directly measured in an experiment. This strategy was first used to detect a two qubit entangled state

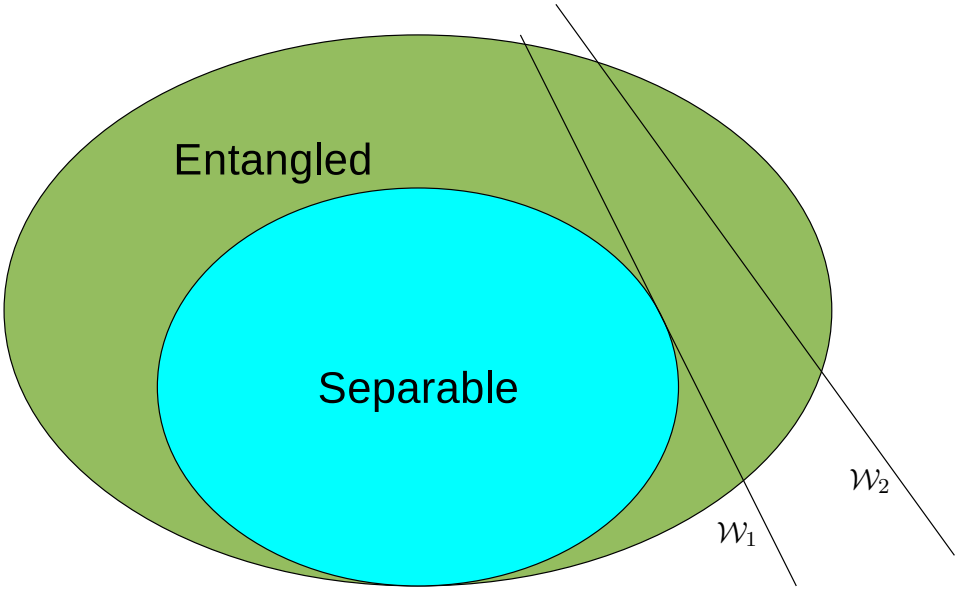


Figure 1.1. *Geometrical interpretation of entanglement witnesses. Every witness defines a hyperplane (lines on the plot above) in the space of states, which divides the whole space into two halves. One half corresponds to the entangled states, the another half consists of the states that are not detected by the witness. The convex set of separable states lies in the second half. The witness* $\mathcal{W}_1$ *detects more states than the witness* $\mathcal{W}_2$*.* $\mathcal{W}_1$ *is* finer *than* $\mathcal{W}_2$*.*

[73]

$$\mathcal{W}_- = \frac{1}{2}\mathbb{1} - |\Psi^-\rangle\langle\Psi^-| = \frac{1}{4}\left(\mathbb{1} + \sigma_x \otimes \sigma_x + \sigma_y \otimes \sigma_y + \sigma_z \otimes \sigma_z\right). \tag{1.61}$$

Due to their experimental accessibility entanglement witnesses became a standard tool in entanglement detection in experiments. For instance, entanglement in linear cluster states and GHZ states with different numbers of photons was observed in this way (see Chapter 6 in [67] and also references therein). One of the open questions here is the *optimality* of witnessing entanglement in the experimental sense. It turns out that from the experimental point of view it is not always the best strategy to measure the optimal witness [74].

1.3.4 Bell inequalities

In the remainder of the section we discuss Bell inequalities that are the oldest tool to detect entanglement. John Bell [75], who aimed to describe the Einstein-Podolsky-Rosen paradox quantitatively, introduced an inequality that bounds classical correlations. If measurements on a quantum state violate a Bell inequality, then the state must be entangled.

Let us consider the following gedankenexperiment. Imagine that two experimentalists (Alice and Bob) are located in spatially distinct labs. Both of them are capable of performing only two measurements, which are described by observables A_1, A_2 and B_1, B_2 for Alice and Bob respectively. Then if the state is only classically correlated

$$\langle A_1 B_1 \rangle + \langle A_2 B_1 \rangle + \langle A_1 B_2 \rangle - \langle A_2 B_2 \rangle \leq 2 \tag{1.62}$$

holds [76, 77]. Such an inequality is called Bell inequality. Because it is used rather often this particular inequality has however its own name CHSH inequality, due to Clauser, Horne, Shimony and Holt, who first introduced this inequality [76].

In order to see how these measurements can be realized in practice we pick a particular example. Assume we possess a source that emits pairs of spin-$\frac{1}{2}$ particles. After leaving the source, the particles fly apart along the z axis. These measurements A_i, B_j $(i, j = 1, 2)$ correspond to the measurements of particles in the x-y plane along vectors $\overrightarrow{a}_i$ and $\overrightarrow{b}_j$. These vectors can be characterized by azimuthal angles $\phi_1^a = 0$, $\phi_2^a = \pi/2$ for Alice and $\phi_1^b = \pi/4$, $\phi_2^b = 3\pi/4$ for Bob. The outcome of each measurement is assumed to be dichotomic $+$ or $-$. The mean value $\langle A_i B_j \rangle$ (or correlation coefficient) in the inequality (1.62) can be written in terms of probabilities [6, 67]

$$\langle A_i B_j \rangle = P_{++}\left(\overrightarrow{a}_i, \overrightarrow{b}_j\right) + P_{--}\left(\overrightarrow{a}_i, \overrightarrow{b}_j\right) - P_{+-}\left(\overrightarrow{a}_i, \overrightarrow{b}_j\right) - P_{-+}\left(\overrightarrow{a}_i, \overrightarrow{b}_j\right). \tag{1.63}$$

The CHSH inequality can also be written in terms of probabilities CH inequality - and reads [78]

$$P_{++}\left(\overrightarrow{a}_1, \overrightarrow{b}_1\right) - P_{--}\left(\overrightarrow{a}_2, \overrightarrow{b}_2\right) + P_{+-}\left(\overrightarrow{a}_1, \overrightarrow{b}_1\right) + P_{-+}\left(\overrightarrow{a}_2, \overrightarrow{b}_1\right) \geq 0 \tag{1.64}$$

Now we provide an example of quantum state that violates Inequality (1.62). Assume the source produces spin-$\frac{1}{2}$ particles in a singlet state $|\Psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$. Alice and Bob use the following set of observables in order to perform their measurements

$$A_1 = -\sigma_x,\ A_2 = -\sigma_y,\ B_1 = \frac{\sigma_x + \sigma_y}{\sqrt{2}},\ B_2 = \frac{\sigma_x - \sigma_y}{\sqrt{2}}. \tag{1.65}$$

The direct calculation gives $\langle A_1 B_1 \rangle + \langle A_2 B_1 \rangle + \langle A_1 B_2 \rangle - \langle A_2 B_2 \rangle = 2\sqrt{2}$. Interestingly, one can show that no quantum state can give a bigger violation of the CHSH inequality than $2\sqrt{2}$. This bound is known as *Cirel'son bound* [79].

Originally Bell inequalities were introduced to test the fundamental question of inconsistency of quantum mechanics with local hidden variable (LHV) models or in other words the non-local nature of quantum mechanics. An LHV model suggests the existence of a hidden parameter λ in a theory, such that for example the result of coincidence measurement in a Bell experiment, mentioned above, can be written in a factorized form

$$P_{ab}\left(\overrightarrow{a}_i, \overrightarrow{b}_j\right) = \int d\lambda \rho(\lambda) P_a^A\left(\overrightarrow{a}_i, \lambda\right) P_b^B\left(\overrightarrow{b}_i, \lambda\right). \tag{1.66}$$

Here the source is supposed to produce states that are described by a hidden variable λ with probability $\rho(\lambda)$ and $P_a^A(\overrightarrow{a}_i, \lambda)$ and $P_b^B\left(\overrightarrow{b}_i, \lambda\right)$ are probabilities of certain measurement outcomes a and b in Alice's and Bob's lab respectively. Note that Alice and Bob share the same hidden variable λ. In the considered example we assumed that the measurement outcomes were dichotomic, i.e. can take only two values ± 1, but generally a and b can be any real number from the interval $[-1, 1]$. The fact that the probability of measurement outcome in the integral is factorized is implied by the locality assumption, i.e. for a fixed λ Alice's probabilities does not depend on Bob's choice of observables.

Using the normalization of probabilities and considering all possible measurement results for the Bell experiment described above, one arrives at the conclusion that for any LHV model the CHSH inequality must hold.

Experimental justification of incompatibility of local realistic theories with quantum mechanics is not, however, decisive yet, because of the existense of *locality loophole* and *detection loophole*. The locality loophole was closed in an experimant with photons [11] and the detection loophole in an ion trap experiment [80]. However, there is no loophole-free experiment yet. Closing these loopholes and hence refuting LHV theories is an important problem of fundamental character.

1.4 Entanglement measures

In this section we briefly discuss basic notions of entanglement measures. Quantification of entanglement is an important task in quantum information theory. However, there is no unique measure of entanglement. Inspired by different tasks there are also various different entanglement measures. Nevertheless, an entanglement measure has to fulfill certain conditions.

1.4.1 Requirements for entanglement measures

As a tool for entanglement quantification an entanglement measure (also called *entanglement monotone*) has to quantify the amount of entanglement in a given state ρ. The conditions, which an entanglement measure $E(\rho)$ has to satisfy, were first introduced in Ref. [81]. Here we list these properties without any deep discussion and suggest Refs. [83, 82, 67] for further reading.

1. If the state ρ is separable, then $E(\rho) = 0$.
2. The function $E(\rho)$ should not change under local unitary transformations
$$E(\rho) = E(U_A \otimes U_B \rho U_A^\dagger \otimes U_B^\dagger) \tag{1.67}$$
3. Since entanglement cannot be produced by LOCC, an entanglement measure cannot increase under LOCC operations
$$E(\Lambda_{LOCC}(\rho)) \leq E(\rho), \tag{1.68}$$

where Λ_{LOCC} is a positive map implemented by LOCC.

4. $E(\rho)$ should be convex

$$E\left(\sum_i p_i \rho_i\right) \leq \sum_i p_i E(\rho_i). \tag{1.69}$$

Note that this property is often demanded and fulfilled by most entanglement measures, although not all measures fulfill this property.

5. Sometimes one also demands an entanglement measure to be an additive function

$$E(\rho_1 \otimes \rho_2) = E(\rho_1) + E(\rho_2). \tag{1.70}$$

However this property is also violated by some measures or is very hard to prove.

We comment a little bit more on the property (1.68), since we are going to use it in this work. Sometimes this condition is replaced by a different requirement that $E(\rho)$ should not increase under LOCC *on average*. That means that if a LOCC transformation maps the initial state ρ to states ρ_i with certain probabilities p_i, the function $E(\rho)$ should satisfy

$$\sum_i p_i E(\rho_i) \leq E(\rho). \tag{1.71}$$

Note that this condition is stronger than (1.68), but the most reasonable entanglement measures fulfill also this last condition.

1.4.2 Some examples of entanglement measures

Before starting with some examples we briefly discuss a possible strategy of constructing an entanglement measure. We will be using this strategy later on. Firstly, one defines the measure $E(|\psi\rangle)$ for pure states. In the second step, which is called *convex roof construction*, one extends the measure on the set of mixed states

$$E(\rho) = \inf_{p_i, |\psi_i\rangle} \sum_i p_i E(|\psi_i\rangle), \tag{1.72}$$

where the infimum is taken over all possible decompositions of the state ρ.

This construction has two essential advantages. First of all, the property of convexity is automatically fulfilled for mixed states. Secondly, in many cases it is easier to check all requirements, which an entanglement measure has to satisfy, on the pure states and then extend them on the case of the mixed states. Furthermore, it is noteworthy that even if the constructed measure turns out not to fulfill the requirements listed in section 1.4.1, one can use it to lower bound some already known entanglement measure. Finally, we point out that the optimization (1.72) is a very hard computational task and only for special cases results are known.

In order to point out the important relation between entanglement measures and entanglement criteria we start with the *negativity of entanglement* [84].

Definition 1.24. *The negativity of entanglement is defined as*

$$N(\rho) = \frac{||\rho^{T_A}||_1 - 1}{2}. \tag{1.73}$$

As one can see from the definition, this measure is defined as the violation of the PPT criterion and hence does not detect any bound entangled states. The main advantage of this measure is that it is really easy to compute. However, it is not an additive function. To make this function additive one can introduce the logarithmic negativity $E_N(\rho) = \log_2 ||\rho^{T_A}||_1$, but in this case one looses the convexity.

Another very important measure for quantification of bipartite quantum correlations is the concurrence [85, 86, 87].

Definition 1.25.

$$Concurrence of a pure quantum state is defined as C(|\psi\rangle) = \sqrt{2(1 - \mathrm{tr}\,(\rho^2))}. \tag{1.74}$$

It is useful to express the concurrence in terms of the Schmidt coefficients of a state [87, 88]

$$C(|\psi\rangle) = 2\sqrt{\sum_{i<j} \lambda_i \lambda_j}. \tag{1.75}$$

For the mixed states it is defined via convex roof construction (1.72) and can be analytically computed for the case of two qubits [86].

As it has already been mentioned there exist a lot of entanglement measures such as the *von Neumann-Rényi entropy*, which is quite often used to quantify entanglement in ground states of quantum spin models (note that this is not an entanglement measure for mixed states). Concurrence of two qubits can be connected to *Entanglement of formation* and *entanglement of distillation* is a lower bound for the negativity. Apart from these measures there are measures that were motivated by certain physical implementations, for example *localizable entanglement*. The *geometric measure of entanglement* is an example of measures, which are induced by particular distance in the Hilbert space. The *mutual information* can be seen as an entropic generalization of an entanglement measure induced by a distance in the space of mixed states, i.e. in $\mathcal{B}(\mathcal{H})$ with a Hilbert-Schmidt norm. Since the discussion of entanglement measures is not in the main focus of this thesis we refer the interested reader to excellent reviews on the theory of entanglement [82, 67].

1.4.3 Semidefinite programs in entanglement theory

As one could guess from previous sections many problems in quantum information theory involve optimization over the convex set of separable states. The decision whether a given multipartite state is entangled, minimization of expectation values of entanglement witnesses or evaluation of entanglement measures are examples of such problems [34].

A semidefinite program (SDP) represents a particular type of convex optimization problem and corresponds to the optimization of a linear function subjected to linear constraints. A typical form of SDP is

$$\begin{aligned} &\text{minimize } c^T \overrightarrow{x}, \\ &\text{subject to } F(\overrightarrow{x}) \geq 0,\ F(\overrightarrow{x}) = F_0 + \sum_{i=1}^{n} x_i F_i \end{aligned} \tag{1.76}$$

Here c is a given vector specifying the problem, F_i are some Hermitian matrices and $\overrightarrow{x} = (x_1, x_2, \ldots, x_n)$ is a vector of variables, over which the minimization is performed. In a particular case, namely when $c = 0$, the problem reduces to the so-called *feasibility problem*, which is to decide, whether the linear constraints in (1.76) can be satisfied for some value of $\overrightarrow{x}$.

A very important property of a SDP is its duality structure. The dual problem is given via Lagrange approach

$$\inf_{x\in\mathbb{R}^n} \sup_{Z\geq 0} \left\{ c^T \overrightarrow{x} - \mathrm{Tr}\left(F(\overrightarrow{x})Z\right) \right\} \geq \sup_{Z\geq 0} \inf_{x\in\mathbb{R}^n} \left\{ -\mathrm{Tr}\left(F_0 Z\right) + \sum_i \left(c_i - \mathrm{Tr}\left(F_i Z\right)\right) x_i \right\}. \tag{1.77}$$

The supremum on the right hand side of the (1.77) is bounded from below if and only if the infimum stays finite for all $\overrightarrow{x} \in \mathbb{R}^n$. The last is the case only if

$$c_i = \mathrm{Tr}\left(F_i Z\right),\ \forall i. \tag{1.78}$$

Hence for every SDP there exists a corresponding dual problem of the form:

$$\begin{aligned} &\text{maximize } -\mathrm{Tr}\left(F_0 Z\right), \\ &\text{subject to } Z \geq 0,\ \mathrm{Tr}\left(F_i Z\right) = c_i, \end{aligned} \tag{1.79}$$

where Z is a Hermitian matrix and is variable over which the maximization is performed. The dual problem itself belongs to the class of semidefinite programs. Any solution of the dual problem gives a lower bound on the solution of the primal problem and vica versa. This property is referred to as weak duality, meaning that for any feasible x and Z, which fulfill the constraints in (1.76) and (1.79),

$$c^T \overrightarrow{x} + \mathrm{Tr}\left(F_0 Z\right) = \mathrm{Tr}\left(F(\overrightarrow{x})Z\right) \geq 0 \tag{1.80}$$

holds. If one of the constraints (or both of them) in (1.76) and (1.79) are fulfilled strictly, then one speaks about strong duality, which means that there exist $x^\star$ and $Z^\star$ such that

$$c^T \overrightarrow{x^\star} + \mathrm{Tr}\left(F_0 Z^\star\right) = 0. \tag{1.81}$$

In Fig.1.2 we schematically present how the dual problem can be used in optimization problems. Imagine our goal is to minimize a function $f\left(\overrightarrow{x}\right)$ (e.g. $f\left(\overrightarrow{x}\right) = c^T \overrightarrow{x}$ in Problem (1.76)). A numerical optimization will give us an answer, which is in general bigger than the real minimum of the function f: nummin

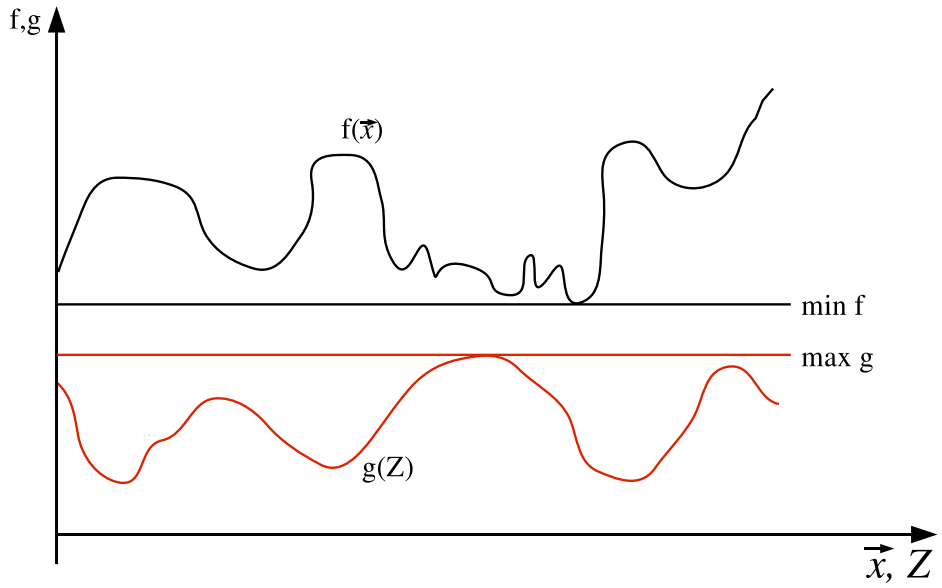


Figure 1.2. *Primal (black line) and dual (red line) problems. Using the duality property of the SDP one can numerically achieve bounds on the minimum of a given function f. Generally, Ineq. (1.82) holds, which gives an interval that the* min f *belongs to.*

$(f) >$ min (f). Now we can use the duality property and maximize a function $g(Z)$ $(g(Z) = -\mathrm{Tr}\,(F_0 Z)$ in Problem (1.79)). Again the numerically achieved maximum will be smaller than real maximum of g. However using the dual structure we can give an interval, which the real minimum of the function $f\,(\overrightarrow{x})$ belongs to:

$$\text{nummin}\,(f) > \min(f) \geq \max(g) > \text{nummax}\,(g). \tag{1.82}$$

In the case of the strong duality, where theoretical values of $\min(f)$ and $\max(g)$ are equal the duality can be used as a test of the quality of the numerical minimization.

An important example of SDPs are feasibility problems. For these problem the vector c in (1.76) is equal to zero, so the primal problem consists in only checking the feasibility conditions. For the dual problem it means that $\mathrm{Tr}\,(F_0 Z) \geq 0$ has to hold for all feasible Z. Therefore if there is a feasible Z such that $\mathrm{Tr}\,(F_0 Z) < 0$ than the primal problem has no solutions [89].

Semidefinite programs can be used to construct tests for the separability problem. These tests are constructed to approximate the convex set of separable states as exactly as possible. There are two basic strategies to carry out this approximation. The first one (see *e. g.* [89]) is to approximate the set of separable states from outside, *i. e.* at each step the inseparability of a given state is tested. The second strategy concerns with approximating the set of separable states from inside [90], *i. e.* at each step one has to answer the question whether the state is separable or it cannot be decided. Following this strategy one detects separability instead of inseparability.

Using either of the strategies one can construct a complete hierarchy of separability tests. This hierarchy converges and gives with certainty the answer to the separability problem. Although the time efficiency of each step scales only polynomially with the dimension of the Hilbert space, the size of the matrix $F(\overrightarrow{x})$ in the semidefinite program (1.76) grows exponentially with the number of steps in the hierarchy. This is in agreement with the fact that the separability problem, considered as a *weak membership* problem, is *NP*-hard [91, 92]. That means the decision whether a given $d \times d$ state is separable or not with accuracy ϵ requires an exponential in d number of steps.

1.5 Entanglement in condensed matter systems

In this section we will briefly discuss some modern directions that became popular in recent decades and were facilitated by the progress in the quantum information theory.

1.5.1 Entanglement in critical phenomena

Entanglement as a purely quantum mechanical feature is interesting from the fundamental point of view for solid state physics as well and plays a crucial role in critical phenomena. Under criticallity one usually understands the phenomenon of phase transition and says the system, described by its Hamiltonian, *is critical* if it has several phases and undergoes a phase transition for certain values of external parameters, e.g. temperature, pressure or magnetic field, or internal parameters, e.g. the strength of the spin-spin coupling. All phase transitions can be cast into two categories: *first order phase transitions* or discontinuous phase transitions and *second order phase transitions* or continuous phase transitions. The discontinuous transitions involve a latent heat, i.e. when the system undergoes a phase transition of this type a fixed amount of energy is either absorbed or released. The second order phase transitions are characterized by the power law decay of correlations. No latent heat is involved there. A very important sub-class of continuous phase transitions are *quantum phase transitions*. These transitions occur at zero temperature and correspond to an abrupt change of the ground state of the many-body system, when some of the system's parameter are varied [93]. Because a quantum phase transition occurs at $T = 0$ the correlations in the system are of purely quantum character. The phenomenon of quantum phase transitions cannot be explained in the framework of classical statistical mechanics and must be considered from a conceptually different point of view [94]. As it has been realized in [95, 96, 97] for the quantum phase transitions the amount of entanglement grows considerably at the critical point. We illustrate this behavior on two examples.

Example 1: Concurrence. Concurrence is suited at best as measure for entanglement between two particles in a spin model. All spin models we consider in the examples have one spatial dimension. First of all let us consider a model with

Ising type interaction in an external transverse magnetic field. It consists of spin-$\frac{1}{2}$ particles that can be described by the following Hamiltonian

$$H_I = -\sum_{i=1}^{N}(\lambda\sigma_i^x\sigma_{i+1}^x + \sigma_i^z) \tag{1.83}$$

with periodic boundary conditions.

The model defined by the Hamiltonian in Eq. (1.83) is exactly solvable and the ground state of the model is known. As one can conclude already from the Hamiltonian the ground state $|\psi_0(\lambda)\rangle$ depends heavily on the parameter λ. Two limiting cases are pretty obvious though: for $\lambda \to \infty$ the state will tend to be a product state of the form

$$|\psi_0(\infty)\rangle = |+\rangle^{\otimes N}, \tag{1.84}$$

whereas for $\lambda = 0$ the ground state will be

$$|\psi_0(0)\rangle = |0\rangle^{\otimes N}. \tag{1.85}$$

The existence of the phase is adjudicated by two different ground states. The critical point for the Ising chain lies at $\lambda_c = 1$. The amount of entanglement, which is shared between two sites of the chain can be analyzed by the concurrence [95, 97]. The behavior of the concurrence of nearest neighbors is depicted on FIG. 1.3(a) [95].

Depending on the size of the system the minimum of the first derivative of the nearest neighbor concurrence with respect to the critical parameter λ becomes more and more clear. In the thermodynamic limit the concurrence itself is presented in the right inset of FIG. 1.3(a). The concurrence has an infinite slope at $\lambda = 1$ and the minimum of $\partial_\lambda C(1)$ tends to minus infinity

$$\partial_\lambda C(1) = \frac{8}{2\pi^2}\ln|\lambda - \lambda_c| + const. \tag{1.86}$$

The last equation describes the behavior of nearest neighbor entanglement in the critical region. The next to nearest neighbor concurrence is also different from zero [95, 97] and is presented in FIG. 1.3(b).

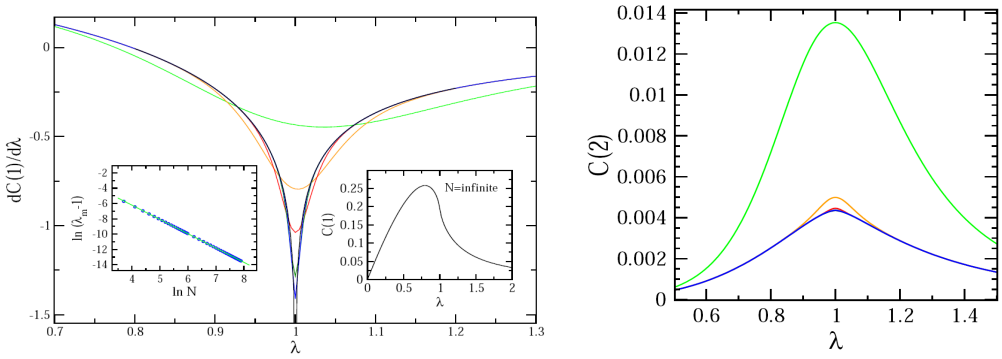
Besides the fact that the value of the next to nearest neighbor concurrence is two orders of magnitude smaller that the value of $C(1)$ there is a peculiar fact that has to be mentioned here. Namely, the maximum of $C(2)$ is precisely at the critical point for arbitrary system size and its value drops with the system size. Since $\partial_\lambda C(2)|_{\lambda_c} = 0$ the singular behavior of $C(2)$ is described by its second derivative

$$\partial_\lambda^2 C(2) = 0.108\ln|\lambda - \lambda_c| + const. \tag{1.87}$$

The next next nearest neighbor concurrence is zero for all values of the critical parameter λ.

Yet another spin system that undergoes quantum phase transition but possesses richer properties is the so-called XY-model. Its anisotropic version is described by the following Hamiltonian

$$H_{XY} = -\frac{\lambda}{2}\sum_{i=1}^{N}\left\{(1+\gamma)\sigma_i^x\sigma_{i+1}^x + (1-\gamma)\sigma_i^y\sigma_{i+1}^y\right\} + \sum_{i=1}^{N}\sigma_i^z. \tag{1.88}$$



(a) (b)

Figure 1.3. (a) *First derivative of the nearest neighbors concurrence with respect to the critical parameter* λ *is presented. Different curves correspond to different sizes of the ring* $N = 11, 42, 101, 251, 401, \infty$. *When the system's size is increased the minimum gets more sharp. In the left inset one can see that the position of the minimum also changes with the system size (finite size effects) but tends as* $N^{-1.87}$ *to the real value* $\lambda_c = 1$, *where a logarithmic divergence for an infinite system is present. The right inset shows the behavior of the concurrence itself in the thermodynamic limit. The maximum occurs below the critical value* $\lambda_c = 1$ *and is not related to the critical properties of the Ising model. This picture was taken from [95].* (b) *The next to nearest neighbor concurrence* $C(2)$ *in the critical region of the Ising chain as function of the critical parameter* λ *is presented. Different curves correspond to different system sizes. Generally the value of* $C(2)$ *is by two order of magnitudes smaller than the value of* $C(1)$. *Surprisingly, the position of the maximum of* $C(2)$ *does not depend on the size of the system and is precisely at the critical point* $\lambda_c = 1$. *The maximum increases if the system's size increases. This picture was taken from [95].*

Before we present known results we should comment on the Hamiltonian (1.88). Firstly, as one can easily verify, the Ising model, discussed above is a special case of the XY-model: $H_{XY}(\gamma = 1) = H_I$. Secondly, for anisotropy parameter $\gamma \in (0, 1]$ the models H_{XY} belong to the Ising universality class and in the thermodynamic limit they undergo a quantum phase transition at $\lambda_c = 1$.

The exact solubility simplifies the calculation of the concurrence, which is determined by the two-site density matrix. In FIG. 1.4(a) and FIG. 1.4(b) we present the results from [97] concerning the concurrence in the XY-chain. It is worth to note the transition from Ising ($\gamma = 1$) to the XX model, where after the phase transition the concurrence $C(1)$ saturates and stays at some finite value. In the case of the next nearest neighbor concurrence one observes the same behavior as in the Ising model: at the criticallity $\lambda = 1$ the concurrence $C(2)$ has its maximum. Interestingly the value of the maximum varies slightly depending on γ. On the half

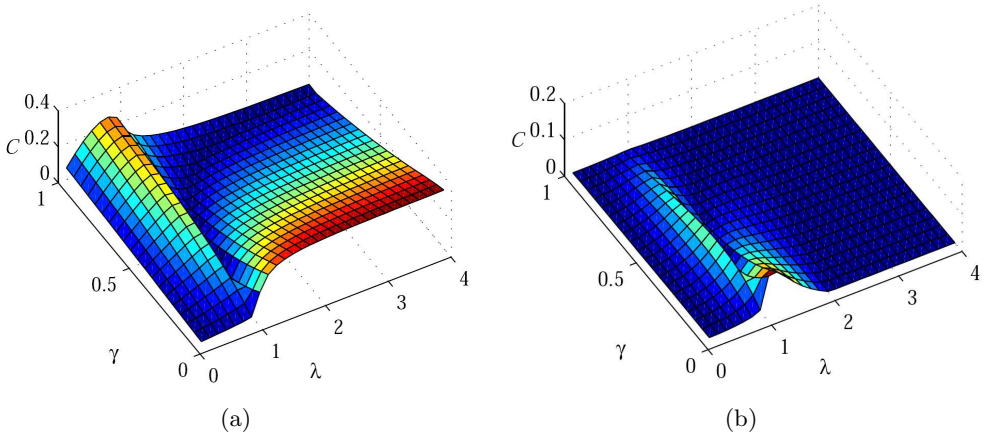


Figure 1.4. (a) *The nearest neighbor concurrence in the ground state of the XY chain. The phase transition that occurs at $\lambda = 1$ affects the nearest neighbor concurrence for all values of the anisotropy parameter γ. In the XX model $\gamma = 0$ the concurrence $C(1)$ saturates at some finite value.* (b) *The next to nearest neighbor concurrence in the ground state of the XY chain. Along the critical line $\lambda = 1$ the next nearest neighbor concurrence $C(2)$ has its maximum, as in the case of the Ising model, almost everywhere. The exception is the region of low anisotropy where γ tends to zero and the model becomes more and more XX-like. This picture was taken from [97].*

way from the Ising to XX model it takes its biggest value. For the XX model the concurrence $C(2)$ drops rather fast when one goes deeper into the region where the XX coupling dominates the external magnetic field. As for the Ising model all long distance concurrences $C(N)$ vanish for $N > 2$.

One might think that vanishing of $C(N)$ for either Ising and XY-models is a signal of relatively small amount of entanglement in their ground states. This assumption is, however, not correct. By considering concurrence one takes into account only two particle entanglement. The more complete picture is provided if one calculates the von Neumann entropy, which is the subject of our second example.

Example 2: von Neumann entropy. In the thermodynamical limit the von Neumann entropy in the critical region can be expressed by a simple formula [100, 101]:

$$S^I_{vN}(L) = \frac{1}{6}\log L + O\left(\frac{1}{L}\right) + const \tag{1.89}$$

for $L \to \infty$, where L denotes the size of the block of the system. This logarithmic divergence of the von Neumann entropy indicates the presence of highly entangled states and complements the observations made for the concurrence.

For the XY-model the von Neumann entropy was calculated as well [100, 101, 102, 103]. An analytical expression for the von Neumann entropy in thermodynamical limit for $L \to \infty$ was provided in [102]. Qualitatively it is important to note, that

the von Neumann entropy of the ground state of the one dimensional XY model diverges logarithmically at criticallity, which is reminiscent of the behavior in the Ising model (1.89)

$$S_{vN}^{XY}(L) = c\log(L) + const. \tag{1.90}$$

Surprisingly the scaling of the von Neumann entropy obeys in many cases quite general rules. For many models it grows as the boundary of the considered block. This type of scaling is called *area law* and holds for a big variety of the systems possessing critical behavior (see [105] and references therein).

There are several approaches that can be used to estimate entanglement in a given condensed matter system. In the examples presented above, one uses the ground state of a particular Hamiltonian explicitly in order to calculate the amount of entanglement in the system. A nice review on the entanglement investigations by direct calculation of the ground states of many-body systems can be found in [106].

Example 3: Witnesses. A different type of approach consists of using the Hamiltonian itself as an observable that can be used to examine what quantum states can be detected with it. This kind of estimation involves a witness operator that is constructed as

$$W_H = H - \inf_{\rho\in S}\{\mathrm{Tr}\,(\rho H)\}, \tag{1.91}$$

where S is the set of all separable states.

The estimation of the energy can be done for a big variety of spin models. The figure of merit of such estimation is twofold. Firstly, the estimation turns out to be very useful for the detection of entanglement in thermal states. Secondly, it sheds some light also on the type of entanglement that is present in various spin models. Namely, estimating the energy one can analyze what type of multipartite entanglement is consistent with the energy threshold, i.e. which type of multipartite entanglement must be present in order that the state has a particular energy [98, 99, 67].

1.5.2 Entanglement in real-space renormalization techniques

In this section we discuss an advantageous role of entanglement in renormalization group techniques. Applied to quantum field theory and statistical mechanics renormalization group techniques are very well developed, see for example [107, 108] and references therein. The idea of renormalization is rather simple to explain. It consists in discarding degrees of freedom in a system, which are considered to be not important for the physical behavior. The decision which degrees of freedom to keep and which to discard is the main issue in the definition of a particular renormalization scheme.

The fact that entanglement plays an important role in many-body systems led to the question whether one can use it to improve already known renormalization schemes. The first suggestion in this direction made in [96] was concerned with improving the already known renormalization group algorithm that was known to

fail in the case of critical systems. This renormalization method is called *density-matrix renormalization group* (DMRG). Using the entanglement. described by the von Neumann entropy, as a benchmark for optimization in the DMRG approach one was able to improve its accuracy [96, 110] and to correct the wrong exponential decay of the correlation function at the phase transition.

The DMRG is a well established method to calculate properties of one dimensional quantum systems numerically. It gives a rather good description of many-body systems in 1D: approximations to ground or thermal states or even dynamics of a given system can be achieved using the DMRG. However, as it was noted in [96], using the knowledge from quantum information theory one can make the DMRG even more accurate and even solve some of its intrinsic problems. One of the problems of the original DMRG one has been aiming to solve was the wrong scaling behavior of the correlation function in the critical region of many-body systems that undergo a phase transition. As simple as it is, the idea to take entanglement of a state into account was also somewhat genius. According to [96], the state optimization after each step in the DMRG should be carried out in a such a way that the amount of entanglement in this state is nearly the same as in the state before the renormalization step. As it turned out, the entire DMRG can be understood in terms of optimization over the so-called *matrix product states* (MPS) [111, 112, 113]. The DMRG flow has a certain fixed point. The wave function that corresponds to this fixed point is an MPS:

$$|Q\rangle = \sum_{\{s_j\}} \mathrm{Tr}\left(\mathcal{Q} A[s_n] \dots A[s_1]\right) |s_n \dots s_1\rangle, \tag{1.92}$$

where $|Q\rangle$ represents a state of n d-dimensional systems s_i, with matrices $A[s_i]$ of the size $D[s_i] \times D[s_{i+1}]$. The size of matrices A is the size of the virtual space, which they are acting on. The ansatz wave function $|Q\rangle$ is uniform in the bulk. Its boundary conditions are represented by the matrix $\mathcal{Q}$ under the trace. For example the case $\mathcal{Q} = \mathbb{1}$ corresponds to the state, which is translational symmetric with periodic boundary conditions. For $D = 2$ the state (1.92) is an exact solution for the one-dimensional AKLT model, which is defined by the Hamiltonian [114]

$$H_{AKLT} = \sum_{n=0}^{N-1} \left\{ \vec{S}_n \cdot \vec{S}_{n+1} - \frac{1}{3} \left(\vec{S}_n \cdot \vec{S}_{n+1} \right)^2 \right\}. \tag{1.93}$$

Since it has been realized that optimization over a certain class of entangled states improves the performance of DMRG there were several attempts to generalize this renormalization technique to higher dimensions and also to improve its performance further. Various classes of states arose, which were used to approximate eigenstates of quantum many-body Hamiltonians: *projected entangled-pair states* (PEPS) [115, 116] or *tensor product states* (TPS) [117, 118, 119, 120], which are the two-dimensional generalization of MPS (note that the latter were applied also to classical spin systems) or *weighted graph states* [121, 122]. Recently an another class of states was introduced: the so-called *concatenated tensor network* (CTS) states [123], however their performance is not well investigated yet.

To summarize: using the concepts of the quantum information theory one was able to shed light on some of the problems in condensed matter theory. Realizing the crucial role of entanglement in strongly correlated many-body systems led to the reappraisal of various concepts in physics of quantum phase transitions. Nowadays a lot of work in this direction is concentrated on realizing the type of entanglement that can be present in eigenstates of particular Hamiltonians. As one has already agreed on, the eigenstates of critical Hamiltonians should be highly entangled. This makes the search for the eigenstates slightly easier, since they are supposed to occupy not the whole Hilbert space but only a rather small part of it. However, the term highly entangled state is a bit rambling, since there are a lot of different types of entanglement in many-body systems. The classification of multipartite entanglement is a wide open question itself and different systems may, in fact, have different types of multipartite entanglement in their thermal or ground states [98]. So further investigations of the particular type of entanglement that can appear in e.g. ground states of many-body systems is of a big importance for both fields: condensed matter physics and quantum information theory.

1.5.3 Disordered systems

The investigation of disordered systems is motivated by a simple fact: models with constant parameters describing spin-spin interactions or local action of the magnetic field, are mathematical idealizations. One can introduce disorder in different ways. There exist different theoretical models to describe the behavior of disordered systems. The subject of investigations in this thesis will be models *without frustration*.

At first sight one could think that introducing disorder in a model and describing the couplings as stochastic variables will impede already difficult studies of the model and make in intractable. Surprisingly, it is not always the case. It turns out that in some cases one can achieve even more information about the disordered model as for its non-random analog. Particularly in one dimension ground state properties of quantum spin systems are relatively well understood [124]. For 2D only partial answers are known. For instance it has been claimed in [125] that the von Neumann entropy deviates from the area law for the 2D random transverse field Ising model. However, the aforementioned results are based on particular renormalization technique - *strong disorder renormalization group* approach. For one-dimensional systems there exists an analytical proof, that this method converges [126, 127], whereas for 2D there is only numerical evidence.

In this thesis we will introduce another renormalization scheme, which should improve the usual strong disorder renormalization group method.

To finish this section we would like to mention that the behavior of the entanglement in disordered quantum spin systems is essentially unresolved problem. On the one hand one could guess that disorder should reduce the entanglement amount in a ground state state in a given system. On the other hand, as it has been argued in [125], the disorder causes building of clusters, which are happened to be in a highly entangled state, namely in the N-particle GHZ state $\frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes N} + |1\rangle^{\otimes N}\right)$.

Chapter 2

Covariance matrices for finite dimensional systems

In the introductory chapter we discussed entanglement properties of Gaussian states. There the main tool for entanglement detection in a state was its covariance matrix (1.22), which was characterized by the uncertainty relation (1.23). In this chapter we focus on covariance matrices for finite-dimensional systems. We will analyze the relationship between the CMs and quantum states, described by a density matrix ρ. We will show that any state ρ can be described unambiguously in terms of non-symmetric covariance matrices and one looses this unambiguity in the case of the symmetric CMs. To this end we provide an example of two qubit states, which have the same CM but different separability properties. In the end of the chapter we investigate general properties of the CMs and their transformation laws under the unitary evolution of quantum state ρ.

2.1 Definition of covariance matrices

In this section we define CMs and fix our notation (see [129] and references therein).

In what follows let ρ be a pure or mixed quantum state, described by a (positive) density operator in a d-dimensional Hilbert space $\mathcal{H}$ and let $\{M_k : k = 1, \ldots, N\}$ a suitable set of observables. Unless stated otherwise, we will always assume that these observables are orthonormal observables with respect to the Hilbert-Schmidt scalar product between observables, i.e., they fulfill

$$\mathrm{Tr}\,(M_i M_j) = \delta_{i,j}. \tag{2.1}$$

Furthermore, we will typically assume that the M_i form a complete basis and span the whole observable algebra. This implies that there are $N = d^2$ different M_i, and that any other observable can be expressed as a linear combination of the M_i.

As an example for such a set of observables for the case of a single qubit, one can consider the (appropriately normalized) Pauli matrices,

$$M_1 = \frac{\mathbb{1}}{\sqrt{2}}, \quad M_2 = \frac{\sigma_x}{\sqrt{2}}, \quad M_3 = \frac{\sigma_y}{\sqrt{2}}, \quad M_4 = \frac{\sigma_z}{\sqrt{2}}. \tag{2.2}$$

We can now formulate the main definitions for this work.

Definition 2.1 (Covariance matrix)**.** *The $d^2 \times d^2$ covariance matrix $\gamma = \gamma(\rho, \{M_k\})$ and the $d^2 \times d^2$ symmetric covariance matrix $\gamma^S = \gamma^S(\rho, \{M_k\})$ are defined by their matrix entries as*

$$\gamma_{i,j} = \langle M_i M_j \rangle - \langle M_i \rangle \langle M_j \rangle, \tag{2.3}$$

$$\gamma^S_{i,j} = \frac{\langle M_i M_j \rangle + \langle M_j M_i \rangle}{2} - \langle M_i \rangle \langle M_j \rangle. \tag{2.4}$$

Sometimes, the difference between the linear part of a CM and the nonlinear part becomes relevant. Therefore, we define the linear part of γ as $\mathfrak{g}_{i,j} = \langle M_i M_j \rangle$ and the linear part of the symmetric CM as $\mathfrak{g}^S_{i,j} = \langle M_i M_j + M_j M_i \rangle / 2$.

We will often for simplicity of notation also write $\gamma(\rho)$ or $\gamma(\{M_k\})$ instead of $\gamma(\rho, \{M_k\})$, or simply γ. We will also sometimes indicate with respect to what state an expectation value is taken, so $\langle M_i \rangle = \langle M_i \rangle_\rho$. It is straightforward to see that γ is a complex Hermitian matrix. The matrix γ^S in turn is real and symmetric. Both γ and γ^S are positive semidefinite, $\gamma, \gamma^S \geq 0$ [130].

Note finally that for odd d, there is another basis of orthonormal observables that can equally be used and that is commonly employed in the mathematical physics literature in the context of discrete Weyl systems [131]. Let $A(0,0)$ be the parity operator that maps $P(0,0) : |x\rangle \mapsto |-x\rangle$, where $|x\rangle \in \{|0\rangle, \ldots, |d-1\rangle\}$, meant modulo d. Then, for $(q,p) \in \mathbb{Z}_d^2$ let

$$P(q,p) = W(q,p) P(0,0) W(q,p)^\dagger \tag{2.5}$$

the translated versions of $P(0,0)$ in discrete phase space, where $W(q,p)$ are the discrete Weyl operators [1]. The operators $\{M_{(q,p)}\} = \{P(q,p)\sqrt{d}\}$ then form a set of Hilbert-Schmidt orthonormal Hermitian matrices. This is the standard set of observables when phase-space methods are made use of.

2.2 Covariance matrices for bipartite systems

In the focus of this work is the situation where the Hilbert space is a tensor product $\mathcal{H} = \mathcal{H}^A \otimes \mathcal{H}^B$ of Hilbert spaces of two subsystems A and B. We consider finite-dimensional systems, and denote the dimension of $\mathcal{H}^A$ ($\mathcal{H}^B$) with d_A (d_B), respectively, such that the dimension of the tensor product Hilbert space is $d = d_A \times d_B$. We can choose a basis of the observable algebra in A as $\{A_k : k = 1, \ldots, d_A^2\}$ and in B as $\{B_k : k = 1, \ldots, d_B^2\}$, and consider the set of $d_A^2 + d_B^2$ observables

$$\{M_k\} = \{A_k \otimes \mathbb{1}, \mathbb{1} \otimes B_k\}. \tag{2.6}$$

Note that this set is not tomographically complete, since observables like $A_k \otimes B_l$ are missing. However, this set can be employed to define a very useful form of CMs.

[1] Let $X(q)|j\rangle = |j+q\rangle$ and $Z(p)|j\rangle = e^{2\pi i p j/d}|j\rangle$ be shift and multiply operators, then the Weyl operators are defined as $W(q,p) = e^{\pi i (d+1) pq/d} Z(p) X(q)$.

Definition 2.2 (Block covariance matrices)**.** *Let ρ be a state of a bipartite system, and let $M_k = \{A_k \otimes \mathbb{1}, \mathbb{1} \otimes B_k\}$ be a set of observables as outlined above. Then, the block covariance matrix $\gamma(\rho, \{M_k\})$ has the entries $\gamma_{i,j} = \langle M_i M_j \rangle - \langle M_i \rangle \langle M_j \rangle$ and consequently a block structure:*

$$\gamma = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix}, \tag{2.7}$$

where $A = \gamma(\rho_A, \{A_k\})$ and $B = \gamma(\rho_B, \{B_k\})$ are CMs of the reduced states of systems A and B, and

$$C_{i,j} = \langle A_i \otimes B_j \rangle - \langle A_i \rangle \langle B_j \rangle. \tag{2.8}$$

Similarly, we can define a symmetric block covariance matrix $\gamma^S(\{M_k\})$, for which A and B are the corresponding symmetric CMs, while C remains unchanged.

2.3 Covariance matrices as description of quantum states

Is it possible to completely reconstruct the state from a given CM? As our separability criterion uses the CM to decide separability, this question is important in order to understand, whether all states can be detected. We will discuss it in this subsection. Let us first show how CMs depend on the set of observables $\{M_k : k = 1, \ldots, N\}$:

Proposition 2.3 (Transformation of covariance matrices)**.** *Let $\gamma(\{M_k\})$ be a CM as defined in (2.3). If $\{K_k\}$ is another set of observables, connected to the $\{M_k\}$ by a basis transformation $K_i = \sum_{i=1}^N O_{i,j} M_j$ with some matrix O then $\gamma(\{K_k\})$ is given by*

$$\gamma(\{K_k\}) = O \gamma(\{M_k\}) O^T. \tag{2.9}$$

Note that O is an orthogonal matrix if K_i and M_i are orthonormal bases.

Proof: A direct calculation gives

$$\begin{aligned} \gamma(\{K_k\})_{i,j} &= \sum_{l,m} \langle O_{i,l} M_l O_{j,m} M_m \rangle - \langle O_{i,l} M_l \rangle \langle O_{j,m} M_m \rangle \\ &= \sum_{l,m} O_{i,l} \gamma(\{M_k\})_{l,m} O^T_{m,j}, \end{aligned} \tag{2.10}$$

which proves the claim. ■

The main point is that the previous proposition allows us to choose the basis which we want to express our CM in arbitrarily, since we know how the CM will be transformed under a basis transformation in the space of observables.

We can now come back to the initial question: Suppose we are given some CM with a fixed basis of observables. Are we able to reconstruct the physical state from this CM uniquely? We will start answering this question by considering a single system.

Proposition 2.4 (Characterization of states via non-symmetric covariance matrices)**.** *Given a non-symmetric CM with tomographically complete set of observables, we can reconstruct the corresponding physical state unambiguously.*

Proof: We choose the following basis of the observables:

$$D_i = |i\rangle\langle i|, \quad i = 1, \ldots, d, \tag{2.11}$$

$$X_{i,j} = \frac{1}{\sqrt{2}}(|i\rangle\langle j| + |j\rangle\langle i|), \quad 1 \leq i < j \leq d, \tag{2.12}$$

$$Y_{k,l} = \frac{i}{\sqrt{2}}(|k\rangle\langle l| - |l\rangle\langle k|), \quad 1 \leq k < l \leq d. \tag{2.13}$$

These observables form an orthonormal basis, and we will refer to this basis as to the standard basis later on. As in any basis M_k, we can write the state as $\rho = \sum_k \langle M_k\rangle M_k$, it suffices to know the first moments $\langle M_k\rangle$. From Eq. (2.3) one can see that $\gamma_{i,j} - \gamma_{j,i} = \langle [M_i, M_j]\rangle$. In the following we will show that in the chosen basis, all first moments can be obtained from expectation values of commutators.

For the chosen standard basis we can explicitly calculate all commutators

$$[D_k, X_{k,l}] = \frac{i}{\sqrt{2}} Y_{k,l}, \quad [D_k, Y_{k,l}] = -\frac{i}{\sqrt{2}} X_{k,l}, \tag{2.14}$$

$$[X_{k,l}, Y_{k,l}] = i(|k\rangle\langle k| - |l\rangle\langle l|). \tag{2.15}$$

Hence, all expectation values of the $X_{i,j}$ and $Y_{k,l}$ can be calculated. The same is true for the diagonal elements: Using the fact that the trace of the density matrix is equal to one, we can calculate all the diagonal elements from the mean values of $[X_{k,l}, Y_{k,l}]$. ■

Clearly, the same approach can be used for bipartite systems, if we use the CM in the full (and not in a block) form. In this case we can use a product basis $\{|i_1, i_2\rangle\}$. Identifying $(i_1, i_2) =: i$ we can define the standard basis as above and find all first moments from the covariance matrix.

As we have seen, the non-symmetric CM defined in Eq. (2.3) describes the physical state completely. The knowledge of the symmetric CM in Eq. (2.4) is, however, not enough:

Proposition 2.5 (Inequivalence of states and symmetric covariance matrices)**.** *The knowledge of the symmetric CM γ^S does, in general, not determine the state ρ completely.*

Proof: We prove the claim by providing a counterexample. Let us take a single qubit. As observables we take the appropriate normalized Pauli matrices. The symmetric CM has the following entries

$$\gamma^S_{0,j} = \frac{\langle \mathbb{1}\sigma_j\rangle + \langle \sigma_j \mathbb{1}\rangle}{4} - \frac{\langle \mathbb{1}\rangle\langle \sigma_j\rangle}{2} = 0 = \gamma^S_{i,0}, \tag{2.16}$$

$$\gamma^S_{i,j} = \frac{\langle \{\sigma_i, \sigma_j\}\rangle}{4} - \frac{\langle \sigma_i\rangle\langle \sigma_j\rangle}{2} = \frac{\delta_{i,j} - \langle \sigma_i\rangle\langle \sigma_j\rangle}{2}. \tag{2.17}$$

From this we can determine the norm of the mean value of the spin component in a certain direction, but not its sign. Hence we know the length of the Bloch vector of the system, up to some reflection to the origin, which corresponds to simultaneous change of signs of all $\langle\sigma_i\rangle$'s.

One might think that the case of one qubit constitutes a special case. However, the same ambiguity will arise if one embedded a qubit in a higher dimensional, say, three level system. As it can be checked, the additional observables in the basis of observables $\{M_k\}$ will not provide any further information. ■

To summarize: The knowledge of the symmetric CM of a qubit alone is not sufficient to decide between two alternatives of states which have opposite (symmetric to the origin) Bloch vectors. Also, merely the additional knowledge of a single bit (the sign) is needed to make this correspondence unambiguous. This, however, is specific to the qubit case. We will now turn to investigating the same question for the block CM defined in Eq. (2.7):

Proposition 2.6 (Relationship between bipartite states and block covariance matrices)**.** *For block CMs γ and γ^S on a bipartite system, the following statements hold:*

(i) The (non-symmetric) block CM γ determines the bipartite state ρ_{AB} completely.

(ii) The symmetric block γ^S does not determine ρ_{AB} completely.

Proof: Obviously, given a non-symmetric block CM for the set of variables $A_k \otimes \mathbb{1}$ and $\mathbb{1} \otimes B_l$ we can determine first all $\langle A_k\rangle$ and $\langle B_l\rangle$ for the reduced state ρ_A in the same way as in Proposition 2.4 from the blocks A and B of γ. Then, knowing the block C we can fix the rest $\langle A_k \otimes B_l\rangle$ as

$$\langle A_k \otimes B_l\rangle = C_{k,l} + \langle A_k\rangle\langle B_l\rangle \tag{2.18}$$

and hence *(i)* is proved.

The validity of *(ii)* is straightforward to see for two qubit states, as there will be the same lack of information on the mean values of observables as in Proposition 2.5 and hence γ^S_{AB} does not provide the whole information about the state. ■

The fact that the symmetric block CM γ^S does not determine the state completely will later be important for the discussion of our entanglement criteria. Therefore, let us investigate this correspondence for the case of two qubits in some more detail. For that, let A_i and B_j be Pauli matrices. We may write the state in the form

$$\rho_{AB} = \frac{1}{4}\sum_{i,j} \lambda_{i,j}\sigma_i^A \otimes \sigma_j^B, \tag{2.19}$$

where $\lambda_{i,j} = \mathrm{Tr}\left(\rho\sigma_i^A \otimes \sigma_j^B\right)$.

As one can see from Eq. (2.18) we have two possibilities of changing the $\lambda_{i,j}$ while keeping the $C_{i,j}$ invariant: We can (i) flip the signs of both of the Bloch vectors of the reduced density matrices, ($\lambda_{0,j}$ and $\lambda_{i,0}$ for $i,j = 1,2,3$), while keeping the left hand side of Eq. (2.18) invariant. Alternatively, we can (ii) flip the sign of only one of them, which implies that we also have to change the left hand side of Eq. (2.18).

Concerning (i), one can directly calculate the transformed state ρ^{inv}. It turns out that the eigenvalues of ρ and ρ^{inv} are the same, suggesting that they are connected by a unitary transformation maybe in addition with a global transposition which transforms one state to the other. Actually the unitary transformation is a local unitary one, and one has the following transformation:

$$\begin{aligned} \left(\rho^{\text{inv}}\right)^T &= U^\dagger \rho_{AB} U, \\ U &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \end{aligned} \tag{2.20}$$

Since there is no physical process which corresponds to a transposition of a state, there are two physically different states ρ and ρ^{inv} which give rise to the same covariance matrix and which are connected by the simultaneous flip of the Bloch vectors of their subsystems. Nevertheless we can see from Eq. (2.20) that these states have the same entanglement properties, because there is a local unitary operation in addition to a global transposition connecting them. These transformations do not change the outcome of the PPT criterion, and in fact do not change the entanglement properties of any two-qubit quantum state.

Concerning (ii), it also possible to flip the Bloch vector of only one of the subsystems in a such a way that the whole covariance matrix will remain unaltered. This kind of transformation is done by

$$\begin{aligned} \langle \sigma_i^A \rangle &\mapsto -\langle \sigma_i^A \rangle, \\ \langle \sigma_i^A \otimes \sigma_j^B \rangle &\mapsto \langle \sigma_i^A \otimes \sigma_j^B \rangle - 2\langle \sigma_i^A \rangle \langle \sigma_j^B \rangle, \end{aligned} \tag{2.21}$$

resulting in a transformation of ρ to a different ρ^{inv}. Such a change of the state is nontrivial and can give rise to a matrix ρ^{inv} with negative eigenvalues, which clearly does not correspond to any state. Two more cases that should be discussed. As one can see from a numerical search, there are some states ρ, for which ρ^{inv} is still a state and ρ and ρ^{inv} are either both separable or both entangled. But there exist also states which alter their separability properties after a Bloch vector inversion. As an example of states where ρ and ρ^{inv} have different separability properties, consider the states of the form

$$\rho_\varepsilon = \frac{\varepsilon}{2} \begin{pmatrix} 1+r & 0 & 0 & t \\ 0 & 0 & 0 & 0 \\ 0 & 0 & s-r & 0 \\ t & 0 & 0 & 1-s \end{pmatrix} + (1-\varepsilon) \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{2.22}$$

ρ_ε is a slight modification of the family of the states introduced in Ref. [65] and which are known to be detected by PPT but not by CCNR criterion for certain

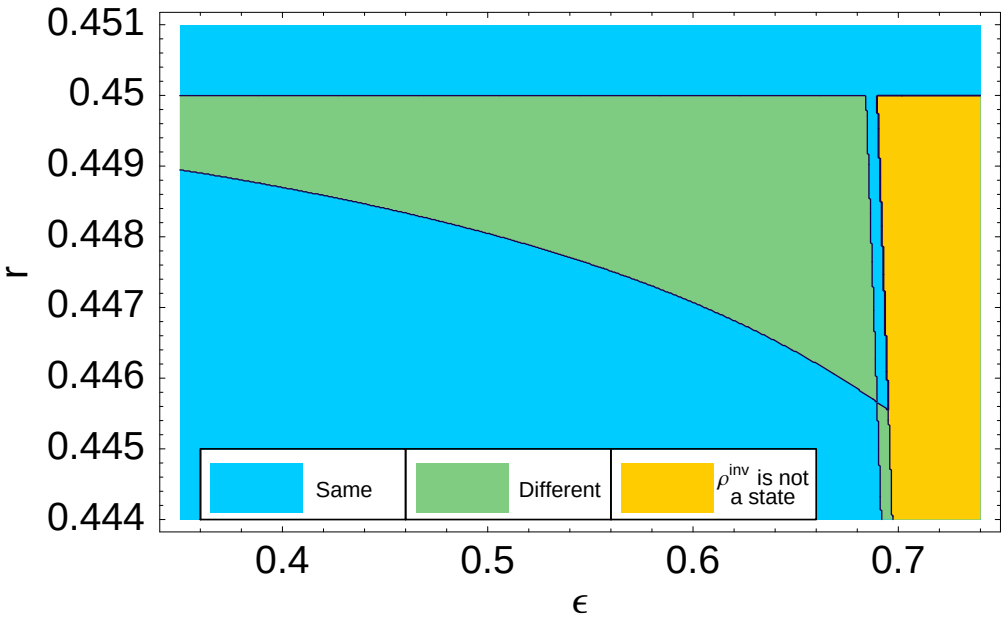


Figure 2.1. *Entanglement properties of ρ_ε and ρ_ε^{inv} are revealed by the PPT criterion for $s = 0.45$ and $t = \frac{1}{16}$. ε and r are varied. Three regions corresponds to three different cases. The region "Same" corresponds to the case where ρ_ε and ρ_ε^{inv} are either both separable or both entangled. The region "Different" corresponds to the situation where ρ_ε is separable but ρ_ε^{inv} is entangled or vice versa. The last region consists of states ρ_ε for which the inversion of the Bloch vector of one of the subsystems leads to ρ_ε^{inv} which is not positive semidefinite anymore.*

parameters. The inverted form $\rho_\varepsilon^{\mathrm{inv}}$ of this states can be calculated analytically. The states ρ_ε are known to be PPT for $(t = 0, \varepsilon = 1)$. Going away from $\varepsilon = 1$ and changing other parameters one can find regions where ρ_ε and $\rho_\varepsilon^{\mathrm{inv}}$ have different entanglement properties.

As we can see from Fig. 2.1 there are three different regions corresponding to the different physical situations. The most interesting region is the "Different" region where entanglement properties of the inverted state are different from that of the initial one. This means that any separability criterion which uses only the symmetric CM will not detect these states, as the symmetric CM is compatible with a separable as well as with an entangled state. These states will not be detected by the CMC, and also not by a variety of other criteria, as we will see later.

2.4 Properties of covariance matrices

In this section we will prove several properties of CMs which are important for our later discussion. This concerns mainly properties of CMs for pure states and the

behavior of CMs under the mixing of states. We will first show in the subsequent proposition that a suitable choice of observables can dramatically simplify the form of CM γ for pure states.

Proposition 2.7 (Covariance matrices of pure states)**.** *Let G_i be a tomographically complete set of observables of a d-dimensional system. If ρ is a pure state then γ (as a $d^2 \times d^2$ matrix) fulfills:*

(i) The rank is given by $Rank(\gamma) = d - 1$.

(ii) The nonzero eigenvalues of γ are equal to 1, hence $Tr(\gamma) = d - 1$.

(iii) Consequently, we have $\gamma^2 = \gamma$.

Proof: Without any loss of generality we assume $\rho = |1\rangle\langle 1|$ and take as observables the ones of the standard basis (2.13). Calculating directly and reordering of the matrix elements afterword's gives a block structure [2]

$$\gamma = \bigoplus_{k=1}^{d-1} [B_k] \bigoplus \mathbb{O}_{d^2-2d+2} \quad \text{with} \quad B_k = \begin{pmatrix} 1/2 & i/2 \\ -i/2 & 1/2 \end{pmatrix}, \tag{2.23}$$

where $\mathbb{O}_k$ denotes a $k \times k$ matrix of zeros. The matrix in Eq. (2.23) has the desired properties. ■

From this we can directly read off the properties of the symmetric form of the covariance matrix:

Corollary 2.8 (Properties of symmetric CMs for pure states)**.** *Let $\{G_i\}$ be a tomographic complete set of observables of a d-dimensional quantum system. If ρ is a pure state, then γ^S (as $d^2 \times d^2$ symmetric matrix) fulfills:*

(i) The rank is given by $Rank(\gamma^S) = 2(d - 1)$.

(ii) The nonzero eigenvalues of γ^S are equal to $1/2$, hence $Tr(\gamma) = d - 1$.

We now turn to a proposition concerning the trace of a CM for mixed states.

Proposition 2.9 (Trace of CMs)**.** *Let ρ be a mixed state. Then*

$$Tr(\gamma(\rho)) = d - Tr\left(\rho^2\right)) \tag{2.24}$$

which implies that $d - 1/d \geq Tr(\gamma(\rho)) \geq d - 1$. This holds also for γ^S.

Proof: By definition $\mathrm{Tr}(\gamma) = \sum_i \gamma_{i,i} = \sum_i \delta^2(M_i) = \sum_i (\langle M_i^2 \rangle - \langle M_i \rangle^2)$. The first summation is trivial, since we have $\sum_k M_k^2 = d\mathbb{1}$ [132]. Furthermore we can write $\rho = \sum_k \langle M_k \rangle M_k$ which implies that $\sum_k \langle M_k \rangle^2 = \mathrm{Tr}\left(\rho^2\right)$, and further $1/d \leq \mathrm{Tr}\left(\rho^2\right) \leq 1$. The statement for γ^S follows directly from the fact that $\mathrm{Tr}(\gamma) = \mathrm{Tr}\left(\gamma^S\right)$. ■

We can also estimate the operator norm (i.e., the maximal eigenvalue) of CMs.

[2] We denote by $A \oplus B$ a 2×2 block matrix with A and B on the diagonal, and zero matrices elsewhere.

Proposition 2.10 (Operator norm of CMs)**.** *For the CM $\gamma(\rho)$ and its linear part $\mathfrak{g}(\rho)$ the operator norm is bounded by*

$$\|\mathfrak{g}(\rho)\| \leq \|\rho\| \text{ and } \|\gamma(\rho)\| \leq \|\rho\|. \tag{2.25}$$

The same bounds hold for symmetric CMs.

Proof: Let us first consider $\mathfrak{g}(\rho)$. We have $\|\mathfrak{g}(\rho)\| = \max_{|x\rangle}\langle x|\mathfrak{g}(\rho)|x\rangle = \langle x_0|\mathfrak{g}(\rho)|x_0\rangle = \mathrm{Tr}\left(\rho AA^\dagger\right)$ with $\mathrm{Tr}\left(AA^\dagger\right) = 1$. This is clearly smaller than $\|\rho\|$. For $\gamma(\rho)$ this follows then from $\langle AA^\dagger\rangle - \langle A\rangle\langle A^\dagger\rangle \leq \langle AA^\dagger\rangle$. ■

Finally, CMs also satisfy an interesting majorization relation. This has its root in the way how one can relate CMs to the rotated CMs of the pure states occurring in their convex decompositions in terms of pure states.

Proposition 2.11 (Majorization relation for CMs)**.** *For any (mixed) state ρ, both the linear part $\mathfrak{g}(\rho)$ with entries $\mathfrak{g}_{i,j} = \langle M_i M_j\rangle$ as well as the CM $\gamma(\rho)$ satisfy*

$$\sum_{j=1}^{k} \lambda_j[\mathfrak{g}(\rho)], \sum_{j=1}^{k} \lambda_j[\gamma(\rho)] \leq \min(k, d - \delta_\gamma \frac{1}{d}), \tag{2.26}$$

for the non-increasingly ordered eigenvalues, where $\delta_\gamma = 1$ for $\gamma(\rho)$ $\delta_\gamma = 0$ if $\mathfrak{g}(\rho)$ is considered.

Proof: This is a consequence of $\|\gamma(\rho)\|, \|\mathfrak{g}(\rho)\| \leq 1$ as well as of $\mathrm{Tr}\left(\gamma(\rho)\right) \leq d - \frac{1}{d}$ and $\mathrm{Tr}\left(\mathfrak{g}(\rho)\right) \leq d$. ■

2.5 Explicit form of the block CM for pure states

In this section we pick up an example and calculate symmetric block CM of a pure bipartite state, which is written in the Schmidt decomposition $|\psi\rangle = \sum_i \sqrt{\lambda_i}|i_A\rangle \otimes |i_B\rangle$. Consider $d_A = d_B = d$. This example will be used later in chapter 6 where we consider entanglement quantification with covariance matrices.

Again for convenience we choose the local orthogonal observables (LOOs) from the standard basis (2.13), which satisfy following commutation relations:

$$\begin{aligned}
\{D_i, D_j\} &= \delta_{ij}\left(|i\rangle\langle j| + |j\rangle\langle i|\right), & \{D_i, X_{ij}\} &= X_{ij}, \\
\{D_i, Y_{ij}\} &= Y_{ij}, & \{X_{ij}, Y_{ij}\} &= 0, \\
\{X_{ij}, X_{ij}\} &= D_i + D_j, & \{Y_{ij}, Y_{ij}\} &= D_i + D_j.
\end{aligned} \tag{2.27}$$

Note that this is not the complete set of relations, however other relations will not give any contribution to the CM and hence we leave them out here.

The mean values for the state $|\psi\rangle$ are given by

$$\begin{aligned}
&\langle X_{ij}^A \otimes \mathbb{1}\rangle = \langle \mathbb{1} \otimes X_{ij}^B\rangle = \langle Y_{ij}^A \otimes \mathbb{1}\rangle = \langle \mathbb{1} \otimes Y_{ij}^B\rangle = 0 \\
&\langle D_i^A \otimes \mathbb{1}\rangle = \langle \mathbb{1} \otimes D_i^B\rangle = \lambda_i \\
&\langle \{D_i^A, D_j^A\} \otimes \mathbb{1}\rangle = (\lambda_i + \lambda_j)\delta_{ij}
\end{aligned} \tag{2.28}$$

The blocks A, B and C of the $\gamma^S(|\psi\rangle)$ can be therefore written as 3×3 block matrices. Because of the relations (2.27) and (2.28) a lot of terms in these blocks will be equal to zero an we have the structure

$$A, B, C = \begin{pmatrix} D^{A/B/C} & 0 & 0 \\ 0 & X^{A/B/C} & 0 \\ 0 & 0 & Y^{A/B/C} \end{pmatrix}, \tag{2.29}$$

Since the off-diagonal terms can be calculated straightforward

$$\begin{aligned}
&\langle D_i^A \otimes D_j^B\rangle - \langle D_i^A\rangle\langle D_j^B\rangle = \lambda_i\delta_{ij} - \lambda_i\lambda_j, \\
&\langle D_i^A \otimes X_{qr}^B\rangle = \langle D_i^A \otimes Y_{qr}^B\rangle = \langle X_{pq}^A \otimes Y_{rs}^B\rangle = 0, \\
&\langle X_{pq}^A \otimes X_{rs}^B\rangle = \sqrt{\lambda_p\lambda_q}\delta_{pr}\delta_{qs}, \\
&\langle Y_{pq}^A \otimes Y_{rs}^B\rangle = -\sqrt{\lambda_p\lambda_q}\delta_{pr}\delta_{qs},
\end{aligned} \tag{2.30}$$

we can write the blocks in (2.29) as follows

$$\begin{aligned}
D = D_{ij}^{A/B/C} &= \lambda_i\delta_{ij} - \lambda_i\lambda_j, \\
X = X^{A/B} &= \frac{1}{2}\mathrm{diag}\{\lambda_i + \lambda_k\}, 1 \le i < k \le d, \\
Y = Y^{A/B} &= \frac{1}{2}\mathrm{diag}\{\lambda_i + \lambda_k\}, 1 \le i < k \le d, \\
X^C &= \mathrm{diag}\{\sqrt{\lambda_p\lambda_q}\}, 1 \le p < q \le d, \\
Y^C &= \mathrm{diag}\{-\sqrt{\lambda_p\lambda_q}\}, 1 \le p < q \le d.
\end{aligned} \tag{2.31}$$

Finally, we arrive at the general form of the CM for a pure state as a function its Schmidt coefficients:

$$\gamma^S(|\psi\rangle) = \begin{pmatrix} D & 0 & 0 & D & 0 & 0 \\ 0 & X & 0 & 0 & X^C & 0 \\ 0 & 0 & Y & 0 & 0 & Y^C \\ D & 0 & 0 & D & 0 & 0 \\ 0 & X^C & 0 & 0 & X & 0 \\ 0 & 0 & Y^C & 0 & 0 & Y \end{pmatrix} \tag{2.32}$$

with the blocks given in Eq. (2.31).

2.6 Mixing property of covariance matrices

Separable states are those states that can be written as convex combinations of product states. Therefore we have to understand the behavior of CMs under mixing of states for the derivation of separability criteria. An important property of covariance matrices which we refer to as concavity property is the following:

Proposition 2.12 (Concavity property)**.** *Let $\rho = \sum_k p_k \rho_k$ be a convex combination of states ρ_k, then*

$$\gamma(\rho) \geq \sum_k p_k \gamma(\rho_k). \tag{2.33}$$

Clearly, this implies the same relation for the symmetrized CM γ^S.

Proof: As shown in Ref. [37] this inequality holds for an arbitrary symmetric CM γ^S. Moreover, since $\langle M_i M_j \rangle_\rho = \sum_k p_k \langle M_i M_j \rangle_{\rho_k}$ for all i, j, we have for the non-linear part that

$$-\langle M_i \rangle_\rho \langle M_j \rangle_\rho \geq -\sum_k p_k \langle M_i \rangle_{\rho_k} \langle M_j \rangle_{\rho_k} \tag{2.34}$$

as a matrix inequality for the matrices $X_{i,j} = -\langle M_i \rangle_\rho \langle M_j \rangle_\rho$ and $Y_{i,j} = -\sum_k p_k \langle M_i \rangle_{\rho_k} \langle M_j \rangle_{\rho_k}$. From this, the above inequality follows for the non-symmetric CM γ. ■

This property will later be used to derive the separability criterion.

2.7 Transformations of observables and validity of covariance matrices

Transformations as generated by a general orthogonal matrix O used in Proposition (2.3) do in general not preserve the positivity of the state ρ (see Ref. [133] for discussion). Only a subgroup will correspond to unitary transformations on the level of states. Here, we will clarify how unitary transformations of the state are reflected by orthogonal transformations on the level of CMs.

For this aim, let us consider the case that ρ is transformed by some unitary transformation $\rho \mapsto U^\dagger \rho U$. Equivalently, we can transform the operator basis, denoted as $\{G_i\}$, as

$$G_i \mapsto H_i = U G_i U^\dagger = \sum_j O_{i,j} G_j. \tag{2.35}$$

It is then easy to see that the transformation of the CM is

$$\gamma(\rho) \mapsto O \gamma(\rho) O^T = \gamma(U^\dagger \rho U), \tag{2.36}$$

We can now ask in what way O depends on U, and which orthogonal $O \in O(d^2)$ correspond to a unitary $U \in U(d)$ acting in state space as described above. That is, we look for the group representation of $U(d)$ in the space of CMs (compare also the metaplectic representation of symplectic transformations in discrete Weyl systems, see Ref. [131]). The following theorem gives an answer to this question.

Proposition 2.13 (Transformation laws for CMs)**.** *Let $U \in U(d)$. Then the $O \in O(d^2)$ representing U as described above (2.35) is given by*

$$O = \Gamma^T (U^T \otimes U^\dagger) \Gamma^*, \tag{2.37}$$

where Γ *is a* $d^2 \times d^2$ *square matrix constructed as* $\Gamma_{\alpha,\beta|i} = G_i^{\alpha,\beta} = (|G_1\rangle, |G_2\rangle, \dots)$*, where we understand* α, β *as a row index,* $G_i^{\alpha,\beta}$ *as vectors and construct* $\Gamma_{\alpha,\beta|i}$ *from them.*

Proof: Let us first explain some properties of the matrix Γ. This matrix has entries which are just the basis vectors G_i written as columns. Moreover, $\Gamma\Gamma^\dagger = \mathbb{1} = \Gamma^\dagger\Gamma$, i.e., Γ is a unitary, since

$$(\Gamma^\dagger\Gamma)_{i,j} = \sum_k \Gamma^\dagger_{ik}\Gamma_{kj} = \sum_{\alpha,\beta}(G_i^{\alpha,\beta})^* G_j^{\alpha,\beta} = \sum_{\alpha,\beta}(G_i^{\beta,\alpha})G_j^{\alpha,\beta} = \mathrm{Tr}\,(G_i G_j) = \delta_{i,j}, \tag{2.38}$$

where we have used the orthogonality and hermiticity of G_i. However Γ is a special unitary, since the columns correspond to orthonormal Hermitian observables. Now we have in Eq. (2.35)

$$\sum_j O_{i,j} G_j^{\alpha,\beta} = \sum_j G_j^{\alpha,\beta}\left(O^T\right)_{j,i} = \left(\Gamma O^T\right)_{\alpha,\beta|i}, \tag{2.39}$$

where we have used the definition of Γ and the fact that the expression in the middle of Eq. (2.39) is nothing but i-th column of ΓO^T. Conversely,

$$(UG_iU^\dagger)_{\alpha,\beta} = U_{\alpha,\delta}G_i^{\delta,\gamma}U^\dagger_{\gamma,\beta} = U_{\alpha,\delta}U^*_{\beta,\gamma}\Gamma_{\delta,\gamma|i} = (U\otimes U^*)_{\alpha,\beta,\delta,\gamma}\Gamma_{\delta,\gamma|i} = (U\otimes U^*\Gamma)_{\alpha,\beta|i}, \tag{2.40}$$

where the definition of Γ and $A_{i,k}\otimes B_{l,m} \equiv (A\otimes B)_{i,l,k,m}$ was used. Therefore we can write

$$\begin{aligned} O^T &= \Gamma^\dagger(U\otimes U^*)\Gamma = \Gamma^T(U^*\otimes U)\Gamma^*, \\ O &= \Gamma^\dagger(U^\dagger\otimes U^T)\Gamma = \Gamma^T(U^T\otimes U^\dagger)\Gamma^*, \end{aligned} \tag{2.41}$$

where we used that O is real. With these representations, we can finally check the orthogonality of the O as

$$\begin{aligned} O^TO &= \Gamma^T(U^*\otimes U)\Gamma^*\Gamma^T(U^T\otimes U^\dagger)\Gamma^* = \Gamma^T(U^*\otimes U)\mathbb{1}(U^T\otimes U^\dagger)\Gamma^* \\ &= \Gamma^T(U^*U^T\otimes UU^\dagger)\Gamma^* = \Gamma^T\Gamma^* = \mathbb{1}. \end{aligned} \tag{2.42}$$

■

It is an interesting open question to see how CMs are transformed under general completely positive maps, $\rho \mapsto \sum_i A_i\rho A_i^\dagger$, where $\{A_i\}$ are Kraus operators, directly expressed in terms of the Kraus operators.

At the very beginning we have given two definitions of covariance matrices for the symmetric and non-symmetric case (2.3,2.4). We will discuss this difference also later in the chapter. However at this stage we mention a single connection between these two definitions for block CMs:

Proposition 2.14 (Block forms of CMs under local basis transformations)**.** *It is not possible to achieve for the block CMs* $\gamma = \gamma^S$ *via local basis transformations of the operator basis. The only states for which this relation holds have the reduced states* $\rho_A = Tr(\rho)_B = \mathbb{1}/d_A$ *and* $\rho_B = Tr(\rho)_A = \mathbb{1}/d_B$*, where* $d_{A,B}$ *are the dimensions of* $\rho_{A,B}$*. It follows that* $\gamma = \gamma^S$ *cannot be achieved by local unitary operations either.*

Proof: First note that if we write γ as in Eq. (2.7) in the block wise form, A, B correspond to CMs of the subsystems A, B and C has entries of the form $\langle A_i \otimes B_j \rangle - \langle A_i \rangle \langle B_j \rangle$, where A_i, B_j are observables taken for subsystems A, B.

The condition $\gamma = \gamma^S$ is equivalent to the condition $\gamma = \gamma^T$, in particular $A = A^T$ and $B = B^T$. If we change the local bases on A and B via $O = O^A \oplus O^B$ the CM gets to

$$\gamma' = (O^A \oplus O^B)\gamma(O^A \oplus O^B)^T. \tag{2.43}$$

As we can immediately see $\gamma'^T = (O^A \oplus O^B)\gamma^T(O^A \oplus O^B)^T = \gamma'$ if and only if $\gamma^T = \gamma$, so the symmetry of CM does not depend on the particular choice of basis in observable space.

Therefore we are able to choose the standard basis. Let us consider only subsystem A, i.e., left upper block of matrix γ, and let us assume that $A = A^T$ holds. As we have showed already, we can obtain ρ_A from the matrix A by use of the commutators $A_{i,j} - A_{j,i} = \langle [M_i^A, M_j^A] \rangle$. However, all those commutators vanish for the case $A = A^T$. Since then $\langle X_{k,l} \rangle = \langle Y_{k,l} \rangle = 0$ for all k, l, it follows that ρ_A is diagonal. The diagonal elements can be also determined as in Prop. 2.4 and since also $\langle Z_{k,l} \rangle = 0$ for all k, l, it follows that $\rho_A = \mathbb{1}/d_A$, which completes the first part of the proof.

Finally, local unitary transformations are only a subclass of the orthogonal transformations considered before, hence $\gamma = \gamma^T$ cannot be achieved by a local unitary transformation of ρ neither. ■

2.8 Conclusion

After we investigated in detail properties of covariance matrices of quantum states in finite-dimensional Hilbert spaces, we introduce in the next chapter an entanglement criterion, which is formulated in terms of symmetric covariance matrices. Further, we will investigate the properties of this criterion and evaluate it.

Chapter 3

The covariance matrix criterion for separability

Based on the properties of covariance matrices, discussed in the last chapter, we formulate an entanglement criterion, which will be the main topic of discussion for the next few chapters. We call this criterion the covariance matrix criterion (CMC). After formulating and proving the criterion we point out the most evolving problem in the evaluation of the CMC.

Proposition 3.1 (Covariance matrix criterion)**.** *Let ρ be a separable state and A_i (B_i) be orthogonal observables on $\mathcal{H}_A$ ($\mathcal{H}_B$), where the dimensions of the Hilbert spaces are d_A (d_B, respectively). Define $M_i = A_i \otimes \mathbb{1}$ for $i = 1, \ldots, d_A^2$ and $M_i = \mathbb{1} \otimes B_i$ for $i = d_A^2 + 1, \ldots, d_B^2 + d_A^2$. Then there exist pure states $|\psi_k\rangle\langle\psi_k|$ for A and $|\phi_k\rangle\langle\phi_k|$ for B and convex weights p_k such that if we define $\kappa_A = \sum_k p_k \gamma(|\psi_k\rangle\langle\psi_k|)$ and $\kappa_B = \sum_k p_k \gamma(|\phi_k\rangle\langle\phi_k|)$ the inequality*

$$\gamma^S(\rho, \{M_i\}) \geq \kappa_A \oplus \kappa_B \Leftrightarrow \begin{pmatrix} A & C \\ C^T & B \end{pmatrix} \geq \begin{pmatrix} \kappa_A & 0 \\ 0 & \kappa_B \end{pmatrix} \tag{3.1}$$

holds. This means that the difference between left and right hand side must be positive-semidefinite. If there are no such $\kappa_{A,B}$ then the state ρ must be entangled.

Proof: First note that for this special choice of M_i, for any product state

$$\gamma(\rho_A \otimes \rho_B, \{M_i\}) = \gamma(\rho_A, \{A_i\}) \oplus \gamma(\rho_B, \{B_i\}) \tag{3.2}$$

holds. Now, since any separable state can be written as $\rho = \sum_k p_k |\psi_k\rangle\langle\psi_k| \otimes |\phi_k\rangle\langle\phi_k|$, we can apply Prop. (2.12) and arrive at the conclusion. ■

Note that the CMC is manifestly invariant under a change of the observables $\{A_k\}$ and $\{B_k\}$, as we know from Proposition 2.3 [see also Eq. (2.43)]; however, a suitable choice of them may simplify the evaluation a lot. Also, note that we have formulated the CMC for symmetric CMs, we will later discuss the case of non-symmetric CMs.

Obviously, as such, as formulated as in Prop. 3.1, it is not clear that the CMC leads to an efficient and physically plausible test for separability: The main problem is to characterize the possible κ_A and κ_B. As such, the formulation still contains an optimization over all pure product states. We will refer to an "evaluation of the CMC" hence whenever we can identify a property of $\kappa_{A,B}$ that will render the above criterion an efficient test.

Some properties of we have derived above, notably

$$\mathrm{Tr}\,(\kappa_A) = d_A - 1 \tag{3.3}$$

(see Proposition 2.8), which we will use subsequently. We will now turn to feasible ways to evaluate the CMC. As a first step, we have to derive conditions on the blocks of a block matrix as in Eq. (3.1), which follow from the positivity condition in Eq. (3.1). Then, we ask how the observables $\{A_k\}$ and $\{B_k\}$ must be chosen in order to make a violation of Eq. (3.1) manifest.

Note the formal similarity of the condition $\gamma \geq \kappa_A \oplus \kappa_B$ to tests for separability for Gaussian states for systems with canonical coordinates (1.56) discussed in the first chapter.

In the next chapter we address the question of the evaluation of the CMC. Based on the general properties of covariance matrices and using several mathematical tricks one can derive corollaries from the general CMC, presented in this chapter, which detect many bound entangled states and which are easily to compute.

Chapter 4

Evaluation of the CMC

In order to evaluate the CMC presented in the previous chapter, we follow several strategies. In the first part of this chapter we present strategies based on matrix invariants such as eigenvalues or singular values. Namely, we address the characterization of positive semidefinite matrices of a block structure in terms of singular values of their submatrices. This characterization will result in an entanglement criterion in terms of singular values of the off-diagonal blocks C of the covariance matrix γ. We show that this criterion is equivalent to the extension of the computable cross-norm or realignment (CCNR) criterion, discussed in Ref. [135], and stronger than the criterion based on Bloch representation of the density matrices, discussed in Ref. [136]. We conclude that both criteria are corollaries of the general CMC.

In the second part of the chapter we apply the derived criteria to states, written in a specific form. Firstly, one can use Schmidt decomposition of density matrix and choose the Schmidt basis as local observables for constructing the covariance matrix of the state. The resulting criterion in this case is strictly stronger than CCNR criterion and as a consequence of this detects bound entangled states. Secondly, since stochastic local operations assisted by classical communication (SLOCC) do not affect separability, we apply the CMC to states, which are written in standard form, discussed in Refs. [138, 139, 140]. The resulting criterion turns out to be really strong for systems with $\dim(\mathcal{H}_A) = \dim(\mathcal{H}_B) = d$ and necessary and sufficient for two qubits.

In the remainder of the chapter we show the equivalence of the CMC and local uncertainty relations. Thereafter we discuss two qubit case in more detail and show how one can cast the CMC in framework of the semidefinite programming and test derived criteria on several bound entangled states.

4.1 Evaluation of the CMC via singular values of submatrices

As a start, we state the following Lemma:

Lemma 4.1 (Block covariance matrices and unitarily invariant norms)**.** *If a positive matrix partitioned in block form is positive semidefinite,*

$$\begin{pmatrix} A & C \\ C^T & B \end{pmatrix} \geq 0, \tag{4.1}$$

then

$$|||A|||\,|||B||| \geq |||\,|C|\,|||^2, \tag{4.2}$$

holds, where $|||.|||$ is any unitarily invariant norm. Specifically, this holds true for any Ky-Fan norm $\|.\|_{KF}$ defined as the sum of the largest k singular values. If we sum over all singular values, we arrive at the largest Ky-Fan norm, which is the trace norm.

Proof: The proof of this statement is actually a corollary of Theorem 3.5.15 of Ref. [21]. It is shown that

$$|||A^p|||\,|||B^p||| \geq |||(C^\dagger C)^{p/2}|||^2, \tag{4.3}$$

for any $p > 0$ and any unitarily invariant norm. For $p = 1$ this is the result we are interested in. We will nevertheless present an alternative proof of this statement for Ky-Fan norms $\|A\|_{KF}\|B\|_{KF} \geq \|C\|_{KF}^2$, below, as the proof of Proposition 4.9 will make use of this proof.

Independently of the proof presented above we found an alternative proof of the Lemma 4.1. For a matrix as in Eq. (4.1) the following condition has to be fulfilled:

$$\begin{pmatrix} \langle\alpha| \\ \langle\beta| \end{pmatrix} \begin{pmatrix} A & C \\ C^T & B \end{pmatrix} \begin{pmatrix} |\alpha\rangle & |\beta\rangle \end{pmatrix} \geq 0, \tag{4.4}$$

for all vectors $|\alpha\rangle, |\beta\rangle$, which implies that $\langle\alpha|A|\alpha\rangle + \langle\beta|B|\beta\rangle \geq 2\langle\alpha|C|\beta\rangle$, where we took $-|\beta\rangle$ instead of $|\beta\rangle$ for convenience. Especially, we can take $|\alpha\rangle = \alpha|\psi_k\rangle$ and $|\beta\rangle = \beta|\phi_k\rangle$, where the vectors $|\psi_k\rangle$ and $|\phi_k\rangle$ are singular vectors from the singular value decomposition of C and $\langle\psi_k|C|\phi_k\rangle = \sigma_k(C)$ is the k-th singular value. Hence

$$\alpha^2\langle\psi_k|A|\psi_k\rangle + \beta^2\langle\phi_k|B|\phi_k\rangle \geq 2\alpha\beta\langle\psi_k|C|\phi_k\rangle. \tag{4.5}$$

Note that $\langle\psi_k|A|\psi_k\rangle$ and $\langle\psi_k|A|\psi_k\rangle$ are greater than zero, because A and B are positive semidefinite matrices. Taking the sum over k and noting that for A and B expressions like $\sum_{k=1}^K\langle\psi_k|A|\psi_k\rangle$ are a lower bound on the K-th Ky-Fan norm [21] we get

$$\alpha^2\|A\|_{KF} + \beta^2\|B\|_{KF} \geq 2\alpha\beta\|C\|_{KF}. \tag{4.6}$$

The last formula is necessary and sufficient condition for the 2×2 matrix

$$\begin{pmatrix} \|A\|_{KF} & \|C\|_{KF} \\ \|C\|_{KF} & \|B\|_{KF} \end{pmatrix} \geq 0 \tag{4.7}$$

to be positive semidefinite and having a non-negative determinant, from which the claim follows. ■

Using the last Lemma we have:

Proposition 4.2 (CMC evaluated using singular values)**.** *Let*

$$\gamma = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix} \tag{4.8}$$

be a CM. Then, if ρ is separable, we have

$$\|C\|_{Tr}^2 \leq \left[1 - Tr\left(\rho_A^2\right)\right]\left[1 - Tr\left(\rho_B^2\right)\right]. \tag{4.9}$$

If this inequality is violated, then ρ must be entangled.

Proof: We prove the claim applying the formula (4.2) directly, yielding

$$\|C\|_{Tr}^2 \leq \|A - \kappa_A\|_{Tr}\|B - \kappa_B\|_{Tr} \tag{4.10}$$

Since $A - \kappa_A$ as well as $B - \kappa_B$ are Hermitian positive semidefinite matrices (due to concavity property of CMs) their trace norm will coincide with their trace. Hence $\|A - \kappa_A\|_{Tr} = \mathrm{Tr}\,(A) - \mathrm{Tr}\,(\kappa_A) = 1 - \mathrm{Tr}\left(\rho_A^2\right)$, where we have used Corollary 2.9 and the fact that $\sum_i A_{i,i} = \sum_i (\langle A_i^2\rangle - \langle A_i\rangle^2) = \langle d_A \mathbb{1}\rangle - \mathrm{Tr}\left(\rho_A^2\right)$, since $\mathrm{Tr}\,(A_i A_j) = \delta_{i,j}$ and $\rho_A^2 = \sum_{i,j}\langle A_i\rangle\langle A_j\rangle A_i A_j$. ■

Interestingly, this criterion has been proven already in a different context:

Remark 4.3 (CMC and the criterion of Ref. [135])**.** *The separability criterion in Proposition 4.2 is nothing but the separability criterion proposed in Theorem 1 of Ref. [135], hence the criterion of Ref. [135] is a corollary of the CMC.*

Let us now connect the CMC to another type of entanglement criteria: There are several separability criteria in the literature which are based on the Bloch representation of density matrices. This representation in our case is just some particular choice of observables, namely one has to detach the identity from all others generators, which then have to be traceless. The fact that one of the observables is the identity, can simplify the CMC sometimes.

By definition the entries of the matrix C are given by

$$C_{i,j} = \langle A_i \otimes B_j\rangle - \langle A_i\rangle\langle B_j\rangle, \tag{4.11}$$

which consists of a linear (in the sense of mean values) and quadratic part. We define $\mathfrak{C}$ as the linear part of C, i.e., $\mathfrak{C}_{i,j} = \langle A_i \otimes B_j\rangle$. Let us further consider $\mathfrak{C}^{\mathrm{red}}$ as the submatrix of $\mathfrak{C}$, where the entries $\langle \mathbb{1}_A \otimes B_j\rangle$ and $\langle A_i \otimes \mathbb{1}_B\rangle$ are omitted, i.e., the first row and the first column are removed. Similarly, we can define matrices like $\mathfrak{A}$ and $\mathfrak{B}$ from A and B. In the same spirit, we can define a submatrix of κ as κ^{red}. Note that $\mathrm{Tr}\,(\kappa) = \mathrm{Tr}\left(\kappa^{\mathrm{red}}\right)$, as the missing diagonal entry is the variance of $\mathbb{1}$, which is vanishing.

We are now able to establish a connection between the CMC and criteria based on the Bloch representation of density matrices:

Proposition 4.4 (Relationship between CMC and criteria based on Bloch representations)**.** *Let*

$$\gamma = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix} \tag{4.12}$$

be a CM. Then if ρ is separable, we have

$$\|\mathfrak{C}^{red}\|_{Tr}^2 \leq \big(1 - \frac{1}{d_A}\big)\big(1 - \frac{1}{d_B}\big). \tag{4.13}$$

If this inequality is violated, then ρ must be entangled.

Proof: First, we can define two vectors $|\psi\rangle^{A/B}$ with entries

$$|\psi^A\rangle_i = \langle A_i\rangle \quad |\psi^B\rangle_i = \langle B_i\rangle \tag{4.14}$$

resulting in $C = \mathfrak{C} - |\psi^A\rangle\langle\psi^B|$. Similar relations hold for A and B, so we can write the condition in CMC (3.1) in the form

$$\underbrace{\begin{pmatrix} \mathfrak{A} - \kappa_A & \mathfrak{C} \\ \mathfrak{C}^T & \mathfrak{B} - \kappa_B \end{pmatrix}}_{X} - \begin{pmatrix} |\psi^A\rangle \\ |\psi^B\rangle \end{pmatrix} \begin{pmatrix} \langle\psi^A| \\ \langle\psi^B| \end{pmatrix}^T \geq 0. \tag{4.15}$$

Positivity of the left hand side implies positivity of the first term X alone, since we subtract only one projector which is itself positive. Concerning positivity of X we can take $\mathfrak{A}^{\rm red}$, $\mathfrak{B}^{\rm red}$, $\mathfrak{C}^{\rm red}$, and $\kappa^{\rm red}$ instead, since positivity of a matrix implies positivity of all its main minors. Using Eq. (4.2), we get

$$\|\mathfrak{C}^{\rm red}\|_{Tr} \leq \|\mathfrak{A}^{\rm red} - \kappa_A^{\rm red}\|_{Tr}\|\mathfrak{B}^{\rm red} - \kappa_B^{\rm red}\|_{Tr}. \tag{4.16}$$

Using that $\mathrm{Tr}\left(\hat{\mathfrak{A}}^{\rm red}\right) = \sum_{i\geq 2}\langle A_i^2\rangle = \langle d_A \mathbb{1}_A\rangle - \langle \mathbb{1}_A/d_A\rangle$ and $\mathrm{Tr}\left(\kappa_A^{\rm red}\right) = d_A - 1$ proves the claim. ■

Interestingly, this separability criterion has also been proven before:

Remark 4.5 (CMC and the criterion of Ref. [136])**.** *The separability criterion in Proposition 4.4 is nothing but the separability criterion for Bloch representations proposed in Ref. [136], hence the criterion of Ref. [136] is a corollary of the CMC.*

Note that in Ref. [136] the observables have been normalized in a different way, leading to a slightly different formula.

Remark 4.6 (Connection between Propositions 4.4 and 4.2)**.** *Proposition 4.2 is strictly stronger than Proposition 4.4.*

This fact was proven in version 5 of [135].

Let us finish this subsection with a remark on the possible use of other Ky-Fan norms in the above argument. In fact, we do know more about the singular values (here eigenvalues) of κ_A and κ_B than their sum:

Lemma 4.7 (Ky-Fan norms of matrices in the CMC)**.** *The matrices κ_A (and similarly κ_B) in Proposition 3.1 satisfy*

$$\sum_{j=1}^{k} \lambda_j(\kappa_A) \leq \min(k, d_A - 1), \tag{4.17}$$

for the non-increasingly ordered eigenvalues of κ_A (and κ_B).

Proof: One can argue as in Proposition 2.11, using the fact that a convex combination of matrices leads to more mixed matrices in the sense of majorization [21]. ■

This property can immediately be applied to evaluate the CMC, making use of Proposition 4.1 and Weyl's inequalities[1] For example, if we consider $d_A = d_B = d$ and the k-Ky-Fan norm $\|.\|_{KF^{(k)}}$ for $k = (d^2 - d + 1 + s)$, we can apply the first of Weyl's inequalities with $i = 1$, and $s = 1, \ldots, d-1$, to conclude that

$$\begin{aligned} \|A - \kappa_A\|_{KF^{(k)}} &= \sum_{j=1}^{k} \lambda_j(A - \kappa_A) \leq \sum_{j=1}^{k} \lambda_1(A) + \sum_{j=1}^{k} \lambda_j(-\kappa_A) \\ &= (d^2 - d + 1 + s)\|A\| - \sum_{j=d^2-k+1}^{d^2} \lambda_j(\kappa_A), \end{aligned} \tag{4.20}$$

where $\|A\|$ denotes the spectral norm of A. Using that κ_A will be more mixed in the sense of majorization than $diag(1, \ldots, 1, 0, \ldots, 0)$ of rank $d-1$ and Proposition 2.9, one arrives at

$$\|A - \kappa_A\|_{KF^{(k)}} \leq (d^2 - d + 1 + s)\|A\| - s, \tag{4.21}$$

and a corresponding statement for κ_B. Using Proposition 4.1, one hence arrives at the observation that any separable state ρ on a bipartite Hilbert space satisfies

$$\big((d^2 - d + 1 + s)\|A\| - s\big)\big((d^2 - d + 1 + s)\|B\| - s\big) - \|C\|^2_{KF^{(k)}} \geq 0. \tag{4.22}$$

It is an interesting open question whether more sophisticated uses of the knowledge of spectral properties of κ_A and κ_B can be employed the further sharpen the evaluation of the CMC.

4.2 Evaluation of the CMC via traces of submatrices

Let us first prove a simple condition on the traces of A, B and C, which follows from the CMC. In the following, we always assume that $d_A \leq d_B$. Sometimes we assume that the dimensions are the same, meaning that $d = d_A = d_B$.

[1] Let A, B be Hermitian $n \times n$-matrices. Then, the non-increasingly ordered eigenvalues satisfy

$$\lambda_j(A + B) \leq \lambda_i(A) + \lambda_{j-i+1}(B), i \leq j, \tag{4.18}$$

$$\lambda_j(A + B) \geq \lambda_i(A) + \lambda_{j-i+n}(B), i \geq j. \tag{4.19}$$

Proposition 4.8 (CMC evaluated from traces)**.** *Let*

$$\gamma = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix} \tag{4.23}$$

be the symmetric CM of a state ρ and let $J = \{j_1, \ldots, j_{d_A^2}\} \subset \{1, \ldots, d_B^2\}$ be a subset of d_A^2 pairwise different indices. Then if ρ is separable, we have

$$2 \cdot \sum_{i=1}^{d_A^2} \sum_{j \in J} |C_{i,j}| \leq \sum_{i=1}^{d_A^2} A_{i,i} + \sum_{i=1}^{d_B^2} B_{i,i} - d_A - d_B + 2 = 2 - Tr\left(\rho_A^2\right) - Tr\left(\rho_B^2\right), \tag{4.24}$$

If this inequality is violated, then ρ must be entangled.

Proof: First, note that a necessary condition for a 2×2 matrix

$$X = \begin{pmatrix} a & c \\ c & b \end{pmatrix} \tag{4.25}$$

to be positive semidefinite is that $2|c| \leq a + b$. If ρ is separable, then by the CMC we have $Y = \gamma - \kappa_a \oplus \kappa_B \geq 0$. This implies that all 2×2 minor submatrices of Y have to be positive semidefinite as well. Hence for all i, j we have

$$2|C_{i,j}| \leq A_{i,i} + B_{j,j} - (\kappa_A)_{i,i} - (\kappa_B)_{j,j}. \tag{4.26}$$

Summing over i, j and using Corollary 2.9 proves the claim. ■

We will use this Proposition mainly for the case that $d_A = d_B$ and where we sum over the diagonal entries of C. In this case, it just gives the condition that for separable states:

$$2\mathrm{Tr}\,(C) \leq 2 - \mathrm{Tr}\left(\rho_A^2\right) - \mathrm{Tr}\left(\rho_B^2\right). \tag{4.27}$$

This is a quadratic polynomial in the entries of the state, and may be viewed as a suitable entanglement witness on two specimens on a state. In the light of this fact, the criterion evaluated in this fashion is surprisingly strong. The trace inequality above can be further improved. One can introduce a matrix η_C, such that $\mathbb{1} - \eta_C^T \eta_C \geq 0$, under the trace of the left hand side of Eq. (4.27). Indeed from

$$\begin{pmatrix} A & C \\ C^T & B \end{pmatrix} - \begin{pmatrix} \kappa_A & 0 \\ 0 & \kappa_B \end{pmatrix} \geq 0 \tag{4.28}$$

follows

$$\mathrm{Tr}\left(\begin{pmatrix} A - \kappa_A & C \\ C^T & B - \kappa_B \end{pmatrix} \begin{pmatrix} \mathbb{1} & \eta_C \\ \eta_C^T & \mathbb{1} \end{pmatrix}\right) \geq 0, \text{ for all } \begin{pmatrix} \mathbb{1} & \eta_C \\ \eta_C^T & \mathbb{1} \end{pmatrix} \geq 0. \tag{4.29}$$

It is also worth mentioning here that one can improve Proposition 4.8 by taking 4×4 minor submatrices for evaluation. Then, however, also off diagonal terms of $\kappa_{A/B}$ will occur, for which not many properties are known. This makes the resulting conditions difficult to evaluate.

Physically, Proposition 4.8 says that if the correlations $C_{i,j}$ are sufficiently large, then ρ must be entangled. The question arises, how to find the observables, for which the $C_{i,j}$ are large. There are several ways of doing this. A first result is the following:

Proposition 4.9 (Criterion in Proposition 4.8 and diagonal block matrices)**.** *The criterion in Proposition 4.8 detects most states if the observables are chosen in such a way that C is diagonal. For any state there exist a choice of observables that this can be achieved. However, even with this optimal choice of observables Proposition 4.8 delivers a strictly weaker separability criterion than Proposition 4.2.*

Proof: It is clear that the criterion is optimal, if the trace of C is maximal, which is the case if it is brought into the singular value diagonal form [135, 137]. This can always be achieved [see Eq. (2.43)]. The fact that Proposition 4.2 is stronger, was in a different language proven in Ref. [134].

Interestingly, the fact that Proposition 4.8 is weaker than Proposition 4.2 can also be seen from Eq. (4.6) from the alternative proof of Lemma 4.1. If C is chosen to be diagonal, then Proposition 4.8 reduces to this equation with $\alpha = \beta$. Clearly, allowing α and β to be different, improves the criterion. ■

In the following, however, we will consider two different strategies: Firstly, we use the Schmidt decomposition in operator space of the density matrix [132]. This will lead to a natural choice of the observables $\{A_k\}$ and $\{B_k\}$, and will further connect the CMC to the CCNR criterion.

Secondly, we will consider appropriate local filterings of the state [140, 139, 44, 138]. These are active transformations of the state, which, however, do not change the entanglement properties. As we mentioned in the beginning of the chapter, under this transformations, the state can be transformed into its standard form. In this standard form, the CMC becomes very strong and even necessary and sufficient for two qubits.

4.3 Schmidt decomposition and the CMC

We will first remind ourselves of what is called the Schmidt decomposition in operator space. It is the same construction as the ordinary Schmidt decomposition in the vector space now equipped with the Hilbert-Schmidt scalar product. A general density matrix of a composite system can be written as

$$\rho = \sum_{k=1}^{d_A^2} \sum_{l=1}^{d_B^2} \xi_{k,l} \tilde{G}_k^A \otimes \tilde{G}_l^B, \tag{4.30}$$

with real $\xi_{k,l}$ and the $\{\tilde{G}_l^A\}$ (respectively, $\{\tilde{G}_l^B\}$) form an orthonormal Hermitian basis of observables. The Schmidt decomposition can now be achieved by diagonalizing the above expression using the singular value decomposition of the matrix ξ,

$$\rho = \sum_{k=1}^{d_A^2} \lambda_k G_k^A \otimes G_k^B, \tag{4.31}$$

where we made the assumption that $d_A \leq d_B$. Clearly, the Schmidt coefficients λ_k are real and non-negative. Using the new basis observables $\{G_k^A\}$ and $\{G_k^B\}$ as observables for the construction of the symmetric block CM, we have a normal form of the CMC, which we will call the Schmidt CMC.

Proposition 4.10 (Schmidt CMC)**.** *If ρ is separable, then*

$$2\sum_i |\lambda_i - \lambda_i^2 g_i^A g_i^B| \leq 2 - \sum_i \lambda_i^2 \left[(g_i^A)^2 + (g_i^B)^2\right], \tag{4.32}$$

where we defined $g_i^A = Tr\left(G_i^A\right)$ and $g_i^B = Tr\left(G_i^B\right)$. If this condition is violated, the state must be entangled.

Proof: Using the orthonormality of the $\{G_i^{A/B}\}$, it is not difficult to see that with the observables from the Schmidt decomposition $C_{i,j} = \lambda_i \delta_{i,j} - \lambda_i \lambda_j g_j^A g_i^B$ holds. In addition, we have $\mathrm{Tr}\left(\rho_A^2\right) = \sum_i \lambda_i^2 (g_i^B)^2$. Together with Proposition 4.8 this proves the claim. ■

Interestingly, this Proposition includes the CCNR criterion as a corollary. This shows that the CMC, even without filtering, and evaluated merely via the trace of the blocks, once the matrix is brought to Schmidt form, is stronger than the CCNR, which it implies as a corollary.

Corollary 4.11 (CMC and CCNR)**.** *If a state ρ is separable, then in the Schmidt decomposition*

$$\sum_k \lambda_k \leq 1 \tag{4.33}$$

has to hold. This condition is just the CCNR criterion, hence the CCNR criterion is a corollary of the CMC.

Proof: Using the relations $|a - b| \geq |a| - |b|$ and $a^2 + b^2 \geq 2|ab|$ we have $2\sum_i |\lambda_i - \lambda_i^2 g_i^A g_i^B| \geq 2\sum_i \lambda_i - 2\sum_i \lambda_i^2 |g_i^A g_i^B|$ and $2 - \sum_i \lambda_i^2 [(g_i^A)^2 + (g_i^B)^2] \leq 2(1 - \sum_i \lambda_i^2 |g_i^A g_i^B|)$, which, due to the Proposition 4.10, proves the claim. ■

4.4 Filtering and the CMC

Let us now consider local filtering operations or SLOCC (stochastic local operations assisted by classical communication) [138] of the form

$$\rho \mapsto \tilde{\rho} = (F_A \otimes F_B)\rho(F_A \otimes F_B)^\dagger, \tag{4.34}$$

where and $F_A \in \mathrm{SL}(d_A, \mathbb{C})$ and $F_B \in \mathrm{SL}(d_B, \mathbb{C})$ are invertible matrices on the respective Hilbert spaces. Clearly, such operations cannot map a separable state

into an entangled one (although they might increase entanglement measures). Also, since F_A and F_B are invertible, they will also not destroy any entanglement that may be present in the state. In other words, ρ is entangled if and only if $\tilde{\rho}$ is entangled.

As has been shown in Refs. [138, 140] we can bring any state of full rank (i.e., $\rho > 0$) by such filtering operations in its standard form which is given by

$$\tilde{\rho} = \frac{1}{d_A d_B}\Big(\mathbb{1} + \sum_{k=1}^{d_A^2-1} \xi_k \hat{G}_k^A \otimes \hat{G}_k^B\Big), \tag{4.35}$$

where the $\{\hat{G}_k^A\}$, $\{\hat{G}_k^B\}$ are traceless orthogonal observables. Here, we again assumed that $d_A \leq d_B$.

The idea now is to first apply a filtering operation and bring the state into its normal form. Then, the new separability criteria are applied afterward. Note that the reduction to the normal form is always possible. The merits of this approach are twofold: Firstly, the normal form reduces the number of relevant parameters, while still encoding all information about entanglement and separability. Secondly, the normal form is in a certain sense "more entangled" than the original state, as it was shown in Ref. [44]:

Remark 4.12 (Extremality of states in normal form)**.** *The local filtering operations bringing a mixed state into its normal form are those operations which maximize all entanglement monotones that remain invariant under determinant 1 SLOCC operations.*

Therefore, it may be expected that many separability criteria become stronger if we first bring the state into its normal form. Note, however, that this does not hold for the PPT criterion, as local filtering leaves this criterion invariant.

Following Ref. [140], let us explain briefly an algorithm for transforming a state of a form as in Eq. (4.30) to its normal form in Eq. (4.35). As a starting point, one considers the compact space $D_A \otimes D_B$ of all normalized product density matrices $\rho_A \otimes \rho_B$. For any given density matrix ρ one can define a function f of ρ_A and ρ_B via

$$f_\rho(\rho_A, \rho_B) = \frac{\mathrm{Tr}\left(\rho(\rho_A \otimes \rho_B)\right)}{(\det \rho_A)^{1/d_A} (\det \rho_B)^{1/d_B}}. \tag{4.36}$$

$f_\rho(\rho_A, \rho_B)$ is a family of positive well defined functions on the interior of $D_A \otimes D_B$, where the reduced density matrices both have full rank. Since ρ has also full rank, we have $\mathrm{Tr}\left(\rho(\rho_A \otimes \rho_B)\right) > 0$ and because of compactness of $D_A \otimes D_B$ one has even stronger $\mathrm{Tr}\left(\rho(\rho_A \otimes \rho_B)\right) \geq c_\rho > 0$. Divergence of $f_\rho(\rho_A, \rho_B)$ on the boundary implies that it has a positive minimum on the interior of $D_A \otimes D_B$.

Minimization of the function f_ρ will, as proven in Ref. [140], yield the filtering operations needed. Suppose the minimum value for f_ρ attained for some product density matrix $\tau_A \otimes \tau_B$ with $\det \tau_A > 0$, $\det \tau_B > 0$. Each of them can be decomposed as (see Eq. (66) in Ref. [140])

$$\tau_A = T_A^\dagger T_A, \quad \tau_B = T_B^\dagger T_B, \quad T_{A/B} \in \mathrm{SL}(d_{A/B}, \mathbb{C}), \tag{4.37}$$

where the T_A and T_B are desired local filtering operations. Normalization factors have been ignored.

Using this filtering operations one obtains the new state $\tilde{\rho}$ which has a form

$$\tilde{\rho} = \frac{1}{d_A d_B}\Big(\mathbb{1} + \sum_{i=1}^{d_A^2-1}\sum_{k=1}^{d_B^2-1} \xi_{ik}\hat{G}_i^A \otimes \hat{G}_k^B\Big). \tag{4.38}$$

The final step involves a standard singular value decomposition of ξ_{ik}, which leads to Eq. (4.35). A priori, it is not clear whether the normal form is in some sense unique or not. However, it is easy to see that if we start from a given state and convert it into two different states in a normal form, then these two normal forms have to be connected by a local filtering operation. Using the fact that the reduced states of a state in the normal form are maximally mixed, one can further conclude that two different normal forms can only differ by a local unitary transformation.

In practice, the minimization of $f_\rho(\rho_A, \rho_B)$ in Eq. (4.36) can be performed by an iteration as follows: let us fix ρ_B and consider only the minimization over ρ_A. This minimization can further be split into a minimization over the spectrum of ρ_A and a local unitary transformation. If the spectrum is fixed, the optimal unitary is constructed such that ρ_A and $X = \mathrm{Tr}\left(\rho(\mathbb{1}\otimes\rho_B)\right)_B$ are diagonal in the same basis where the maximal eigenvalue of X has the same eigenvector as the minimal eigenvalue of ρ_A and the second largest eigenvalue of X has the same eigenvector as the second smallest eigenvalue of ρ_A etc. If the basis is fixed, and λ_k (μ_k) are the eigenvalues of ρ_A (X) then a simple calculation using Lagrange multipliers shows that the optimal λ_k fulfill

$$\lambda_k \sim \Big[(\sum_{i\neq k}\mu_i\lambda_i)/(\prod_{i\neq k}\lambda_i)\Big]^{1/2}, \tag{4.39}$$

which can be used for an iterative determination of the optimal λ_k. In this way, the optimization can be iterated, converging to a minimum. Note while it is known that every state can be brought into this normal form, the above procedure of Ref. [140] is not known to be strictly efficient in the physical dimension d. Yet, for "reasonable physical dimensions", the method in practice converges quickly. Moreover, and importantly, at the end of the procedure, one can easily (and efficiently) check via direct inspection whether the obtained filters map the state onto the normal form or not. Global optimality can hence be easily certified.

As one can directly calculate, for a state in the normal form the CM takes a really simple form, namely

$$\gamma = \frac{1}{d_A d_B}\begin{pmatrix} \mathrm{diag}(0, d_B, d_B, \dots) & \mathrm{diag}(0, \xi_1, \xi_2, \dots) \\ \mathrm{diag}(0, \xi_1, \xi_2, \dots) & \mathrm{diag}(0, d_A, d_A, \dots)\end{pmatrix}. \tag{4.40}$$

Using this form we obtain the following strong separability criterion, which we call the filter CMC.

Proposition 4.13 (Filter CMC)**.** *If $d = d_A = d_B$ and ρ is separable, then the coefficients in the filter normal form fulfill*

$$\sum_i \xi_i \leq d^2 - d. \tag{4.41}$$

Proof: The claim obviously follows from Proposition 4.8 and the form of the CM for the normal form of the state. ■

Interestingly, for two qubits we have:

Remark 4.14 (Filter CMC for two qubits)**.** *For two qubits, the filter CMC in Proposition 4.13 is a necessary and sufficient criterion for separability.*

Proof: If a two-qubit state is of full rank, the normal form reads

$$\tilde{\rho} = \frac{1}{4}\Big(\mathbb{1} + \sum_{k=1}^{3} \xi_k \sigma_k^A \otimes \sigma_k^B\Big), \tag{4.42}$$

where $\{\sigma_k^{A/B}\}$ are the Pauli matrices [140]. Such states are diagonal in the Bell basis, and it is known that for these states $\sum_{k=1}^{3} \xi_k \leq 2$ is necessary and sufficient for separability [141, 140]. Note also that the filter normal form can be explicitly stated for two-qubit systems.

If an entangled (or separable) state is not of full rank, it can, as explicitly shown in Ref. [139], be brought by filtering operations arbitrarily close to a Bell diagonal state with finite (or vanishing) concurrence. Such a state will also be detected by the CMC (or not). ■

Direct comparison of this result with the discussion in Section II and Fig. 2.1 (and later the result of Proposition 4.17) might be confusing at this point, since we know already that the CMC itself cannot be necessary and sufficient for two qubits. This can be resolved in the following way: We have already learned that filtering brings the state in the form which in a certain sense contains the maximum amount of entanglement (it maximizes all monotones). This indeed shows that the filter CMC is sometimes a real improvement of the "bare" CMC, and filtering is more than just an appropriate choice of the observables.

Let us now consider the asymmetric case, when $d_A < d_B$. We can formulate for this case following statement:

Proposition 4.15 (Separability criterion for uneven local dimension)**.** *If ρ is separable, then the following inequalities hold*

$$\sum_i \xi_i \leq \frac{d_A d_B}{2}\Big[1 - \frac{1}{d_A} + (d_A^2 - 1)\frac{1}{d_B} + \min(0, -(d_B - 1) + (d_B^2 - d_A^2)\frac{1}{d_B})\Big] \tag{4.43}$$

and

$$\sum_i \xi_i \leq \left[d_A d_B (d_A - 1)(d_B - 1)\right]^{1/2}. \tag{4.44}$$

holds. If one of these inequalities is violated, the state must be entangled.

Proof: Eq. (4.44) is nothing but an application of Proposition 4.4 (or 4.2), it has already been derived in Ref. [136]. Concerning Eq. (4.43), we will again apply Proposition 4.8, but with two modifications. First, when carrying out the sum over $2|C_{i,j}| \leq A_{i,i} + B_{j,j} - \kappa_{A,i,i} - \kappa_{B,j,j}$ [see Eq. (4.26) in Proposition 4.8] we do not sum over all $B_{i,i}$. But then, we cannot subtract all of the $\kappa_{B,i,i}$ anymore, since $d_B^2 - d_A^2$ diagonal elements of κ_B do not occur in the sum.

As a first approach, we can drop completely the summation over all $\kappa_{B,j,j}$, since they are positive anyway. This gives

$$\frac{2}{d_A d_B} \sum_{i=1}^{d_A^2} \xi_i \leq 1 - \frac{1}{d_A} + \frac{d_A^2 - 1}{d_B}, \tag{4.45}$$

justifying one part of Eq. (4.43).

In a second approach, we estimate $\sum_{i=1}^{d_A^2} \kappa_{B,i,i}$. As one can see by direct inspection, the non-vanishing elements of γ in Eq. (4.40) origin only from the linear part of CM (in the spirit of Proposition 4.4 this linear part is denoted by $\mathfrak{g}$). But as we have seen in the proof of Proposition 2.12 that this linear part $\mathfrak{g}$ is just the same as the linear part of the direct sum of $\kappa_A \oplus \kappa_B$ (denoted by $\mathfrak{k}_A \oplus \mathfrak{k}_B$) for separable states, i.e. $\mathfrak{g} = \mathfrak{k}_A \oplus \mathfrak{k}_B$, hence $B = \mathfrak{B} = \mathfrak{k}_B$. This implies that for the diagonal elements of κ_B the relation $\kappa_{B,i,i} \leq \mathfrak{B}_{i,i} = B_{i,i} = 1/d_B$ holds, leading to

$$\sum_{i=1}^{d_A^2} \kappa_{B,i,i} = d_B - 1 - \sum_{i=d_A^2+1}^{d_B^2} \kappa_{B,i,i} \geq d_B - 1 - \left(d_B^2 - d_A^2\right) \frac{1}{d_B}. \tag{4.46}$$

This proves the second part of Eq. (4.43). ■

4.5 Connection to local uncertainty relations

In this section we will further analyze the connection of CMC with the separability criterion based on local uncertainty relations (LURs) [71]. To start with, we again state the LUR criterion as a reminder:

Proposition 4.16 (Criterion based on local uncertainty relations)**.** *Let be $\hat{A}_k$ and $\hat{B}_k$ observables in system A and B, respectively, for which some of the variances on single systems is bounded by constants U_A, U_B such that*

$$\sum_k \delta^2(\hat{A}_k) \geq U_A \text{ and } \sum_k \delta^2(\hat{B}_k) \geq U_B. \tag{4.47}$$

Then, we have for separable states

$$\sum_k \delta^2(\hat{A}_k \otimes \mathbb{1} + \mathbb{1} \otimes \hat{B}_k) \geq U_A + U_B \tag{4.48}$$

and violation implies the presence of entanglement.

Physically, the LURs state that separable states inherit the uncertainty relations from their reduced states, which is not the case for entangled states. Due to this observation the LURs have attracted a considerable interest, and a number of interesting properties have been discovered: LURs can detect bound entangled states [72] and can be used to estimate the concurrence [142]. They can be extended to other formulations of the uncertainty principle [143, 144] and they can be generalized to non-local observables [37]. Finally, they can be viewed as nonlinear entanglement witnesses, which improve the CCNR criterion [132].

For the connection to the CMC we have the following:

Proposition 4.17 (Connection to local uncertainty relations)**.** *A state ρ violates the CMC for symmetric CMs iff it can be detected by a LUR.*

Proof: The proof is an adaption of a similar proof given in Ref. [37]. We will often use the property that CMs can be used to compute variances. Imagine $N = \sum_k \nu_k M_k$ is a linear combination of the M_k with $\nu_k \in \mathbb{R}$, then

$$\delta^2(N) = \sum_{k,l} \nu_k \nu_l (\langle M_k M_l \rangle - \langle M_k \rangle \langle M_l \rangle) = \langle \nu | \gamma(\{M\}) | \nu \rangle. \tag{4.49}$$

Let us now assume that ρ violates the LURs and we can find $\hat{A}_k$, $\hat{B}_k$, U_A and U_B such that Ineq. 4.48 in Proposition 4.16 is violated. We assume that the CMC is fulfilled, i.e., there exist κ_A and κ_B such that for the CM γ we have $\gamma \geq \kappa_A \oplus \kappa_B$. We can write

$$\hat{A}_k = \sum_l \alpha_l^{(k)} A_l \text{ and } \hat{B}_k = \sum_l \beta_l^{(k)} B_l, \tag{4.50}$$

where the $\{A_k\}$ and $\{B_k\}$ are the observables chosen in the definition of γ. This leads to $\delta^2(\hat{A}_k \otimes \mathbb{1} + \mathbb{1} \otimes \hat{B}_k) = \langle \alpha^{(k)} \oplus \beta^{(k)} | \gamma | \alpha^{(k)} \oplus \beta^{(k)} \rangle$. Also, by definition

$$\kappa_A \oplus \kappa_B = \sum_l p_l \gamma(|a_l\rangle\langle a_l|) \oplus \gamma(|b_l\rangle\langle b_l|) \tag{4.51}$$

and hence $\langle \alpha^{(k)} \oplus \beta^{(k)} | \kappa_A \oplus \kappa_B | \alpha^{(k)} \oplus \beta^{(k)} \rangle = \sum_l p_l [\delta^2(\hat{A}_k)_{|a_l\rangle\langle a_l|} + \delta^2(\hat{B}_k)_{|b_l\rangle\langle b_l|}]$. But then summing over k yields

$$\begin{aligned} \sum_k \delta^2(\hat{A}_k \otimes \mathbb{1} + \mathbb{1} \otimes \hat{B}_k) &\geq \sum_{k,l} p_l \left[\delta^2(\hat{A}_k)_{|a_l\rangle\langle a_l|} + \delta^2(\hat{B}_k)_{|b_l\rangle\langle b_l|}\right] \\ &\geq \min_{|a\rangle\langle a|} \sum_k \left[\delta^2(\hat{A}_k)_{|a\rangle\langle a|}\right] + \min_{|b\rangle\langle b|} \sum_k \left[\delta^2(\hat{B}_k)_{|b\rangle\langle b|}\right] \\ &\geq U_A + U_B, \end{aligned} \tag{4.52}$$

which is a contradiction to our assumption that ρ violates the LURs.

To show the converse direction, let us assume that ρ violates the CMC. Let us define a set of matrices as $X = \{x | x = \kappa_A \oplus \kappa_B + P \text{ with } P \geq 0\}$, which geometrically is a closed convex cone. Using this definition, we can formulate the CMC differently,

by saying that if ρ is separable, then $\gamma \in X$. As our ρ violates the CMC, we have $\gamma \notin X$.

According to a corollary to the Hahn-Banach theorem [145] for each $\gamma \notin X$ there exist a symmetric matrix W and a number C such that $\mathrm{Tr}\,(W\gamma) < C$ while

$$\mathrm{Tr}\,(Wx) > C \,\forall x \in X. \tag{4.53}$$

Since X is a non-compact cone, and we can add arbitrary positive operators to the elements of X, we can conclude that $\mathrm{Tr}\,(WP) \geq 0$ has to hold for all $P \geq 0$, and consequently we have $W \geq 0$. Now let us make use of spectral decomposition of W and write $W = \sum_k \lambda_k |\psi_k\rangle\langle\psi_k| =: \sum_k \lambda_k |\alpha^{(k)} \oplus \beta^{(k)}\rangle\langle\alpha^{(k)} \oplus \beta^{(k)}|$. Defining $\hat{A}_k = \sqrt{\lambda_k} \sum_l \alpha_l^{(k)} A_l$ and $\hat{B}_k = \sqrt{\lambda_k} \sum_l \beta_l^{(k)} B_l$ we have for ρ that

$$\mathrm{Tr}\,(W\gamma) = \sum_k \delta^2(\hat{A}_k \otimes \mathbb{1} + \mathbb{1} \otimes \hat{B}_k). \tag{4.54}$$

Furthermore, by definition we have for all $\kappa_A \oplus \kappa_B \in X$ and from Proposition 2.12 it follows that all $\gamma_A \oplus \gamma_B \in X$. Hence for each product state $\rho = \rho_A \otimes \rho_B$ we have $C < \mathrm{Tr}\,(W\gamma_A \oplus \gamma_B) = \sum_k [\delta^2(\hat{A}_k)_{\rho_A} + \delta^2(\hat{B}_k)_{\rho_B}]$. This implies that

$$\begin{aligned} C &< \min_{\rho_A,\rho_B} \big[\sum_k (\delta^2(\hat{A}_k)_{\rho_A} + \delta^2(\hat{B}_k)_{\rho_B}) \big] \\ &< \min_{\rho_A} \big[\sum_k \delta^2(\hat{A}_k)_{\rho_A} \big] + \min_{\rho_B} \big[\sum_k \delta^2(\hat{B}_k)_{\rho_B} \big] \\ &=: U_A + U_B. \end{aligned} \tag{4.55}$$

Finally, since the CMC is violated, $\gamma \notin X$ and $\sum_k \delta^2(\hat{A}_k \otimes \mathbb{1} + \mathbb{1} \otimes \hat{B}_k) = \mathrm{Tr}\,(W\gamma) < C < U_A + U_B$ leading to a violation of the LURs criterion.

Note that in principle this proof also applies to the CMC for non-symmetric CMs. Then, however, the "observables" in the LURs will be non-Hermitian, their variance has to be defined as $\delta^2(X) = \langle XX^\dagger\rangle - \langle X\rangle\langle X^\dagger\rangle$ and their physical interpretation is not so clear.
■

This result show that the LURs for appropriate observables and the CMC are equivalent, however, the CMC has the major advantage that it can be directly evaluated, while for the LURs the appropriate observables have to be identified. Moreover, we can state:

Corollary 4.18 (Insufficiency of LUR to detect all entangled states)**.** *There exist entangled two qubit states which can not be detected by a LUR, hence LURs are not a necessary and sufficient criterion for separability.*

Proof: In the Section 2.3 we have already constructed a family of states ρ_ε which cannot be detected by the CMC, as their symmetric block CM is compatible with a separable as well as an entangled state. This proves the claim. ■

4.6 The CMC for two qubits

After the previous discussion of the situation of Hilbert spaces of arbitrary finite dimension, we now turn to the important simple case of a 2×2-system – two qubits – in some more detail. We take as observables the set $\{A_k\} = \{B_k\} = \{\mathbb{1}/\sqrt{2}, \sigma^x/\sqrt{2}, \sigma^y/\sqrt{2}, \sigma^z/\sqrt{2}\}$ as in Eq. (2.2).

Since these observables contain the identity, one can easily check that many terms in the symmetric block CM vanish. Effectively, γ is actually a 6×6 matrix (denoted by γ^{eff}) originating only from the $\{A_k\}$ and $\{B_k\}$ with $k = 1, 2, 3$ which are not proportional to the identity, and not by an 8×8 as one could guess from the general theory.

To characterize the κ_A in the CMC, note that for a pure state $|a\rangle$ on system A we find, according to Proposition 2.8, the following properties of the 4×4 matrix $\gamma(|a\rangle\langle a|)$:

(i) $Rank(\gamma) = 2$.

(ii) The nonzero eigenvalues of γ are equal to $1/2$ in a suitable basis.

We also know that in the chosen basis, the first row as well as the first column of $\gamma(|a\rangle\langle a|)$ vanish, and we have

$$\gamma(|a\rangle\langle a|) = \mathbb{0}_1 \oplus \gamma(|a\rangle\langle a|)^{\text{eff}}, \tag{4.56}$$

where γ^{eff} is the effective 3×3 CM as above. This has to be of rank two with eigenvalues $1/2$. This implies that $\gamma(|a\rangle\langle a|)^{\text{eff}}$ can be written as

$$\tilde{\gamma}(|a\rangle\langle a|)^{\text{eff}} = \frac{1}{2}(\mathbb{1}_3 - |\phi_a\rangle\langle\phi_a|), \tag{4.57}$$

where $\mathbb{1}_3$ denotes a 3×3 identity matrix, and $|\phi_a\rangle \in \mathbb{R}^3$. In fact, any matrix of this form is a valid CM:

Lemma 4.19. *For any vector $|\phi\rangle \in \mathbb{R}^3$ a matrix of the form $(\mathbb{1}_3 - |\phi_a\rangle\langle\phi_a|)/2$, is a valid CM of some two qubit state. Consequently, the set of valid κ_A is given by all matrices of the form*

$$\kappa_A = \frac{1}{2}(\mathbb{1}_3 - \rho_A), \tag{4.58}$$

where ρ_A is a real 3×3 matrix with trace one and positive eigenvalues.

Proof: We have already shown that the CMs are of the required form, and only have to argue that any matrix of the form $X = (\mathbb{1}_3 - |\phi_x\rangle\langle\phi_x|)/2$ is a valid CM. To see this, note that unitary transformations of the $|a\rangle$ result in orthogonal transformation on $\gamma(|a\rangle\langle a|)^{\text{eff}}$. Moreover, for the special case of a single qubit any orthogonal transformation on γ^{eff} can be generated by a unitary transformation on state space [141], expressing the isomorphism between the Lie-algebras $su(2)$ and $so(3)$. Therefore, we can transform X into $\gamma(|a\rangle\langle a|)^{\text{eff}}$ and construct the corresponding state vector

$|x\rangle$. To finish the argument, note that the set of all κ_A is by definition the set of all convex combinations of pure state CMs. ■

The characterization of κ for one qubit provided by the last Lemma is exhaustive in the following sense:

Lemma 4.20 (Characterization of κs in the case of qubits)**.** *There exist positive matrices X_A and X_B such that $Tr(X_{A/B}) = 1$ and $\gamma \geq X_A \oplus X_B$ if and only if there exist valid $\kappa_{A/B}$ that fulfill the CMC.*

Proof: The sufficiency is given by the last Lemma. Suppose we have found such matrices X. We know, that κs for qubits must have special form, namely $\kappa = \frac{1}{2}(\mathbb{1}_3 - \rho)$. Since X satisfy the condition $\gamma \geq X_A \oplus X_B$ and γ have eigenvalues, which are less or equal than $\frac{1}{2}$ any X can be written in the form $X = \frac{1}{2}(\mathbb{1}_3 - x)$, where $Tr(x) = 1$ and $x \geq 0$ and is exactly of the form (4.58). ■

After having proven this Lemma we can formulate the two-qubit version of the CMC:

Proposition 4.21 (CMC for two qubits)**.** *Let ρ be a state of two qubits and let*

$$\{A_k\} = \{B_k\} = \{\mathbb{1}/\sqrt{2}, \sigma^x/\sqrt{2}, \sigma^y/\sqrt{2}, \sigma^z/\sqrt{2}\} \tag{4.59}$$

be the chosen set of observables. Let γ^{eff} be the 6×6 CM as mentioned before. Then the state ρ fulfills the CMC iff there exist 3×3 density matrices ρ_A and ρ_B such that

$$\gamma^{\mathit{eff}} - \frac{1}{2}\mathbb{1}_6 + \frac{1}{2}(\rho_A \oplus \rho_B) \geq 0. \tag{4.60}$$

Proof: The claim follows if we insert the κ's from Eq. (4.58) into Proposition 3.1. Note that it suffices to find complex ρ_A and ρ_B. If we can identify such matrices, their real part will saturate Eq. (4.60) as well. ■

In this form, the problem is a special instance of an efficiently solvable semidefinite program (SDP) [35, 36] in *primal* form, a *feasibility* problem .

In general, a SDP consists of a linear function $c^T x$ which is minimized subject to a semidefinite constraint

$$F(x) = F_0 + \sum_i x_i F_i \geq 0, \tag{4.61}$$

which is linear in the problem variables x_i. Hence the problem is defined by the real vector c and by the Hermitian or symmetric matrices F_i. If $c = 0$, then the problem is referred to as a *feasibility* problem. Via Lagrange-duality, a *dual* problem can be formulated in which the expression $-\mathrm{Tr}\,(F_0 Z)$ is maximized over a positive semidefinite (Hermitian or symmetric) matrix Z, with the constraints that $\mathrm{Tr}\,(F_i Z) = c_i$. Since

$$c^T x + \mathrm{Tr}\,(F_0 Z) = \mathrm{Tr}\,(F(x) Z) \geq 0 \tag{4.62}$$

holds true due to the positive semidefiniteness of $F(x)$ and Z, solutions of the dual problem deliver a bound on the solutions of the primal problem and vice versa, which is referred to as *weak duality*. Finally, if there is a solution to the primal problem with $F(x) > 0$ or a solution to the dual problem with $Z > 0$, then *strong* duality holds, meaning that a pair (x^*, Z^*) exists such that $c^T x^* + \mathrm{Tr}\,(F_0 Z^*) = 0$ holds. See also Ref. [146] for an extensive treatment of the subject.

For the evaluation of the CMC, we can formulate the problem differently, such that if the primal problem detects the state as entangled, then from the solution of the dual problem local operators can be extracted which allow for the detection of the state with LURs. This is similar in spirit as the solution in the continuous variable case [34].

Explicitly, we formulate the primal problem as

$$\begin{aligned} \min \quad & -\lambda \\ \text{subject to} \quad & \gamma^{\text{eff}} - \kappa_A \oplus \kappa_B \geq 0 \\ & \kappa_{A,B} = \frac{1}{2}\big[(1+\lambda)\mathbb{1}_3 - \rho_{A,B}\big] \geq 0 \\ & \mathrm{Tr}\,(\rho_{A,B}) = 1 + \lambda. \end{aligned} \tag{4.63}$$

In this formulation, the matrices $\kappa_{A,B}$ are positive and have trace $1 + \lambda$. If the constraints can be fulfilled for $\lambda < 0$ only, then the state corresponding to γ^{eff} is entangled. The SDP can be formulated with block-diagonal matrices $\{F_i\}$ collecting all the constraints. For instance, by inserting the definition of $\kappa_{A,B}$ into the first constraint and expressing the equality constraints by a '$\geq$' and a '$\leq$' constraint, we can write F_0 as

$$F_0 = (\gamma^{\text{eff}} - \frac{1}{2}\mathbb{1}_6) \oplus \frac{1}{2}\mathbb{1}_3 \oplus \frac{1}{2}\mathbb{1}_3 \oplus (-1) \oplus 1 \oplus (-1) \oplus 1, \tag{4.64}$$

and the matrices F_i accordingly by choosing a basis for real, symmetric matrices for the blocks. Without loss of generality, the matrix Z can be chosen block-diagonal accordingly. In the order from above we have $Z = Z_1 \oplus Z_2^A \oplus Z_2^B \oplus Z_3^{A1} \oplus Z_3^{A2} \oplus Z_3^{B1} \oplus Z_3^{B2}$, where Z_1 is a 6×6 matrix, $Z_2^{A,B}$ are of dimension 3×3, and $Z_3^{A,B;1,2}$ are scalar. The dual problem can then be formulated as

$$\begin{aligned} \max \quad & -[\mathrm{Tr}\left(\gamma^{\text{eff}} Z_1\right) - 1] \\ \text{subject to} \quad & -\frac{1}{2}[\mathrm{Tr}\,(Z_1) - \mathrm{Tr}\left(Z_2^A\right) - \mathrm{Tr}\left(Z_2^B\right)] = Z_3^{A1} - Z_3^{A2} + Z_3^{B1} - Z_3^{B2} - 1 \\ & (Z_1^{A,B})_{i,i} - (Z_2^{A,B})_{i,i} = -2(Z_3^{A,B;1} - Z_3^{A,B;2}) \\ & (Z_1^{A,B})_{i<j} = (Z_2^{A,B})_{i<j}, \end{aligned} \tag{4.65}$$

where $Z_1^{A,B}$ are the single-particle sub-blocks of system A and B, respectively, and i and j run from 1 to 3. It turns out that Z_1 has the properties of an entanglement witness in the space of covariance matrices (CM-witness) as in the continuous-variables case [34]:

Proposition 4.22 (CM-Witness from dual program)**.** *For every feasible solution Z to the dual problem formulated above, the matrix Z_1 is a CM-witness in the sense that it fulfills $Tr\left(\gamma_S^{eff} Z_1\right) \geq 1$ for all CMs γ_S^{eff} from separable states. Hence if $Tr\left(\gamma^{eff} Z_1\right) < 1$ then the corresponding state is entangled. Further, it is optimal in the sense that $Tr\left(\gamma^{eff} Z_1\right)$ is the minimal value of $Tr\left(\gamma^{eff} X\right)$ for any $X \geq 0$ of the same dimensions.*

Proof: It follows from weak duality that $\mathrm{Tr}\left(\gamma^{\mathrm{eff}} Z_1\right) \geq 1+\lambda$, hence $\mathrm{Tr}\left(\gamma_S^{\mathrm{eff}} Z_1\right) \geq 1$ holds for all γ_S^{eff} from separable states. In this case, strong duality holds, which we prove by providing an example:

$$Z = \frac{3}{2}\mathbb{1}_6 \oplus \mathbb{1}_3 \oplus \mathbb{1}_3 \oplus \frac{3}{4} \oplus 1 \oplus \frac{3}{4} \oplus 1 > 0 \tag{4.66}$$

fulfills all constraints. Hence there exist (λ^*, Z^*) such that $\mathrm{Tr}\left(\gamma^{\mathrm{eff}} Z_1^*\right) = 1 + \lambda^*$ holds, and the dual program reaches the minimal value of $\mathrm{Tr}\left(\gamma^{\mathrm{eff}} Z_1\right)$. ■

If the entanglement of a state is detected by a CW-witness Z_1, then it is possible to write down a LUR detecting the state as well. This is remarkable because it is in general very difficult to find a LUR detecting the entanglement of a given state.

Proposition 4.23 (LUR observables from witness)**.** *Given a CM-witness Z_1, it is possible to define LUR matrices $\{\hat{A}_k\}$ and $\{\hat{B}_k\}$ from Z_1 such that*

$$Tr\left(\gamma^{eff} Z_1\right) = \sum_k \delta^2(\hat{A}_k \otimes \mathbb{1} + \mathbb{1} \otimes \hat{B}_k) \tag{4.67}$$

holds.

Proof: The LUR corresponding to Z_1 can be extracted as shown in the proof of Proposition 4.17: we can spectrally decompose $Z_1 = \sum_k \lambda_k |\psi_k\rangle\langle\psi_k| =: \sum_k \lambda_k |\alpha^{(k)} \oplus \beta^{(k)}\rangle\langle\alpha^{(k)} \oplus \beta^{(k)}|$. Defining the local LUR variables $\hat{A}_k = \sqrt{\lambda_k} \sum_l \alpha_l^{(k)} A_l$ and $\hat{B}_k = \sqrt{\lambda_k} \sum_l \beta_l^{(k)} B_l$ we have for ρ that $\mathrm{Tr}\left(Z_1 \gamma^{\mathrm{eff}}\right) = \sum_k \delta^2(\hat{A}_k \otimes \mathbb{1} + \mathbb{1} \otimes \hat{B}_k)$, where $\{A_k\}$ and $\{B_k\}$ are defined in Eq. (4.59). ■

4.7 Detecting bipartite bound entangled states with the CMC

In this section, we consider different bound entangled states, and investigate the strength of the different criteria discussed in this chapter.

In the first example, we take the 3×3 bound entangled states, called chessboard states, introduced by D. Bruß and A. Peres [147]. They are defined as

$$\rho = \mathcal{N} \sum_{j=1}^{4} |V_j\rangle\langle V_j|, \tag{4.68}$$

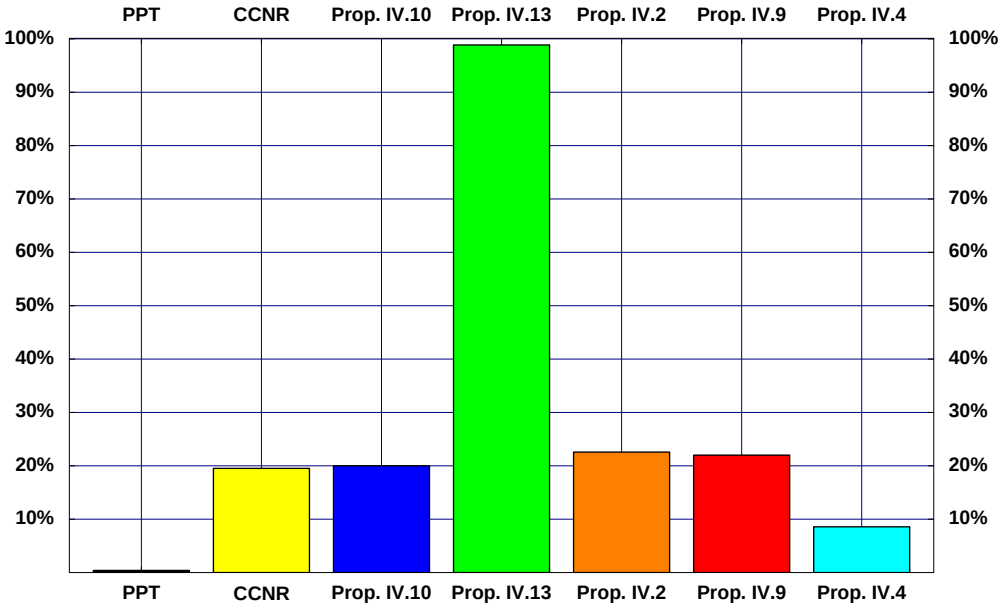


Figure 4.1. *Detection of* 3×3 *chessboard states. For the different criteria the fraction of states which are detected is shown. See text for further details.*

where $\mathcal{N}$ denotes the normalization, and we used the unnormalized vectors

$$\begin{aligned}
|V_1\rangle &= |m,0,ac/n;0,n,0;0,0,0\rangle,\\
|V_2\rangle &= |0,a,0;b,0,c;0,0,0\rangle,\\
|V_3\rangle &= |n,0,0;0,-m,0;ad/m,0,0\rangle,\\
|V_4\rangle &= |0,b,0;-a,0,0;0,d,0\rangle.
\end{aligned} \tag{4.69}$$

Characterization of the family is done by six real parameters. We tested all criteria, presented in this chapter on randomly generated chessboard states, where parameters have been drawn from the normal distribution with zero mean value and standard deviation of two. The results of this test are presented on the Fig. 4.1.

As one can see from Fig. 4.1 the most of the states are detected by bringing first the state in its normal form (Proposition 4.13) - 98.86% of all states. The criterion, which uses an estimation of singular values of the off diagonal block of CM (Proposition 4.2), which was also proposed earlier in [134] detects 22.57%, whereas another criterion proposed in this chapter (Proposition 4.9) detects 22.00%. Moreover the criterion, which uses Schmidt decomposition (Proposition 4.10) detects 20.00% which is more or less the same amount as is detected by CCNR criterion - 19.52%. Finally the criterion presented in Proposition 4.4, which was first proposed by de Vicente [136] detects only 8.57% of randomly generated chessboard states.

As the second example, we consider 3×3 bound entangled states arising from

an unextendible product basis [49], mixed with white noise:

$$
\begin{aligned}
|\psi_0\rangle &= \frac{1}{\sqrt{2}}|0\rangle(|0\rangle - |1\rangle), \quad |\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|2\rangle, \\
|\psi_2\rangle &= \frac{1}{\sqrt{2}}|2\rangle(|1\rangle - |2\rangle), \quad |\psi_3\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle)|0\rangle, \\
|\psi_4\rangle &= \frac{1}{3}(|0\rangle + |1\rangle + |2\rangle)(|0\rangle + |1\rangle + |2\rangle), \\
\rho_{\mathrm{BE}} &= \frac{1}{4}\Big(\mathbb{1} - \sum_{i=0}^{4} |\psi_i\rangle\langle\psi_i|\Big), \\
\rho_{\mathrm{UP}}(p) &= p\rho_{\mathrm{BE}} + (1-p)\frac{\mathbb{1}}{9}.
\end{aligned} \tag{4.70}
$$

These states are detected by Proposition 4.13 for $p \geq 0.8723$ while the best known positive map detects them only for $p \geq 0.8744$ (see [132] and references therein). Besides this we have also tested all other criteria presented in this chapter. Criteria of Propositions 4.2, 4.9 both detect these states for $p \geq 0.8822$. The criterion derived for Schmidt decomposed states (Proposition 4.10) detects the states for $p \geq 0.8834$, whereas the CCNR criterion detects them for $p \geq 0.8897$. Finally Proposition 4.4 detects the states for $p \geq 0.9493$.

In the last example [149] we compare the performance of three particular criteria, namely the CMC evaluated from traces 4.8, the Schmidt CMC 4.10 and the filter CMC 4.13, on two one parametric families of the bound entangled states. These states were introduced in [60] - $\rho_{3\times3}(a)$ and $\rho_{2\times4}(b)$ and are defined for the 3×3 and 2×4 systems respectively:

$$
\rho_{3\times3}(a) = \frac{1}{8a+1}\begin{pmatrix}
a & 0 & 0 & 0 & a & 0 & 0 & 0 & a \\
0 & a & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & a & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & a & 0 & 0 & 0 & 0 & 0 \\
a & 0 & 0 & 0 & a & 0 & 0 & 0 & a \\
0 & 0 & 0 & 0 & 0 & a & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & a & 0 & \frac{1+a}{2} & 0 & \frac{\sqrt{1-a^2}}{2} \\
0 & 0 & 0 & 0 & a & 0 & 0 & a & 0 \\
a & 0 & 0 & 0 & a & 0 & \frac{\sqrt{1-a^2}}{2} & 0 & \frac{1+a}{2}
\end{pmatrix}, \tag{4.71}
$$

$$
\rho_{2\times4}(b) = \frac{1}{7b+1}\begin{pmatrix}
b & 0 & 0 & 0 & 0 & b & 0 & 0 \\
0 & b & 0 & 0 & 0 & 0 & b & 0 \\
0 & 0 & b & 0 & 0 & 0 & 0 & b \\
0 & 0 & 0 & b & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \frac{1+b}{2} & 0 & 0 & \frac{\sqrt{1-b^2}}{2} \\
b & 0 & 0 & 0 & 0 & b & 0 & 0 \\
0 & b & 0 & 0 & 0 & 0 & b & 0 \\
0 & 0 & b & 0 & \frac{\sqrt{1-b^2}}{2} & 0 & 0 & \frac{1+b}{2}
\end{pmatrix}. \tag{4.72}
$$

Testing different criteria on this states shows (FIG. 4.2) that the criteria are indeed not equivalent. For example the $\rho_{3\times3}$ is not detected by *Filter CMC* for some

values of the parameter a, whereas other two criteria detect it for all a. Therefore we conclude that applying filtering operations is not always the best strategy to detect bipartite entanglement.

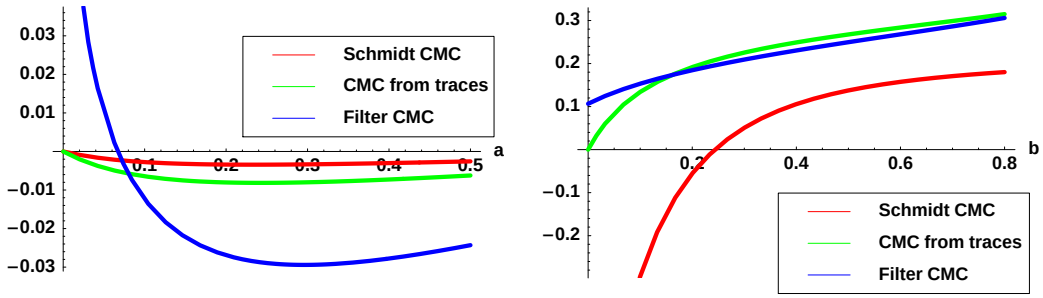


Figure 4.2. Left picture*: Detection of the $\rho_{3\times3}$ depending on the parameter a. For every a the state is detected by the Schmidt CMC and by the CMC evaluated from traces of submatrices of the block covariance matrix. However there is a specific region of parameter a where the filter CMC fails to detect the state.* Right picture*: Detection of the $\rho_{2\times4}$ depending on the parameter b. The state is detected only for certain parameter values and only by the Proposition 4.*

Finally, let us shortly comment on the efficiency of the implementation of all these criteria. The filtering operation can be implemented quite fast, using the simple algorithm outlined above takes a few seconds on a desktop computer (5×5 system: ca. 6 sec., 10×10 system: ca. 24 sec., 15×15 system: ca. 72 sec.). Then, the trace norm of C can be quickly computed as the trace norm of the realignment of the matrix $\rho - \rho_A \otimes \rho_B$ [135]. For comparison, only the first step of the semidefinite program of Ref. [148] requires already ca. 10 min. for a 4×4 system, becoming practically unfeasible for higher dimensions.

4.8 Conclusion

In this chapter, we investigated the covariance matrix criterion (CMC) presented in the previous chapter. We have shown that this is a strong separability criterion, which can be simply evaluated. Combined with filtering it is necessary and sufficient for two qubits and in higher dimensions it detects states where the PPT criterion fails. Moreover, it contains many other separability criteria, which have been proposed to complement the PPT criterion as corollaries.

An interesting question is how to develop a theory similar to ours for entanglement of multipartite systems. Here, however, a significant amount of work has yet to be done, as it is not even obvious how to identify the object corresponding to the block CM for multipartite systems. Some of the results in this direction have been, however, already achieved and we present them in the next chapter

Moreover would be interesting to relate the CMC to quantitative statements, which will be the topic of discussion in chapter 6.

Chapter 5

CMC: generalization to more than two parties

In this chapter we address the question of possible generalizations of the covariance matrix criterion to the multipartite setting. In particular we give a generalization of the CMC formulated in chapter 3 to the case of three parties. After formulating the general criterion we will evaluate it using positive semidefiniteness of the 3×3 block matrix. We test the resulting criterion on the three qubit pure states in the normal form and discuss possible issues of the straightforward generalization of the bipartite CMC and the use of the local observables.

In the second section of this chapter we consider two families of three qubit states that are separable with respect to any bipartition, although not fully separable. Both families are thermal states of particular Hamiltonians. We compare the amount of states detected by the tripartite CMC with the amount detected by the spin squeezing inequalities. For the second family the CMC detects more states than the spin squeezing inequalities.

5.1 General criterion and its evaluation

To start with we observe that having a tripartite state we can describe it in terms of block CM if we choose a set of local observables to construct the CM

$$\gamma = \begin{pmatrix} A & D & E \\ D^\dagger & B & F \\ E^\dagger & F^\dagger & C \end{pmatrix}. \tag{5.1}$$

One can easily see that for any fully product state γ takes a block-diagonal form. Hence, using the concavity property of covariance matrices we can formulate separability criterion in the following way:

Theorem 5.1 (Tripartite CM)**.** *Let ρ be a fully separable tripartite state. Then there exist states matrices κ_A, κ_B and κ_C of the form $\kappa_{A/B/C} =$*

$\sum_i p_i \gamma(|a_i/b_i/c_i\rangle\langle a_i/b_i/c_i|)$ *such that*

$$\gamma - \begin{pmatrix} \kappa_A & 0 & 0 \\ 0 & \kappa_B & 0 \\ 0 & 0 & \kappa_C \end{pmatrix} \geq 0, \tag{5.2}$$

if such matrices κ *do not exist, the state is entangled.*

Before we present some results we mention that there are several strategies to evaluate the criterion in Theorem 5.2. Firstly, one can again resort to semidefinite programming and formulate the problem of searching over all possible κ as a feasibility problem [35, 36]. Secondly, one can deduce computable criteria from the positivity semidefiniteness of the matrix in Eq. (5.2). We start with the second strategy and investigate some properties of 3×3 positive matrices. These properties can be formulated as

Lemma 5.2. *Let* η *be a* 3×3 *real positive matrix*

$$\eta = \begin{pmatrix} a & d & e \\ d & b & f \\ e & f & c \end{pmatrix} \geq 0, \tag{5.3}$$

then

$$\begin{pmatrix} a & |d| & |e| \\ |d| & b & |f| \\ |e| & |f| & c \end{pmatrix} \geq 0 \tag{5.4}$$

is also a positive matrix.

Proof: We shall split the proof into three parts. (i) if all off-diagonal elements of η are positive, the claim follows immediately. (ii) if only two off-diagonal elements of η d and f are negative then, the positivity of the matrix η implies that $v^T \eta v \geq 0$ for all real 3-vectors v. Therefore

$$\begin{pmatrix} -u \\ v \\ -w \end{pmatrix}^T \begin{pmatrix} a & d & e \\ d & b & f \\ e & f & c \end{pmatrix} \begin{pmatrix} -u \\ v \\ -w \end{pmatrix} = \tag{5.5}$$

$$\begin{pmatrix} u \\ v \\ w \end{pmatrix}^T \begin{pmatrix} a & -d & e \\ -d & b & -f \\ e & -f & c \end{pmatrix} \begin{pmatrix} u \\ v \\ w \end{pmatrix} \tag{5.6}$$

holds and therefore

$$\begin{pmatrix} a & -d & e \\ -d & b & -f \\ e & -f & c \end{pmatrix} \geq 0 \Leftrightarrow \begin{pmatrix} a & d & e \\ d & b & f \\ e & f & c \end{pmatrix} \geq 0. \tag{5.7}$$

(iii) finally, if only $e < 0$, we have to prove that positivity of $\eta(e)$ guarantees positivity of $\eta(|e|)$. To this end let us show an equivalence of positive semidefiniteness

of any 3×3 matrix A and positive semidefiniteness of any of its 2×2 submatrix and its determinant.

Necessary condition is trivial. Sufficiency is proved by considering the characteristic polynomial of a 3×3 matrix A, which is given by

$$\chi_A(\lambda) = -\lambda^3 + Tr(A)\lambda^2 - \sum_{i=1}^{3} \det(A_{ii})\lambda + \det A. \tag{5.8}$$

Positivity of all 2×2 submatrices guarantees then that none of the eigenvalues is complex. Now if $\det A$ is negative, then the characteristic polynomial certainly has at least one negative eigenvalue and the matrix A is not positive semidefinite anymore. Therefore the characteristic polynomial (5.8) has only positive roots.

Now consider

$$\begin{aligned} \det \eta &= abc + 2e|f||d| - be^2 - a|d|^2 - c|f|^2 \\ &= abc - 2|e||f||d| - be^2 - a|d|^2 - c|f|^2 \geq 0. \end{aligned} \tag{5.9}$$

Observe that if we take $|e|$ instead of $-|e|$ then the expression on the left hand side of the inequality becomes only larger, since $|e||f||d| > 0$. Hence $\det \tilde{\eta} > \det \eta \geq 0$ and $\eta(e) > 0$ implies $\eta(|e|) > 0$.

Combining the steps (i), (ii) and (iii) we prove the claim of the Lemma. ■

Using the last Lemma we arrive at

Proposition 5.3. *If the state ρ is separable, then*

$$\begin{pmatrix} \|A\|_{Tr} - \|\kappa_A\|_{Tr} & \sum_i |d_{ii}| & \sum_i |e_{ii}| \\ \sum_i |d_{ii}| & \|B\|_{Tr} - \|\kappa_B\|_{Tr} & \sum_i |f_{ii}| \\ \sum_i |e_{ii}| & \sum_i |f_{ii}| & \|C\|_{Tr} - \|\kappa_C\|_{Tr} \end{pmatrix} \geq 0. \tag{5.10}$$

In order to test the performance of the derived entanglement criteria we investigate three qubit pure states. According to [42] any three qubit state can be written in *generalized Schmidt form*.

$$\begin{aligned} |\psi\rangle &= \frac{\lambda_0|000\rangle + \lambda_1 e^{i\phi}|100\rangle + \lambda_2|101\rangle + \lambda_3|110\rangle + \lambda_4|111\rangle}{N}, \\ &\lambda_i \geq 0,\ 0 \leq \phi \leq \pi,\ \sum_i \lambda_i^2 = N. \end{aligned} \tag{5.11}$$

Varying real parameters λ_i and ϕ one achieves eight different families of entangled states. Proposition 5.3 detects most of the entangled three qubit states. Surprisingly, the exceptional case, where Proposition 5.3 fails to detect entanglement is the case of GHZ states. However, even a small coherent perturbation of the GHZ state solves the problem, e.g. the state

$$|\psi'_{GHZ}\rangle = \frac{1}{N}\left(|000\rangle + 10^{-5}|110\rangle + |111\rangle\right) \tag{5.12}$$

is detected.

In order to test whether this is an artifact of the general CMC as stated in Theorem 5.1 we use the first strategy of evaluating the general criterion and formulate the positivity test (5.2) as a special instance of an efficiently solvable semidefinite program (SDP) namely as a feasibility problem. Note that in the case of qubits one can give an exact characterization of $\kappa_{A/B/C}$ in terms of vectors in $\mathbb{R}^3$ (see Lemma 4.58 in chapter 4.6). The SDP for the three-qubit case reads

$$\begin{aligned} &\max t > 0 \\ &\text{subject to } \gamma - t\kappa_A \oplus \kappa_B \oplus \kappa_C \geq 0 \\ &\kappa_{A,B,C} = \frac{1}{2}\left(\mathbb{1}_3 - \rho_{A,B,C}\right) \\ &\rho_{A,B,C} \geq 0,\ Tr(\rho_{A,B,C}) = 1 \end{aligned} \tag{5.13}$$

If the above semidefinite program has a solution only for $t < 1$ then the state is detected by the CMC and must be entangled.

The semidefinite program also fails to detect GHZ states and their mixtures, which can be explained by the fact that any reduced density matrix of such a state is separable. Indeed considering only two qubit reduced density matrices it is impossible to distinguish $|GHZ\rangle\langle GHZ|$ from fully separable state $(|000\rangle\langle 000| + |111\rangle\langle 111|)/2$. This fact has deeper consequences and is reflected in various criteria that detect multipartite entanglement with bi-local observables. For instance in spin squeezing inequalities [50, 51] or in the criterion based on structure factor [151] are based on the following property of entangled states. For mean values of a particular bi-local observable one can always write down a separable state, which gives exactly the same mean value of this particular observable. However the sum of the mean values or their entity cannot be reproduced by a single separable state. For example one can draw analogy with cluster states, for three qubit linear cluster state each of the mean values $\langle ZX\mathbb{1}\rangle = 1$, $\langle \mathbb{1}XZ\rangle = 1$ and $\langle XZX\rangle = 1$ can be fulfilled by different three qubit product states, but it is impossible to fulfill all three equations with any product state.

In other words, in order to detect GHZ states $(|000\rangle + |111\rangle)/\sqrt{2}$ one has to measure three party correlations and since such type of correlations is not considered neither in the CMC or spin squeezing inequalities or in structure factor analysis, none of these approaches is able to detect GHZ states.

5.2 Example: Detection of bound entanglement

Thermal entanglement was discussed recently in several papers. In Ref. [150] it has been shown that there are entangled mixed states of three spins (Fig. 5.1) that are separable with respect to any bipartition. These states were detected by spin squeezing inequalities [50, 51, 150]. In particular the authors of the cited works considered an inequality

$$\delta^2\left(J_x\right) + \delta^2\left(J_y\right) + \delta^2\left(J_z\right) \geq \frac{N}{2}, \tag{5.14}$$

where N is the number of spins and $J_\alpha = \frac{1}{2}\sum_{i=1}^{N}\sigma_\alpha^i$. First family of thermal states we are going to discuss are the states of the following Hamiltonian:

$$H = \vec{S}_1 \cdot \vec{S}_2 + \vec{S}_2 \cdot \vec{S}_3 + \vec{S}_1 \cdot \vec{S}_3 + h\left(\sigma_z^1 + \sigma_z^2 + \sigma_z^3\right). \tag{5.15}$$

This a Hamiltonian describes three spin-$\frac{1}{2}$ particles interacting via Heisenberg in-

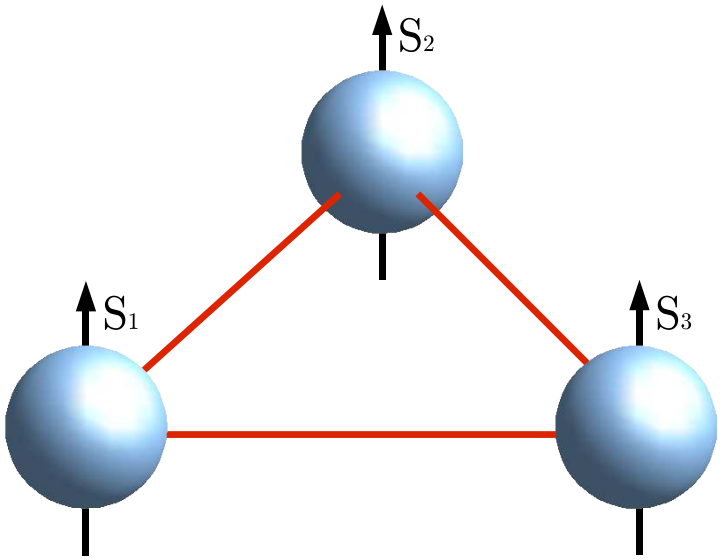


Figure 5.1. *Configuration of three spins interacting via Heisenberg interaction in external magnetic field.*

teraction and subjected to an external magnetic field of the strength h. The thermal states are defined as

$$\rho_T(h) = \frac{\mathrm{e}^{-H/kT}}{\mathrm{Tr}\left(\mathrm{e}^{-H/kT}\right)} \tag{5.16}$$

and represent a two-parametric family of density matrices. Using the spin-squeezing inequalities one was able to find regions on the T-h diagram where all thermal states were PPT with respect to any bipartition although not fully separable.

We applied general criterion (5.2) to the thermal states of the Hamiltonian (5.15) and evaluated it using semidefinite program. For these states, however, the tripartite CMC detects exactly the same amount of states as the spin squeezing inequalities. The results are presented in Fig. 5.2, where the left picture corresponds to the violation of the tripartite CMC and the right picture to the violation of spin squeezing inequality (5.14).

Different colors correspond to different strength of the criteria. In the case of the CMC it corresponds to the value of the parameter t in the semidefinite program (5.13). In the region where magnetic field $h \sim 4 - 6$ and $kT \sim 0.2 - 0.6$ the violation of both criteria becomes of the order of the numerical error, which results in 'discontinuity' of the region of the detected states in Fig. 5.2.

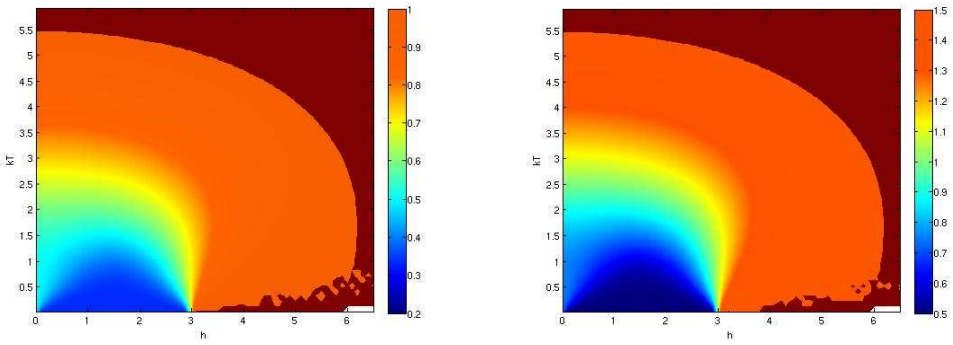


Figure 5.2. *Detection of bound entanglement in thermal states of three spins interacting via Heisenberg interaction in external magnetic field by the tripartite CMC (left side) and by spin squeezing inequalities (right side). Dark red region corresponds to states that are not detected by either of criteria. Variation of the color corresponds to the strength of violation of the criteria. The 'discontinuity' of the region of the states that are detected by either CMC or spin squeezing inequalities is explained by the fact that the violation of either criteria becomes of the order of the numerical error for* $h \sim 4-6$ *and* $kT \sim 0.2-0.6$.

Interestingly, we were able to find another family of the states that is PPT with respect to any bipartition, but which is detected by the CMC and by spin squeezing inequalities. However, in this case, CMC evaluated again by the semidefinite program (5.13) detects more states than spin squeezing inequality does.

These states are also thermal states but of a slightly modified Hamiltonian:

$$H' = \vec{S}_1 \cdot \vec{S}_2 + \vec{S}_2 \cdot \vec{S}_3 + \vec{S}_1 \cdot \vec{S}_3 + h\left(\sigma_z^1 + \sigma_x^2 + \sigma_z^3\right). \tag{5.17}$$

Note that the difference to the Hamiltonian (5.15) is the direction of the magnetic field applied to the second spin. In Fig. 5.2 we present the detection of the thermal states of the Hamiltonian (5.17). The top left picture corresponds to the PPT criterion. Here we characterize states by taking the maximum of three values of negativity corresponding to three different bipartitions. The dark red region corresponds to the states that are PPT with respect to all three bipartitions. The top right picture corresponds to the detection of these states by the spin squeezing inequalities. As in the previous case spin squeezing inequalities are able to detect bound entanglement. The bottom picture shows the detection by the tripartite CMC. As one can easily see, the CMC, in this case, detects more states than either PPT criterion or spin squeezing inequalities.

Provided above examples we can conclude that the tripartite CMC is useful in particular in detection of not fully separable states.

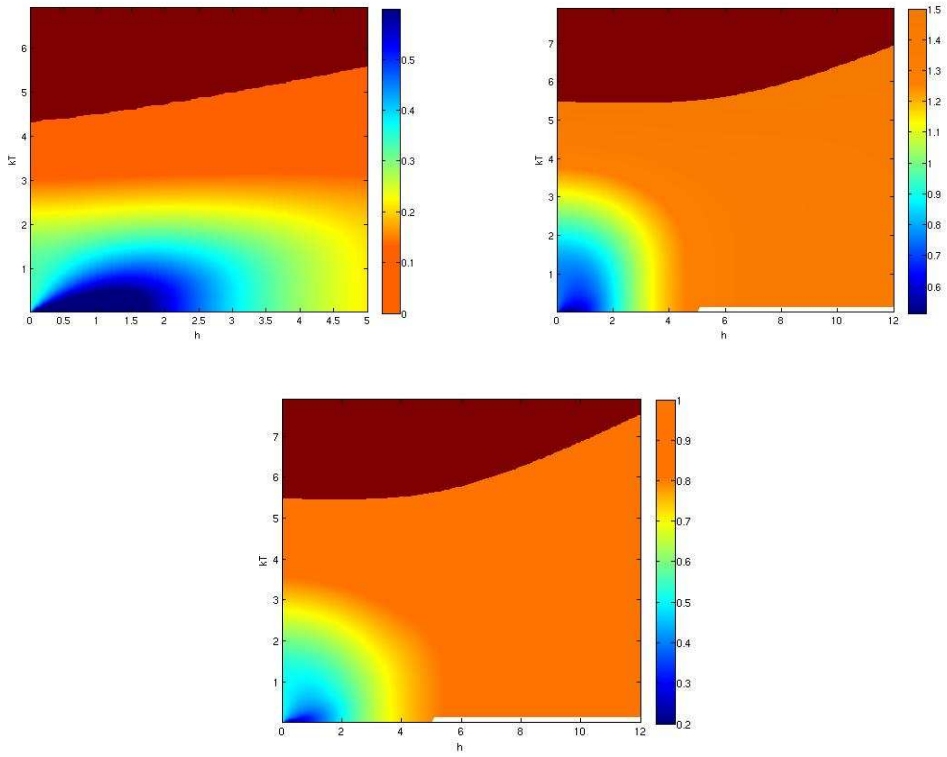


Figure 5.3. *Detection of the thermal states of the Hamiltonian (5.17) for different values of temperature and external magnetic field. Top left: violation of the PPT criterion characterized by negativity. The dark red region corresponds to the PPT-states. The states corresponding to all other colors are definitely NPT states. Top right: detection of the states by spin squeezing inequalities. Dark red region corresponds to the states that are not detected by the spin squeezing inequality. Bottom: detection by the tripartite CMC. For the magnetic field larger than $h = 4$ the criterion detects more PPT states than spin squeezing inequality does.*

5.3 Conclusion

Formulating entanglement criteria for multipartite systems is with no doubt a difficult task. In this chapter a partial answer on the problem of detecting multipartite entangled states was provided. The covariance matrix criterion for three parties, formulated in the beginning of the chapter can be used in addition to the bipartite criterion in order to reveal entanglement structure of a given state. For instance states in the provided example will be never detected by the bipartite CMC. The GHZ states that are not detected by a tripartite criterion are detected by the bipartite criterion.

Chapter 6

Quantification of entanglement with covariance matrices

In chapters 3, 4 and 5 we showed that covariance matrices can be effectively used for entanglement detection. Sometimes, however, one is interested not only in detecting entanglement but also in quantifying it. As we will show in this chapter entanglement quantification can be, at least to some extent, also done in terms of covariance matrices. The idea of quantification of entanglement is reminiscent of the idea we used in chapter 5, as we discussed entanglement detection by a semidefinite program (5.13). There we used parameter t as a strength of violation of the CMC. It turns out that the strength of violation of the criterion can be indeed used for entanglement quantification. In forthcoming sections we define an entanglement parameter, prove its convexity and show how to calculate it for pure and for Schmidt correlated states. Then we turn to general mixed states of $d \times d$ systems and show that the introduced entanglement parameter provides a lower bound on the concurrence for $d \leq 4$ (Eq. (1.74)).

6.1 Definition of the entanglement parameter

In this section we introduce a function based on the bipartite CMC that can be used to estimate the amount of entanglement in a given quantum state. For our purpose we chose a complete set of orthogonal observables A_i on $\mathcal{H}_A$ with $i = 1, ..., d_A^2$ and $\mathrm{Tr}\,(A_i A_j) = \delta_{ij}$ and a similar set B_j for $\mathcal{H}_B$. We will refer to them as local orthogonal observables, an example for $d_A = 2$ are the (appropriately normalized) Pauli matrices and the identity. Note that these observables are reminiscent of the observables of standard basis (2.13) we used in chapter 2. Then, we can consider observables on $\mathcal{H}_A \otimes \mathcal{H}_B$ defined by

$$\begin{aligned} \{M_\alpha\} &= \{A_i \otimes \mathbb{1}, \mathbb{1} \otimes B_j\},\ i = 1, \ldots, d_A^2, \\ &\quad j = d_A^2 + 1, \ldots, d_A^2 + d_B^2, \end{aligned} \tag{6.1}$$

which then also obey $\mathrm{Tr}\,(M_\alpha M_\beta) = \delta_{\alpha\beta}$ and define block form of covariance matrix as in (2.7)

$$\gamma = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix}.$$

As we will use some of propositions from chapter 4 later, we remind some of them here. For block covariance matrices of separable states following inequalities hold (see Propositions 4.8 and 4.2):

$$2\mathrm{Tr}\left(|C|\right) = \left[1 - \mathrm{Tr}\left(\rho_A^2\right)\right] + \left[1 - \mathrm{Tr}\left(\rho_B^2\right)\right], \tag{6.2}$$

$$\|C\|_{tr}^2 \leq \left[1 - \mathrm{Tr}\left(\rho_A^2\right)\right]\left[1 - \mathrm{Tr}\left(\rho_B^2\right)\right], \tag{6.3}$$

If one of this inequality is violated, then ρ must be entangled.

In order to define now our entanglement parameter, let us reformulate the CMC in a slightly different way. Imagine some state ρ is detected as entangled by the CMC. On the one hand there exist no κ_A and κ_B as in Proposition 3.1 such that $\gamma(\rho) - \kappa_A \oplus \kappa_B \geq 0$. On the other hand we can find κ_A^e and κ_B^e and some number $t_e \in [0,1]$ such that $\gamma(\rho) - t_e\kappa_A^e \oplus \kappa_B^e$ is again positive semidefinite:

$$\gamma(\rho_e) - t_e\kappa_A^e \oplus \kappa_B^e \geq 0. \tag{6.4}$$

For a state that is not detected by the CMC (e.g. a separable state) the parameter t can be chosen to be at least one, or even larger than one.

Parametrization of the condition (3.1) in Proposition 3.1 results in a alternative formulation of the CMC:

Theorem 6.1 (Parameterized CMC)**.** *Let ρ be a bipartite state. Assume that we choose pure states $|\psi_k\rangle\langle\psi_k|$ on $\mathcal{H}_A$ and $|\phi_k\rangle\langle\phi_k|$ on $\mathcal{H}_B$ such that $\kappa_A^o = \sum_k p_k\gamma(|\psi_k\rangle\langle\psi_k|)$ and $\kappa_B^o = \sum_k p_k\gamma(|\phi_k\rangle\langle\phi_k|)$ are optimal in the sense that*

$$\gamma - t_o\kappa_A^o \oplus \kappa_B^o \geq 0, \tag{6.5}$$

for some $0 \leq t_o \leq 1$, but

$$\gamma - t\kappa_A \oplus \kappa_B \ngeq 0, \text{ for all } t > t_o \text{ and all } \kappa_A, \kappa_B. \tag{6.6}$$

Then if the state ρ is separable there exist κ_A^o and κ_B^o such that

$$\max_t\{t \leq 1 : \gamma - t\kappa_A^o \oplus \kappa_B^o \geq 0\} = 1, \tag{6.7}$$

otherwise the state is entangled.

This leads to the idea, to use the parameter t_o for entangled states as an entanglement parameter. More precisely, we can define:

Definition 6.2. *Let ρ be a bipartite quantum state with CM $\gamma(\rho)$. We define a function $V(\rho)$ as*

$$V(\rho) = \max_{t,\kappa_A,\kappa_B}\{t \leq 1 : \gamma(\rho) - t\kappa_A \oplus \kappa_B \geq 0\}. \tag{6.8}$$

The entanglement parameter $\mathcal{E}(\rho)$ is then defined as

$$\mathcal{E}(\rho) = 1 - V(\rho). \tag{6.9}$$

The parameter $\mathcal{E}(\rho)$ vanishes for separable states and is larger than zero for all states that are detected by the CMC. This function $\mathcal{E}(\rho)$ is the main topic of study in this chapter and, as we shall see later, can be used to quantify entanglement in quantum states on. A similar function has been already used to quantify entanglement in infinite dimensional systems, namely Gaussian states [152], although there this parameter turned out to be an entanglement monotone only for special operations.

Interestingly, using the parametrized version of the CMC (Theorem 6.1) and inequalities 6.2 and 6.3 one can immediately give a lower bound $\mathcal{E}(\rho)$. We can formulate:

Proposition 6.3 (Bounds on $\mathcal{E}(\rho)$)**.** *Assuming that $d_A = d_B$ we have in the situation from above that*

$$\mathcal{E}(\rho) \geq \frac{Tr\left(\rho_A^2\right) + Tr\left(\rho_B^2\right) + 2\,Tr\left(|C|\right) - 2}{2d_A - 2} \tag{6.10}$$

and

$$\begin{aligned}\mathcal{E}(\rho) \quad \geq \quad & \frac{1}{d_A - 1}\Big\{\frac{Tr\left(\rho_A^2\right) + Tr\left(\rho_B^2\right) - 2}{2} + \\ & + \sqrt{\tfrac{1}{4}[Tr\left(\rho_A^2\right) - Tr\left(\rho_B^2\right)]^2 + \|C\|_{tr}^2}\Big\}.\end{aligned} \tag{6.11}$$

Proof. For the first case, a calculation as in the proof of Proposition 4.8 (see also Ref. [129]) gives a parametrized version of inequality 6.2 and results in

$$2\mathrm{Tr}\left(|C|\right) \leq \mathrm{Tr}\left(A + B - t(\kappa_A + \kappa_B)\right). \tag{6.12}$$

Using $\mathrm{Tr}\left(\gamma(\rho)\right) = d - \mathrm{Tr}\left(\rho^2\right)$ (see Proposition 2.9 and Ref. [129]) gives

$$t \leq \frac{2d_A - \mathrm{Tr}\left(\rho_A^2\right) - \mathrm{Tr}\left(\rho_B^2\right) - 2\mathrm{Tr}\left(|C|\right)}{2d_A - 2}. \tag{6.13}$$

and finally Ineq. (6.10). Ineq. (6.11) can be derived with help of Ineq. (6.3) and from the calculations in Proposition 4.2 (see also Ref. [129]). From

$$\|C\|_{tr}^2 \leq \mathrm{Tr}\left(A - t\kappa_A\right)\mathrm{Tr}\left(B - t\kappa_B\right) \tag{6.14}$$

it follows

$$t^2 - t\frac{\mathrm{Tr}\left(A\right) + \mathrm{Tr}\left(B\right)}{2(d_A - 1)} + \frac{\mathrm{Tr}\left(A\right)\mathrm{Tr}\left(B\right) - \|C\|_{tr}^2}{(d_A - 1)^2} \geq 0. \tag{6.15}$$

Generally the last relation has two solutions, but only one of them does not violate the condition (6.13), namely

$$t \leq \frac{1}{d_A - 1}\left\{\frac{2d_A - \mathrm{Tr}\left(\rho_A^2 + \rho_B^2\right)}{2} - \sqrt{\frac{1}{4}(\mathrm{Tr}\left(\rho_A^2\right) - \mathrm{Tr}\left(\rho_B^2\right))^2 + \|C\|_{tr}^2}\right\}, \tag{6.16}$$

from which Ineq. (6.11) immediately follows. ∎

6.2 Properties of the entanglement parameter $\mathcal{E}$

In this section we investigate general properties of the function $\mathcal{E}(\rho)$. Since the function $\mathcal{E}(\rho)$ should be used to quantify entanglement in a given quantum state, two of the properties that have to be fulfilled should be that it is convex and does not change under local unitary transformations. Indeed, this is the case:

Lemma 6.4. *The entanglement parameter $\mathcal{E}(\rho)$ is invariant under local unitary transformations and is convex in the state, that is for $\rho = p\rho_1 + (1-p)\rho_2$ we have that $\mathcal{E}(\rho) \leq p\mathcal{E}(\rho_1) + (1-p)\mathcal{E}(\rho_2)$.*

Proof: The invariance under local unitary transformations follows simply from the fact that the CMC is invariant under such transformations [137, 129]. In more detail, such transformations map a set of local orthogonal observables to another set of local orthogonal observables, and the CMC does not depend on the choice of the observables.

Concerning convexity, it is sufficient to prove the concavity of $V(\rho)$, i.e. that for any state $\rho = p\rho_1 + (1-p)\rho_2$ the inequality $V(\rho) = \tilde{t} \geq p\tilde{t}_1 + (1-p)\tilde{t}_2 \equiv t'$ holds, where $\tilde{t}_1 = V(\rho_1)$ and $\tilde{t}_2 = V(\rho_2)$.

To prove this we exploit the connection between the CMC and local uncertainty relations (LURs) (see Proposition 4.17 or [137, 129]). $V(\rho) = \tilde{t}$ implies that the parametrized CMC criterion is fulfilled and there exist κ_A, κ_B and $\tilde{t}$ such that $\gamma(\rho) - \tilde{t}\kappa_A \oplus \kappa_B \geq 0$. According to the Proposition 4.17 this means that if we take arbitrary local observables on Alice's and Bob's side $A_k \otimes \mathbb{1}$ and $\mathbb{1} \otimes B_k$ such and define positive constants $U_A = \min_\rho \sum_k \delta^2(A_k)$ and $U_B = \min_\rho \sum_k \delta^2(B_k)$ then

$$\sum_k \delta^2 \left(A_k \otimes \mathbb{1} + \mathbb{1} \otimes B_k\right)_\rho \geq \tilde{t}\,(U_A + U_B)\,. \tag{6.17}$$

Therefore it suffices to show that t' fulfills the last inequality as well. Due to the concavity of the variance we can write

$$\begin{aligned}\sum_k \delta^2 \left(A_k \otimes \mathbb{1} + \mathbb{1} \otimes B_k\right)_\rho \geq\; & p \sum_k \delta^2 \left(A_k \otimes \mathbb{1} + \mathbb{1} \otimes B_k\right)_{\rho_1} \\ & + (1-p) \sum_k \delta^2 \left(A_k \otimes \mathbb{1} + \mathbb{1} \otimes B_k\right)_{\rho_2}\,. \end{aligned} \tag{6.18}$$

Since the states ρ_1 and ρ_2 both fulfill the CMC with the parameters $\tilde{t}_1$ and $\tilde{t}_2$ we can write

$$\begin{aligned} p \sum_k \delta^2 \left(A_k \otimes \mathbb{1} + \mathbb{1} \otimes B_k\right)_{\rho_1} + (1-p) \sum_k \delta^2 (A_k \otimes \mathbb{1} + \\ + \mathbb{1} \otimes B_k)_{\rho_2} \geq \left[\tilde{t}_1 p + \tilde{t}_2 (1-p)\right](U_A + U_B)\,. \end{aligned} \tag{6.19}$$

Note that $\tilde{t}$ is defined as maximal value of all possible t which using (6.18) and (6.19) finishes the proof. ■

A further important property of entanglement measures is they do not increase under local operations assisted with classical communication. This condition can be demanded in two different forms (see e.g. [153, 82]): Minimally, one requires that if $\hat{\rho}$ arises from ρ via some LOCC transformation, then $E(\rho) \geq E(\hat{\rho})$ holds. Often, however, a stronger condition is required and fulfilled, namely that $E(\rho)$ should not increase under LOCC operations *on average*. This means that if an LOCC protocol maps ρ onto some states ρ_i with probabilities p_i, then

$$E(\rho) \geq \sum_i p_i E(\rho_i), \tag{6.20}$$

should hold.

In the following, we will show by giving an example that $\mathcal{E}(\rho)$ can increase on average under LOCC operations. This does not exclude a priori exclude the usability of $\mathcal{E}(\rho)$ as an entanglement monotone (since the requirement might still hold), however, it is a hint that $\mathcal{E}(\rho)$ might not be an entanglement measure. As we will see later, however, $\mathcal{E}(\rho)$ can be very useful to derive lower bounds on the concurrence for mixed states.

Lemma 6.5. *There exists a two-qubit state ρ and an LOCC-protocol, such that $\mathcal{E}(\rho)$ increases on average.*

Proof. We prove the statement by providing an explicit example of a two qubit state, which can be found numerically. To give such an example we pick up a certain family of states. This family is parametrized by four real parameters and was discussed in Section 2.3. Within this family one can find pairs of states ρ and ρ' with the same covariance matrix but where ρ is entangled, while ρ' is not. Hence, ρ can not be detected by the CMC criterion, and $\mathcal{E}(\rho)$ vanishes.

It was shown in Section 4.6 (see also Refs. [137, 129]), however, that after an appropriate filtering operation

$$\rho \mapsto \rho_{\text{filt}} = F_A \otimes F_B \rho F_A^\dagger \otimes F_B^\dagger \tag{6.21}$$

any entangled two-qubit state can be detected by the CMC. Hence $\mathcal{E}(\rho_{\text{filt}}) > 0$ and the filtering operation will give rise to the desired LOCC operation.

To be more concrete, a numerical example of the aforementioned state ρ is

$$\rho = \begin{pmatrix} 0.48508 & 0 & 0 & 0.02094 \\ 0 & 0.33 & 0 & 0 \\ 0 & 0 & 0.00067 & 0 \\ 0.02094 & 0 & 0 & 0.18425 \end{pmatrix}, \tag{6.22}$$

which is not detected by the CMC (see also [129]) but which is clearly NPT and hence entangled. The corresponding filter operations are

$$\begin{aligned} F_A &= \begin{pmatrix} 0.16457 & 0 \\ 0 & 0.98637 \end{pmatrix}, \\ F_B &= \begin{pmatrix} 0.96526 & 0 \\ 0 & 0.26128 \end{pmatrix}. \end{aligned} \tag{6.23}$$

The final state after ρ_{filt} filtering will be

$$\begin{aligned}\rho_{\text{filt}} &= \frac{F_A \otimes F_B \rho' F_A \otimes F_B}{Tr\left(F_A \otimes F_B \rho' F_A \otimes F_B\right)} \\ &= \begin{pmatrix} 0.47636 & 0 & 0 & 0.03336 \\ 0 & 0.02375 & 0 & 0 \\ 0 & 0 & 0.02364 & 0 \\ 0.03336 & 0 & 0 & 0.47626 \end{pmatrix}\end{aligned} \tag{6.24}$$

and is detected by the CMC, hence $\mathcal{E}(\rho_{\text{filt}}) > 0$. Since ρ is not detected, we have $\mathcal{E}(\rho) = 0$.

Using the filter operations F_A and F_B we can now construct a POVM type of measurements for Alice and Bob. The complementary operations are given by

$$\begin{aligned} F_A^c &= (\mathbb{1} - F_A F_A)^{\frac{1}{2}} = \begin{pmatrix} 0.98637 & 0 \\ 0 & 0.16457 \end{pmatrix}, \\ F_B^c &= (\mathbb{1} - F_B F_B)^{\frac{1}{2}} = \begin{pmatrix} 0.26128 & 0 \\ 0 & 0.96526 \end{pmatrix}. \end{aligned} \tag{6.25}$$

With this operations we establish LOCC protocol with four different outcomes

$$\begin{aligned} \rho_1 \equiv \rho_{\text{filt}} &\text{ with probability } p_1 = 0.02570, \\ \rho_2 &\text{ with probability } p_2 = 0.17629, \\ \rho_3 &\text{ with probability } p_3 = 0.46200, \\ \rho_4 &\text{ with probability } p_4 = 0.33601. \end{aligned} \tag{6.26}$$

Important for us is the fact that applying this protocol to a state with $\mathcal{E}(\rho)$ we achieve a state such that $\mathcal{E}(\rho_{\text{filt}})$ with non-zero probability. Therefore $0 = \mathcal{E}(\rho) < \sum_{i=1}^{4} p_i \mathcal{E}(\rho_i)$, and $\mathcal{E}(\rho)$ increases on average under LOCC. ■

Note that for provided example one can check the separability of the state $\tilde{\rho} = \sum_i p_i \rho_i$ as this state has a positive partial transpose though and is therefore separable. Consequently, the protocol given is not a counterexample to the LOCC condition of the first kind.

6.3 Evaluation of $\mathcal{E}(\rho)$ for pure and Schmidt-correlated states

In this section we compute $\mathcal{E}(\rho)$ for pure states and a family of mixed states. We start with the case of two-qubits. Then, we generalize it to d-dimensional systems.

6.3.1 Pure states of two qubits

Using the relations that can be found in Section 2.5, it is straightforward to calculate the CM of a two-qubit state $|\psi\rangle = \sqrt{\lambda_1}|00\rangle + \sqrt{\lambda_2}|11\rangle$ with $\lambda_1 + \lambda_2 = 1$. The CM

will have the familiar block form

$$\gamma(|\psi\rangle) = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix} \tag{6.27}$$

with

$$A = B = \begin{pmatrix} \lambda_1 - \lambda_1^2 & -\lambda_1\lambda_2 & 0 & 0 \\ -\lambda_1\lambda_2 & \lambda_2 - \lambda_2^2 & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{pmatrix},$$
$$C = \begin{pmatrix} \lambda_1 - \lambda_1^2 & -\lambda_1\lambda_2 & 0 & 0 \\ -\lambda_1\lambda_2 & \lambda_2 - \lambda_2^2 & 0 & 0 \\ 0 & 0 & \sqrt{\lambda_1\lambda_2} & 0 \\ 0 & 0 & 0 & -\sqrt{\lambda_1\lambda_2} \end{pmatrix}. \tag{6.28}$$

The next step in the calculation of the parameter t and therefore of the function $\mathcal{E}(\rho)$ is to find the optimal $\kappa_A \oplus \kappa_B$. In the two-qubit case we first guess the correct solution and the prove its optimality.

To construct the matrix $\kappa_A \oplus \kappa_B$ we take two product states $|00\rangle\langle 00|$ and $|11\rangle\langle 11|$ and get $\kappa_A \oplus \kappa_B = \frac{1}{2}\mathrm{diag}\{0,0,1,1,0,0,1,1\}$. Then we calculate the $V(|\psi\rangle)$ from the condition $\gamma - t\kappa_A \oplus \kappa_B \geq 0$. This matrix is positive iff $1 - t \geq 2\sqrt{\lambda_1\lambda_2}$ and therefore for any

$$t \leq 1 - 2\sqrt{\lambda_1\lambda_2} \tag{6.29}$$

we can find κ_A and κ_B such that $\gamma - t\kappa_A \oplus \kappa_B \geq 0$ holds.

Note that taking some particular expansion for $\kappa_A \oplus \kappa_B$, strictly speaking, does not provide any information about the entanglement, except for the case when we are able to find $\kappa_A \oplus \kappa_B$ such that $\gamma - t\kappa_A \oplus \kappa_B \geq 0$ for some $t \geq 1$. Then the state is not detected by the CMC and $\mathcal{E}(\rho) = 0$. However, we can use the Proposition 4.8 to prove the following

Lemma 6.6. *The upper bound on the parameter t for two qubits provided in Eq. (6.29) is tight.*

Proof: Directly applying the relation (6.13) to the two qubit case we have $t \leq 1 - 2\sqrt{\lambda_1\lambda_2}$, which coincides with (6.29) and therefore gives an optimal bound on parameter t. Indeed, on the one hand, it follows immediately from (6.29), that if $t \leq 1 - 2\sqrt{\lambda_1\lambda_2}$ then we can find a decomposition $\kappa_A \oplus \kappa_B$ such that $\gamma - t\kappa_A \oplus \kappa_B \geq 0$ holds. On the other hand, the condition (6.13) implies that for all t, with $t > 1 - 2\sqrt{\lambda_1\lambda_2}$ and for all κ_A and κ_B the relation $\gamma - t\kappa_A \oplus \kappa_B \ngeq 0$ holds. ■

According to the last Lemma the function $\mathcal{E}(|\psi\rangle)$ can be calculated exactly for two-qubit pure states as

$$\mathcal{E}(|\psi\rangle) = 2\sqrt{\lambda_1\lambda_2}. \tag{6.30}$$

6.3.2 Pure states of two qudits

To estimate the parameter t for a pure state of two d-level systems, we follow the same strategy as in the two qubit case and take the states $|kk\rangle\langle kk|$ for the decomposition of $\kappa_A \oplus \kappa_B$ in order to derive the upper bound on the parameter t. We make the ansatz

$$\kappa_A \oplus \kappa_B = \sum_{i=1}^{d} p_i \gamma(|ii\rangle). \tag{6.31}$$

with some probabilities p_i.

The positive semi-definiteness of the matrix $\gamma - t\kappa_A \oplus \kappa_B$ then implies the positive semi-definiteness of 2×2 blocks of the type

$$B^{ij}_{2\times 2} = \begin{pmatrix} \lambda_i + \lambda_j - t(p_i + p_j) & \pm 2\sqrt{\lambda_i \lambda_j} \\ \pm 2\sqrt{\lambda_i \lambda_j} & \lambda_i + \lambda_j - t(p_i + p_j) \end{pmatrix} \tag{6.32}$$

for all $i < j$. Therefore, if for all $i < j$

$$t \leq \frac{\left(\sqrt{\lambda_i} - \sqrt{\lambda_j}\right)^2}{p_i + p_j} \tag{6.33}$$

holds, then we can find κ_A and κ_B such that $\gamma - t\kappa_A \oplus \kappa_B \geq 0$ holds. To achieve the goal and calculate the function $\mathcal{E}(|\psi\rangle)$ we need to prove that the choice of the expansion of the $\kappa_A \oplus \kappa_B$ in Eq. (6.31) was optimal.

Lemma 6.7 (Optimality of the decomposition)**.** *The optimal expansion for $\kappa_A \oplus \kappa_B$ can always be written in a form of the Eq. (6.31):*

$$\kappa_A^{opt} \oplus \kappa_B^{opt} = \sum_{i=1}^{d} p_i \gamma(|ii\rangle). \tag{6.34}$$

Proof. First, we show that for pure states in Schmidt decomposition $\gamma(|\psi\rangle) - t\kappa_B \oplus \kappa_A \geq 0$ is equivalent to $\gamma(|\psi\rangle) - t\kappa \oplus \kappa \geq 0$, for some κ, which can be found explicitly. This κ can be constructed by choosing the product states in a proper way. Indeed, note that since the CM of a state in Schmidt decomposition is symmetric with respect to the interchange of the parties ($A \leftrightarrow B$) the relation $\gamma(|\psi\rangle) - t\kappa_B \oplus \kappa_A \geq 0$ must hold as well. Hence

$$\gamma(|\psi\rangle) - \frac{t}{2}\left(\kappa_A \oplus \kappa_B + \kappa_B \oplus \kappa_A\right) \geq 0. \tag{6.35}$$

Since $\kappa_A \oplus \kappa_B + \kappa_B \oplus \kappa_A = \kappa_A \oplus \kappa_A + \kappa_B \oplus \kappa_B$, the appropriate choice of the product states is

$$|\eta_k\rangle = \begin{cases} |a_i\rangle \otimes |a_i\rangle,\ i = 1, \ldots, d \ \ (\text{for } \kappa_A \oplus \kappa_A), \\ |b_i\rangle \otimes |b_i\rangle,\ i = d+1, \ldots, 2d \ \ (\text{for } \kappa_B \oplus \kappa_B). \end{cases} \tag{6.36}$$

Hence we have $\gamma(|\psi\rangle) - t\kappa \oplus \kappa \geq 0$, with

$$\kappa = \sum_{k=1}^{2d} \tilde{p}_k \gamma|\eta_k\rangle, \tag{6.37}$$

where $\tilde{p}_k = \frac{1}{2}p_{k \bmod d}$.

Secondly, because the blocks D in Eq. (2.32) in Section 2.5 are the same, we note that all diagonal elements D_{ii} from κ must be zero, otherwise only $t = 0$ will satisfy $\gamma(\rho) - t\kappa_A \oplus \kappa_B \geq 0$. This means that the only states, which can appear in the expansion (6.37) are of the form $|\eta_k\rangle = |kk\rangle$, since the $|a_k\rangle$ and $|b_k\rangle$ have to be eigenstates of the operators D_i. ■

Having proved the optimality of the expansion of $\kappa_A \oplus \kappa_B$ in Eq. (6.31) we can now provide the general formula for the function $\mathcal{E}(|\psi\rangle)$ for pure states in the Schmidt decomposition. The value of the function $V(|\psi\rangle)$ is given by the solution of the following max-min problem

$$\alpha^0 = \max_{\mathcal{P}} \min_{i<j} \frac{\left(\sqrt{\lambda_i} - \sqrt{\lambda_j}\right)^2}{p_i + p_j},\ 1 \leq i < j \leq d, \tag{6.38}$$

where the first max is taken over all possible probability distributions $\mathcal{P} = \{p_1, p_2, ...\}$. We present a solution of this problem for the case $d = 3$ and $d = 4$ and give its details in separate section at the end of this chapter:

Proposition 6.8. *(a) If $|\psi\rangle = \sum_{i=1}^{3} \sqrt{\lambda_i}|ii\rangle$ is a pure two-qutrit state, then*

$$\mathcal{E}(\psi) = 2\sqrt{\lambda_{i_0}\lambda_{j_0}} + 2\sqrt{\lambda_{i_0}\lambda_{k_0}} - \lambda_{i_0}, \tag{6.39}$$

where i_0, j_0, k_0 are pairwise different and j_0, k_0 are such that $(\sqrt{\lambda_{j_0}} - \sqrt{\lambda_{k_0}})^2 \geq (\sqrt{\lambda_j} - \sqrt{\lambda_k})^2$ for all j, k.
(b) If $|\psi\rangle = \sum_{i=1}^{4} \sqrt{\lambda_i}|ii\rangle$ is a pure state in a 4×4-system, then

$$\mathcal{E}(\psi) = \max\{\mathfrak{e}_1, \mathfrak{e}_2, \mathfrak{e}_3\}, \tag{6.40}$$

where

$$\begin{aligned} &\mathfrak{e}_1 = 2\sqrt{\lambda_1\lambda_2} + 2\sqrt{\lambda_3\lambda_4}, \quad \mathfrak{e}_2 = 2\sqrt{\lambda_1\lambda_3} + 2\sqrt{\lambda_2\lambda_4}, \\ &\mathfrak{e}_3 = 2\sqrt{\lambda_1\lambda_4} + 2\sqrt{\lambda_2\lambda_3}. \end{aligned} \tag{6.41}$$

Note that in both cases we have for a maximally entangled state $\mathcal{E}(\psi) = 1$.

6.3.3 Schmidt-correlated states

To conclude the section we consider a family of mixed states, for which the introduced function $\mathcal{E}(\rho)$ can be also computed exactly. These states are called Schmidt-correlated (SC) states in the literature [154]. By definition, SC states are a mixture of states that share the same Schmidt basis

$$\rho_{SC} = \sum_{u=1}^{N} q_u |\psi_u\rangle\langle\psi_u|, \text{ with} \tag{6.42}$$

$$|\psi_u\rangle = \sum_{i=1}^{d} \sqrt{\lambda_i^{(u)}}|ii\rangle. \tag{6.43}$$

SC states can be written in computational basis directly as

$$\rho_{SC} = \sum_{ij} \rho_{ij} |ii\rangle\langle jj|, \text{ with } \rho_{ij} = \sum_u q_u \sqrt{\lambda_i^{(u)} \lambda_j^{(u)}}. \tag{6.44}$$

As in the case of pure states, we find for the SC states the optimal decomposition of $\kappa_A \oplus \kappa_B$:

Lemma 6.9 (Optimality for SC states)**.** *In the case of SC states the optimal decomposition of $\kappa_A \oplus \kappa_B$ for the estimation of the parameter $\mathcal{E}(\rho)$ can always be written in the form of Eq. (6.31):*

$$\kappa_A^{opt} \oplus \kappa_B^{opt} = \sum_{i=1}^{d} p_i \gamma(|ii\rangle). \tag{6.45}$$

Proof: There were two essential ingredients in the proof of the Lemma 6.7. First, we used the fact that the CM of a state, written in Schmidt decomposition, is invariant under interchange of parties. Apparently the same invariance does also hold for SC states. Second, we used the fact, that all blocks D of the CM are the same. Using the formulas of the Section 2.5 one easily verifies that $D_{SC}^A = D_{SC}^B = D_{SC}^C$. ■

For these states the problem of calculating the function $\mathcal{E}(\rho)$ reduces to the max-min problem (6.38). This is due to the fact that diagonal elements of the covariance matrix have a pretty simple form for ρ_{SC}. Indeed, using the formulas from the Section 2.5 we calculate directly:

$$\begin{aligned}
&\left(D_{SC}^{A/B/C}\right)_{ij} = \rho_{ii}\delta_{ij} - \rho_{ii}\rho_{jj}, \;\; 1 \le i \le d, \\
&X_{SC}^{A/B} = Y_{SC}^{A/B} = \frac{1}{2}\mathrm{diag}\{\rho_{ii} + \rho_{kk}\}, \;\; 1 \le i < k \le d, \\
&X_{SC}^{C} = -Y_{SC}^{C} = \mathrm{diag}\{\rho_{ik}\}, \; 1 \le i < k \le d.
\end{aligned} \tag{6.46}$$

The 2×2 blocks in Eq. (6.32) will then take the form

$$B_{2\times 2}^{ij} = \begin{pmatrix} \rho_{ii} + \rho_{jj} - t(p_i + p_j) & \pm 2\rho_{ij} \\ \pm 2\rho_{ij} & \rho_{ii} + \rho_{jj} - t(p_i + p_j) \end{pmatrix}, \tag{6.47}$$

which leads to the following max-min problem for $V(\rho_{SC})$

$$\begin{aligned}
V(\rho_{SC}) &= \max_{\mathcal{P}} \min_{i<j} \frac{\rho_{ii} + \rho_{jj} - 2\rho_{ij}}{p_i + p_j} \\
&= \max_{\mathcal{P}} \min_{i<j} \frac{\sum_k q_k \left(\sqrt{\lambda_i^{(k)}} - \sqrt{\lambda_j^{(k)}}\right)^2}{p_i + p_j}.
\end{aligned} \tag{6.48}$$

This problem can be effectively solved numerically or as in Section 6.5 and its solution gives the exact value of the function $\mathcal{E}(\rho_{SC})$. For two qubits one finds

$$\mathcal{E}(\rho_{SC}) = 2\sum_k q_k \sqrt{\lambda_0^{(k)} \lambda_1^{(k)}} \tag{6.49}$$

as a nice analytical expression.

6.4 The entanglement parameter $\mathcal{E}(\rho)$ as a lower bound on the concurrence

In this section we demonstrate that the function $\mathcal{E}(\rho)$ can be used to estimate the amount of entanglement in a quantum state. More specifically, we show how it delivers a lower bound on the concurrence, which is a well known measure of bipartite entanglement. For bipartite pure states in a $d \times d$-system the concurrence is defined as [85, 86, 87]:

$$C(|\psi\rangle) = \sqrt{\frac{d}{d-1}}\sqrt{1 - \mathrm{Tr}\left(\rho_A^2\right)}. \tag{6.50}$$

In this definition, we introduced already a prefactor which guarantees that $0 \leq C \leq 1$, this will turn out to be useful for our purposes.

The concurrences is then extended to mixed states by the convex-roof construction

$$C(\rho) = \min_{p_i, |\psi_i\rangle} \sum_i p_i C(|\psi\rangle), \tag{6.51}$$

where the minimization is taken over all possible decompositions of the state $\rho = \sum_i p_i |\psi_i\rangle$. Of course, this minimization is quite difficult to perform, and only for two-qubits a complete solution is known [86]. Therefore, it is desirable to have at least some lower bounds on the concurrence.

The idea of obtaining lower bounds on C from $\mathcal{E}$ is as follows: Let us assume that one can prove a lower bound like

$$C(|\psi\rangle) \geq \alpha \mathcal{E}(|\psi\rangle) + \beta \tag{6.52}$$

for pure states only with some constants α, β and $\alpha \geq 0$. Then, since $\mathcal{E}$ is convex, the right hand side of Eq. (6.52) is convex, too. By definition, the convex roof is the largest convex function which coincides with C on the pure states. Consequently, $C(\rho) \geq \alpha \mathcal{E}(\rho) + \beta$ holds for all mixed states, too. This trick has already been employed in several works to obtain lower bounds on entanglement measures [88, 134, 142, 155, 156]. However, as the CMC detects many bound entangled states where other criteria fail [129], our results will deliver entanglement estimates for states, where the other methods fail.

6.4.1 Two qubits

Using the Schmidt decomposition, one can express the concurrence for pure states in terms of Schmidt coefficients as [85, 86, 87, 88]

$$C(|\psi\rangle) = \sqrt{\frac{2d}{d-1}}\sqrt{\sum_{i<j} \lambda_i \lambda_j}. \tag{6.53}$$

Comparing (6.53) and (6.30) from the Section 6.3 we see that the concurrence and the function $E(|\psi\rangle)$ coincide for on two qubit pure states

$$\mathcal{E}(|\psi\rangle) = 2\sqrt{\lambda_1 \lambda_2} = C(|\psi\rangle). \tag{6.54}$$

Consequently, $C(\rho) \geq \mathcal{E}(\rho)$ holds for any mixed state. Note, however, that for the special case of two qubits one can calculate the concurrence also directly.

6.4.2 Two qutrits

Using the solution of the problem (6.38) it is possible to derive a lower bound on concurrence for pure states of two d-level systems. Before we proceed, note that [88]:

$$C(\psi) = \sqrt{\frac{2d}{d-1}}\sqrt{\sum_{i<j}\lambda_i\lambda_j} \geq \frac{2}{d-1}\sum_{i<j}\sqrt{\lambda_i\lambda_j}. \tag{6.55}$$

This follows from the fact that

$$\begin{aligned}\sum_{i<j}\lambda_i\lambda_j &= \frac{1}{d(d-1)}\sum_{i<j}\sum_{k<l}(\lambda_i\lambda_j + \lambda_k\lambda_l) \\ &\geq \frac{2}{d(d-1)}\sum_{i<j}\sum_{k<l}\sqrt{\lambda_i\lambda_j\lambda_k\lambda_l} = \frac{2}{d(d-1)}\Big[\sum_{i<j}\sqrt{\lambda_i\lambda_j}\Big]^2.\end{aligned} \tag{6.56}$$

Concerning to qutrits, $\mathcal{E}(|\psi\rangle)$ is given by Eq. (6.39). We have that

$$\begin{aligned}2\sqrt{\lambda_i\lambda_j} + 2\sqrt{\lambda_i\lambda_k} - \lambda_i &= 2\sqrt{\lambda_i\lambda_j} + 2\sqrt{\lambda_i\lambda_k} + 2\sqrt{\lambda_j\lambda_k} - 2\sqrt{\lambda_j\lambda_k} - 1 + \lambda_j + \lambda_k \\ &\leq 2C(|\psi\rangle) + (\sqrt{\lambda_j} - \sqrt{\lambda_k})^2 - 1 \leq 2C(|\psi\rangle).\end{aligned} \tag{6.57}$$

Hence we have for mixed two-qutrit states

$$C(\rho) \geq \frac{\mathcal{E}(\rho)}{2}. \tag{6.58}$$

Using the results from Proposition 6.3 we have, for instance,

$$C(\rho) \geq \frac{1}{4}\Big\{\frac{\mathrm{Tr}\left(\rho_A^2\right) + \mathrm{Tr}\left(\rho_B^2\right) - 2}{2} + \sqrt{\tfrac{1}{4}[\mathrm{Tr}\left(\rho_A^2\right) - \mathrm{Tr}\left(\rho_B^2\right)]^2 + \|C\|_{tr}^2}\Big\}, \tag{6.59}$$

which is an easily computable lower bound that delivers non-trivial estimates for many bound entangled states.

6.4.3 4×4 systems

In this case $\mathcal{E}(|\psi\rangle)$ is given by (6.40). We can directly estimate:

$$\begin{aligned}\mathcal{E}(\psi) &= \max\{\mathfrak{e}_1, \mathfrak{e}_2, \mathfrak{e}_3\} \\ &\leq 2\sqrt{\lambda_1\lambda_3} + 2\sqrt{\lambda_2\lambda_4} + 2\sqrt{\lambda_1\lambda_2} + 2\sqrt{\lambda_3\lambda_4} + 2\sqrt{\lambda_1\lambda_4} + 2\sqrt{\lambda_2\lambda_3} \\ &\leq 3C(|\psi\rangle)\end{aligned} \tag{6.60}$$

and hence for arbitrary mixed states

$$C(\rho) \geq \frac{1}{3}\mathcal{E}(\rho). \tag{6.61}$$

6.4.4 Examples

Let us discuss the strength of these lower bounds by considering some examples. Let us first consider Bell-diagonal two-qubit states. For them, the reduced states ρ_A and ρ_B are maximally mixed, and then Proposition 6.3 delivers the bound $C(\rho) \geq \mathrm{Tr}\,(|C|) - 1/2$. On the other hand, it is known that for Bell diagonal states the concurrence is given by $C(\rho) = 2\lambda_{\max} - 1$, where $\lambda_{\max}$ is the maximal eigenvalue, i.e., the maximal overlap with some Bell state [85]. Noting that $\lambda_{\max} = [1 + 2\mathrm{Tr}\,(|C|)]/4$ (this can be easily seen if the closest Bell state is the singlet state and we take appropriately normalized Pauli matrices as observables in the definition of the matrix C), one finds that our lower bound is tight for Bell diagonal states.

For general two-qubit states, the lower bound cannot be tight, as they are entangled two-qubit states, which are not detected by the CMC. On the other hand, any full rank two qubit state can be brought to a Bell-diagonal state by filtering operations. Since it is known how the concurrence changes under filtering operations [139], one could use the filtering and our lower bound to determine the concurrence for arbitrary two-qubit states.

For two qutrits, our bound is not tight for states like $|\psi\rangle = (|00\rangle + |11\rangle + |22\rangle)/\sqrt{3}$ or $|\psi\rangle = (|00\rangle + |22\rangle)/\sqrt{2}$, however, for the latter the reason lies in the fact that the bound (6.55) is not tight. On the other hand, the presented method delivers nontrivial lower bounds for many bound entangled states (such as the the family of chessboard states), as many states of this type are detected by the CMC [129], but not by the PPT or CCNR criterion (which means that the methods from Ref. [88] must fail). Similarly, our methods can be used to estimate the entanglement of bound entangled states for 4×4-systems.

6.5 Solution of the max-min problem for $d = 3$ and $d = 4$

In this section we discuss the possible ways of solving the max-min problem:

$$\tilde{t} = \max_{\mathcal{P}} \min_{i<j} \frac{\left(\sqrt{\lambda_i} - \sqrt{\lambda_j}\right)^2}{p_i + p_j},\ 1 \leq i < j \leq d. \tag{6.62}$$

We consider the cases $d = 3$ and $d = 4$. We define

$$b_{ij} \equiv \left(\sqrt{\lambda_i} - \sqrt{\lambda_j}\right)^2, \tag{6.63}$$

$$\alpha_{ij} \equiv \frac{b_{ij}}{p_i + p_j} = \alpha_{ji}. \tag{6.64}$$

For $d = 3$ there are only three different α's that can be arranged in a tableaux as in FIG.6.1(a).

The properties of the solution can be summarized as follows:

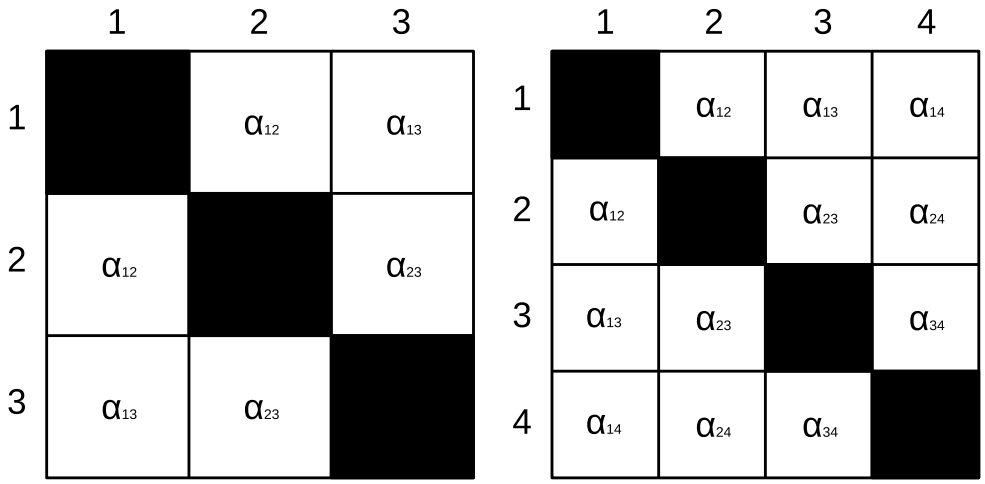


Figure 6.1. *(a) In the case $d = 3$ there are only three elements α_{ij}. These elements are written in the form of tableaux in order to visualize the problem considered. (b) Tableaux of the elements α_{ij} in the max-min problem for $d = 4$.*

Lemma 6.10. *(a) Consider the optimization problem in Eq. (6.62) for d=3 with the only assumption that $b_{ij} \geq 0$ for d=3. Let j_0, k_0 be such that*

$$b_{j_0 k_0} = \max\{b_{jk}\}. \tag{6.65}$$

Then the optimal solution α^0 is given by

$$\alpha^0 = \min\left\{\alpha^I, \alpha^{II}\right\}, \tag{6.66}$$

where

$$\alpha^I = \frac{1}{2}(b_{12} + b_{13} + b_{23}), \tag{6.67}$$

$$\alpha^{II} = b_{i_0,j_0} + b_{i_0,k_0} \tag{6.68}$$

with $j_0 \neq i_0 \neq k_0$.
(b) For the same problem, if the b_{ij} are given via Eq. (6.63) as functions of Schmidt coefficients and fulfill therefore further restrictions, the optimum is always given by

$$\alpha^0 = \alpha^{II} = 1 + \lambda_{i_0} - 2\sqrt{\lambda_{i_0}\lambda_{j_0}} - 2\sqrt{\lambda_{i_0}\lambda_{k_0}}. \tag{6.69}$$

Then we also have that $\alpha^{II} = \min_{ijk}\{1 + \lambda_i - 2\sqrt{\lambda_i\lambda_j} - 2\sqrt{\lambda_i\lambda_k}\}$ where the i, j, k are pairwise different.

Proof: (a) Let us first assume only that $b_{ij} \geq 0$. In the max-min problem (6.62) the maximization is taken over all possible probability distributions. It is convenient to distinguish two cases:

Case 1: The optimal probability distribution does not have any zero elements. Assume $\mathcal{P}_0$ is the optimal distribution and $p_i^0 \neq 0\ \forall i$. We show that this optimal distribution necessarily has to be such that $\alpha_{12}^0 = \alpha_{13}^0 = \alpha_{23}^0 = \alpha^0$, otherwise the optimality is violated. Indeed, assume that this is not case. Then, without loss of generality, we can write $\alpha_{12}^0 \leq \alpha_{13}^0 \leq \alpha_{23}^0$, where one of the inequalities must be strict. Now consider some distribution $\mathcal{P}'$ such that

$$p_1' = p_1^0 - 2\epsilon, \quad p_2' = p_2^0 + \epsilon, \quad p_3' = p_3^0 + \epsilon \tag{6.70}$$

with some $\epsilon > 0$. The coefficients α_{ij} will change and become according to the new distribution $\mathcal{P}'$

$$\alpha_{12}' > \alpha_{12}^0, \quad \alpha_{13}' > \alpha_{13}^0, \quad \alpha_{23}' < \alpha_{23}^0. \tag{6.71}$$

Since the parameter ϵ can be chosen arbitrarily small the number α_{12}' will be still the minimal one, i.e. $\alpha_{12}' = \min_{i<j} \alpha_{ij}'$. But $\alpha_{12}' > \alpha_{12}^0$. Consequently the distribution $\mathcal{P}'$ gives a bigger minimum of the set $\{\alpha_{ij}\}$ than the distribution $\mathcal{P}_0$, which contradicts the assumption that $\mathcal{P}_0$ is optimal. Hence we conclude that $\alpha_{12}^0 = \alpha_{23}^0$ must hold, which implies $\alpha_{12}^0 = \alpha_{13}^0 = \alpha_{23}^0$.

Having established that if $\mathcal{P}_0$ is optimal and contains no zero elements, then $\alpha_{12}^0 = \alpha_{13}^0 = \alpha_{23}^0 = \alpha^0$ holds, we can calculate α^0 explicitly. We have

$$\alpha^0 = \frac{b_{12}}{p_1^0 + p_2^0} = \frac{b_{13}}{p_1^0 + p_3^0} = \frac{b_{23}}{p_2^0 + p_3^0}. \tag{6.72}$$

Multiplying by the denominators summing up these equations gives

$$2\alpha^0(p_1^0 + p_2^0 + p_3^0) = b_{12} + b_{13} + b_{23}. \tag{6.73}$$

Because $p_1^0 + p_2^0 + p_3^0 = 1$ we arrive at

$$\alpha^I \equiv \alpha^0 = \frac{1}{2}(b_{12} + b_{13} + b_{23}). \tag{6.74}$$

Case 2: The optimal probability distribution $\mathcal{P}_0$ has at least one zero element. This means that one $\alpha_{ij}^0 = b_{ij}$ independently of the two free parameters of the probability distribution. We can distinguish three cases, and assume for definiteness $b_{12} \leq b_{13} \leq b_{23}$.

(i) If $\alpha_{12}^0 = b_{12}$ (that is, $p_3^0 = 0$), then clearly $\alpha_{ij}^0 \geq b_{ij}$ for $i, j = 1, 3$ and $i, j = 2, 3$. Then we have $\min\{\alpha_{ij}^0\} = \alpha_{12}^0$. But then decreasing one of the p_1 or p_2 and increasing consequently p_3^0 will lead to an increasing of α_{12}^0 and an better solution which belongs to case 1. So a solution with $\alpha_{12}^0 = b_{12}$ can never be optimal.

(ii) If $\alpha_{13}^0 = b_{13}$ the optimal probability distribution has to be such that $\alpha_{13}^0 \leq \alpha_{12}^0$ and $\alpha_{13}^0 \leq \alpha_{23}^0$. But as in the case (i) one can directly see that this leads to case 1 and can never be optimal.

(iii) Finally, consider the case $\alpha_{23}^0 = b_{23}$. Then, one can see as in case 1 one can achieve $\alpha_{12}^0 = \alpha_{13}^0$ without giving up optimality. More precisely, the optimal

probability distribution has to fulfill this from the beginning (if α^0_{12} and α^0_{13} are the minima) or it can be achieved (if α^0_{23} is the minimum).

This leads as in case 1 to the conclusion, that we have

$$\alpha^0_{12} = \frac{b_{12}}{p^0_2} = \frac{b_{13}}{p^0_3} \Rightarrow \alpha^0_{12} = b_{12} + b_{13}, \tag{6.75}$$

and consequently

$$\alpha^{II} \equiv \alpha^0_{12} = b_{12} + b_{13} = 1 + \lambda_1 - 2\sqrt{\lambda_1\lambda_2} - 2\sqrt{\lambda_1\lambda_3}. \tag{6.76}$$

However, it is not yet clear what the $\min\{\alpha_{ij}\}$ is. Two cases can be distinguished:

(iiia) If $\alpha^0_{12} \geq \alpha^0_{23} = b_{23}$ one would take $\min\{\alpha^0_{ij}\} = \alpha^0_{23} = b_{23}$, but then, one can improve it further as in the cases (i) and (ii) by going to the case I and taking finally α^I from Eq. (6.74). Note that $\alpha^I = (\alpha^{II} + b_{23})/2$. Therefore, if $\alpha^{II} = \alpha^0_{12} \geq \alpha^0_{23} = b_{23}$ one has also that $\alpha^I \leq \alpha^{II}$, so effectively one takes $\min\{\alpha^I, \alpha^{II}\}$.

(iiib) If $\alpha^0_{12} < \alpha^0_{23} = b_{23}$ we take $\min\{\alpha^0_{ij}\} = \alpha^{II}$ and going to case 1 does not bring anything. But in this case, we have $\alpha^I \geq \alpha^{II}$, so effectively one takes again $\min\{\alpha^I, \alpha^{II}\}$.

Finally, let us discuss shortly the meaning of the choice j_0 and k_0 in Eq. (6.65) as one may consider also $\alpha^{II}_{j,k}$ in Eq. (6.68) with other indices. However, one can directly compute that $\alpha^{II}_{i,j} < \alpha^I$ is equivalent to $b_{ij} + b_{ik} < b_{jk}$ and this can only be true, if j and k are chosen as in Eq. (6.65). In other words, the $\alpha^{II}_{j,k}$ for other indices than j_0, k_0 can never contribute and one could alternatively write that $\alpha_0 = \min\{\alpha^I, \alpha^{II}_{12}, \alpha^{II}_{13}, \alpha^{II}_{23}\}$.

(b) Let us now assume that the b_{ij} stem from Schmidt coefficients as in Eq. (6.63). We know from the previous discussion that we have to take α^{II} iff $b_{i_0j_0} + b_{i_0k_0} \leq b_{j_0k_0}$. In terms of the Schmidt coefficients, this implies that

$$(\sqrt{\lambda_{j_0}} - \sqrt{\lambda_{k_0}})^2 \geq (\sqrt{\lambda_{i_0}} - \sqrt{\lambda_{j_0}})^2 + (\sqrt{\lambda_{i_0}} - \sqrt{\lambda_{k_0}})^2. \tag{6.77}$$

This, however, is true for any triple of positive real numbers $\sqrt{\lambda_\nu}$, if j_0 and k_0 are chosen as in Eq. (6.65). Then, its also clear that the α^{II} chosen is minimal among all the $b_{ij} + b_{ik}$. ■

Further, we discuss the case $d = 4$. The elements α_{ij} are again embedded in a tableaux as in Fig. 6.1(b). We begin with studying of properties of the optimal probability distribution $\mathcal{P}_0$. Suppose as in the case $d = 3$ that α^0_{ij} correspond to the optimal probability distribution $\mathcal{P}_0$ and that $\alpha^0_{12} = \min_{ij}\{\alpha^0_{ij}\}$. We can formulate:

Lemma 6.11. *The solution of the max-min problem (6.38) for $d = 4$ is given by*

$$\alpha^0 = \min\{\mathfrak{a}^I, \mathfrak{a}^{II}, \mathfrak{a}^{III}\}, \tag{6.78}$$

where

$$\begin{aligned} \mathfrak{a}^I &= 1 - 2\sqrt{\lambda_1\lambda_2} - 2\sqrt{\lambda_3\lambda_4}, \\ \mathfrak{a}^{II} &= 1 - 2\sqrt{\lambda_1\lambda_3} - 2\sqrt{\lambda_2\lambda_4}, \\ \mathfrak{a}^{III} &= 1 - 2\sqrt{\lambda_1\lambda_4} - 2\sqrt{\lambda_2\lambda_3}. \end{aligned} \tag{6.79}$$

Proof: The proof proceeds in several steps.
Step 1. Let us first consider optimal probability distributions $\mathcal{P}_0 = \{p_1^0, p_2^0, p_3^0, p_4^0\}$ where all p_i^0 are nonzero. In this case we show that for $\alpha^0_{k_0 l_0} = \min\{\alpha^0_{ij}\}$ at least one of the three equations must hold:

$$\begin{aligned} \alpha^0_{k_0 l_0} &= \alpha^0_{12} = \alpha^0_{34}, \\ \alpha^0_{k_0 l_0} &= \alpha^0_{13} = \alpha^0_{24}, \\ \alpha^0_{k_0 l_0} &= \alpha^0_{14} = \alpha^0_{23}. \end{aligned} \tag{6.80}$$

The idea of the proof of the above statement is similar to the idea of the proof of the Lemma 6.10, i.e. we consider small perturbations of the optimal probability distribution $\mathcal{P}_0$ that increase the minimal element α^0 (note that we dropped the indices k_0 and l_0 in order to shorten notation) and therefore destroy the optimality if some additional constraints are not fulfilled. As we will see, these constraints will give us the conditions (6.80).

Let us assume for definiteness that the optimal α^0 is given by α^0_{12}. We can consider the following four transformations of the p_i :

$$\begin{aligned} T_1: &\quad p_1' = p_1^0 - 3\epsilon, \quad p_i' = p_i^0 + \epsilon \text{ for } i \neq 1, \\ T_2: &\quad p_2' = p_2^0 - 3\epsilon, \quad p_i' = p_i^0 + \epsilon \text{ for } i \neq 2, \\ T_3: &\quad p_3' = p_3^0 + 3\epsilon, \quad p_i' = p_i^0 - \epsilon \text{ for } i \neq 3, \\ T_4: &\quad p_4' = p_4^0 + 3\epsilon, \quad p_i' = p_i^0 - \epsilon \text{ for } i \neq 4, \end{aligned} \tag{6.81}$$

where ϵ can be chose arbitrarily small. All the transformation increase α^0_{12}, but all have to keep the optimality of the probability distribution, so that minimal α given by $\mathcal{P}'$ cannot be larger than α^0_{12}. From transformation T_1 it follows that $\mathcal{P}_0$ is optimal if and only if $\alpha^0_{12} = \min\{\alpha^0_{23}, \alpha^0_{24}, \alpha^0_{34}\}$, as these entries decrease under the transformation. Similarly, it follows from T_2 that $\alpha^0_{12} = \min\{\alpha^0_{13}, \alpha^0_{14}, \alpha^0_{34}\}$, and from T_3 that $\alpha^0_{12} = \min\{\alpha^0_{13}, \alpha^0_{23}, \alpha^0_{34}\}$, and finally from T_4 that $\alpha^0_{12} = \min\{\alpha^0_{14}, \alpha^0_{24}, \alpha^0_{34}\}$. Given this finite number of possibilities, one can directly check that either $\alpha^0_{12} = \alpha^0_{34}$ or $\alpha^0_{12} = \alpha^0_{13} = \alpha^0_{24}$ or $\alpha^0_{12} = \alpha^0_{14} = \alpha^0_{23}$ must hold for optimal probability distribution $\mathcal{P}_0$ which proves the first claim.

From these conditions we see that there are the three candidates for the optimal α^0:

$$\begin{aligned} &\alpha^0 = \alpha^0_{12} = \alpha^0_{34}, \\ &\quad \Rightarrow \alpha^0 = \mathfrak{a}^I = b_{12} + b_{34} = 1 - 2\sqrt{\lambda_1\lambda_2} - 2\sqrt{\lambda_3\lambda_4}, \\ &\alpha^0 = \alpha^0_{13} = \alpha^0_{24}, \\ &\quad \Rightarrow \alpha^0 = \mathfrak{a}^{II} = b_{13} + b_{24} = 1 - 2\sqrt{\lambda_1\lambda_3} - 2\sqrt{\lambda_2\lambda_4}, \\ &\alpha^0 = \alpha^0_{14} = \alpha^0_{23}, \\ &\quad \Rightarrow \alpha^0 = \mathfrak{a}^{III} = b_{14} + b_{23} = 1 - 2\sqrt{\lambda_1\lambda_4} - 2\sqrt{\lambda_2\lambda_3}. \end{aligned} \tag{6.82}$$

Step 2. At this point, we have identified three candidates for the α^0, but is is not clear yet, which one should be taken.

We will show now, however, that only the minimum of these can give a valid solution. For that, assume that one has a probability distribution $\mathcal{P}_1$ which has the optimal $\alpha^0(\mathcal{P}_1) = \mathfrak{a}^I$. Then $\alpha^0_{34} = \alpha^0_{12} = \min_{ij}\{\alpha^0_{ij}\}$ and hence

$$\begin{aligned} &\alpha^0_{12} \leq \alpha^0_{13} \Rightarrow b_{12}(p^0_1 + p^0_3) \leq b_{13}(p^0_1 + p^0_2), \\ &\alpha^0_{34} \leq \alpha^0_{23} \Rightarrow b_{34}(p^0_2 + p^0_4) \leq b_{24}(p^0_3 + p^0_4). \end{aligned} \tag{6.83}$$

Consequently, $b_{12} + b_{34} \leq b_{13} + b_{24}$ and hence $\mathfrak{a}^I \leq \mathfrak{a}^{II}$. Similarly, it follows that $\mathfrak{a}^I \leq \mathfrak{a}^{III}$. So if one finds a solution, then it has to be the minimum of all $\mathfrak{a}^k$.

This also shows that if there is a second solution $\mathcal{P}_2$ with $\alpha^0(\mathcal{P}_2) = \mathfrak{a}^{II}$, then $\alpha^0(\mathcal{P}_1) = \alpha^0(\mathcal{P}_2)$ must hold, since $\mathfrak{a}^I \leq \mathfrak{a}^{II}$ and $\mathfrak{a}^{II} \leq \mathfrak{a}^I$. Note also that the arguments leading to this did not require the assumption that the probability distributions have nonzero elements.

Summarizing Step 1 and Step 2, we can state that if there is a optimal probability distribution with non-zero elements, then the solution is given by

$$\alpha^0 = \min\{\mathfrak{a}^I, \mathfrak{a}^{II}, \mathfrak{a}^{III}\}. \tag{6.84}$$

Step 3. Now we have to consider the cases where the optimal probability distribution has some zero elements. Let us first consider the case that there is exactly one zero element.

There exist two possibilities. The first one arises, when the minimum is given by α^0_{12} and $p^0_4 = 0$. Then, the transformations T_1, T_2 and T_4 in Eq. (6.81) can still be applied, but we have to modify T_3, since there are no negative probabilities

$$\hat{T}_3 : p'_3 = p^0_3 + 2\epsilon, \quad p'_i = p^0_i - \epsilon \text{ for } i = 1, 2, \quad p'_4 = p^0_4 = 0. \tag{6.85}$$

This transformation leads exactly to the same condition as T_3 above $\alpha^0_{12} = \min\{\alpha^0_{13}, \alpha^0_{23}, \alpha^0_{34}\}$. Therefore, the same conclusion as in Step 1 can be drawn. Similarly, by considering $\hat{T}_4$, one can show that if $p^0_3 = 0$, the conclusion from Step 1 still holds.

The second possibility arises, if the minimum is again given by α^0_{12}, but this time $p^0_1 = 0$. Then, only T_2 in Eq. (6.81) can be applied. We define the modified transformations:

$$\begin{aligned} \tilde{T}_3 &: p'_3 = p^0_3 + 2\epsilon, \quad p'_i = p^0_i - \epsilon \text{ for } i = 2, 4, \quad p'_1 = p^0_1 = 0, \\ \tilde{T}_4 &: p'_4 = p^0_4 + 2\epsilon, \quad p'_i = p^0_i - \epsilon \text{ for } i = 2, 3, \quad p'_1 = p^0_1 = 0. \end{aligned} \tag{6.86}$$

Then, repeating the argumentation from Step 1, one arrives at the same conclusion, apart from the special case: $\alpha^0_{12} = \alpha^0_{13} = \alpha^0_{14} < \alpha^0_{kl}$ for $k, l \in \{2, 3, 4\}$ holds.

In this special case, we have that $\alpha^0 = (b_{12} + b_{13} + b_{14})$ and consequently $p^0_k = b_{1k}/(b_{12} + b_{13} + b_{14})$ for $k = 2, 3, 4$. Since $\alpha^0_{23} = b_{23}/(p^0_2 + p^0_3) > \alpha^0 = (b_{12} + b_{13} + b_{14})$ it follows that $b_{23} > b_{12} + b_{13}$. Generally we have $b_{kl} > b_{1k} + b_{1l}$, for $k, l \in \{2, 3, 4\}$.

Due to the definition of the b_{ij}, it means that the Schmidt coefficients have to fulfill

$$(\sqrt{\lambda_k} - \sqrt{\lambda_l})^2 > (\sqrt{\lambda_1} - \sqrt{\lambda_k})^2 + (\sqrt{\lambda_1} - \sqrt{\lambda_l})^2 \tag{6.87}$$

for $k, l \in \{2, 3, 4\}$. Since the $\sqrt{\lambda_k}$ are positive real numbers, this can only hold if $\sqrt{\lambda_1}$ is inside the interval $[\sqrt{\lambda_k}; \sqrt{\lambda_l}]$. As there are three intervals, and two of them intersect in only one point, we must have that $\sqrt{\lambda_1} = \sqrt{\lambda_i}$ for some $i \in \{2, 3, 4\}$, which implies that the corresponding $b_{1i} = 0$ and $\alpha^0_{1i} = 0$. Since $\alpha^0_{12} = \alpha^0_{13} = \alpha^0_{14}$ all of them must be zero and hence $\alpha^0 = 0$ and all $b_{1k} = 0$ for any $k \in \{2, 3, 4\}$. Physically, this means that all Schmidt coefficients are the same and the state is a maximally entangled one. But then also $\mathfrak{a}^I = \mathfrak{a}^{II} = \mathfrak{a}^{III} = 0$, so this special case does not deliver a novel solution.

Step 4. Let us now consider the case, where two or more p^0_i equal zero.

Let us first assume that exactly two p^0_i are zero, namely $p^0_2 = p^0_3 = 0$. Then $\alpha^0_{14} = b_{14}$ and $\alpha^0_{23} = \infty$ are independent of the probability distribution. However, if we make the transformation

$$\mathfrak{T} : p'_i = p^0_i - \epsilon \;\; i \in \{1, 4\}, \;\; p'_k = p^0_k + \epsilon \;\; k \in \{2, 3\}, \tag{6.88}$$

the minimal value α^0 does not decrease (as all $\alpha^0_{12}, \alpha^0_{13}, \alpha^0_{24}, \alpha^0_{34}$ remain constant, α^0_{14} increases and α^0_{23} can still be considered close to $+\infty$ due to the infinitesimality of ϵ). Therefore we arrive at a solution, where none of the p^0_i is zero and which is as good as a solution with $p^0_2 = p^0_3 = 0$. Thus we conclude that solutions given by distributions with two zero elements are contained in solutions characterized in Step 1.

Finally, we have to discuss the case that three p^0_i equal zero and consequently the remaining one equals one. This can be excluded with a similar transformation as in Eq. (6.88). Assume $p^0_1 = 1$ and the rest probabilities are zero, then the transformation similar to $\mathfrak{T}$ reads

$$\tilde{\mathfrak{T}} : p'_1 = p^0_1 - 3\epsilon \;\; p'_k = p^0_k + \epsilon \;\; k \in \{2, 3, 4\}. \tag{6.89}$$

None of the elements α'_{ij} will be smaller than α^0_{ij}, which finishes the proof. ■

6.6 Conclusion

In conclusion, we have introduced an entanglement parameter $\mathcal{E}$ that quantifies the violation of the covariance matrix criterion. We have shown that this parameter is convex and invariant under local unitary operations, but it can increase on average under local operations and classical communication. Most importantly the parameter $\mathcal{E}$ can be used to deliver lower bounds on the concurrence.

Chapter 7

Local renormalization method for random systems

Questions of entanglement detection and quantification discussed in previous chapters are of big importance for quantum information science. Up to now we considered quantum states as a rather abstract mathematical object, i.e. in most cases we characterized a physical state by its density matrix. We did not draw any connection to real physical systems (ensembles of interacting free atoms or electrons, atoms periodically ordered in a lattice of a solid or trapped in a periodic optical lattice an so on), which the state is supposed to describe. In Section 5.2, however, we discussed states that correspond to a real physical system described by a certain Hamiltonian. Investigation of entanglement properties of such states is therefore of a big interest, since one knows for sure that these states exist in nature.

As we mentioned in introductory chapter to this thesis, entanglement plays an important role in quantum phase transitions. For several many-body critical systems entanglement amount is known to grow when the temperature decreases and the system is in the vicinity of its critical point. Furthermore it is known that the description of these systems is usually a hard task. With exception of few models, where an exact solution is known. So, there seems to be a relation between hardness of solving, describing or simulating a system and amount of entanglement it possesses in the ground state. The subject of our study will be systems that can be described by Hamiltonians defined on a two dimensional rectangular grid of atoms, which interact only with their nearest neighbors and might be subjected to an external magnetic field. Moreover we consider systems, where the strength of the nearest neighbor interaction and of the local magnetic field is a stochastic variable, i.e. it varies from spatially, described by its mean value and the variance.

In order to investigate to which extent this kind of systems can be simulated on the classical computer and how is this connected with the strength of disorder, we introduce a real-space renormalization transformation for random spin systems on 2D lattices. The general method is formulated for random systems and results from merging two well known real space renormalization techniques, namely the strong disorder renormalization technique (SDRT) and the contractor renormalization (CORE). We analyze the performance of the method on the 2D random transverse field Ising model (RTFIM).

7.1 Short historical overview

Most physical systems are disordered and the description and modeling of such systems is one of the most special problems in condensed matter physics. In the early 70's the role of the disorder in physical systems was discussed in several papers. Harris [157] formulated a criterion for the relevance of the weak disorder caused by locally random impurities in the system. According to the criterion, the relevance of the disorder depends on the sign of the critical exponent for the specific heat. Just one year later, Imry and Ma [158] formulated another criterion, which points out the relevance of the weak disorder in less than four dimensions (the ordered state became unstable against an arbitrarily weak random field). As it became clear later these criteria can be understood in terms of the real space renormalization group (see for instance [159, 160] and references therein). Real space renormalization group (RG) methods for quantum disordered systems were applied first in the late 70. In the pioneering work on this topic Ma, Dasgupta and Hu considered a spin-1/2 antiferromagnetic Heisenberg chain, where the coupling strengths were assumed to be stochastically distributed [175]. The authors studied the model at zero temperature using a method that essentially relies on the reduction of the number of degrees of freedom in the system. Their approach attracted a lot of attention, was extensively studied and developed further by Fisher [126, 127] and has been used to investigate a big variety of systems in one and two dimensions (a review on the real space RG approach can be found in [124]). The method has recently been referred to as strong disorder renormalization technique (SDRT).

Indeed it turned out that the behavior of a system with randomness is in many cases quite different from the non-random case. The main ingredient of the disordered systems, which has no counterpart in the systems without disorder, is the existence of so called rare regions, i.e., regions possessing atypical properties (for the phase under consideration) compared to the rest of the system. It is known that this kind of rare effects can govern the behavior of the systems at long distances and result in exotic phases, e.g. Griffiths-McCoy [161, 162, 167, 169, 163, 164, 124] phase. It is worth to note that the application of the method to two dimensional systems is not straightforward, since it distorts the geometry of the underlying lattice, and only numerical calculations are possible. Therefore analytic proofs like asymptotic exactness of the SDRT in thermodynamical limit (see [126, 127]) do not apply. We will come back to the SDRT in the next section and discuss it in more detail. Despite its beauty, the SDRT is a perturbative method and applying it to the finite sized systems may cause a problem. A non-perturbative RG method, that for our knowledge has not been applied to random systems yet, was introduced by Morningstar and Weinstein in [109]. This method is called contractor renormalization (CORE) group approach and is especially suited for lattice systems (for CORE applications see [177, 178, 179, 180, 181, 176, 182, 183, 184]). By definition, this method keeps the eigenvalues of the low energy sector and produces an optimal truncation operator from the original Hilbert space to the effective one. In other words, the CORE is a non-perturbative block-spin renormalization, which uses exact diagonalization to extract the effective interactions in a coarse grained system.

Having a non-perturbative method on the one hand and ideas of spatially local renormalization of the system from the SDRT on the other hand, we introduce a method that unifies both techniques and is suited to investigate two dimensional disordered systems. The purpose of this chapter is to show that such merging is possible and results in a non-perturbative real space renormalization transformation for 2D quantum systems at zero temperature that preserves the underlying lattice geometry.

A reliable real space renormalization group method for description of the low temperature behavior of some system gives information about the long distance properties of the system while keeping the fundamental structure of the ground state. This fact is especially relevant in quantum random systems where the entanglement properties of the ground state have been identified as the key feature in understanding the behavior of these materials [168, 171, 172]. Since the method we are about to introduce involves local real-space renormalization steps we will have to analyze errors introduced by these local operations. As a benchmark we are going to use statistical arguments, showing that long range interactions are not important in the renormalized system and therefore can be neglected, i.e., if we consider a model that initially has only nearest neighbors interactions, we can neglect next nearest or more sophisticated terms introduced by renormalization and proceed further with a model that has only nearest neighbor interactions. The statistical justification of the fact that our method can be applied locally in the real space and without renormalizing the whole lattice at once, is a crucial point here.

7.2 Real space renormalization group methods and random systems

7.2.1 Strong Disorder Renormalization Technique

The name strong disorder renormalization technique reveals perfectly the idea of real space RG for random systems introduced by Ma, Dasgupta and Hu in [175].

There are *a priori* several different situations that can appear in disordered systems in the thermodynamical limit. When the size of the system increases and the effective disorder becomes a major effect compared to the thermal or to the quantum fluctuations, this effective disorder can either become

- smaller and smaller without bound: the system is then controlled by a pure fixed point,
- larger and larger without bound: the system is then controlled by an infinite disorder or infinite-randomness fixed point (IRFP),
- or it may converge towards a finite level: the system is then controlled by a finite disorder fixed point.

A class of systems whose critical behavior is governed by an infinite-randomness fixed point (IRFP) is characterized by a very broad distribution of couplings and a dynamical exponent z that becomes infinite at the critical point. In certain models, any initial disorder, even very small, drives the system towards the IRFP at the large scale: in particular, this is the case for the random anti-ferromagnetic quantum spin$-1/2$ chain (see also [126]).

We will illustrate very briefly a concrete scheme for renormalization of systems with infinitely strong disorder in one dimension on example of the random transverse field quantum Ising chain (RTFIC) (for detailed consideration see [127]). The system has the following Hamiltonian

$$H = -\sum_{(ij)} J_{ij}\sigma_i^z\sigma_j^z - \sum_i h_i\sigma_i^x. \tag{7.1}$$

The basic strategy is to find the strongest coupling in the chain (it can be either $\{J_{ij}\}$ or $\{h_i\}$) and minimize the corresponding term in the Hamiltonian. The degrees of freedom associated with this maximum energy scale $\Omega_0 = \max\{J_{ij}, h_i\}$ are then frozen at lower energy scales.

If the strongest coupling is a field, say h_k then the spin σ_k is put in its local ground state, i.e., in the x-direction, causing it to become non-magnetic. Effective interactions are then generated between its nearest neighbors; but, as all other nearby couplings are likely to be much smaller than h_i, these can be treated by second order perturbation theory. This introduces new effective interactions

$$\tilde{J}_{ij} \simeq \frac{J_{ik}J_{kj}}{h_k}, \tag{7.2}$$

where i and j are the nearest neighbors of k.

If the strongest coupling is an interaction, say J_{kl}, then two spins are combined forming a cluster which, in the zeroth order of perturbation theory, has a double degenerate ground state (both up or both down) and thus can be represented again by an effective two-level particle: a new spin. The effective local magnetic field being applied to the cluster (kl) is

$$\tilde{h}_{(kl)} \simeq \frac{h_k h_l}{J_{kl}}, \tag{7.3}$$

which results from the second order perturbation theory, where magnetic fields, acting on two spins are considered to be small.

The magnetization of the cluster will be the sum of magnetization of single spins k and l, i.e., it changes additively $m_{(kl)} = m_k + m_l$. Since all new couplings are smaller than the initial one Ω_0, the energy is rescaled and the maximum energy is reduced (for more details see [126, 127]). Note that the decimation as described above would change the geometry of the system in dimensions higher than $D = 1$, so that we would have to consider the spins to be the vertexes of a somewhat random graph with the RG modifying the spatial structure in these larger dimensions [124, 164].

If the quantum disordered phase is renormalized, the fields eventually tend to dominate the bonds and at small values of Ω almost all decimations are cluster annihilation and the effective interactions connecting them becoming weaker and weaker; in the procedure of the renormalization, the system hence becomes a collection of asymptotically uncoupled clusters with a broad distribution of effective fields. In the ordered phase, in contrast, the interactions tend to dominate the fields at low energies, and most decimations are thus decimations of bonds; eventually this causes an infinite cluster to form. The zero temperature quantum transition between these phases is a novel kind of percolation with the annihilation and aggregation of clusters competing at all energies at the critical point [124, 164, 175, 126, 127].

Before closing this section we would like to point out that the SDRT consists of successive local renormalizations in the real space, where no long range interactions are considered. It means that after an elementary renormalization step the system is described by a Hamiltonian with only nearest neighbors interactions (if one had started with a nearest neighbors interactions Hamiltonian) and no next nearest neighbors appear in the Hamiltonian. Strictly speaking, after every RG step the ground state of the effective Hamiltonian will deviate from the ground state of the initial one, but the error will become asymptotically small in the thermodynamical limit as has been proven by Fisher in [127]. This is the feature we want to retain in our ansatz later on.

7.2.2 The CORE method

The CORE is the Hamiltonian version of the Kadanoff-Wilson real space RG transformation for lattice field theories and lattice spin systems and relies on contraction and cluster expansion techniques. We briefly sketch the main idea of the CORE and how it works and refer to Ref. [109] for details.

The first step in this method is to choose small clusters, elementary blocks which cover the lattice. After that, one picks up some of the clusters (since the CORE was introduced for systems with no disorder and with translation symmetry, all clusters are the same) and considers the part of the whole Hamiltonian that corresponds to this cluster. In what follows we call this part of the Hamiltonian cluster Hamiltonian. For the cluster Hamiltonian one has to choose states that are relevant for the description of physical behavior of the cluster (the number and the form of these states can vary depending on the particular model). The span of the chosen states forms the effective Hilbert space of the cluster. Then a projection P_{eff} on the effective Hilbert space of the cluster is constructed. This projection is used to obtain the so-called range-1 terms of the Hamiltonian expansion ($h_i^{(1)} = P_{eff} H^i_{cluster} P_{eff}$). The range-2 terms arise from the Hamiltonian that corresponds to two adjacent (connected) clusters. The states of the effective Hilbert space of the connected clusters are obtained by taking tensor products of the states single clusters. Afterward a unitary matrix is constructed by means of which the range-2 terms are produced (this matrix is called triangulation matrix [109]). This procedure is iterated to achieve the range-N terms. Finally the expansion of the truncated Hamiltonian, which is

the effective Hamiltonian after single renormalization step is written as

$$H_{\text{eff}} = \sum_i h_i^{(1)} + \sum_{<i,j>} h_{i,j}^{(2)} + \sum_{<i,j,k>} h_{i,j,k}^{(3)} + \cdots \tag{7.4}$$

where $h_{i_1,\ldots i_N}^{(N)}$ stands for range-N term. For more details and rigorous proof that the truncated Hamiltonian can be expanded in this way, we refer the reader to Ref. [109].

Note that for the construction of the range-N terms in the expansion (7.4) one obtains the eigenvalues $\{\epsilon_n\}$ and eigenvectors $\{|n\rangle\}$ by the exact diagonalization of N contiguous clusters. The optimal truncation operator (triangulation matrix) is obtained by a Gram-Schmidt orthogonalization of the eigenvectors of the Hamiltonian projected on the effective Hilbert space. In this way, a basis $\{|\phi_n\rangle\}$ (the remnant eigenstates of the range-N Hamiltonian) is built such that the first vector overlaps with the lowest energy eigenvector and those above, the second one with the second lowest and those above and so on, i.e.,

$$|\phi_n^N\rangle = \sum_{m \geq n} \lambda_m |m\rangle. \tag{7.5}$$

In fact, this reduced basis stems from the QR-decomposition of the overlap matrix between the reduced Hilbert space and the space of exact eigenvectors of the complete Hamiltonian[181].

Usually, two situations can occur after several steps of the renormalization. The Hamiltonian either flows to a point where it can be solved exactly and the correlation length in the effective lattice model goes to zero, or the system is self-similar at every scale, the correlation length diverges and the mass gap goes to zero: at this point, the system is said to be at the critical point.

In summary, the CORE has two major advantages over traditional perturbative real-space renormalization schemes:

- the CORE is not an expansion in weak/strong bonds between block-spins. Its convergence does not necessarily depend on the existence of a large gap to the discarded states of the Hilbert space.
- the CORE is based on an exact mapping form the original Hamiltonian to an effective Hamiltonian, whose truncation error can be estimated numerically by calculating higher orders in the expansion.

Finishing this section we point out that when the Hilbert space dimension is reduced, the CORE provides a good description of the initial states in terms of the renormalized states. In order to estimate the quality of the description of the states from the constructed effective Hilbert space, one can use an overlap of the lowest energy states $|m\rangle$ with the remnant states $|\phi_m^N\rangle$, when the range-N term in the expansion is constructed. Note that both issues are related, as the closer the truncated space is to the exact one, the smaller is the number of terms that should be kept in the cluster expansion for a given error.

7.2.3 Combining the CORE and the SDRT

In this section we provide the idea how to construct a real space renormalization method for two dimensional disordered systems. The details concerning the accuracy of the method are presented in section 7.3.

General idea of the method

The real space RG method we are about to introduce combines the SDRT to target the clusters to be decimated as the ones with the biggest energy gaps and the CORE as a tool to obtain the effective dynamics at a new scale.

To begin with we elaborate on the notion of a renormalization step. A single renormalization step involves one single ladder of the whole lattice with its direct neighborhood, which reflects the fact that each renormalization step is done locally in the lattice. Before we explain how to target the ladder and how to renormalize it, we point out that such renormalization step will preserve the initial rectangular structure of the lattice. In Fig.7.1 we show how a 4×4 lattice looks like before and after the single renormalization step. The region that is involved in the renormalization is marked with green color, the rest of the lattice remains unrenormalized and marked black. Renormalization of the green region results in a chain of effective particles (red dots in Fig. 7.1) and effective couplings either between these effective particles (blue dashed lines in Fig. 7.1) or between the effective particles and their uninvolved neighbors (red dashed lines in Fig. 7.1). Finally one is left with a 3×4 rectangular lattice.

The choice of the ladder occurs according to the position of the local two spin Hamiltonian with the biggest gap between the first an the second excited state. Once this Hamiltonian is found, the whole ladder is renormalized. The criterion of targeting the ladder is arbitrary, but might have an impact on the outcome of the procedure for some Hamiltonians. For example one can target the ladder, which contains a maximal number of local Hamiltonian with a rather big energy gap, albeit the local Hamiltonians with a maximum energy gap does not belong to the ladder. We leave the discussion of the different strategies of the ladder targeting as an open question.

Every renormalization step (renormalization of a ladder with its direct neighborhood) is a sequence of two basic renormalization transformations. In order to see how these basic transformations enter the renormalization, we discuss the renormalization of the ladder in more details. First, the ladder is decomposed into four-spin blocks, such that some of the blocks form chains and some of them form plaquettes (from Fig.7.2 a) to Fig.7.2 b)). The chain terms correspond to the interaction of every rung (two spins) of the ladder to its nearest neighbors. The plaquette terms describe interactions between two rungs inside the ladder. Note that every pair of spins in the ladder (the rung) contributes to two plaquette terms and to one chain term. After the decomposition, each term, representing one of the two basic lattice substructures is renormalized separately using the CORE. This leads to a set of

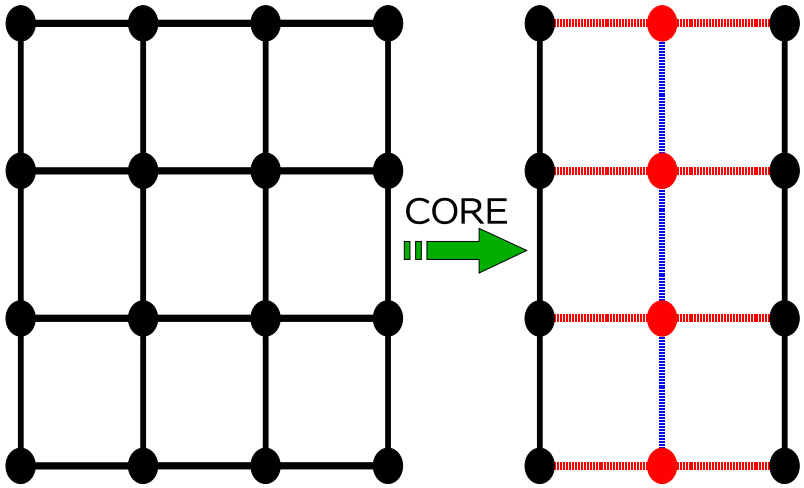


Figure 7.1. *Single renormalization step: renormalization of one ladder with its direct neighborhood in a* 4×4 *lattice (green colored spins and bonds of the* 4×4 *lattice). Red dots are new effective 2-level systems, which interact via effective couplings between each other (blue dashed lines). Note that the ladder is not necessarily a column, it can be also a row of the initial lattice.*

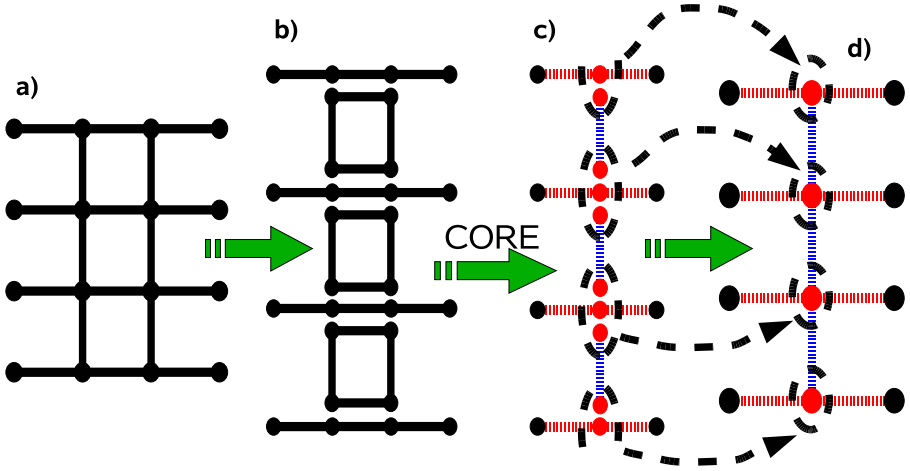


Figure 7.2. *Four essential constituents of the single renormalization step: a) choice of the relevant ladder b) decomposition of the ladder into 4 particle terms: plaquettes and chains c) renormalization of each 4 particle term via CORE d) averaging of the local effective terms (dashed circles) and assembling of the effective Hamiltonians into a renormalized lattice.*

effective 2 and 3 particle Hamiltonians (Fig. 7.2 c)). In the final step the effective Hamiltonians are assembled to the renormalized Hamiltonian on the smaller lattice (Fig. 7.2 d)).

The renormalization step can hence be summarized as follows:

1. Target the ladder with the biggest local energy gap.
2. Define the reduced Hilbert space by the lowest energy sector of every pair of spins in the ladder and the rest of the untouched spins in the lattice.
3. Compute exactly the eigenvalues of the four spin problem (the hardest computational step).
4. Obtain the Hamiltonian on the next scale and rescale the unit of distance and energy.

Repeating renormalization steps, discussed above, will result in a renormalization of the whole spin lattice. The effective Hamiltonian after renormalization will contain less degrees of freedom as the initial one and will be defined on a coarse grained (but still rectangular) lattice.

It is noteworthy that step 2. and 3. of the algorithm rely on an unusual implementation of the CORE method. In the introductory part we mentioned that CORE makes use of a uniform blocking of the lattice (elementary blocks have the same form because of the translational symmetry and used to construct the range-1 terms of the Hamiltonian expansion). Since we now perform the renormalization transformation locally (translational symmetry does not apply in the presence of randomness), we need to introduce a non-uniform blocking. The details of the non-uniform blocking will be discussed on an example in the next section, where a four spin chain is renormalized. In Sec. III, we analyze the performance of the non-uniform blocking in presence of disorder and take a particular type of two-body Hamiltonians which describe spin$-1/2$ particles interaction via Ising type of interaction and exposed to an external magnetic field in transversal direction.

Elementary steps for the successive renormalization transformation.

The elementary renormalization transformations of the four spin terms mentioned above can be divided into two groups.

The first type is renormalization of a plaquette, that results in two new particles and new coupling strengths between them (Fig. 7.3). We use the CORE to renormalize spins in the plaquette configuration. Each pair forms an elementary cluster and used to construct the range-1 term. The interaction between two effective particles is given by the range-2 term.

The second type is a renormalization of 4 spins in a chain configuration (Fig. 7.4). The latter introduces effective interactions to the neighboring spins that increase the accuracy of the method. To use the CORE as it described in Fig. 7.4 we need to

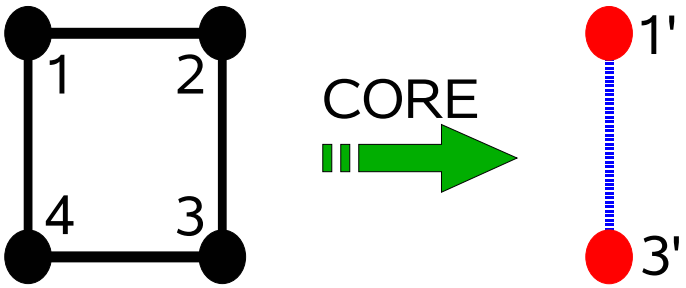


Figure 7.3. *Renormalization of four spins in a plaquette configuration. The renormalization transformation results in two new particles* $1'$ *and* $3'$ *and an interaction between them.*

modify it. That is to say the size of the elementary clusters varies. We call this way of implementation of the CORE - non-uniform blocking. Elementary clusters are formed by central spins and spins on the boundaries. To construct the range-1 terms the initial Hilbert space of the boundary spins are kept, whereas the effective Hilbert space of the central two spins is spanned by the ground state and by the first excited state of the two spin Hamiltonian. The range-2 terms are achieved by constructing the triangulation matrix, while the effective Hilbert space is a tensor product of the Hilbert spaces of two boundary spins and the span of the two lowest eigenstates of the Hamiltonian of two central spins. This modification reflects the fact that the renormalization transformation is local in real space due to intrinsic disorder of the system.

Figure 7.4. *Renormalization of four spins in a chain configuration. The renormalization transformation results in three particles* 1, $2'$ *and* 4. *The interaction between the particles is of the short range character (only nearest neighbors interact).*

7.3 Estimation of long distance and multi-spin interactions

In order to investigate the performance of the elementary renormalization transformations described briefly in section 7.2.3 we pick up a particular model that is a 2D random transverse field quantum Ising model (RTFIM). The Hamiltonian of the 2D RTFIM possesses $\mathbb{Z}_2$-symmetry that can be exploited in the renormalization transformation and provides a special form of the effective Hamiltonian after each

renormalization step (the same observations were made for the 1D Ising model in [109]).

7.3.1 $\mathbb{Z}_2$-symmetry of the 2D Random Transverse Field Ising Model

The 2D RTFIM is described by the Hamiltonian

$$H = -\sum_{(ij)} J_{ij}\sigma_i^z\sigma_j^z - \sum_i h_i\sigma_i^x \tag{7.6}$$

where $\{J_{ij}\}$ are random interactions and the random transverse fields $\{h_i\}$ leading to the quantum fluctuations. The specific form of the distribution will be defined later.

As we explain in the introduction, this Hamiltonian has two different phases. On the one hand, if the strength of the magnetic field is bigger than the interaction, the system is in the quantum disordered phase. On the other hand, if the strength of the interaction dominates over the magnetic field, the system is in the ordered phase. The phase transition between these phases is described by an infinite disorder quantum critical point. In the whole phase diagram, there is a global $\mathbb{Z}_2$-symmetry of the Hamiltonian that any RG transformation should respect. Although this fact is well known, it is also true that real space renormalization group transformations always generate long-range and multi-spin interaction. The most simple and relevant interaction that fulfills all the symmetries of our model is the random transverse field Ising model (Eq. (6)). Nonetheless, in what follows we will see that more general interactions are possible and, in fact, we will use a more general Hamiltonian (see Eq. (8)) that still fulfills all the symmetry properties but can improve the accuracy of the results.

This Hamiltonian is invariant under the transformation $\sigma_i^z \to -\sigma_i^z$ ($\mathbb{Z}_2$-symmetry). The CORE has to preserve this symmetry so that the most general form the renormalized Hamiltonian can take is

$$H_{\text{eff}} = -\sum_{\{\mu\},i} g_{\{\mu\}}\hat{O}_i^{\{\mu\}}, \quad \hat{O}_i^{\{\mu\}} = \sigma_i^{\mu_1}\sigma_{i+1}^{\mu_2}\cdots\sigma_{i+n}^{\mu_n} \tag{7.7}$$

where i is the site index, $\{\mu\} = \{\mu_1, \ldots, \mu_n\}$ is the multi-index ($\mu_i \in \{u, x, y, z\}$) and the $g_{\{\mu\}}$'s are the couplings.

Due to the $\mathbb{Z}_2$-symmetry of the model the only operators that can appear in the one particle Hamiltonian in the cluster expansion are $\{\sigma^0, \sigma^x\}$; in the two particle nearest neighbor interactions, the symmetries allow terms of the form $\{\sigma^z\sigma^z\}$ from the Ising interaction and also $\{\sigma^x\sigma^x, \sigma^y\sigma^y\}$ and the only three site operators that can appear are: $\{\sigma^x\sigma^x\sigma^x, \sigma^x\sigma^z\sigma^z, \sigma^z\sigma^z\sigma^x, \sigma^z\sigma^x\sigma^z, \sigma^x\sigma^y\sigma^y, \sigma^y\sigma^y\sigma^x, \sigma^y\sigma^x\sigma^y, \sigma^x\sigma^0\sigma^x, \sigma^y\sigma^0\sigma^y, \sigma^z\sigma^0\sigma^z\}$. From the above discussion we conclude that the $\mathbb{Z}_2$-symmetry puts certain constrains on the form of the range-N terms that can appear in the expansion of the effective Hamiltonian (7.4).

Exploiting the symmetry arguments we will investigate the relevance of the range-3 and range-4 terms that remain in the expansion (7.4), when the renormalization follows the $\mathbb{Z}_2$-symmetry

$$H_{\text{eff}}^{Ising} = \sum_i h_i^{(1)} + \sum_{<i,j>} h_{i,j}^{(2)} + \sum_{<i,j,k>} h_{i,j,k}^{(3)} + \cdots$$

To achieve the task we will consider several scenarios of non-uniform and uniform blocking in various toy models.

7.3.2 Chain of four spins

First of all we consider a chain of four spins, which after renormalization becomes a chain of three spins (Fig. 7.5). (This step is an essential part of renormalization transformation as discussed in section 7.2.3). The encircled pair of spins and spins on the boundaries of the chain form the range-1 Hamiltonians. The effective Hamiltonian consists of range-1, -2, and -3 terms.

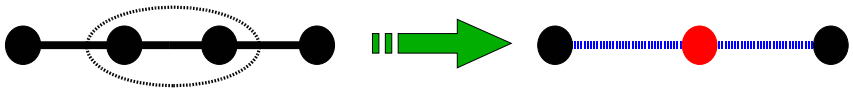


Figure 7.5. *Renormalization of four spins of the RTFIM in a chain configuration using a non uniform blocking. The encircled pair of spins and spins on the boundaries of the chain are used to form range-1 terms for the effective Hamiltonian. The circles on the right hand side of the figure correspond to the range-1 terms in the effective Hamiltonian. These circles are connected by the lines that correspond to range-2 terms.*

Our goal here is to estimate the range-3 terms, which appear in the effective Hamiltonian. There are 10 possible terms in the range-3 Hamiltonian that satisfy the $\mathbb{Z}_2$-symmetry (see section 7.3.1). As our simulations show all this terms are negligibly small in the presence of disorder. In Fig. 7.6 we present the XX (the upper picture) and ZZ (the lower picture) couplings between the first and the third particle of the renormalized chain. The initial couplings were uniformly distributed on the interval $[0, 1]$ and presented statistics were taken after testing 10^5 different configurations. As one can see from the Fig. 7.6 the resulting distributions of both XX and ZZ couplings are symmetric and centered at 0. The standard deviations are 0.704 and 0.746 for XX and ZZ interactions respectively.

7.3.3 Ladder of six spins. Uniform blocking

In our next example we consider a ladder of six spins, that we transform to a chain of three spins using the uniform blocking (Fig. 7.7). The encircled pairs of spins

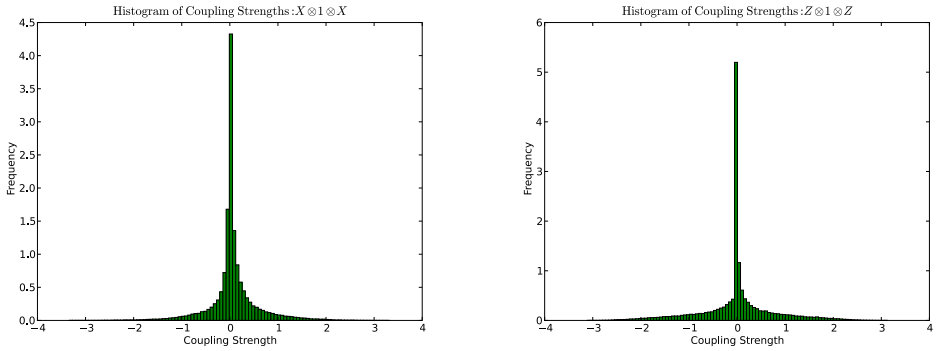


Figure 7.6. *Renormalization of four spins of the RTFIM in a chain configuration using a non-uniform blocking. (Left plot) XX coupling between the first and the third particle.* $\langle \sigma_x \otimes \mathbb{1} \otimes \sigma_x \rangle = 0.041$, $\sigma(\sigma_x \otimes \mathbb{1} \otimes \sigma_x) = 0.704$. *(Right plot) ZZ coupling between the first and the third particle.* $\langle \sigma_z \otimes \mathbb{1} \otimes \sigma_z \rangle = 0.003$, $\sigma(\sigma_z \otimes \mathbb{1} \otimes \sigma_z) = 0.746$.

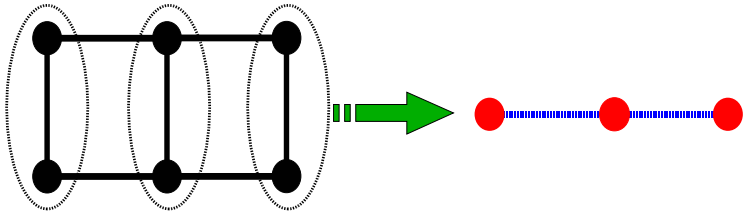


Figure 7.7. *Renormalization of six spins of the RTFIM using a uniform blocking. To form range-1 terms of the effective Hamiltonian the encircled pairs of spins are used. The circles on the right hand side of the figure correspond to the range-1 terms in the effective Hamiltonian. These circles are connected by the lines, that correspond to range-2 terms.*

are taken to form range-1 terms in the expansion of the effective Hamiltonian. As in the previous example the expansion will comprise up to range-3 terms.

In Fig. 7.8 we present the distributions of XX and ZZ coupling strengths between the first and the third particle in the resulting chain. The initial distribution was again a uniform distribution from the interval $[0, 1]$ and we collected statistics after testing 10^5 configurations. As in the previous example both of the resulting distributions have a peak at 0 and standard deviations 0.500 and 0.0996 for XX and ZZ interactions respectively.

7.3.4 Ladder of six spins. Non-uniform blocking

In the last example in this section we consider a ladder of six spins, that one transforms to a plaquette of four spins using a non-uniform blocking (see Fig. 7.9). Two

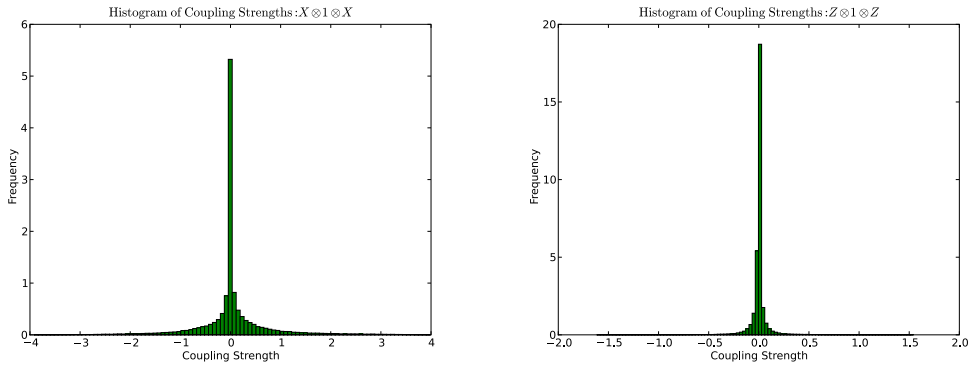


Figure 7.8. *Renormalization of six spins of the RTFIM using a uniform blocking. (Left plot) XX coupling between the first and the third particle. $\langle \sigma_x \otimes \mathbb{1} \otimes \sigma_x \rangle = 0.064$, $\sigma(\sigma_x \otimes \mathbb{1} \otimes \sigma_x) = 0.500$. (Right plot) ZZ coupling between the first and the third particle. $\langle \sigma_z \otimes \mathbb{1} \otimes \sigma_z \rangle = 0.0003$, $\sigma(\sigma_z \otimes \mathbb{1} \otimes \sigma_z) = 0.0996$.*

encircled pairs of spins and two single spins are used to derive the range-1 terms of the effective Hamiltonian. In this case the resulting Hamiltonian will contain also range-4 terms. Our goal here is to show that range-4 terms present in the effective Hamiltonian can be dropped.

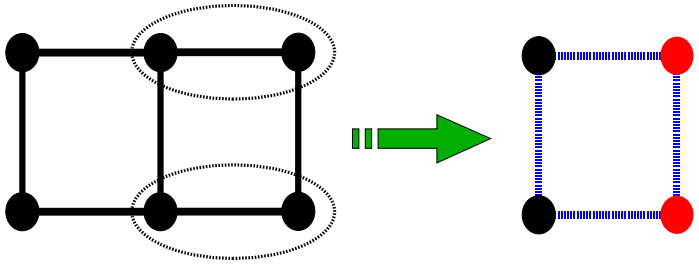


Figure 7.9. *Renormalization of six spins of the RTFIM using a non-uniform blocking. To form range-1 terms of the effective Hamiltonian the encircled pairs of spins and two single spins (the not encircled ones) are used. The circles on the right hand side of the figure correspond to the range-1 terms in the effective Hamiltonian. These circles are connected by the lines, that correspond to range-2 terms.*

In Fig. 7.10 we present statistics for two of the range-4 terms in the effective Hamiltonian, that satisfy the $\mathbb{Z}_2$-symmetry of the Ising model. These terms are $\sigma_x\sigma_x\sigma_x\sigma_x$ and $\sigma_Z\sigma_Z\sigma_Z\sigma_Z$. The mean value of both distributions can be with a good approximation considered to be zero. The standard deviation is 0.823 and 0.240 for the $XXXX$ and $ZZZZ$ term respectively.

Finally, we present analogous statistics for the corresponding range-3 terms (Fig.

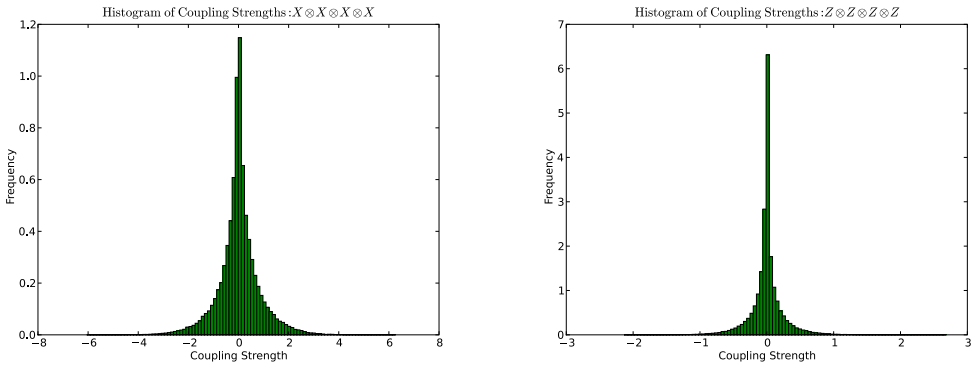


Figure 7.10. *Renormalization of six spins of the RTFIM using a non-uniform blocking. (Left plot) XXXX plaquette coupling of the range-4 term.* $\langle \sigma_x \otimes \sigma_x \otimes \sigma_x \otimes \sigma_x \rangle = 0.024$, $\sigma(X \otimes X \otimes X \otimes X) = 0.823$. *(Right plot) ZZZZ plaquette coupling of the range-4 term.* $\langle \sigma_z \otimes \sigma_z \otimes \sigma_z \otimes \sigma_z \rangle = 0.001$, $\sigma(\sigma_z \otimes \sigma_z \otimes \sigma_z \otimes \sigma_z) = 0.240$.

7.11). These terms correspond to the next nearest neighbor interactions in the renormalized model. We can compare these results with the results of the previous section, where we considered the transformation of the six spin ladder to a three spin chain. The mean value here is 0.034 for XX and 0.032 for ZZ interaction. The corresponding standard deviation is 0.835 and 0.805 for XX and ZZ interactions respectively.

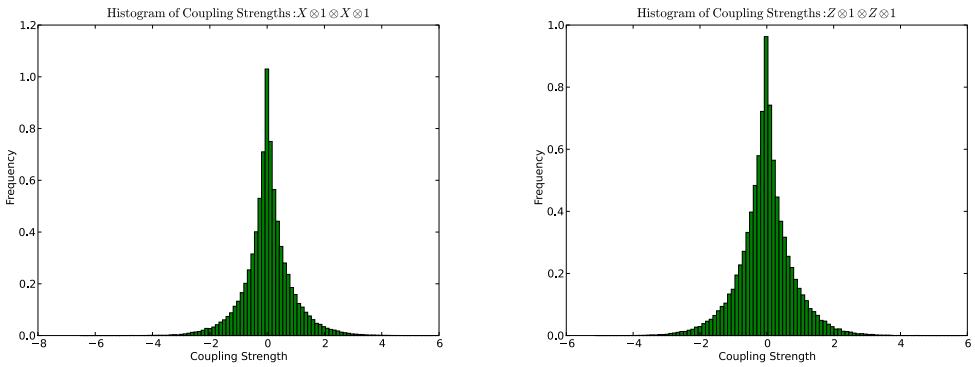


Figure 7.11. *Renormalization of six spins of the RTFIM using a non-uniform blocking. (Left plot) XX coupling between the first and the third particle.* $\langle \sigma_x \otimes \mathbb{1} \otimes \sigma_x \otimes \mathbb{1} \rangle = 0.034$, $\sigma(\sigma_x \otimes \mathbb{1} \otimes \sigma_x \otimes \mathbb{1}) = 0.835$. *(Right plot) ZZ coupling between the first and the third particle.* $\langle \sigma_z \otimes \mathbb{1} \otimes \sigma_z \otimes \mathbb{1} \rangle = 0.032$, $\sigma(\sigma_z \otimes \mathbb{1} \otimes \sigma_z \otimes \mathbb{1}) = 0.805$.

From the presented examples we conclude that one can apply the non-uniform

blocking to perform the renormalization transformation locally in the real space. Our numerical results show that the range-3 and range-4 terms are small and average out and therefore can be neglected in further considerations. Indeed, as it can be seen from our numeric, there are equal number of couplings with negative and positive signs. These contributions cancel each other in average. Since *a priori* no particular distribution of initial couplings was assumed, this fact substantiates the assumption that in the case of appropriate, by means of [127], distribution of couplings the contribution from the long-range interactions to the effective Hamiltonian becomes negligible.

It could, for example, happen that the encircled pair of spins has a non-degenerate ground state and a double degenerate first excited state. This is true if for example both local magnetic fields are much stronger than the coupling. Such situation is unfavorable for the construction of a range-1 term in the expansion of the effective Hamiltonian, since in every range-1 term we keep two states. This, as we believe, is the main source of errors that cause a rather big variance of the distributions of the strengths of range-3 and range-4 terms presented in this section. Now if we assigned a particular coupling strength to each bond and a particular magnetic field to each spin on the lattice, we would avoid the error, and the all range-3 and range-4 terms would turn exactly to zero, which is illustrated by the fact that all of them have an arbitrarily small mean value.

In the renormalization transformation, introduced in this chapter, one chooses a particular part of a lattice (a ladder), that corresponds to a suitable distribution of couplings and magnetic fields. According to previous numerical evidence, this choice allows to write the resulting Hamiltonian after every renormalization step in the form, which contains only range-1 and range-2 terms

$$H_{\text{eff}} = -\sum_{\langle i,j\rangle}\left(J_{ij}^{z}\sigma_i^z\sigma_j^z + J_{ij}^{x}\sigma_i^x\sigma_j^x + J_{ij}^{y}\sigma_i^y\sigma_j^y\right) - \sum_i h_i\sigma_i^x \tag{7.8}$$

with nearest neighbors interactions J and local magnetic fields h_i^x.

Summarizing Subsections B, C and D we point out that the sharp form of the distributions of the long-range terms in Figs. 6, 8, 10, 11 indicates that our method can be applied to the disordered transverse field Ising model. Our conclusion relies on the applicability of the SDRT for two dimensional systems and its exactness in one dimensional systems. However, there is neither theoretical nor numerical justification for dropping out these terms in our method for general type of two-body Hamiltonians. Rigorous treatment of these terms for Ising type of interaction as well as for general type of two body interaction will be left as an open problem.

7.3.5 Renormalization of the basic constituent of the ladder and flow for consecutive steps

In the last part of this section we investigate the performance of the renormalization transformation applied to a toy model, which is a basic constituent of a ladder. In

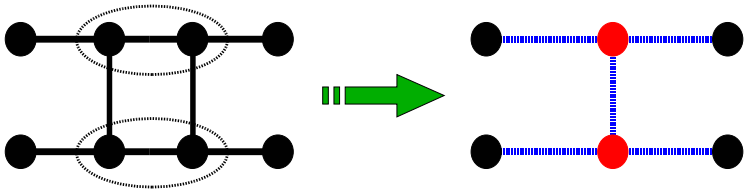


Figure 7.12. *The basic constituent of the renormalization step: two 4-spin chains, whose central spins are coupled. The renormalization involves two central spins of both chains and results in two new spin-$\frac{1}{2}$ particles (red circles) and five effective interactions (blue dashed lines).*

other words we investigate the basic constituent of the renormalization step, as it is described in section 7.2.3.

The toy model is presented in the Fig. 7.12. Two chains of four spins are coupled such that the central spins form two rungs of a ladder. The renormalization transformation involves two rungs, while the boundary spins are kept untouched. The basic renormalized systems consists of six particles that interact as shown in Fig. 7.12. Red circles correspond to effective particles that originate from clustering of two central spins of both chains.

In the Fig. 7.13 we compare the spectra of the initial model (with eigenvalues λ_n^{exact}) and the model after the renormalization (with eigenvalues λ_n^{eff}) and we define the absolute error as $e_n = \frac{|\lambda_n^{\text{exact}} - \lambda_n^{\text{eff}}|}{\lambda_n^{\text{exact}}}$. The absolute error for the first gap is smaller than 10^{-3}. The error grows slightly, as one considers higher energy levels and is of the order of $6 \cdot 10^{-3}$ for the fourth gap. From this observation we conclude that the low energy levels of the initial Hamiltonian are reproduced with a very good accuracy.

So far we have analyzed one component of our suggested renormalization procedure, the statistical properties of the non-uniform CORE method as applied to several typical local lattice systems. We now turn to the statistical properties of the renormalization procedure if all steps are put together, including a choice of ladder to be renormalized, i.e., in the following we subsequently apply non-uniform CORE renormalization steps to ladders that are selected according to the size of the gaps. This procedure implies a concatenation of several renormalization steps, as performed on the local effective systems. Repeating renormalization steps causes a renormalization flow of the (statistical) distribution of coupling strengths. The flow of the couplings is then subject to statistical analysis.

We demonstrate the method using the example of the Ising Hamiltonian with uniform random couplings (as before in the analysis of the local steps) on a 4×4 rectangular lattice. In spite of small size lattice it is possible to perform three consecutive renormalization steps.

Fig. 7.14 depicts the development of the variance of the initial distribution over three successive renormalization steps. We observe a broadening of the distributions.

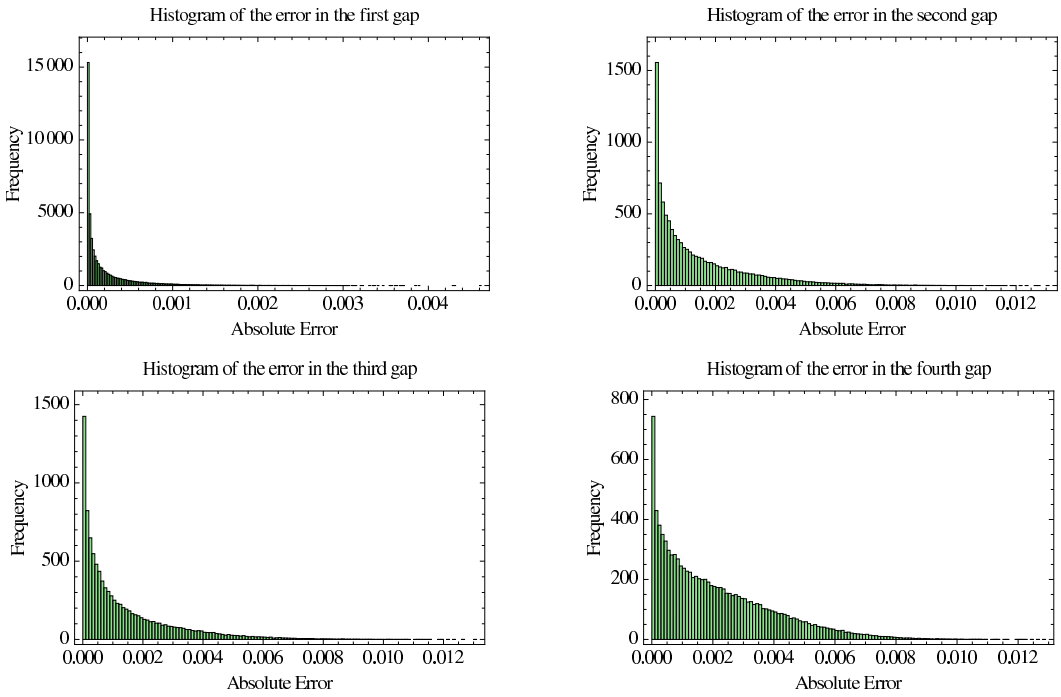


Figure 7.13. *Renormalization of eight spins of the RTIM using a non-uniform blocking. Histograms of the error in the first eigenvalues between the effective Hamiltonian and the exact Hamiltonian. The mean values of the errors that appears in the plots are: first gap* $(2 \cdot 10^{-4})$*, second gap* $(1.4 \cdot 10^{-3})$*, third gap* $(1.4 \cdot 10^{-3})$*, fourth gap* $(2 \cdot 10^{-3})$.

The final outcome, as we believe, indicates a broadening of the initial (in our example uniform) distribution of local magnetic fields and coupling strengths, caused by the renormalization. Therefore, the results presented in Fig. 7.14 indicate that the defined RG method flows towards the infinite randomness fixed point for Ising type of interaction in the Hamiltonian.

7.4 Conclusion

We have introduced a renormalization transformation for disordered systems on 2D lattices that preserves the geometry of the underlying rectangular lattice. The transformation is done using the real space renormalization group method CORE with non-uniform blocking. We tested the ability of the non-uniform blocking on the random Ising Hamiltonian. Our numerical tests showed that the ferromagnetic random Ising model is self-similar, i.e. it can be described again by an Ising model with nearest neighbor interactions and local magnetic fields. This fact is in agreement with the conjecture proposed in the Ref. [164]. Furthermore we argue that there is a rigorous analytical form of the introduced renormalization transformation and that the renormalization flow has a certain fixed point.

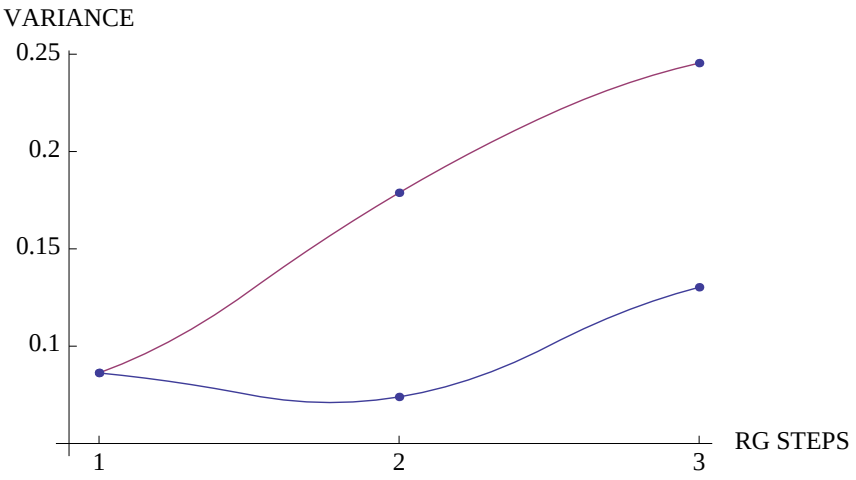


Figure 7.14. *RG evolution of the width of the field distribution (red color) and bond distributions (blue color) for a typical case. The RG evolution is in the direction of decreasing number of spins. Although no conclusive, the increasing width indicates the RG flow towards infinite randomness.*

We close this chapter by mentioning that the method presented in this chapter offers itself to go beyond the usual randomness and investigate models possessing a spin glass phase[165, 166, 170, 174]. Also, since Hamiltonian of a spin model can be used to investigate entanglement properties of the model [173, 67], our method provides also a tool for studying the entanglement in 2D disordered quantum spin models.

Bibliography

[1] A. Einstein, N. Podolski, and N. Rosen, *Phys. Rev.* **47**, 777 (1935).

[2] E. Schrödinger, *Naturwissenschaften* **23**, 807 (1935); **23**, 823 (1935); **23**, 844 (1935).

[3] R. Feynman, *Internat. J. Theoret. Phys*, **21**, 467 (1982).

[4] D. Deutsch, *Proc. Roy. Soc. A*, **400**, 96 (1985).

[5] C. H. Bennett, G. Brassard, *Proc. IEEE Int. Conference on Computers, Systems, and Signal Processing, Bangalore, India*, (1984), `www.research.ibm.com/people/b/bennetc/bennettc198469790513.pdf`.

[6] A. K. Ekert, *Phys. Rev. Lett.*, **67**, 661 (1991).

[7] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wootters, *Phys. Rev. Lett.*, **70**, 1895 (1993).

[8] P. Shor, *SIAM J. Comp.*, **26**, 1484 (1997).

[9] L. Grover, *Phys. Rev. Lett.*, **79**, 325 (1997).

[10] `www.quantenkryptographie.at/`

[11] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, *Phys. Rev. Lett.*, **81**, 5039 (1999).

[12] J.-W. Pan, D. Bouwmeester, M. Daniell, H. Weinfurter, and A. Zeilinger, *Nature*, **403**, 515 (2000).

[13] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood and I. L. Chuang, *Nature*, **414**, 883 (2001).

[14] S. Gulde, M. Riebe, G. P. T. Lancaster, C. Becher, J. Eschner, H. Häffner, F. Schmidt-Kaler, I. L. Chuang and R. Blatt, *Nature*, **421**, 48 (2003).

[15] N. Linden, S. Popescu, *Phys. Rev. Lett.*, **87**, 047901 (2001).

[16] G. Vidal, *Phys. Rev. Lett.* **91**, 147902 (2003).

[17] E. Knill, R. Laflamme, *Phys. Rev. Lett.* **81**, 5672 (1998).

[18] A. Datta, G. Vidal, *Phys. Rev. A* **75**, 042310 (2007).

[19] `http://www.quantiki.org/wiki/index.php/Open_Problems`.

[20] R. A. Horn and C. R. Johnson, *Matrix Analysis*, Cambridge University Press (1985).

[21] R. A. Horn and C. R. Johnson, *Topics in Matrix Analysis*, Cambridge University Press (1991).

[22] R. F. Werner, *J. Math. Phys.* **25**, 1404 (1984).

[23] E. P. Wigner, *Phys. Rev.* **40**, 749 (1932).

[24] R. G. Littlejohn, *Phys. Rep.* **138**, 193 (1986).

[25] Y. Lai, H. A. Haus *Quant. Opt.* **1**, 99 (1989).

[26] W. Son, J. Kofler, V. Vedral, Č. Brukner, *Phys. Rev. Lett.* **102**, 110404 (2009).

[27] R. Raussendorf, H. J. Briegel, *Phys. Rev. Lett.* **86**, 5188 (2001).

[28] R. Raussendorf, D. E. Browne, H. J. Briegel, *Phys. Rev. A* **68**, 022312 (2003).

[29] P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, A. Zeilinger *Nature* **434**, 169 (2005).

[30] C.-Y. Lu, X.-Q. Zhou, O. Gühne, W.-B. Gao, J. Zhang, Z.-S. Yuan, A. Goebel, T. Yang, J.-W. Pan *Nature* **3**, 91 (2007).

[31] M. Gu, C. Weedbrook, N. C. Menicucci, T. C. Ralph, P. van Loock *Phys. Rev. A* **79**, 062318 (2009).

[32] R. F. Werner, M. M. Wolf, *Phys. Rev. Lett.* **86**, 3658 (2001).

[33] G. Giedke, B. Kraus, M. Lewenstein, J. I. Cirac, *Phys. Rev. Lett.* **87**, 167904 (2001).

[34] P. Hyllus and J. Eisert, *New J. Phys.* **8**, 51 (2006).

[35] L. Vandenberghe, S. Boyd, *SIAM Rev.* **38**, 49 (1996).

[36] C. Helmberg, *Eur. J. Oper. Res.* **137**, 461 (2002).

[37] O. Gühne, *Phys. Rev. Lett.* **92**, 117903 (2004).

[38] A. R. Usha Devi, R. Prabhu, A. K. Rajagopal, *Phys. Rev. Lett.* **98**, 060501 (2007).

[39] A. R. Usha Devi, M. S. Uma, R. Prabhu, A. K. Rajagopal, *Phys. Lett. A*, **364**, 203 (2007).

[40] A. Miranowicz, M. Piani, P. Horodecki, R. Horodecki, `quant-ph/0605001`

[41] W. Dür, G. Vidal, J. I. Cirac, *Phys. Rev. A*, **62**, 062314 (2000).

[42] A. Acín, A. Adrianov, L. Costa, E. Jane, J. I. Latorre, R. Tarrach, *Phys. Rev. Lett.*, **85**, 1560 (2000).

[43] F. Verstraete, J. Dehaene, B. De Moor, H. Verschelde, *Phys. Rev. A*, **65**, 052112 (2002).

[44] F. Verstraete, J. Dehaene, B. De Moor, *Phys. Rev. A*, **68**, 012103 (2003).

[45] L. Lamata, J. León, D. Salgado, E. Solano, *Phys. Rev. A*, **74**, 052336 (2006).

[46] L. Lamata, J. León, D. Salgado, E. Solano, *Phys. Rev. A*, **75**, 022318 (2007).

[47] B. Kraus, `arXiv:0909.5152`

[48] A. Acín, D. Bruß, M. Lewenstein, and A. Sanpera, *Phys. Rev. Lett.*, **87**, 040401 (2001).

[49] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, B. M. Terhal, *Phys. Rev. Lett.*, **82**, 5385 (1999).

[50] G. Tóth, C. Knapp, O. Gühne and H. J. Briegel, *Phys. Rev. Lett*, **99**, 250405 (2007).

[51] G. Tóth, C. Knapp, O. Gühne, H. J. Briegel, *Phys. Rev. A* **79**, 042334 (2009).

[52] A. Peres, *Phys. Rev. Lett.*, **77**, 1413 (1996).

[53] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, W. K. Wootters, *Phys. Rev. Lett.*, **76**, 722 (1996).

[54] N. Gisin, *Phys. Lett. A*, **210**, 151 (1996).

[55] M. Horodecki, P. Horodecki, and R. Horodecki, *Phys. Rev. Lett.*, **80**, 5239 (1998).

[56] K. Horodecki, M. Horodecki, P. Horodecki, J. Oppenheim, *Phys. Rev. Lett.*, **94**, 160502 (2005).

[57] P. Horodecki, M. Horodecki, R. Horodecki, *Phys. Rev. Lett.*, **82**, 1056 (1999).

[58] R. Augusiak, P. Horodecki, *Phys. Rev. A*, **74**, 010305(R) (2006).

[59] M. Horodecki, P. Horodecki, and R. Horodecki, *Phys. Lett. A*, **223**, 1 (1996).

[60] P. Horodecki, *Phys. Lett. A*, **223**, 333 (1997).

[61] M. Horodecki, P. Horodecki, *Phys. Rev. A*, **59**, 4206 (1999).

[62] M. A. Nielsen, J. Kempe, *Phys. Rev. Lett.*, **86**, 5184 (2001).

[63] T. Hiroshima, *Phys. Rev. Lett.*, **91**, 057902 (2003).

[64] O. Rudolph, *J. Phys. A: Math. Gen.*, **33**, 3951 (2000).

[65] O. Rudolph, *Phys. Rev. A*, **67**, 032312 (2003).

[66] K. Chen, L, Wu, *Quant. Inf. Comp.*, **3**, 193 (2003).

[67] O. Gühne, G. Tóth, *Physics Reports*, **474**, 1 (2009).

[68] M. D. Reid, P. D. Drummond *Phys. Rev. Lett.*, **60**, 2731 (1988).

[69] L.-M. Duan, G. Giedke, J. I. Cirac, P. Zoller *Phys. Rev. Lett.*, **84**, 2722 (2000).

[70] R. Simon, *Phys. Rev. Lett.*, **84**, 2726 (2000).

[71] H. F. Hofmann, S. Takeuchi *Phys. Rev. A*, **68**, 032103 (2003).

[72] H. F. Hofmann, *Phys. Rev. A*, **68**, 034307 (2003).

[73] M. Barbieri, F. De Martini, G. Di Nepi, P. Mataloni, G. M. D'Ariano, C. Macchiavello, *Phys. Rev. Lett.*, **91**, 227901 (2003).

[74] O. Gühne, *private communications*

[75] J. S. Bell, *Physics*, **1**, 195 (1964).

[76] J. F. Clauser, M. A. Horne, A. Shimony, R. A. Holt, *Phys. Rev. Lett.*, **23**, 880 (1969).

[77] J. F. Clauser, M. A. Horne, A. Shimony, R. A. Holt, *Phys. Rev. Lett.*, **24**, 549(E) (1970).

[78] J. F. Clauser, M. A. Horne, *Phys. Rev. D*, **10**, 526 (1976).

[79] B. S. Cirel'son, *Lett. Math. Phys.*, **4**, 93 (1980).

[80] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, D. J. Wineland, *Nature*, **409**, 791 (2001).

[81] V. Vedral, M. Plenio, M. A. Rippin, P. L. Knight, *Phys. Rev. Lett*, **78**, 2275 (1997).

[82] R. Horodecki, P. Horodecki, M. Horodecki, K. Horodecki, *Rev. Mod. Phys.*, **81**, 865 (2009).

[83] M. J. Donald, M. Horodecki, O. Rudolph, *J. Math. Phys.*, **43**, 4252 (2002).

[84] G. Vidal, R. F. Werner, *Phys. Rev. A*, **65**, 032314 (2002).

[85] S. Hill, W. K. Wootters, *Phys. Rev. Lett.*, **78**, 5022 (1997).

[86] W. K. Wootters, *Phys. Rev. Lett.*, **80**, 2245 (1998).

[87] P. Rungta, V. Bužek, C. M. Caves, M. Hillery, G. J. Milburn, *Phys. Rev. A*, **64**, 042315 (2001).

[88] K. Chen, S. Albeverio, S.-M. Fei, *Phys. Rev. Lett.*, **95**, 040504 (2005), K. Chen, S. Albeverio, and S.-M. Fei, *Phys. Rev. Lett.* **95**, 210501 (2005).

[89] A. C. Doherty, P. A. Parrilo, F. M. Spedalieri, *Phys. Rev. A*, **69**, 022308 (2004).

[90] M. Navascues, M. Owari, M. B. Plenio, `arXiv:0906.2735v1`

[91] L. Gurvits, `quant-ph/0303055`.

[92] L. Ioannou, *Quant. Inf. Comp.* **7**, 335 (2007)

[93] S. Sachdev, *Quantum Phase Transitions*, Cambridge University Press, Cambrigde (2000).

[94] J. Preskill, *J. Mod. Optics*, **47**, 127 (2000).

[95] A. Osterloh, L. Amico, G. Falci, R. Fazio, *Nature*, **416**, 608 (2002).

[96] T. J. Osborne, M. A. Nielsen, *Quant. Inf. Proc.*, **1**, 45 (2002).

[97] T. J. Osborne, M. A. Nielsen, *Phys. Rev. A*, **66**, 032110 (2002).

[98] O. Gühne and G. Tóth, *Phys. Rev. A*, **73**, 052319 (2006).

[99] O. Gühne and G. Tóth, *Appl. Phys. B*, **82**, 237 (2006).

[100] G. Vidal, J. I. Latorre, E. Rico, and A. Kitaev, *Phys. Rev. Lett.*, **90**, 227902 (2003).

[101] J. I. Latorre, E. Rico, G. Vidal, *Quant. Inf. Comp.*, **4**, 048 (2004).

[102] A. R. Its, B.-Q. Jin, V. E. Korepin, *Journal Phys. A: Math. Gen.*, **38**, 2975 (2005).

[103] I. Peschel, *Journal Stat. Mech.*, **P12005**, (2004).

[104] F. Franchini, A. R. Its, V. E. Korepin, *J. Phys. A: Math. Theor.*, **41**, 025302 (2008).

[105] J. Eisert, M. Cramer, M. B. Plenio,arXiv:0808.3773.

[106] L. Amico, R. Fazio, A. Osterloh, and V. Vedral, *Rev. Mod. Phys.*, **80**, 517 (2008).

[107] L. Ts. Adzhemyan, N. V. Antonov, A. N. Vasiliev, *Field Theoretic Renormalization Group in Fully Developed Turbulence*, Gordon and Breach (1999).

[108] M. E. Fisher, *Rev. Mod. Phys.*, **70**, 653 (1998).

[109] C. J. Morningstar, M. Weinstein, *Phys. Rev. D*, **54**, 4131 (1996).

[110] U. Schollwöck, *Rev. Mod. Phys.*, **77**, 259 (2005).

[111] S. Östlund, S. Rommer, *Phys. Rev. Lett.*, **75**, 3537 (1995).

[112] S. Rommer, S. Östlund, *Phys. Rev. B*, **55**, 2164 (1997).

[113] F. Verstraete, D. Porras, J. I. Cirac, *Phys. Rev. Lett.*, **93**, 227205 (2004).

[114] I. Affleck, T. Kennedy, E. H. Lieb, H. Tasaki, *Comm. Math. Phys.*, **115**, 477 (1988).

[115] F. Verstraete, J. I. Cirac, arXiv:cond-mat/0407066.

[116] F. Verstraete, J. I. Cirac, V. Murg, *Adv. Phys.*, **87**, 143 (2008).

[117] G. Sierra, M. A. Martin-Delgado, arXiv:cond-mat/9811170.

[118] Y. Hieida, K. Okunishi, Y. Akutsu, *New J. Phys.*, **1**, 7 (1999).

[119] K. Okunishi, T. Nishino, *Prog. Theor. Phys.*, **103**, 541 (2000).

[120] M. A. Martin-Delgado, M. Roncaglia, G. Sierra, *Phys. Rev. B*, **64**, 075117 (2001).

[121] S. Anders, M. B. Plenio, W. Dür, F. Verstraete, H. J. Briegel, *Phys. Rev. Lett.*, **97**, 107206 (2006).

[122] S. Anders, H. J. Briegel, W. Dür, *New J. Phys.*, **9**, 361 (2007).

[123] R. Hübener, V. Nebendahl, W. Dür arXiv:0904.1925.

[124] F. Igloi, C. Monthus, *Phys. Rep.*, **412**, 277 (2005).

[125] R. Yu, H. Saleur, S. Haas, *Phys. Rev. B*, **77**, 140402(R) (2008).

[126] D. S. Fisher, *Phys. Rev. Lett.*, **69**, 534 (1992).

[127] D. S. Fisher, *Phys. Rev. B*, **51**, 6411 (1995).

[128] E. Shchukin and W. Vogel, *Phys. Rev. Lett.* **95**, 230502 (2005).

[129] O. Gittsovich, O. Gühne, P. Hyllus, J. Eisert, *Phys. Rev. A*, **78**, 052319 (2008).

[130] H. P. Robertson, *Phys. Rev.* **46**, 794 (1934).

[131] A. Vourdas, *Rep. Prog. Phys.* **67**, 267 (2004).

[132] O. Gühne, M. Mechler, G. Tóth, P. Adam, *Phys. Rev. A*, **74**, 010301(R) (2006).

[133] S. Yu, N. Liu, *Phys. Rev. Lett.* **95**, 150504 (2005).

[134] C.-J. Zhang, Y.-S. Zhang, S. Zhang, G.-C. Guo, *Phys. Rev. A*, **76**, 012334 (2007).

[135] C.-J. Zhang, Y.-S. Zhang, S. Zhang, G.-C. Guo, *Phys. Rev. A*, **77**, 060301(R) (2008).

[136] J. I. de Vicente, *Quantum Inf. Comput.* **7**, 624 (2007).

[137] O. Gühne, P. Hyllus, O. Gittsovich, J. Eisert, *Phys. Rev. Lett.* **99**, 130504 (2007).

[138] A. Kent, N. Linden, S. Massar, *Phys. Rev. Lett.* **83**, 2656 (1999).

[139] F. Verstraete, J. Dehaene, B. De Moor, *Phys. Rev. A*, **64**, 010101 (R) (2001).

[140] J.M. Leinaas, J. Myrheim, E. Ovrum, *Phys. Rev. A*, **74**, 012313 (2006).

[141] R. Horodecki, M. Horodecki, *Phys. Rev. A*, **54**, 1838 (1996).

[142] J.I. de Vicente, *Phys. Rev. A*, **75**, 052320 (2007); **77**. 039903(E) (2008).

[143] O. Gühne, M. Lewenstein, *Phys. Rev. A*, **70**, 022316 (2004).

[144] J.I. de Vicente, J. Sánchez-Ruiz, *Phys. Rev. A*, **71**, 052325 (2005).

[145] See,*e.g.* A. N. Kolmogorov, S. V. Fomin, *Introductory Real Analysis*, Dover Publications, Inc. New York (1970).

[146] S. Boyd, L. Vandenberghe, *Convex Optimization*, Cambridge University Press, Cambridge (2004).

[147] D. Bruß, A. Peres, *Phys. Rev. A* **61**, 30301(R) (2000).

[148] A. C. Doherty, P. A. Parrilo, F. M. Spedalieri, *Phys. Rev. Lett.* **88**, 187904 (2002).

[149] O. Gittsovich, O. Gühne, P. Hyllus, J. Eisert, AIP Conf. Proc. **1110**, 63 (2009), *Proceedings of the Ninth International Conference on Quantum Communication, Measurement and Computing, QCMC 2008*, Calgary.

[150] C. Knapp, *Diploma thesis*, University of Innsbruck, February 2009.

[151] P. Krammer, H. Kampermann, D. Bruß, R. A. Bertlmann, L. C. Kwek, C. Macchiavello, *Phys. Rev. Lett.* **103**, 100502 (2009).

[152] G. Giedke, J. I. Cirac, *Phys. Rev. A*, **66**, 032316 (2002).

[153] V. Vedral, M. B. Plenio, *Phys. Rev. A*, **57**, 1619 (1998); M. B. Plenio, *Phys. Rev. Lett.* **95**, 090503 (2005).

[154] E. M. Rains, *Phys. Rev. A*, **60**, 179 (1999); E. M. Rains, *Phys. Rev. A*, **63**, 019902(E) (2001); S. Virmani, M. F. Sacchi, M. B. Plenio, D. Markham, *Phys. Lett. A*, **62**, 288 (2001); Y.-X. Chen, D. Yang, *Quant. Inf. Proc.*, **1**, 5 (2002); T. Hiroshima, M. Hayashi, *Phys. Rev. A*, **70**, 030302(R) (2004).

[155] J.I. de Vicente, *K. Phys. A: Math. Theor.*, **41**, 065309 (2008).

[156] L. Li-Guo, T. Cheng-Lin, C. Ping-Xing, Y. Nai-Ching, *Chinese Phys. Lett.* **26**, 060306 (2009).

[157] A. B. Harris,*J. Phys. C: Solid State Phys.*, **7**, 1671 ((1974).

[158] Y. Imry, S.-K. Ma. *Phys. Rev. Lett.*, **35**, 1399 (1975).

[159] J. Cardy, *Scaling and Renormalization in Statistical Physics*, Cambridge University Press, (2000).

[160] G. Refael, D. S. Fisher, *Phys. Rev. B*, **70**, 064409 (2004).

[161] R. B. Griffiths, *Phys. Rev. Lett.*, **23**, 17 (1969).

[162] B. M. McCoy, *Phys. Rev. Lett.*, **23**, 383 (1969).

[163] C. Pich, A. P. Young, H. Rieger, N. Kawashima, *Phys. Rev. Lett.*, **81**, 5916 (1998).

[164] O. Motrunich, S.-C. Mau, D. A. Huse, D. S. Fisher, *Phys. Rev. B*, **61**, 1160 (2000).

[165] M. Mezard, G. Parisi, M. Virasoro, *Spin Glass Theory and Beyond*, World Scientific Publishing Company (1987).

[166] P. Young, A. P. Young, *Spin Glasses & Random Fields*, World Scientific Publishing Company (1998).

[167] A. H. Castro Neto, G. Castilla, B. A. Jones, *Phys. Rev. Lett.*, **81**, 3531 (1998).

[168] S. Ghosh, T. F. Rosenbaum, G. Aeppli, S. N. Coppersmith, *Nature (London)*, **425**, 48 (2003).

[169] H. Rieger, A. P. Young, *Phys. Rev. B*, **54**, 3328 (1996).

[170] D. Das, B. K. Chakrabarti, editors, *Quantum Annealing and Related Optimization Methods*, Springer-Verlag (2005).

[171] C. Ancona-Torres, D. M. Silevitch, G. Aeppli, and T. F. Rosenbaum, *Phys. Rev. Lett.*, **101**, 057201 (2008).

[172] L. Fidkowski, G. Refael, N. Bonesteel, J. E. Moore, `arXiv:0807.1123v1`.

[173] M. A. Nielsen, I. L. Chuang, *Quantum computation and quantum information*, Cambridge Univ. Press (2000).

[174] L. F. Cugliandolo, D. R. Grempel, C. A. da Silva Santos, *Phys. Rev. B*, **64**, 014403 (2001).

[175] S.-K. Ma, C. Dasgupta, C.-K. Hu, *Phys. Rev. Lett.*,**43**, 1434 (1979).

[176] M. S. Siu, M. Weinstein, *Phys. Rev. B*,**75**, 184403 (2007).

[177] E. Altman, A. Auerbach, *Phys. Rev. B*,**65**, 104508, (2002).

[178] E. Berg, E. Altman, A. Auerbach, *Phys. Rev. Lett.*,**90**, 147204 (2003).

[179] R. Budnik, A. Auerbach, *Phys. Rev. Lett.*,**93**, 187205 (2004).

[180] S. Capponi, A. Lauchli, M. Mambrini, *Phys. Rev. B*,**70**, 104424 (2004).

[181] M. S. Siu, M. Weinstein, *Phys. Rev. B*,**77**, 155116 (2008).

[182] A. Auerbach, `arXiv:cond-mat/0510738v1`.

[183] S. Capponi, `arXiv:cond-mat/0510785v1`.

[184] A. Abendschein, S. Capponi, *Phys. Rev. B*,**76**, 064413 (2007).

LIST OF PUBLICATIONS

- O. Gühne, P. Hyllus, O. Gittsovich, J. Eisert,
  Covariance matrices and the separability problem,
  Phys. Rev. Lett. 99, 130504 (2007), `quant-ph/0611282`

- O. Gittsovich, O. Gühne, P. Hyllus, J. Eisert,
  Unifying several separability conditions using the covariance matrix criterion
  Phys. Rev. A, 78, 052319 (2008), `arXiv:0803.0757`

- O. Gittsovich, O. Gühne, P. Hyllus, J. Eisert,
  Covariance matrix criterion for separability
  AIP Conf. Proc. **1110**, 63 (2009),
  Proceedings of the *Ninth International Conference on Quantum Communication, Measurement and Computing, Calgary 2008 (QCMC)*

- O. Gittsovich, R. Hübener, H. J. Briegel, E. Rico,
  Local renormalization method for random systems
  `arXiv:0908.1312`, accepted to *New J. of Physics*

- O. Gittsovich, O. Gühne,
  Quantifying entanglement with covariance matrices
  `arXiv:0912.3018`

DANKSAGUNG

In erster Linie möchte ich mich bei meinen Betreuern Prof. Dr. Hans J. Briegel und Dr. Otfried Gühne bedanken, die die Ducrhführung dieser Arbeit durch ihre moralische und finanzielle Unterstützung ermöglicht haben.

Ein besonderer Dank gebührt Dr. Otfried Gühne. Seine Ideen, Ratschläge und steter Optimismus zum Gelingen meiner Arbeit beigetragen haben. Er war immer bereit meine Fragen zu beantworten unabhängig davon, ob diese Fragen wissenschaftlichen Inhaltes waren oder den Alltag betrafen.

Außerdem möchte ich Dr. Matthias Kleinmann, Sönke Niekamp, Bastian Jungnitsch für die mühsamste Arbeit, nämlich für das Korrekturlesen meiner Arbeit danken. Ein Dank gilt auch anderen Mitgliedern der Arbeitsgruppe Briegel, mit denen man sich abseits des universitären Alltags treffen und unterhalten konnte.

Ein Dank gilt auch natürlich meiner Lebensgefärtin Kasia, die mir in moralischer Hinsicht während des gesamten Enstehungsprozesses dieses Werkes beiseite stand und dadurch die Weiterarbeit erleichtete.

Zuletzt danke ich meinen lieben Eltern, ohne deren Unterstützung mein wissenschaftlicher Werdegang gar nicht möglich wäre.