On multipartite symmetric states in Quantum Information Theory

Der Gemeinsamen Naturwissenschaftlichen Fakultät
der Technischen Universität Carolo-Wilhelmina
zu Braunschweig
zur Erlangung des Grades eines
Doktors der Naturwissenschaften
(Dr. rer. nat.)
genehmigte
Dissertation

von Tilo Eggeling

aus Bad Harzburg

1.Referent: Prof. Dr. Reinhard F. Werner
2.Referent: Prof. Dr. Martin Wilkens
Eingereicht am: 16. Januar 2003
Mündliche Prüfung (Disputation) am: 2. April 2003

Druck: 2003

Teilergebnisse aus dieser Arbeit wurden mit Genehmigung der Gemeinsamen Naturwissenschaftlichen Fakultät, vertreten durch den Mentor der Arbeit, in folgenden Beiträgen vorab veröffentlicht:

Publikationen

- T. Eggeling, R. F. Werner: *Separability properties of tripartite states with $U \otimes U \otimes U$ symmetry,* Phys.Rev.A **63** 042111.
- T. Eggeling, R. F. Werner: *Hiding classical data in multipartite quantum states,* Phys.Rev.Lett. **89** 097905.

Eine vollständige Publikationsliste befindet sich auf Seite 149.

Tagungsbeiträge

- T. Eggeling, R. F. Werner: *Separabilitätseigenschaften von $U \otimes U \otimes U$-invarianten Zuständen dreigeteilter Systeme,* (Vortrag), DPG Frühjahrstagung 2000, Fachverband Theoretische und Mathematische Grundlagen der Physik, Dresden (Germany), 20.–24.03.2000.
- T. Eggeling, R. F. Werner: *Separability properties of tripartite states with $U \otimes U \otimes U$ symmetry,* (Poster), Coherent Evolution in noisy Environments, MPI für Physik komplexer Systeme, Dresden (Germany), 20.–25.05.2001.
- T. Eggeling, R. F. Werner: *Separability properties of tripartite states with $U \otimes U \otimes U$ symmetry,* (Poster), 2$^{\text{nd}}$ ESF QIT Conference, Gdansk (Poland), 10.–18.07.2001.
- T. Eggeling, R. F. Werner: *Hiding classical data in multipartite quantum states,* (Poster), QRandom II, MPI für Physik komplexer Systeme, Dresden (Germany), 27.01.–01.02.2002.
- T. Eggeling, R. F. Werner: *Hiding classical data in multipartite quantum states,* (Vortrag), DPG Frühjahrstagung 2002, Fachverband Quantenoptik, Osnabrück (Germany), 04.–08.03.2002.
- T. Eggeling, R. F. Werner: *Hiding classical data in multipartite quantum states,* (Poster), International Conference on Quantum Information, Oviedo (Spain), 13.–18.07.2002.
- T. Eggeling, R. F. Werner, M. M. Wolf: *Optimizing the "residual bipartite fidelity" in multipartite systems,* (Vortrag), ESF workshop IQING, London (UK), 19.–22.09.2002.

Introduction

More than 50 years after its publication, Shannon's "*A mathematical theory of communication*" [Sha48] still influences today's physics. In the late 50s Jaynes [Jay57a, Jay57b] succeeded in describing statistical mechanics from an information theoretical point of view by using the method of maximum-entropy inference (nowadays called Jaynes' principle). The reconciliation of information theory and quantum theory, however, took much longer. The starting point was given by Benioff in 1980 ([Ben80], see also [Deu85, Fey86]) where he gave a description of a Hamiltonian that can be interpreted as a Turing machine. The vision of the quantum computer was born. In the following years the capabilities of a quantum computer like the exponentially growing speed-up in factorizing large numbers (Shor's algorithm [Sho94]) or in database searches (Grover's algorithm [Gro96]) and the phenomenon of quantum teleportation (see [BBC$^+$93]) led to an almost exponential interest in quantum computing from the military and the industrial side. Recently, various proposals have been made on how to build such a quantum computer. They involved ion traps, liquid NMR, quantum dots and optical lattices. However, nowadays it seems as if for the next ten years the quantum computer may remain a vision like the Holy Grail due to the immense experimental demands.

Fortunately, in the light of this vision quantum information theory evolved meanwhile to a large independent field of research. It has become a widely structured field involving physicists, mathematicians, computer scientists and electrical engineers. Its main pillars are quantum computing, quantum communication and entanglement theory.

Quantum computation is concerned with the development of quantum circuits and algorithms for future quantum computers. Latest developments concern the hidden subgroup problem and search algorithms. Methods of translating algorithms into quantum circuits have already been developed. One of the major challenges is now to develop good error correcting codes for arbitrary systems.

Quantum communication comprises various communication protocols that have been developed for or adapted to quantum information. Among the best known protocols are quantum key distribution, quantum teleportation and superdense coding. Quantum key distribution was the first application of quantum information to be realized in experiments. In fact, first implementations are already available commercially (see www.idquantique.com).

Entanglement has been revalued by quantum information theory from a fundamental property of quantum systems to a new resource which may be used up or used as a catalyst in quantum information processing. It is the glue that connects the various elements of quantum information theory and at the same time the most important new ingredient that enables us to perform new quantum protocols. In 1935 Schrödinger [Sch35] coined the German word "Verschränktheit" for a mysterious inseparability he encountered while investigating states of compound systems. What he and Einstein, Podolsky and Rosen (see [EPR35]) had found was the first instance of quantum correlations among particles/parties. In the last few years, a growing interest has been devoted to the theory of entanglement. Most of the results were obtained for low dimensional systems (e.g. qubits) and for systems that could be simplified making use of symmetries.

This thesis is devoted to the study of entanglement in multipartite systems. The characterisation of general multipartite states involves approximately d^{2N} real parameters, where d is the dimension of the single system and N is the number of systems. In order to be able to investigate entanglement properties in multipartite systems, in chapter 2 we therefore introduce families of multipartite states that can be described with only few parameters. As a tool we use symmetry groups to reduce the complexity of the problem. In chapter 3 we characterize the separability/inseparability properties of this state family in the special case of $N = 3$. Chapters 4 and 5 are concerned with the operational aspects of the entanglement contained in these states. In chapter 4 we use the introduced states, amongst other things, to demonstrate the security of multipartite quantum data hiding and to give a constructive scheme of this protocol. The last chapter relates entanglement sharing to quantum telecloning.

Note to the reader: The experienced reader may skip the first chapter which contains a very short overview of the concepts and mathematical tools used in the following chapters. Chapters 3, 4 and 5 are based on chapter 2 and can be read separately. A short summary of the results presented in this thesis can be found on page 137.

Contents

Chapter 1

Basic concepts

> "Eh bien, l'algèbre est un outil, comme la charrue ou le marteau, et un bon outil pour qui sait l'employer."
>
> (Jules Verne, *Autour de la Lune*)

Quantum information theory can be seen as 'ordinary' quantum theory from an information theoretical point of view. Many new aspects of quantum theory arise from the peculiar quantum nature of quantum information. Especially the rise of entanglement from the hidden depths of the foundations of quantum theory to a central ingredient of quantum information theory shows that they are worth being studied beyond the level of standard quantum theory textbooks.

The purpose of this chapter is to provide the basic notions of quantum theory and the mathematical tools as they will be used throughout this thesis.

1.1 States and state transformations

In most textbooks states are described as wavefunctions and transformations are given by some Hamiltonian dynamics. All influences are modelled by a corresponding Hamilton operator leading to an invertible time evolution of the states. However, this is only true as long as one can assume the system to be closed, i.e. as not interacting with an external environment. Since the general situation in quantum information involves the interaction with an active environment causing decoherence (e.g. a heat bath or some experimentalists), we start by recalling the more general formulations (see [Per93, Lud76]).

1.1.1 States and measurements

In the framework of quantum theory every system of degrees of freedom is described by a separable complex Hilbert space[1] $\mathcal{H}$. For example a system with a finite number f of discrete degrees of freedom like a spin is assigned the Hilbert space $\mathcal{H} = \mathbb{C}^f$ with the usual scalar product $\langle\psi|\varphi\rangle = \sum_{i=1}^{f} \overline{\psi}_i \varphi_i$. Every system can be prepared in various ways corresponding to different configurations x of some set of configurations X. A measurement corresponds to a test whether the system in question has a certain property y out of some set of properties Y. Since quantum theory is a statistical theory it describes only the statistics of the outcome of a measurement, i.e. it gives the probability $p(y|x)$ of the outcome y (the system has property y) given that the system was prepared according to x. A state describing a preparation procedure $x \in X$ is assigned a positive operator $\rho_x \in \mathcal{B}(\mathcal{H})$ with $\mathrm{tr}[\rho_x] = 1$ called density operator which is sometimes identified with the state itself. The tests are modelled by a positive operator valued measure (POVM) called observable, that is a set of positive operators $\{M_y | y \in Y\} \subset \mathcal{B}(\mathcal{H})$, respecting the completeness condition $\sum_{y\in Y} M_y = \mathbb{1}$. The probabilities are then given by

$$p(y|x) = \mathrm{tr}[M_y \rho_x]. \tag{1.1}$$

A statistical mixture ρ_{sm} of states $\{\rho_i\}$ is described by a convex combination of the corresponding density operators:

$$\rho_{\text{sm}} = \sum_i \lambda_i \rho_i \quad \text{where} \quad \lambda_i \geq 0, \quad \sum_i \lambda_i = 1 \tag{1.2}$$

giving the set of states $\mathcal{S}(\mathcal{H})$ the structure of a convex set. Conversely, not all states can be written as a convex combination. In fact, there are states that are special in the sense that they cannot be decomposed into a convex combination of other states. These states are called extremal as they are the extremal points (see [Roc72]) of the convex set $\mathcal{S}(\mathcal{H})$. For finite dimensional Hilbert spaces they correspond to rank

[1] A Hilbert space is said to be separable if it has a countable dense subset. In Hilbert spaces lacking this property the superposition principle is no longer valid (see [Per93]).

one projections. Such projections encode the sharpest possible preparation procedures and are thus called *pure* states. These density operators can be written as

$$\rho_{\text{pure}} = |\psi\rangle\langle\psi| \tag{1.3}$$

for some vector $|\psi\rangle \in \mathcal{H}$. In this formulation all vectors $e^{i\varphi}|\psi\rangle$, $\varphi \in \mathbb{R}$ are equivalent in the sense that they lead to the same density operator ρ_{pure} so that they can be collected into a ray. Thus pure states correspond to such a ray, rather than to a vector in Hilbert space.

A set of two independent systems is modelled by the tensor product of the single Hilbert spaces[2]: $\mathcal{H}_{A\&B} = \mathcal{H}_A \otimes \mathcal{H}_B$. This formulation of independence is motivated by the fact that a tensor product of measurements on such independently prepared subsystems leads to the product of the single probabilities as known from the description of classical independent probability distributions:

$$\operatorname{tr}[(M_i \otimes N_j)(\rho_1 \otimes \rho_2)] = \operatorname{tr}[M_i\rho_1]\operatorname{tr}[N_j\rho_2]. \tag{1.4}$$

More generally, one can give a description of the state of a subsystem even in the case that the subsystems have not been prepared independently. For this, one only has to ignore the outcomes of measurements on the other subsystems to get a description of the subsystem of interest:

$$\sum_{j\in J} \operatorname{tr}[\rho(M_i \otimes N_j)] = \operatorname{tr}[\rho(M_i \otimes \mathbb{1})] \overset{\text{def}}{=} \operatorname{tr}[\rho_A M_i]. \tag{1.5}$$

The density operator ρ_A is called the reduced density operator and corresponds to the analogue of a marginal probability distribution induced by the state of the compound system. In the case of a pure state of a compound system the reduced states are not necessarily pure. This can be seen easily by looking at a bipartite system. Any vector $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ can be written with respect to a product basis as $|\psi\rangle = \sum_{i,j}^{d_1,d_2} \psi_{i,j}|e_i \otimes f_j\rangle$. In the special situation of a bipartite system it is possible to "diagonalize[3]" the coefficient matrix $\psi_{i,j}$ giving an even simpler description:

$$|\psi\rangle = \sum_{i=1}^{\min(d_1,d_2)} \lambda_i |e_i \otimes f_i\rangle \qquad \lambda_i \geq 0. \tag{1.6}$$

[2] The field underlying the Hilbert space of a quantum theory is closely connected to the notion of statistical independence. Using a complex field leads to the tensor product for independent systems in contrast to a real field (see [Fuc02]).

[3] In the case of a rectangular matrix it can be brought into diagonal form plus zero rows or columns.

For any vector on a bipartite system this so-called Schmidt decomposition (see [Sch07]) exists and is unique up to a relabelling of the elements. Using this representation the reduced density operator of an arbitrary pure state of a bipartite system reads $\rho_A = \sum_{i=1}^{d_1} \lambda_i^2 |e_i\rangle\langle e_i|$. Conversely one can *purify* an arbitrary mixed state of a single system to a pure state on a larger compound Hilbert space as long as the second subsystem is chosen to be large enough. Taking the spectral decomposition of the mixed state as $\rho = \sum_i \lambda_i^2 |\psi_i\rangle\langle\psi_i|$ one directly gets a purification via $|\varphi\rangle = \sum_i \lambda_i |\psi_i \otimes \psi_i\rangle$. This purification is of course not unique since one can choose the dimension of the ancillary Hilbert space arbitrarily as long as it is larger than or equal to that of the original system.

Analogously, one can purify a POVM to a projective measurement on a larger compound system. For an m-valued POVM one needs an ancillary system of dimension m or greater for the purification. The POVM elements M_i can be seen as the reduced operators of the ith projection on the compound system (Naimark's dilation theorem, see [Hol82]).

For systems composed of more than two subsystems the Schmidt decomposition does not exist in general. In very special cases there exists a multiorthogonal[4] decomposition, which is then unique [EB94].

1.1.2 State transformations

Often the system of interest is in some way coupled to its environment. The evolution of the closed system, i.e. subsystem plus environment, can then be described within the well-known Hamiltonian formalism. In this case the Hamilton operator H generates a unitary time evolution:

$$\rho_{t_0+t} = U_t \rho_{t_0} U_t^*, \qquad U_t = e^{iHt}. \tag{1.7}$$

Ignorance of the environment leads to a non-unitary (and thus not necessarily invertible) time evolution for the reduced state that can be modelled with a Lindblad form, which is sometimes called the master equation (e.g. in quantum optics) [Lin76]. However, this is still not the most general description of a state transformation as it does not take

[4] One of the properties of the Schmidt decomposition is that the corresponding bases $\{e_i\}$ and $\{f_j\}$ are biorthogonal, that is $\langle e_i|e_{i'}\rangle = \delta_{i,i'}$ and $\langle f_j|f_{j'}\rangle = \delta_{j,j'}$. Similarly, one can try to decompose a pure multipartite state into tensor products of vectors forming "sitewise" an orthonormal basis.

into account that the system itself may be transformed (e.g. a two-level system into a three-level system).

From an abstract point of view a *state transformation* $T: \mathcal{S}(\mathcal{H}_1) \to \mathcal{S}(\mathcal{H}_2)$ has to be a positive linear trace preserving map. Positivity and trace preservation ensure that the outcome is again a density operator. Linearity is necessary for the statistical mixture of states to be consistent[5]. Now since the system under consideration can be a subsystem of a larger one, positivity is not enough to guarantee that the outcome is a valid state. In fact, it may well be that the map transforms the reduced density operator correctly, but to be in compliance with the interpretation as a marginal probability distribution it also has to transform the overall state correctly. For this we have to demand complete positivity of the map T, i.e. $T \otimes id_n$ has to be positive for all $n \in \mathbb{N}$. In quantum information theory such completely positive linear trace preserving maps have been called *channels* in analogy to classical information theory. The quantum information of the input system $\mathcal{H}_1$ is processed by the channel and encoded into the output system $\mathcal{H}_2$:

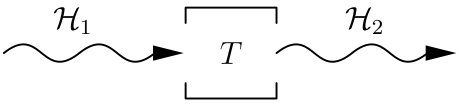


Figure 1.1: Black box picture of a quantum channel.

By Kraus' representation theorem a channel $T: \mathcal{S}(\mathcal{H}_1) \to \mathcal{S}(\mathcal{H}_2)$ can be mathematically described by a set of operators $K_i: \mathcal{H}_1 \to \mathcal{H}_2$ (Kraus operators) such that

$$T(\rho) = \sum_{i=1}^{N} K_i \rho K_i^*, \qquad \sum_{i=1}^{N} K_i^* K_i = \mathbb{1}, \tag{1.8}$$

where $N \leq \dim \mathcal{H}_1 \dim \mathcal{H}_2$ Kraus operators suffice for modelling an arbitrary channel T (see [Kra83]). However, this representation is not unique. Different sets of Kraus operators can describe the same channel. The concept of a channel is very versatile. In fact all kinds of operations (see below) can be described as special channels. A measurement is a channel converting quantum into classical information.

[5] If we assume that the quantum dynamics is not linear, the evolved mixed state is not the mixture of the evolved states and we lose the interpretation of "mixture". Such nonlinear quantum theories are usually nonlocal in the sense that they admit superluminal signalling (see for instance [SBG01]).

Classical information can be converted into quantum information by a parameter dependent preparation. An instrument is a channel that gives classical and quantum information from a quantum input.

The standard situation in quantum information is that a compound system is being manipulated by various experimentalists in separate laboratories. These manipulations called *protocols* or *operations* build a second pillar of quantum information theory besides entanglement. Depending on the amount, kind and direction of communication among the different parties, there are different classes of protocols:

> **LOCC:** If the parties are allowed to communicate only classically and to do only local operations the protocol is said to be of LOCC type (**L**ocal **O**perations and **C**lassical **C**ommunication).
>
> **PPT:** A protocol respecting the positivity of the partial transpose (see 1.2.2) is called PPT.
>
> **1-way q/c:** If the parties are allowed to transmit quantum/classical information in one direction the protocol is called a one-way quantum/classical communication protocol.
>
> **2-way q/c:** Analogously if the parties are allowed to exchange quantum/classical information freely in both directions the protocol is said to be a two-way quantum/classical communication protocol.

Proper mathematical characterizations of all these classes are not always possible. The LOCC protocols for example could involve an infinite number of rounds of classical information transmission from one party to another where each round could then depend on the information transmitted in all the preceding rounds. Nevertheless a few facts are known:

1. All these classes are closed under concatenation if the direction of the communication is maintained for 1-way protocols.
2. The LOCC class is a strict subset of the PPT class (see chap. 4).
3. The 1-way classes are by definition a strict subset of the 2-way classes which can be obtained by concatenating 1-way protocols with different directions.
4. 1-way quantum communication is equivalent to shared entanglement plus 1-way classical communication.

The last fact is maybe the most surprising one. It stems from the protocol known as quantum teleportation. This protocol describes how to use a shared maximally entangled pair (i.e. a quantumly correlated state, see (1.12)) together with 1-way classical communication to teleport an unknown quantum state without transmitting the quantum system itself [BBC$^+$93].

1.1.3 Duality of states and state transformations

One new aspect of quantum theory due to quantum information is a very intimate relation between channels and bipartite states. In fact there is a very useful one-to-one mapping translating between them which is sometimes referred to as the Jamiołkowski-dualism (see [Jam72]):

Lemma 1.1.1: Let ρ be a state on $\mathcal{H} \otimes \mathcal{K}$. Then there are a Hilbert space $\mathcal{H}'$, a pure state σ on $\mathcal{H} \otimes \mathcal{H}'$ and a channel $T\colon \mathcal{B}(\mathcal{K}) \to \mathcal{B}(\mathcal{H}')$ such that

$$\rho = (\mathrm{id}_{\mathcal{B}(\mathcal{H})} \otimes T)[\sigma]. \tag{1.9}$$

If the restriction of σ to $\mathcal{H}'$ is chosen to be non-singular this decomposition is unique up to unitary equivalence. That is, any other decomposition $(\mathrm{id}_{\mathcal{B}(\mathcal{H})} \otimes T')[\sigma']$ is of the form $\sigma' = U\sigma U^*$ and $T'[X] = U^*T[X]U$ with some unitary operator U.

(See [Wer01b] for a proof.) Now fixing the pure state σ to be e.g. a maximally entangled state $|\psi_+\rangle$ (see (1.12) below) leads to a one-to-one correspondence of states ρ and channels T (see subsection 5.2.1 for an example).

Results of the entanglement theory of bipartite systems can thus be translated to results on channels: Separable channels correspond to separable states, PPT preserving channels to PPT states, isotropic states to depolarizing channels, Werner states to depolarizing channels followed by a transposition and so on.

1.2 Classical and quantum correlations

Any interaction between independently prepared subsystems usually destroys the statistical independence. Let us take for example two independently prepared spin-$\frac{1}{2}$ particles. If we let them interact via an Ising- or Heisenberg-type interaction they may become correlated in the sense that the outcomes of measurements performed on the single spins may be correlated due to the past interaction.

The classification and quantification of these correlations is known as the theory of entanglement. Their exploitation for new protocols was the starting point of quantum information theory. In recent years the aspect of entanglement as a resource has led to a growing knowledge of entanglement: It is needed for performing certain protocols, it can be used up and sometimes even returned just like a catalyst. In the following subsections we will summarize the classification of these correlations and some means to measure their strength.

1.2.1 Classical vs. quantum correlations

In 1964 John Bell noticed that there was more to these correlations between quantum mechanical subsystems than what was known from classical probability distributions. He was able to derive an inequality that any local classical model must satisfy [Bel64]. However, with a simple computation he showed that quantum theory can violate it. This inequality was turned into a key experiment for the validity of quantum theory. First reliable experimental tests were performed by Aspect [AGR81] in 1981 supporting quantum theory.

The violation of Bell's inequality was the first proof that quantum theory is capable of correlating subsystems in a much "stronger" way than classical theories can. Since then the threshold given by the inequality was used to distinguish between classical correlations, i.e. correlations that can be described by a local classical model, and quantum correlations. In 1989 Werner [Wer89] gave a mathematical characterization of those states that contain only classical correlations. He called a state classically correlated (separable[6]) iff (if and only if) it can be approximated (e.g. in trace norm) by density matrices of the form:

$$\rho = \sum_i p_i \rho_i^{(1)} \otimes \rho_i^{(2)}, \qquad \forall i\colon p_i \geq 0, \quad \sum_i p_i = 1. \tag{1.10}$$

Conversely any state that cannot be approximated in this way is called entangled[7]. This definition of "classically correlated" states is intuitive since any such state can be prepared in the following way: Take

[6] The term separable was introduced by [Hor94] in the context of informationally coherent systems and has nothing to do with the separability of the underlying Hilbert space.

[7] In 1935 Schrödinger coined the term "verschränkt" for it (see [Sch35]).

two independent laboratories and one joint random number generator characterized by the probability distribution $\{p_i\}$. The random numbers are then communicated to both laboratories. Depending on these numbers the experimentalists (Alice and Bob) perform parameter dependent preparations of their systems preparing the states $\rho_i^{(1)}$ and $\rho_i^{(2)}$ respectively. The state of the composite system is then of the form (1.10) and was clearly prepared using classical correlations only (see figure 1.2).

States showing the strongest classical correlations possible are called *maximally correlated* and have the form[8]:

$$\rho = \sum_{i,j} \alpha_{ij} |ii\rangle\langle jj|, \tag{1.11}$$

with a hermitian α with unit trace (see [Rai99]). In fact, if Alice and Bob share such a state they will always obtain the same results for any measurement. Analogously there are states that are maximally quantum correlated called *maximally entangled*. The prototype of such a maximally entangled state is

$$|\psi_+\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |ii\rangle. \tag{1.12}$$

Both notions can be extended to multipartite states in a natural way.

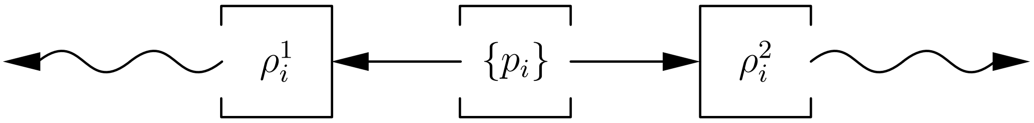


Figure 1.2: Black box picture of a preparation procedure for separable states.

In the same article Werner proved that the set of states obeying Bell's inequality and the set of classically correlated states are not identical, i.e. there are entangled states that admit a local classical model. As a first example he constructed a family of states (nowadays called Werner states) for which we could easily compute the maximal violation of Bell's inequality (see subsection 3.2.2) and check the separability. Both tasks, the computation of the maximal violation of Bell's

[8] We slightly abuse the notation and write for short $|ij\rangle$ instead of $|i\rangle \otimes |j\rangle$ or $|i \otimes j\rangle$.

inequality and the separability check in general are hard to accomplish and in the special case of Werner states were only made possible by the use of symmetry in the construction of that family of states. As we will see below, symmetry helps to reduce the complexity of these tasks.

1.2.2 Separability criteria

Although the characterization of separable states is rather simple the definition itself is easily applicable only in the case of pure states. In that case one directly sees that they are separable iff they are product states: $|\psi\rangle\langle\psi| = |\psi^1 \otimes \psi^2\rangle\langle\psi^1 \otimes \psi^2| \equiv |\psi^1\rangle\langle\psi^1| \otimes |\psi^2\rangle\langle\psi^2|$.

For mixed states, however, only in some simple cases (two-qubit[9] systems, qubit-qutrit[10] systems, symmetric states, Gaussian states) analytical solutions have been achieved. Since the general situation is still open a lot of necessary conditions have been derived. The most important separability criteria are: matrix reorderings, the reduction criterion, conditional entropies and majorization. It is known that the matrix reorderings can be used to derive the reduction criterion[VW02]. The relations of majorization to the first two classes are not known whereas it was shown that the entropic criteria can be derived from majorization [NK01].

1.2.2.1 Matrix reorderings

This set of criteria is based on the convexity of the trace norm[11], i.e. $\|\lambda\rho_1 + (1-\lambda)\rho_2\|_1 \leq \lambda\|\rho_1\|_1 + (1-\lambda)\|\rho_2\|_1$. Due to convexity, for any linear map L acting on a composite system without increasing the trace norm of a product state ($\|L(\bigotimes_i \rho_i)\|_1 \leq 1$) the inequality

$$\|L(\rho_{\text{separable}})\|_1 \leq 1 \tag{1.13}$$

must hold for any separable state. In [HHH02, Fan02] it was shown that this condition is not only necessary but also sufficient for separability, i.e. if a state ρ does not fulfill (1.13) for any such map L it has to be entangled.

A special class of such contractive maps are matrix reorderings. Abstractly speaking such a reordering corresponds to a permutation of the

[9] A qubit is a quantum bit, i.e. a two-level system like a spin-1/2 particle.

[10] A qutrit is a quantum trit corresponding to a three-level system like a spin-1 particle.

[11] The trace norm is given by $\|A\|_1 = \mathrm{tr}[|A|] = \mathrm{tr}\left[\sqrt{A^*A}\right]$.

indices of the coefficient matrix:

$$(\mathcal{R}_\pi\rho)_{i_1 i_2 \dots i_N j_1 j_2 \dots j_N} = \rho_{\pi(i_1 i_2 \dots i_N j_1 j_2 \dots j_N)} \tag{1.14}$$

with $\rho_{i_1 i_2 \dots i_N j_1 j_2 \dots j_N} = \langle i_1 i_2 \dots i_N | \rho | j_1 j_2 \dots j_N \rangle$, where π denotes an element of the permutation $\mathfrak{S}_N$. In the case of bipartite systems ($N = 2$) the possible reorderings lead to only two inequivalent separability criteria. The corresponding linear maps are the partial transposition

$$\Theta_1(|i\rangle\langle j| \otimes |k\rangle\langle l|) = |j\rangle\langle i| \otimes |k\rangle\langle l| \tag{1.15}$$

and

$$|i\rangle\langle j| \otimes |k\rangle\langle l| \mapsto |j\rangle\langle k| \otimes |i\rangle\langle l| \tag{1.16}$$

which corresponds to the realignment map

$$L^r(A \otimes B) = |A\rangle\langle \overline{B}|, \tag{1.17}$$

where the vectors of the last ketbra contain the entries of the operators A and B realigned into vectors. The first criterion corresponds to the positivity of the partial transpose also known as the Peres criterion [Per96]:

$$\|\Theta_1(\rho)\|_1 \leq 1 \Leftrightarrow \Theta_1(\rho) \geq \mathbf{0} \tag{1.18}$$

which for 2×2 and 2×3 systems is known to be sufficient [HHH96]. However, for higher dimensions entangled states having a positive partial transpose exist as was shown for 3×3 systems in [Hor97] (so-called *bound entangled states*, i.e. entangled states that cannot be distilled). The second criterion is exactly Rudolph's cross norm criterion [Rud00] which can be written as

$$\|\Theta_1(\rho\mathbb{F})\|_1 \leq 1, \tag{1.19}$$

with the Flip operator $\mathbb{F}$, which is defined by $\mathbb{F}(\varphi \otimes \psi) = \psi \otimes \varphi$ for all $\varphi, \psi \in \mathcal{H}$.

1.2.2.2 The reduction criterion

In a similar way separability can be reformulated in terms of positive maps instead of linear contractions [HHH96]. A state ρ of a bipartite system $\mathcal{H}_1 \otimes \mathcal{H}_2$ is separable if and only if for any positive map $\Lambda\colon \mathcal{B}(\mathcal{H}_2) \to \mathcal{B}(\mathcal{H}_1)$ the inequality

$$(\mathrm{id}_{\mathcal{B}(\mathcal{H}_1)} \otimes \Lambda)\rho \geq \mathbf{0} \tag{1.20}$$

holds. Thus taking any specific positive map gives a necessary condition for states to be separable. In the case of the reduction criterion this map is

$$\Lambda(X) = \mathrm{tr}[X]\mathbb{1} - X. \tag{1.21}$$

As one can see these positive maps need not be trace preserving as in this case. The resulting criterion was very important in the context of entanglement distillation (see (1.35)).

1.2.2.3 Conditional entropies

One of the most helpful analogies between quantum information theory and classical information theory is that between a density operator ρ and a classical probability distribution $\{p_x\}$. A lot of quantities have thus been intuitively "quantized" like for example the Shannon entropy $H(X)$ of a probability distribution. In the classical theory entropy is a well understood term given by[12]

$$H(X) = -\sum_{x \in X} p_x \log p_x \tag{1.22}$$

and is seen as a measure quantifying the resources needed to store information [NC00].

In the case of a joint probability distribution $\{p_{x,y}\}$ for two random variables one can ask how uncertain one is about the value of one variable, say X, given that Y is known. A measure for this uncertainty is the conditional entropy

$$H(X|Y) = H(X,Y) - H(Y), \tag{1.23}$$

where $H(X,Y) = -\sum_{x,y} p_{x,y} \log p_{x,y}$ denotes the joint entropy, i.e. the usual entropy of the joint system. The quantum analogue of the Shannon entropy

$$S(\rho) = -\mathrm{tr}[\rho \log \rho] = -\sum_i \lambda_i \log \lambda_i, \quad \text{with } \lambda_i \text{ eigenvalues of } \rho \tag{1.24}$$

is called von Neumann entropy and was used to derive similar quantities like the conditional entropy of a composite quantum system ρ^{AB}:

$$S(\rho^A|\rho^B) = -\mathrm{tr}\left[\rho^{AB} \log \rho^{AB}\right] + \mathrm{tr}\left[\rho^B \log \rho^B\right], \tag{1.25}$$

ρ^A and ρ^B denoting the respective reduced density operators of ρ^{AB}.

[12] The Shannon entropy is uniquely determined by a set of axioms (see [OP93]).

For classical random variables $H(X|Y)$ is known to be positive. The failure of this analogy for quantum systems can be used as a separability criterion. Using the reduction criterion (which is obviously met by all separable states) and operator monotonicity of the logarithm one can readily prove that the conditional entropy of separable states is always positive:

$$\begin{aligned} S(\rho^A|\rho^B) &= -\mathrm{tr}\big[\rho^{AB}\log\rho^{AB}\big] + \mathrm{tr}\big[\rho^B\log\rho^B\big] \\ &= -\mathrm{tr}\big[\rho^{AB}\log\rho^{AB}\big] + \mathrm{tr}\big[\rho^{AB}(\log\rho^B\otimes\mathbb{1})\big] \\ &\geq -\mathrm{tr}\big[\rho^{AB}\log\rho^{AB}\big] + \mathrm{tr}\big[\rho^{AB}\log\rho^{AB}\big] = 0. \end{aligned}$$

The same holds for a whole family of entropies

$$S_\alpha(\rho) = \frac{\log\mathrm{tr}[\rho^\alpha]}{1-\alpha} \tag{1.26}$$

known as quantum Rényi entropies which include the von Neumann entropy for $\alpha = 1$ [VW02].

1.2.2.4 Majorization

The last separability criterion we want to recall here is the majorization criterion presented in [NK01]. It relies on the fact that the difference of the “mixedness” of a state and the “mixedness” of its reductions is in some way related to its entanglement. In fact, whenever the reduced states are “more mixed” than the overall state, it is entangled.

Majorization is a mathematical tool used for measuring the disorder of two d-dimensional vectors. For two vectors $x = (x_1, \ldots, x_d) \in \mathbb{R}^d$ and $y = (y_1, \ldots, y_d) \in \mathbb{R}^d$, x is said to be majorized by y ($x \prec y$) iff

$$\sum_{j=1}^{k} x_j^\downarrow \leq \sum_{j=1}^{k} y_j^\downarrow \qquad \forall k = 1, \ldots, d \tag{1.27}$$

where $x^\downarrow$ denotes the rearrangement of the entries of x in decreasing order. This rather abstract notion of disorder can be motivated by the fact that x is majorized by y if and only if x can be written as a convex combination of permutations of y [Bha97]. From this point of view it seems intuitive to think of x as being more disordered than y.

With this tool it is possible to show [NK01] that if a state ρ^{AB} is separable, then

$$\lambda(\rho^{AB}) \prec \lambda(\rho^A) \qquad \text{and} \qquad \lambda(\rho^{AB}) \prec \lambda(\rho^B) \tag{1.28}$$

where $\lambda(\rho^x)$ denotes the vector given by the ordered set of eigenvalues of the respective density operator.

1.2.3 Quantifying entanglement

Entanglement is still a very new resource. It is thus not surprising that it is not clear yet how to measure it or at least how to compute the known measures of entanglement. Since it enables new protocols like teleportation one could try to characterize the entanglement of a state via the best possible accuracy with which it allows such a protocol (operational measures). On the other hand one can see entanglement from a geometrical perspective and characterize its amount by some distance to the set of separable states (distance measures). A first abstract attempt to characterize valid figures of merit mathematically was given by [Vid00].

The status quo of abstract characterizations of such figures of merit (real valued measures[13]) E is given by the following minimal set of requirements (or axioms):

1. Any entanglement measure should vanish on separable states:
$$E(\rho_{\text{separable}}) = 0. \tag{M1}$$
2. Entanglement cannot increase under LOCC operations, i.e. for any entanglement measure
$$E(L_{\text{LOCC}}(\rho)) \leq E(\rho) \tag{M2}$$
must hold for any LOCC operation L_{LOCC} and any state ρ.
3. Mixing of states decreases the overall entanglement and thus
$$E(\lambda\rho_1 + (1-\lambda)\rho_2) \leq \lambda E(\rho_1) + (1-\lambda)E(\rho_2) \tag{M3}$$
should hold for any pair of states ρ_1 and ρ_2.
4. Any entanglement measure should be continuous. For any two sequences $\rho_n, \sigma_n \in \mathcal{B}(\mathcal{H}_n^A \otimes \mathcal{H}_n^B)$ such that $\|\rho_n - \sigma_n\|_1 \to 0$ for $n \to \infty$
$$\frac{E(\rho_n) - E(\sigma_n)}{1 + \log_2 \dim \mathcal{H}_n^A \otimes \mathcal{H}_n^B} \to 0 \tag{M4}$$
should hold for $n \to \infty$.

[13] not in measure theoretical sense

5. The last requirement is concerned with the character of entanglement as a physical resource. If we take several entangled states separately and join them to one composite system the overall entanglement should be the sum of the amounts of the single states:

$$E(\rho \otimes \sigma) = E(\rho) + E(\sigma). \tag{M5}$$

This property is called *additivity* of the entanglement measure.

5.' Since requirement (M5) is quite restrictive it is sometimes weakened to allow for a larger class of entanglement measures. Additivity in the strong sense of (M5) is then replaced by *weak additivity*:

$$E(\rho^{\otimes N}) = NE(\rho). \tag{M5'}$$

Conditions (M1)-(M4) can sometimes be checked whereas (M5) and (M5') turned out to be hard to prove, at least for the known candidates. Various alterations of (M5) have thus been proposed besides (M5') like asymptotic additivity or subadditivity in order to allow for an even larger class of functionals.

As always due to the Schmidt decomposition (1.6) the situation for pure bipartite states is quite clear. In that case the axioms (M1)-(M5) uniquely define one functional, namely the von Neumann entropy of the reduced density operator [DHR02]:

$$E_{\text{pure}}(|\psi\rangle\langle\psi|) = -\text{tr}[\rho_A \log \rho_A] = -\sum_i \lambda_i^2 \log \lambda_i^2, \tag{1.29}$$

which can be easily expressed by the Shannon entropy of the squared Schmidt coefficients.

It is not known whether this uniqueness holds when going to mixed or multipartite states. Furthermore for multipartite systems it is clear that one single figure of merit will not suffice to quantify the different kinds of entanglement possible. In fact bipartite entanglement is not the only kind of entanglement that occurs. If we take for example a tripartite system (Alice, Bob and Charlie) then one can consider the bipartite entanglement between Alice on one side and Bob and Charlie on the other (A$|$BC split) as being of the same kind to that of the AB$|$C and CA$|$B splits but not to the tripartite entanglement present in the overall system. That is, there exist states that are separable with respect to all bipartite splits but not fully separable (see subsection 3.1.2).

The most important measures used for the entanglement of mixed states can be grouped into three sets, operational measures, distance measures and measures induced by the convex roof construction. Since distance measures are usually defined on a state space regardless of the structure of the underlying system, these measures can be used to quantify the N-partite entanglement of N-partite systems. In contrast to that operational measures stem from protocols which usually use bipartite setups and are thus applicable to bipartite entanglement only.

Due to the vast number of possibilities we limit ourselves to recalling only the most important entanglement measures used:

> **Convex roof construction** This construction is used to extend a measure defined on pure states to the regime of mixed states. In the case of the entanglement measure on pure states E_{pure} this leads to the so-called entanglement of formation:
>
> $$E_{\text{OF}}(\rho) = \inf_{\{p_i,\psi_i\}} \sum_i p_i E_{\text{pure}}(\psi_i), \qquad \sum_i p_i = 1, \quad p_i \geq 0, \tag{1.30}$$
>
> where the infimum is taken over all ensembles $\{p_i \psi_i\}$ fulfilling $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$.
>
> **Distance measures** The first measure constructed from this geometrical point of view was the relative entropy of entanglement [VP98]:
>
> $$E_{\text{RE}}(\rho) = \inf_{\sigma \text{sep.}} S(\rho, \sigma), \tag{1.31}$$
>
> with the von Neumann relative entropy $S(\rho, \sigma) = \text{tr}[\rho \log \rho - \rho \log \sigma]$. Similar measures can be derived by taking other distance functions such as the trace norm difference $\|\rho - \sigma\|_1$, the relative entropy with reversed entries (see [EAP02]) etc., or other sets like the biseparable or the PPT set. However, the relative entropy has one more property that singles it out as an appropriate distance measure. In fact the maximal entropic distance to the separable regime is bounded from above by $\log d$ regardless of the number of involved parties: For bipartite systems we know that
>
> $$\log d \leq \sup_\rho \inf_{\sigma \in \mathcal{B}} S(\rho, \sigma) \leq \sup_\rho \inf_{\sigma \in \mathcal{D}} S(\rho, \sigma), \tag{1.32}$$
>
> where $\mathcal{B}$ denotes the set of biseparable states and $\mathcal{D}$ separable states. Taking σ to be the separable maximally correlated state

$\tilde{\sigma} = \frac{1}{d}\sum |kk\cdots k\rangle\langle kk\cdots k|$, this expression can be bounded from above by

$$\begin{aligned}\sup_{\rho}\inf_{\sigma\in\mathcal{D}} S(\rho,\sigma) &\le \sup_{\rho} S(\rho,\tilde{\sigma}) \\ &\le \sup_{\psi} -\log\frac{1}{d}\cdot\sum_{k}\langle\psi|kk\cdots k\rangle\langle kk\cdots k|\psi\rangle = \log d\end{aligned} \tag{1.33}$$

where the last inequality follows from the joint convexity of the relative entropy (see [OP93]).

Operational measures In this set there are the two extremal entanglement measures: Entanglement cost E_{C} and entanglement of distillation E_{D}. These two measures are called extremal since for any functional E satisfying (M1)-(M5') (and not necessarily (M5))

$$E_{\mathrm{D}}(\rho) \le E(\rho) \le E_{\mathrm{C}}(\rho) \tag{1.34}$$

holds for all ρ [DHR02].

In the case of a distillation protocol one is interested in extracting as much entanglement as possible from a finite number of states in the following sense: Given n copies of the same bipartite state ρ one can try to approximate m_n copies of the maximally entangled state of two qubits applying a LOCC map corresponding to a protocol $\mathcal{P}$. The entanglement of distillation is then defined as:

$$E_{\mathrm{D}}(\rho) = \sup_{\mathcal{P}}\lim_{n\to\infty}\frac{m_n}{n}, \quad \text{such that} \quad \|\rho^{\otimes n} - \rho_{\max}^{\otimes m_n}\|_1 \to 0. \tag{1.35}$$

It is the optimal rate at which one can “distill” maximally entangled states out of the given state ρ.

Entanglement cost is defined in a dual way as the optimal rate at which m_n maximally entangled states can be converted via some protocol $\mathcal{P}$ into n copies of some target state ρ:

$$E_{\mathrm{C}}(\rho) = \sup_{\mathcal{P}}\lim_{n\to\infty}\frac{m_n}{n}, \qquad \|\rho_{\max}^{m_n} - \rho^{\otimes n}\|_1 \to 0. \tag{1.36}$$

With these definitions of entanglement cost and entanglement of distillation one natural question to ask is whether entanglement transformations are reversible. This intuition turned out to be false due to the existence of bound entangled states (entangled states with zero distillable entanglement) having nonzero entanglement cost [VC01].

1.3 Symmetries, groups and all that jazz

Symmetry is the key concept used throughout this thesis. To show how it is related to the powerful tools of algebra we recall the basic definitions and apply them to a simple example which we will use later on (see chapter 3), namely the permutation group $\mathfrak{S}_3$ of three elements.

Since in the end we are interested in concrete quantum systems we finish this chapter with the notion of a C*-algebra which will contain all the operators acting on our concrete systems.

1.3.1 Symmetries, groups and representations

Symmetry is a property of objects first introduced in aesthetics for describing the harmony of proportions[14]. The contemporary description of a symmetric object is that it is invariant under the action of some transformation mapping it onto itself (an automorphism), like a reflection or a rotation. As an example let us take as object the arrangement of three "things" labelled A, B and C. If the "things" labelled A and B are equal we call the arrangement symmetric as it is invariant under the transformation $g_{(12)}$ permuting the labels A and B. This symmetry transformation is obviously not the only one possible for the object under consideration. If all three "things" were equal the arrangement would be invariant under any permutation of the three labels. The set of all possible symmetry transformations of such an abstract object forms a group[15] $\mathcal{G}$, in our case the permutation group

$$\mathfrak{S}_3 = \{e, g_{(12)}, g_{(23)}, g_{(31)}, g_{(123)}, g_{(321)}\}. \tag{1.37}$$

Such a group contains the identity e (the "do nothing" transformation), the inverse g^{-1} of any element $g \in \mathcal{G}$ (the reverse transformation) and is closed under the concatenation $g_1 \circ g_2$ of transformations (sequential application of transformations), i.e. $g_1 \circ g_2 \in \mathcal{G}$ for all g_1, $g_2 \in \mathcal{G}$. A complete picture of the action of a group (concatenation) is given by the group table:

As one can readily read off the group table the group action of the $\mathfrak{S}_3$ is not commutative, i.e. the group is not abelian. In that case the group

[14] One of the first if not the first to use the word symmetry was Polykleitos (see [Pol74]). He used the word $\sigma\upsilon\mu\mu\epsilon\tau\rho\iota\alpha$ (same measure) in the context of the bilateral symmetry of bodies. He described the use of symmetry in his treatise called Canon as a set of proportions to be used by sculptors in order to achieve "the beautiful" in it.

[15] A group may have a whole continuum of elements like in the case of rotations.

$\circ$	e	$g_{(12)}$	$g_{(23)}$	$g_{(31)}$	$g_{(123)}$	$g_{(321)}$
e	e	$g_{(12)}$	$g_{(23)}$	$g_{(31)}$	$g_{(123)}$	$g_{(321)}$
$g_{(12)}$	$g_{(12)}$	e	$g_{(321)}$	$g_{(123)}$	$g_{(31)}$	$g_{(23)}$
$g_{(23)}$	$g_{(23)}$	$g_{(123)}$	e	$g_{(321)}$	$g_{(12)}$	$g_{(31)}$
$g_{(31)}$	$g_{(31)}$	$g_{(321)}$	$g_{(123)}$	e	$g_{(23)}$	$g_{(12)}$
$g_{(123)}$	$g_{(123)}$	$g_{(23)}$	$g_{(31)}$	$g_{(12)}$	$g_{(321)}$	e
$g_{(321)}$	$g_{(321)}$	$g_{(31)}$	$g_{(12)}$	$g_{(23)}$	e	$g_{(123)}$

Figure 1.3: The group table of $\mathfrak{S}_3$.

table would have been invariant under transposition. Another fact one can see looking at the group table is that the elements of the group can be divided into conjugacy classes, i.e. into sets of group elements that are related via the conjugation with a third group element:

$$a \sim b \Leftrightarrow \exists u \in \mathcal{G} \colon u \circ a \circ u^{-1} = b, \qquad a, b \in \mathcal{G}. \tag{1.38}$$

$\mathfrak{S}_3$ has three conjugacy classes that are characterized by the cycle representation[16] of the permutations:

$$\{e\}, \qquad \{g_{(12)}, g_{(23)}, g_{(31)}\}, \qquad \{g_{(123)}, g_{(321)}\}. \tag{1.39}$$

The abstract nature of the notion of a group is at the same time its most appealing character since it can be applied to almost any kind of underlying objects. When, however, dealing with concrete objects, say three identical quantum systems as in our case, one needs a representation of the group. Such a representation is a mapping D of the group onto the set of concrete transformations of the objects which respects the concatenation, i.e. $D(g_1 \circ g_2) = D(g_1)D(g_2)$ (a homomorphism). In case of three identical quantum systems $\mathcal{H} = \mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d$ for example, we could take the representation $D \colon \mathcal{G} \to \mathcal{B}(\mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d)$ mapping a permutation g onto a unitary operator V_g which permutes the single tensor factors:

$$D \colon \pi \mapsto V_\pi = \sum_{i,j,k=1}^{d} |\pi(ijk)\rangle\langle ijk|, \qquad \forall \pi \in \mathfrak{S}_3. \tag{1.40}$$

The fact that this group of symmetry transformations can be implemented by a set of unitary operators is not a coincidence. In fact Wigner

[16] A cycle of length r is the permutation $i_1 \to i_2 \to \cdots \to i_r \to i_1$, i.e. it cyclically permutes the subset $(i_1, i_2, \ldots, i_r)$ of $\{1, 2, \ldots, N\}$ and leaves the rest unchanged. Any permutation can be uniquely decomposed into disjoint cycles.

[Wig31] proved that any linear bijective map $T: \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{H})$ of the state space of some Hilbert space onto itself (automorphism) can be implemented as $T(\rho) = U\rho U^*$ via a unitary or anti-unitary operator U which is unique up to a phase[17].

Any representation space supporting a unitary representation can be decomposed into a direct sum of invariant subspaces, that is of subspaces $\mathcal{K} \subset \mathcal{H}$ with $D(g)\mathcal{K} \subset \mathcal{K}$ for all $g \in \mathcal{G}$. The representation D induces a subrepresentation on each of these invariant subspaces. As a result any unitary representation can be decomposed into a direct sum of irreducible representations[18], that is a sum of representations on subspaces $\mathcal{K}_i$ having only the trivial invariant subspaces $\{0\}$ and $\mathcal{K}_i$ itself. The decomposition into irreducible subrepresentations is unique (up to a relabelling). For our example we get the decomposition

$$D \cong \bigoplus_{\nu_+} D_+ \oplus \bigoplus_{\nu_-} D_- \oplus \bigoplus_{\nu_0} D_0 \tag{1.41}$$

into the trivial representation D_+ corresponding to the Bose subspace, the alternating representation D_- corresponding to the Fermi subspace and a two-dimensional[19] representation D_0 corresponding to parastatistics, each with a respective multiplicity $\nu_{+/-/0}$.

Just like states are dual to observables[20], there is an object dual to a group $\mathcal{G}$, namely the dual group $\widehat{\mathcal{G}}$ consisting of the functions $\hat{g}: \mathcal{G} \to \mathbb{C}$, satisfying $\hat{g}(h_1 \circ h_2) = \hat{g}(h_1)\hat{g}(h_2)$, called characters. To each unitary representation D of a group is associated the character

$$\chi: \mathcal{G} \to \mathbb{C}, \qquad \chi(g) = \mathrm{tr}[D(g)]. \tag{1.42}$$

Since any unitary representation can be decomposed into a direct sum of irreducible components it is not surprising that any character can be written as a sum of characters corresponding to the irreducible representations. Due to the cyclicity of the trace it is clear that a character is a constant function on the conjugacy classes. It is thus sufficient to

[17] If not chosen properly this phase can lead to a projective representation: $D(g_1)D(g_2) = e^{i\varphi(g_1,g_2)}D(g_1 \circ g_2)$. The group can then be enlarged by adding these phases to the group. The resulting group is called the central extension and can be represented by a non-projective representation.

[18] Actually, this is only true for unitary representations of compact groups (see [FH91]).

[19] The dimension of an irreducible representation is given by the dimension of the respective invariant subspace and can be read off the character table as the value of the corresponding character taken on the unit element.

[20] States can be seen as maps $\rho: \mathcal{B}(\mathcal{H}) \to \mathbb{C}$ via $A \in \mathcal{B}(\mathcal{H}) \mapsto \mathrm{tr}[\rho A] \in \mathbb{C}$.

give its value for one element per conjugacy class only. The character table of a group $\mathcal{G}$ thus gives full knowledge of the dual group $\widehat{\mathcal{G}}$:

	$\{e\}$	$\{g_{(12)}, g_{(23)}, g_{(31)}\}$	$\{g_{(123)}, g_{(321)}\}$
χ_+	1	1	1
χ_-	1	-1	1
χ_0	2	0	1

Figure 1.4: The character table of $\mathfrak{S}_3$.

For the special case of the permutation group $\mathfrak{S}_n$ acting on n "objects" there is a nice graphical method to represent the irreducible representations. If we take n boxes and arrange them into a tabular in a way that the number of boxes decreases from row to row and from column to column we get the so-called Young frames. For $\mathfrak{S}_3$ these would be

$$\chi_+ \cong \begin{array}{|c|c|c|}\hline \; & \; & \; \\ \hline \end{array} \qquad \chi_0 \cong \begin{array}{|c|c|}\hline \; & \; \\ \hline \; & \multicolumn{1}{c}{} \\ \cline{1-1} \end{array} \qquad \chi_- \cong \begin{array}{|c|}\hline \; \\ \hline \; \\ \hline \; \\ \hline \end{array} \tag{1.43}$$

Assigning the numbers $1, \ldots, n$ to the boxes in ascending order we get the Young tableaux:

$$\begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline \end{array} \qquad \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 & \multicolumn{1}{c}{} \\ \cline{1-1} \end{array} \qquad \begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 & \multicolumn{1}{c}{} \\ \cline{1-1} \end{array} \qquad \begin{array}{|c|}\hline 1 \\ \hline 2 \\ \hline 3 \\ \hline \end{array} \tag{1.44}$$

The dimension of an irreducible representation can then be computed by counting the number of Young tableaux of the corresponding Young frame.

1.3.2 C*-algebras

The set of unitary operators $D(g)$ has more properties than those defining a group. Besides concatenating two of them (operator product) we can add operators and we can take their adjoints in $\mathcal{B}(\mathcal{H})$. Furthermore we can take the norm given on $\mathcal{B}(\mathcal{H})$ and look at the closure of linear combinations of unitary operators $D(g)$. The result is a C*-algebra, i.e. a normed algebra with a norm satisfying the Gelfand property

$$\|A^* A\| = \|A\|^2. \tag{1.45}$$

These operations have no counterpart in the group itself but can be used to define new objects. Taking formal linear combinations of the group elements we get the structure of an algebra, the group algebra $\mathcal{A}(\mathcal{G})$:

$$\sum_{g\in\mathcal{G}} f(g)g \in \mathcal{A}(\mathcal{G}), \qquad f: \mathcal{G} \to \mathbb{C} \tag{1.46}$$

(for simplicity we identify the element of the group algebra with its characteristic function f). As such it has a center

$$\mathcal{Z}(\mathcal{A}(\mathcal{G})) = \{g \in \mathcal{A}(\mathcal{G}) | g \circ h = h \circ g, \forall h \in \mathcal{A}(\mathcal{G})\} \tag{1.47}$$

which contains the projections onto the irreducible representations sometimes called the central projections. In our case they can be constructed easily by summing up the elements of the group weighted with the value of the character for the respective element:

$$\begin{aligned} p_+ &= \frac{1}{6}(e + g_{(12)} + g_{(23)} + g_{(31)} + g_{(123)} + g_{(321)}), \\ p_- &= \frac{1}{6}(e - g_{(12)} - g_{(23)} - g_{(31)} + g_{(123)} + g_{(321)}), \\ p_0 &= \frac{1}{3}(2e - g_{(123)} - g_{(321)}) = e - p_+ - p_-. \end{aligned} \tag{1.48}$$

In the case of non finite groups the summation in (1.48) is a little more subtle. For “nice” groups (locally compact unimodular groups) we can substitute the sum with the integration over the Haar measure [Sim96]:

$$\frac{1}{|\mathcal{G}|}\sum_{g\in\mathcal{G}} f(g) \longrightarrow \int_{g\in\mathcal{G}} f(g)d\mu_H(g). \tag{1.49}$$

For such “nice” groups this measure is uniquely defined and bears the invariance property

$$\int_{g\in\mathcal{G}} f(g\circ h)d\mu_H(g) = \int_{g\in\mathcal{G}} f(h\circ g)d\mu_H(g) = \int_{g\in\mathcal{G}} f(g)d\mu_H(g), \tag{1.50}$$

for all $h \in \mathcal{G}$, i.e. it is left and right invariant under group multiplications.

The second operation, the adjunction, can be taken to be a general star operation *, that is a map with the properties known from the adjunction: $A^{**} = A$, $(AB)^* = B^*A^*$ and $(\lambda A)^* = \overline{\lambda}A^*$ for all $\lambda \in \mathbb{C}$. Once equipped with the star operation the group algebra is not a C*-algebra yet, but merely a *-algebra. To make it a C*-algebra we need to define a C*-norm on it but since this is a very subtle point we omit it here (see [Ped79] instead).

The representation we had for the group $\mathcal{G}$ can be used as a representation of the group C*-algebra only if it is compatible with the star operation. For this it has to respect the star operation, i.e. for any element f of the group C*-algebra we must have $D(f^*) = D(f)^*$ (*-homomorphism).

As for the group itself we can decompose the group C*-algebra (and even every finite dimensional C*-algebra) into a direct sum of matrix algebras corresponding to the invariant subspace of the irreducible representations. In the case of an abelian group these will obviously be functions on the complex numbers only.

Another object we will need later on is the so-called commutant of an algebra. If we take a subalgebra $\mathcal{A}_1 \subset \mathcal{A}$ this is the set

$$\mathcal{A}_1' = \{a \in \mathcal{A} | ab = ba, \forall b \in \mathcal{A}_1\} \tag{1.51}$$

which again forms an algebra. The center of an algebra is thus the abelian subalgebra given by the commutant with respect to itself.

Chapter 2

Multipartite symmetric states

> "Symmetry, as wide or narrow as you may define its meaning, is one idea by which man through the ages has tried to comprehend and create order, beauty, and perfection."
>
> (Herrmann Weyl, *Symmetry*)

One of the difficulties in the theory of entanglement is that state spaces are usually fairly high dimensional convex sets. Therefore, to explore in detail the potential of entangled states one often has to rely on lower dimensional "laboratories".

There are basically two different ways of reducing a high dimensional convex set to lower dimensional sets. Firstly, we may consider *projections* of the given set by considering only a subset of the coordinates describing a point in the original convex set (see figure 2.1) and ignoring the others. Secondly, we may consider *sections* of the convex set, i.e. intersections with suitable lower dimensional hyperplanes (see figure 2.1) by fixing some of the coordinates.

As one can see in figure 2.1 both methods lead to lower dimensional sets but give only partial knowledge of the original higher dimensional object. To have a representative description it would thus be best to have a section being at the same time a projection (or vice versa) like in figure 2.2.

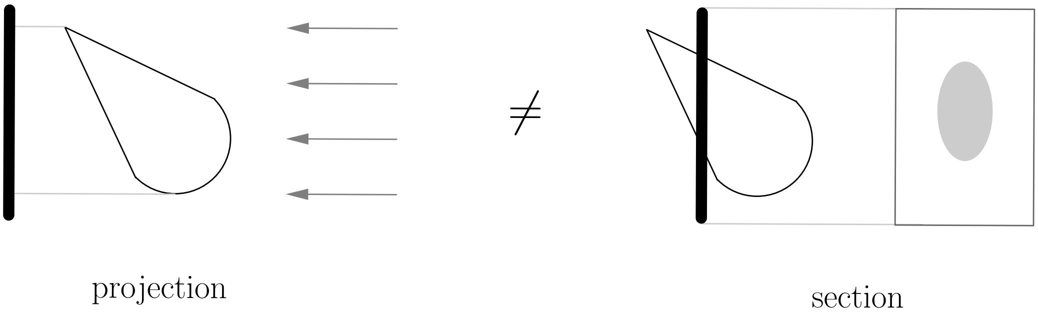


Figure 2.1: Sketch of a projection and of a section of a convex set.

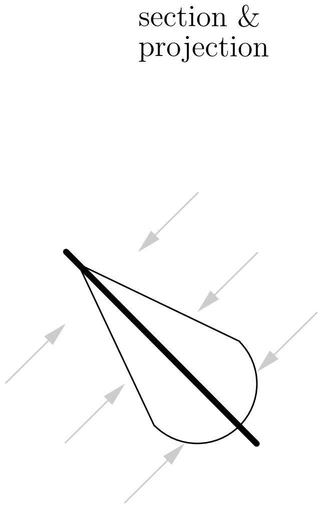


Figure 2.2: Sketch of a section which at the same time is a projection.

This is, of course, not always possible. For example, the only sections of a 3-ball, which are also images of a projection, are the intersections with planes or lines going through the origin.

However, in the special case of the presence of a compact group of affine symmetries acting on the convex set there is fortunately a constructive method of obtaining such sections. The fixed points under the group action can be taken as a section. The corresponding projection onto these fixed points is then given by averaging over the group action. This technique was first used for the construction of a one-parameter family of bipartite states [Wer89], which has come to be known as "Werner states".

Since this chapter will mainly deal with generalizations of this example we start by giving a detailed description of how to apply the abstract idea to derive it. In the following sections we will then present generalizations with respect to the number of particles and to the group of symmetry transformations. We conclude by proving some simple relations between symmetric states of different numbers of subsystems.

Further examples of multipartite symmetric states can be constructed by composing the basic examples presented here like $UUV\overline{V}$-invariant states for instance (see [EVWW01]) or by taking appropriate subgroups like $\{\mathbb{1}\otimes\mathbb{1}, \sigma_x\otimes\sigma_x, \sigma_y\otimes\sigma_y, \sigma_z\otimes\sigma_z\} \subset U(2)\otimes U(2)$ (see [BDSW96]).

2.1 Werner states

By Wigner's Theorem [Wig31] the symmetries of quantum state spaces can be implemented by unitary operators. The section and the projection can thus be written as

$$[\rho, U_g]_- = \mathbf{0}, \forall g \in \mathcal{G} \iff \rho = \int_{\mathcal{G}} U_g \rho U_g^* d\mu_H(g) \overset{\text{def}}{=} \mathcal{T}_{\mathcal{G}}(\rho). \tag{2.1}$$

For the study of entanglement the interesting groups are those which respect the decomposition of the total Hilbert space into a tensor product, i.e. local unitaries like $U \otimes V$, $U, V \in U(d)$. The section in question can thus be written as $[\rho, U \otimes V]_- = \mathbf{0}$ for all $U, V \in U(d)$. The corresponding projection is then given by the group average over the Haar measure[21] [Sim96]: $\int (U \otimes V)\rho(U^* \otimes V^*) d\mu_H(U) d\mu_H(V)$. Unfortunately this "twirling" operation leaves only one state invariant, namely the completely chaotic one $\rho = \mathbb{1}/d^2$. This can be seen when looking at the section. Since $U(d)$ is an irreducible representation of itself it is clear that the only invariant operators are multiples of the identity[22] $\mathbb{1}$ and by normalization the statement follows.

In order to have a slightly larger family of states it was thus convenient to take the smaller local group given by local unitary operators of the form $U \otimes U$. Generally averaging over a smaller group leads to a larger commutant. For the group algebra of $\{U \otimes U | U \in U(d)\}$ one can easily compute[23] that the commutant is given by the set of operators spanned by $\{\mathbb{1}, \mathbb{F}\}$. Therefore any density operator $\rho \in \mathcal{B}(\mathbb{C}^d \otimes \mathbb{C}^d)$ having "Werner symmetry" can be written as

$$\rho_W(f) = \frac{1}{d^3 - d}\left[(d - f)\mathbb{1} + (df - 1)\mathbb{F}\right], \qquad -1 \le f \le 1 \tag{2.2}$$

[21] If the group is chosen properly the commutant given by the section condition will result into a finite set of operators $\{O_i\}$. In this case the integral will depend only on the expectation values $\mathrm{tr}[\rho O_i]$ and needs therefore not to be computed explicitly by parameterizing the Haar measure which can be quite cumbersome.

[22] Actually, the twirling leads to states having chaotic reductions. But since these states would have to be invariant under any $U \otimes V$ operators, they have to commute with all operators of an operator basis $U_i \otimes U_j$ and therefore have to be proportional to the identity.

[23] It suffices to take diagonal unitaries and row permutations as special $U \otimes U$ rotations for the computation.

with $f = \mathrm{tr}[\rho_W(f)\mathbb{F}]$. This family of states can be described by one single parameter instead of $d^4 - 1$ which is the number of real parameters needed for a general state on $\mathcal{B}(\mathbb{C}^d \otimes \mathbb{C}^d)$. Nonetheless it was versatile enough to investigate the relation of entanglement to the violation of Bell inequalities ([Wer89]). In fact in the same article the separable Werner states were already characterized in the following way:

Lemma 2.1.1: A Werner state $\rho_W(f) \in \mathcal{B}(\mathbb{C}^d \otimes \mathbb{C}^d)$ is separable iff

$$f \geq 0 \tag{2.3}$$

holds.

Proof: The proof is very simple. We start by looking at where pure product states $|\varphi \otimes \psi\rangle$ are being twirled on, i.e. by looking at the expectation value $\langle\varphi \otimes \psi|\mathbb{F}|\varphi \otimes \psi\rangle = |\langle\varphi|\psi\rangle|^2 \geq 0$. Since the expectation value $\mathrm{tr}[\rho\mathbb{F}]$ is a linear function of the density operator ρ this condition holds obviously for convex combinations too. Conversely any Werner state having a non-negative expectation value f can be written as the projection of a pure product state. Since the twirl operation is LOCC by construction it is clear that the resulting Werner state has to be separable. ■

As already mentioned this family of states turned out to be very useful for the investigation of entanglement [Pop95, HH99]. This was first of all due to the fact that separability within this family could be decided easily. Secondly there is a simple operation, the twirl (group averaging), which can be used to come back to this family after some manipulation of the state. Furthermore when mixing various states of this family the result is still within this set.

Entropic quantities can easily be computed since this family of states is commutative, i.e. any two such states commute. In addition the spectrum and eigenvectors are fixed by their simple structure: These states have only two different eigenvalues $\lambda_+ = \frac{1+f}{2\nu_+}$ and $\lambda_- = \frac{1-f}{2\nu_-}$ with the multiplicities $\nu_+ = \frac{d^2+d}{2}$ and $\nu_- = \frac{d^2-d}{2}$. The corresponding eigenvectors form a basis of the Bose (λ_+) and Fermi (λ_-) subspace respectively. In fact the normalized symmetric and antisymmetric projectors $\rho_\pm = \frac{\mathbb{1}\pm\mathbb{F}}{d^2 \pm d}$ are the extremal Werner states, i.e. the endpoints of the line given by $f \in [-1, 1]$. Once again this is not a coincidence but a manifestation of the algebraic nature of these states as we will see in the following sections.

2.2 Multipartite Werner states

One obvious N-partite generalization of these states is, of course, to take the group $\mathcal{G} = \{U^{\otimes N}\}$ with $U \in U(d)$. The hard part will then be to compute the commutant of its group algebra to have a parametrisation of the resulting state $\mathcal{S}_{U^{\otimes N}}$ family[24]. It is clear that a direct computation like in footnote 23 will not give such a general result. Fortunately there are some sophisticated tools from representation theory that will do it for us. Since the proof is rather lengthy and technical, a subsection of its own has been devoted to it. The second subsection will then deal with commutative and thus even simpler subsets of this family of states.

2.2.1 Duality of $U(d)$ and $\mathfrak{S}_N$

For the proof that the commutant of the algebra generated by $\{U^{\otimes N}\}$ is *exactly* the group algebra of the $\mathcal{S}_N$[25] we follow [Sim96] and begin with a lemma characterizing the vector space generated by $\{x \otimes \cdots \otimes x | x \in \mathcal{H}\}$:

Lemma 2.2.1 ([Sim96], IX.11.4): Let $\mathcal{H}$ be a Hilbert space and the $\mathcal{S}_N$ act on $\mathcal{H}^{\otimes N}$ by permuting the tensor factors. Also let $S^N(\mathcal{H}) \subset \mathcal{H}^{\otimes N}$ be the set of vectors that are invariant under all permutations $V_\pi \in \mathcal{S}_N$. Then $S^N(\mathcal{H})$ is the smallest space containing the set $\{x \otimes \cdots \otimes x | x \in \mathcal{H}\}$.

Proof. Take the map $P\colon x \mapsto x \otimes \cdots \otimes x$. By definition derivatives of P are limits of sums of values $P(x)$ and thus still lie in the smallest space $\mathcal{K}$ generated by $\{x \otimes \cdots \otimes x | x \in \mathcal{H}\}$. On the other hand a direct computation gives:

$$\frac{\partial}{\partial\lambda_2 \cdots \partial\lambda_N} P(e_1 + \lambda_2 e_2 + \cdots + \lambda_N e_N)\Bigg|_{\lambda_2=0,\ldots,\lambda_N=0} \\ = \sum_{\pi \in \mathfrak{S}_N} V_\pi(e_1 \otimes \cdots \otimes e_N) = N! \cdot \mathrm{Sym}_N(e_1 \otimes \cdots \otimes e_N), \quad (2.4)$$

with the symmetrizer $\mathrm{Sym}_N = \frac{1}{N!}\sum_{\pi\in\mathfrak{S}_N} V_\pi$. Then, varying the vectors $e_1, \ldots, e_N$ over all elements of some basis of $\mathcal{H}$, we obtain the result

[24] We will denote families of symmetric states with the symbol $\mathcal{S}$ like the usual state space and attach the respective symmetry group as an index ($U^{\otimes N}$ in this case).

[25] We distinguish here between the group $\mathfrak{S}_N$ itself and the group of the representatives of the group elements $\mathcal{S}_N = \{V_\pi | \pi \in \mathfrak{S}_N\}$. Unless stated otherwise we will use the "natural" representation of the permutation group defined in (1.40) given by the permutation of the tensor factors.

that $\mathcal{K} \supset \mathrm{Range}(\mathrm{Sym}_N) = S^N(\mathcal{H})$. But since $P(x) \in S^N(\mathcal{H})$ it is clear that $\mathcal{K} \subset S^N(\mathcal{H})$ holds and thus $\mathcal{K} = S^N(\mathcal{H})$. ■

With this lemma we can now prove that the $SU(d)$ and the $\mathfrak{S}_N$ act dually on the Hilbert space $\mathcal{H} = (\mathbb{C}^d)^{\otimes N}$ via the representations[26] $D^1(\pi) = V_\pi$ as in (1.40) and $D^2(U) = U^{\otimes N}$ in the sense that the group algebras $\mathcal{A}(D^2(SU(d)))$ and $\mathcal{A}(D^1(\mathfrak{S}_N))$ are commutants of each other:

$$\mathcal{A}(D^1(\mathfrak{S}_N))' = \mathcal{A}(D^2(SU(d))). \tag{2.5}$$

Theorem 2.2.2 ([Sim96], IX.11.5): $SU(d)$ and $\mathfrak{S}_N$ act dually on $(\mathbb{C}^d)^{\otimes N}$ via the representations $D^1(\pi) = V_\pi \in \mathcal{S}_N$ as in (1.40) and $D^2(U) = U^{\otimes N}$.

Proof. As always the proof splits into an easy and a hard part. In fact it is obvious that the set $\{A^{\otimes N} | A \in SU(d)\}$ and thus the algebra $\mathcal{B}$ it generates lie in the commutant $\mathcal{A}(\mathcal{S}_N)'$. Therefore only the converse inclusion (the hard part) remains to be shown. For this we start by noting that $\mathcal{B}$ is quite large as it contains $\{A^{\otimes N} | A \in \mathcal{B}(\mathbb{C}^d)\}$. To see this let $X \in \mathrm{su}(d)$[27]. Then $(e^{tX})^{\otimes N}$ is in $\mathcal{B}$ and again by definition also its derivative which is:

$$\frac{\mathrm{d}}{\mathrm{d}t}(e^{tX})^{\otimes N}\bigg|_{t=0} = X \otimes \mathbb{1} \otimes \cdots \otimes \mathbb{1} + \cdots + \mathbb{1} \otimes \mathbb{1} \otimes \cdots \otimes X \overset{\text{def}}{=} \mathrm{d}\Gamma(X). \tag{2.6}$$

Addition of multiples of the identity leads to $\mathrm{d}\Gamma(X + \lambda\mathbb{1}) = \mathrm{d}\Gamma(X) + \lambda N \mathbb{1}$ which is again in $\mathcal{B}$. Furthermore we have it that for $X, Y \in \mathbf{u}(d)$ $\mathrm{d}\Gamma(X) + i\mathrm{d}\Gamma(Y) = \mathrm{d}\Gamma(X + iY)$ lies in $\mathcal{B}$ too and therefore also their exponentials. Such exponentials can be written as $A^{\otimes N}$ with an invertible $A \in \mathcal{B}(\mathcal{H})$. Since the invertible operators are dense in $\mathcal{B}(\mathcal{H})$ and $\mathcal{B}$ is closed we have proved that $\{A^{\otimes N} | A \in \mathcal{B}(\mathcal{H})\} \subset \mathcal{B}$. Finally we have

$$\begin{aligned} \mathcal{A}(\mathcal{S}_N)' &= \{\Gamma \in \mathcal{B}((\mathbb{C}^d)^{\otimes N}) | V_\pi \Gamma = \Gamma V_\pi \text{ for all } \pi \in \mathfrak{S}_N\} \\ &= \{\Gamma \in \mathcal{B}((\mathbb{C}^d)^{\otimes N}) | V_\pi \Gamma V_\pi^{-1} = \Gamma \text{ for all } \pi \in \mathfrak{S}_N\} \\ &= \mathrm{span}\{A^{\otimes N} | A \in \mathcal{B}(\mathbb{C}^d)\} \subset \mathcal{B}. \end{aligned} \tag{2.7}$$

To sum up we have proved that $\mathcal{A}(\mathcal{S}_N)' = \mathcal{B} = \mathcal{A}(D^2(SU(d)))$. ■

As all permutation operators V_π commute with $\mathbb{1}^{\otimes N}$ it is clear that this result extends to the commutant of $\{U^{\otimes N} | U \in U(d)\}$. Coming back to the multipartite Werner states ($\mathcal{S}_{U^{\otimes N}}$) this already gives a possibility of parametrising them in a similar way as for the bipartite case:

[26] Note that the concept of duality depends directly on the chosen representations.

[27] The $\mathrm{su}(d)$ is the group of generators of the Lie algebra $SU(d)$.

Any multipartite Werner state $\rho \in \mathcal{S}_{U^{\otimes N}}$ is uniquely determined by the $N!$ expectation values $x_\pi = \operatorname{tr}[\rho V_\pi]$ just like a bipartite Werner state is completely described by its expectation value with the Flip f (and with the identity). This is a remarkable reduction of the complexity if one compares these $N! - 1$ parameters with the $d^{2N} - 1$ needed for characterizing an arbitrary state. Moreover this parameterisation is independent of the dimension!

However, the constraints for these parameters to describe a state, i.e. for the described operator to be positive and of unit trace, are not easy to derive. For that it might be appropriate to go to another set of parameters that are in that sense more suitable. One such set of parameters can be derived by taking a closer look at the representations $D^1(\mathfrak{S}_N)$ and $D^2(SU(d))$. As one might think they are *not* irreducible. In analogy to (1.41) they can be decomposed into

$$\begin{aligned} D^1(\mathfrak{S}_N) &= \bigoplus_{\mathcal{Y}} P_{\mathcal{Y}} D^1(\mathfrak{S}_N) P_{\mathcal{Y}} \\ \text{and} \quad D^2(SU(d)) &= \bigoplus_{\mathcal{Y}} P_{\mathcal{Y}} D^2(SU(d)) P_{\mathcal{Y}}, \end{aligned} \tag{2.8}$$

where the $\mathcal{Y}$ are the Young frames labelling the irreducible representations of $\mathfrak{S}_N$ and the $P_{\mathcal{Y}}$ are the projections onto the invariant subspaces of the respective irreducible representations $\mathcal{Y}$. Putting a little effort into it we can prove the following:

Corollary 2.2.3: The Hilbert space $\mathcal{H} = \left(\mathbb{C}^d\right)^{\otimes N}$ and the representations D^1 and D^2 can be decomposed in the following way:

$$\begin{aligned} \mathcal{H} &= \bigoplus_{\mathcal{Y}} \mathcal{H}_{\mathcal{Y}} \otimes \mathcal{K}_{\mathcal{Y}}, \\ D^1(\pi) &\cong \bigoplus_{\mathcal{Y}} D^1_{\mathcal{Y}}(\pi) \otimes \mathbb{1}_{\mathcal{K}_{\mathcal{Y}}}, \quad \pi \in \mathfrak{S}_N, \\ D^2(U) &\cong \bigoplus_{\mathcal{Y}} \mathbb{1}_{\mathcal{H}_{\mathcal{Y}}} \otimes D^2_{\mathcal{Y}}(U), \quad U \in U(d), \end{aligned} \tag{2.9}$$

where the $D^1_{\mathcal{Y}}$ and $D^2_{\mathcal{Y}}$ are irreducible representations with multiplicity 1 of $\mathfrak{S}_N$ and $SU(d)$ respectively.

Proof. The proof follows directly from the simple observation that the subrepresentations in (2.8) act dually on $\left(\mathbb{C}^d\right)^{\otimes N}$, too. This means that $P_{\mathcal{Y}} \mathcal{A}\left(D^1(\mathfrak{S}_N)\right) P_{\mathcal{Y}} = P_{\mathcal{Y}} \mathcal{A}\left(D^2(SU(d))\right)' P_{\mathcal{Y}}$. Now since we are dealing with finite dimensional C*-algebras we have that due to

$$\begin{aligned}&P_{\mathcal{Y}}\mathcal{A}\left(D^1(\mathfrak{S}_N)\right)P_{\mathcal{Y}}\cap P_{\mathcal{Y}}\mathcal{A}\left(D^1(\mathfrak{S}_N)\right)'P_{\mathcal{Y}}\\&=P_{\mathcal{Y}}\mathcal{A}\left(D^1(\mathfrak{S}_N)\right)P_{\mathcal{Y}}\cap P_{\mathcal{Y}}\mathcal{A}\left(D^2(SU(d))\right)P_{\mathcal{Y}}\\&=\mathbb{C}\mathbb{1},\end{aligned}\tag{2.10}$$

both $P_{\mathcal{Y}}\mathcal{A}\,(D^1(\mathfrak{S}_N)\,P_{\mathcal{Y}}$ and $P_{\mathcal{Y}}\mathcal{A}\,(D^2(SU(d)))\,P_{\mathcal{Y}}$ must be factors (see for example [BR79]), that is isomorphic to some $\mathcal{B}(\mathcal{H})\otimes\mathbb{1}$. For each Young frame $\mathcal{Y}$ there are unitary operators $U^1_{\mathcal{Y}}$ and $U^2_{\mathcal{Y}}$ implementing these isomorphisms such that

$$\begin{aligned}U^1_{\mathcal{Y}}P_{\mathcal{Y}}D^1P_{\mathcal{Y}}U^{1*}_{\mathcal{Y}}&=D^1_{\mathcal{Y}}\otimes\mathbb{1}_{\mathcal{K}_{\mathcal{Y}}}\\\text{and}\quad U^2_{\mathcal{Y}}P_{\mathcal{Y}}D^2P_{\mathcal{Y}}U^{2*}_{\mathcal{Y}}&=\mathbb{1}_{\mathcal{H}_{\mathcal{Y}}}\otimes D^2_{\mathcal{Y}},\end{aligned}\tag{2.11}$$

where the $D^i_{\mathcal{Y}}$ are irreducible representations and the identity represents the corresponding multiplicity. Since the $P_{\mathcal{Y}}$ commute with D^1 and D^2 the decomposition (2.9) follows by summing over all Young frames $\mathcal{Y}$. ■

As the $D^2_{\mathcal{Y}}$ act irreducibly on the $\mathcal{K}_{\mathcal{Y}}$ any operator X commuting with all $U^{\otimes N}$ rotations will be of of the form $X=\bigoplus_{\mathcal{Y}}X^1_{\mathcal{Y}}\otimes\mathbb{1}_{\mathcal{K}_{\mathcal{Y}}}$. To characterize such invariant operators it will thus be enough to have a set of operators building a basis for the $\mathcal{B}(\mathcal{H}_{\mathcal{Y}})$. This decomposition suggests the following parametrisation: Take as basis operators the central projections onto the irreducible representations of the $\mathfrak{S}_N$, i.e. the Young projections $P_{\mathcal{Y}}$. To each frame $\mathcal{Y}$ take a set of operators $\{R^{\mathcal{Y}}_i\}$ that can serve as the generators of su$(\dim\mathcal{Y})$. The advantage of this set of parameters is that positivity and the unit trace can be checked on each direct summand, i.e. for each Young frame $\mathcal{Y}$, individually. For an example see chapter 3 where we will treat the case $N=3$ in detail.

2.2.2 Commutative subfamilies of states

One of the nice features of the family of bipartite Werner states is that it is commutative. From the algebraic point of view this is obvious since we are dealing with the group algebra of $\mathfrak{S}_2$ which is an abelian algebra. This, however, is no longer true for $N>2$. As commutativity of the states simplifies the computation of distance measures and entanglement monotones it would be interesting to have a “laboratory” for multipartite systems bearing this property.

Fortunately there are various subsets of the multipartite Werner states $\mathcal{S}_{U^{\otimes N}}$ that have this nice property of being commutative. One such subset is given by the analogue of the extremal bipartite Werner states, namely the states given by the normalized Young projections $\rho_\mathcal{Y} = \{\frac{P_\mathcal{Y}}{\mathrm{tr}[P_\mathcal{Y}]}\}$. These states span the fully permutation invariant multipartite Werner states[28] $\mathcal{S}_{U^{\otimes,N}\times\mathcal{S}_N} \subset \mathcal{S}_{U^{\otimes,N}}$. The corresponding state space is a simplex and can be obtained from the state space of multipartite Werner states by the *non-local* twirling operation given by the averaging over $\mathcal{S}_N$, i.e. $\rho \mapsto \frac{1}{N!}\sum_{\pi\in\mathfrak{S}_N} V_\pi^*\rho V_\pi$. It is clear that due to the non-locality of the twirling operation the entanglement will not be affected in a monotonic way. This operation itself will therefore not be useful for the investigation of multipartite entanglement. Nevertheless the state family itself can be used for this purpose.

As already mentioned, the corresponding state space is a simplex spanned by the extremal states which are given by the normalized Young projections. Any such state can thus be written as $\rho = \sum_\mathcal{Y} \lambda_\mathcal{Y}\rho_\mathcal{Y}$ where $\sum_\mathcal{Y} \lambda_\mathcal{Y} = 1$ and $\lambda_\mathcal{Y} \geq 0$. This again implies that the spectrum and the eigenvectors are completely fixed in the following way: For each Young frame we have as many different eigenvalues as the dimension of the corresponding irreducible representation $\dim\mathcal{Y}$, each with a dimension dependent multiplicity of $\frac{\mathrm{tr}[P_\mathcal{Y}]}{\dim\mathcal{Y}}$. The corresponding eigenvectors can be chosen to be a basis of the respective invariant subspace $P_\mathcal{Y}\mathcal{H}$. For a concrete example we refer again to chapter 3 where we will compute some entanglement monotones for the corresponding permutation invariant states.

This is, however, neither the only commutative subfamiliy nor the biggest possible. If we leave the center of the group algebra $\mathcal{A}(\mathcal{S}_N)$ we can indeed find larger abelian subalgebras. All we need is to recall that we are dealing with a finite dimensional C*-algebra which is as such isomorphic to a direct sum of matrix algebras (see [BR79]). This corresponds exactly to the decomposition into invariant subspaces of corollary 2.2.3. To get a Cartan subalgebra[29] we thus need only to find a complete set of projections for each matrix algebra in the direct sum. In our case if we take, for example, $N = 3$ the permutation invariant subalgebra has the minimal projections P_+, P_- and P_0 corre-

[28] Note that the concatenation of two twirls ($\mathcal{T}_\mathcal{G}$ and $\mathcal{T}_\mathcal{H}$) does not lead to a twirl on a larger group. However, this is true if the two representations of $\mathcal{G}$ and $\mathcal{H}$ act dually (see (2.5)). In this case one obtains the twirl on the direct product of the two groups: $\mathcal{T}_\mathcal{H}(\mathcal{T}_\mathcal{G}(\mathcal{A})) = \mathcal{T}_{\mathcal{H}\times\mathcal{G}}(A)$. If the two representations do not act dually one can show that the iteration of both, $\mathcal{T}_\mathcal{G}\circ\mathcal{T}_\mathcal{H}$ and $\mathcal{T}_\mathcal{H}\circ\mathcal{T}_\mathcal{G}$, leads to the intersection of the single commutants as invariant subspace in the limit of infinite iterations.

[29] A Cartan subalgebra is a maximal abelian subalgebra, maximal in the sense that it cannot be enlarged by adding more elements of the algebra.

sponding to the trivial, the alternating and the standard representation (see [FH91]). The standard representation is two-dimensional and has, therefore, two standard tableaux:

$$\begin{array}{|c|c|}\hline & \\ \hline \\ \cline{1-1}\end{array} \quad \cong \quad \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 \\ \cline{1-1}\end{array} \quad + \quad \begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 \\ \cline{1-1}\end{array}. \tag{2.12}$$

Just like for the frames there are projections onto the standard tableaux. But contrary to those these projections are minimal for the whole group algebra and not only for its center. In consequence the corresponding minimal projections

$$\begin{aligned}\begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 \\ \cline{1-1}\end{array} \quad &\cong \quad P_{0,1} = \mathbb{1} + V_{(12)} - V_{(13)} - V_{(132)} \\ \begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 \\ \cline{1-1}\end{array} \quad &\cong \quad P_{0,2} = \mathbb{1} - V_{(12)} + V_{(13)} - V_{(123)}\end{aligned} \tag{2.13}$$

do not lie in the center any more. Nevertheless we have $P_0 = P_{0,1} + P_{0,2}$, so taking the algebra spanned by $\{P_+, P_-, P_{0,1}, P_{0,2}\}$ we get a larger abelian subalgebra which cannot be enlarged any further. This choice is obviously not unique since we have the freedom to choose the basis in the two-dimensional eigenspace of P_0. It is therefore not surprising that there are various equivalent Cartan subalgebras.

This second construction can be done explicitly for any N too. There is an explicit method of deriving the projection onto a Young tableau based on the corresponding standard tableau only (see [Sim96]). Since the group algebra is a *maximal* abelian subalgebra it is clear that its commutant is the subalgebra itself. Therefore we also have a corresponding (non-local) twirl given by the averaging over the elements of the maximal abelian subalgebra.

Comparing the second subfamiliy with the first one sees that all we did was to divide the eigenspaces of the Young projections into finer subspaces, namely the eigenspaces of the projections onto the standard tableaux. Any two different eigenvalues of a permutation invariant state are now given *different* subspaces making the spectrum even simpler. The corresponding eigenvectors can then be chosen to be a basis of the projection onto the respective standard tableau.

2.3 Orthogonally symmetric states

Besides Werner states other families of bipartite symmetric states have been of importance for quantum information like Bell-diagonal states, isotropic states, orthogonally invariant states etc. Both, the isotropic states and the orthogonally invariant states, are closely related to the Werner states.

Isotropic states have been named after the property of the corresponding dual channel (see 1.1.3 and [HH99]), namely that it does not prefer any direction in the state space. They are related to the Werner states via partial transposition in the sense that the commutants of $\{U \otimes U\}$ and $\{U \otimes \overline{U}\}$ are mapped onto each other by the partial transposition[30]. In fact, a simple computation shows that the commutant of $\{U \otimes \overline{U}\}$ is spanned by $\{\mathbb{1}, |\Omega\rangle\langle\Omega|\}$ with the maximally entangled state $|\Omega\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |ii\rangle$ (see (1.12)).

The orthogonally symmetric states have been introduced to have a larger bipartite symmetric family than the Werner and the isotropic ones. This family contains both the Werner and the isotropic states and can be obtained by taking the smaller group given by $U \otimes U = U \otimes \overline{U}$. The result is the family of states that are invariant under real unitary rotations, i.e. orthogonal rotations $O \otimes O$. The commutant of the smaller group algebra of $\{O \otimes O | O \in O(d)\}$ is, of course, larger being spanned by $\{\mathbb{1}, \mathbb{F}, |\Omega\rangle\langle\Omega|\}$.

For both families multipartite generalizations are quite obvious. This section is devoted to the largest among these families, namely the $O^{\otimes N}$ invariant states, and to a nice graphical representation of the corresponding algebra.

2.3.1 The "chip" representation

The commutant of the $O^{\otimes N}$ invariant states can be computed easily using the basic fact they are finite dimensional C*-algebras[31]. Therefore we have (see [BR79]):

$$\big(\mathcal{A}(U^{\otimes N}) \cap \mathcal{A}(U^{\otimes N-1} \otimes \overline{U})\big)' = \mathcal{A}(U^{\otimes N})' \vee \mathcal{A}(U^{\otimes N-1} \otimes \overline{U})'. \tag{2.14}$$

From this we see that all groups with one complex conjugated site are equivalent for our purpose, since they all generate the commutant for $O^{\otimes N}$ invariant operators. Furthermore it is clear that the algebra generated by the right side of (2.14) also contains all commutants of operators being invariant under $U^{\otimes n} \otimes \overline{U^{\otimes N-n}}$ for any $0 \leq n \leq N$. To

[30] Note that partial transpositions and complex conjugations are basis-dependent.

[31] Finite dimensional C*-algebras are automatically weakly closed, i.e. von Neumann-algebras.

describe the commutant of $\{O^{\otimes N}|O \in O(d)\}$ we can thus concentrate on the commutants of $\{U^{\otimes N}|U \in U(d)\}$ and $\{U^{\otimes N-1} \otimes \overline{U}|U \in U(d)\}$.

One fundamental property will be the size of the generated group algebra which will give a hint on the possible decompositions into irreducible representations. To keep the computations simple we start by introducing a graphical notation for the operators involved which we will denote as the "chip" representation.

Any permutation operator V_π of the "natural" representation of the $\mathfrak{S}_N$ can be written in Dirac notation as

$$V_\pi = \sum_{i_1,\ldots,i_N}^{d,\ldots,d} |\pi(i_1,\ldots,i_N)\rangle\langle i_1,\ldots,i_N|, \tag{2.15}$$

where $\pi(i_1,\ldots,i_N)$ denotes the π-permuted entries $i_1,\ldots,i_N$. Graphically such a ketbra can be interpreted as a "chip" having N pins on the right (inputs) and N pins on the left (outputs). A permutation operator then corresponds to a "chip" connecting the inputs with the outputs via the respective permutation:

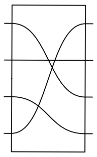
$$V_{(2)(143)} \equiv$$ 

Figure 2.3: The visualization of a permutation as a "chip".

The partial transpositions swap some of the inputs with the corresponding outputs and can generate loops on both sides:

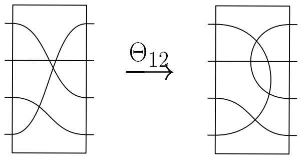


Figure 2.4: The action of a partial transposition on a "chip".

Products of elements of the "chip" group can be computed easily by joining the outputs of the first with the inputs of the second "chip":

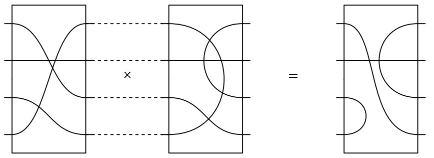


Figure 2.5: Building the product of two “chips”.

The adjoint operator is equal to the representing operator of the inverse group element[32] and can thus be obtained by interchanging inputs and outputs:

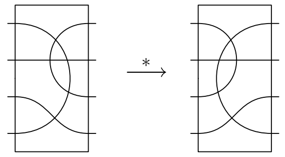


Figure 2.6: Taking the adjoint of a “chip”.

Finally we can also compute the trace of a chip graphically. The trace of a chip is equal to d^l, where l is the number of loops that emerge from connecting the inputs with the outputs:

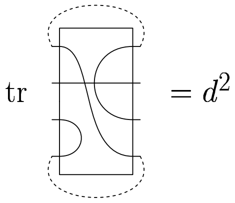


Figure 2.7: Computing the trace of a “chip”.

Using this graphical notation we can now easily count the number of elements in the commutant of $\mathcal{O}^{\otimes\mathcal{N}}$.

Corollary 2.3.1: The commutant of $\mathcal{A}(O^{\otimes N})$ is given by the “chip” algebra, which is a finite dimensional C*-algebra of order $(2N-1)!!$.

[32] This is, however, only due to the fact that we are using a unitary representation, which is the general case.

Proof. By construction we have already obtained that the "chip" algebra is the commutant of $\mathcal{A}(O^{\otimes N})$. What remains to be done is to count the number of such "chips". As any ketbra corresponds to one connection of two pins we can count the number of different sets of connections. For the first one we get $2N-1$ possible connections with the first input pin. For the second connection we may not use the first input pin, the corresponding connected pin and the next input pin leaving $2N-3$ possibilities and so on. ■

If we take, for example, $N=2$ we get $\dim \mathcal{A}(O^{\otimes 2})' = 3!! = 3$ "chips" which correspond to $\{\mathbb{1}, \mathbb{F}, |\Omega\rangle\langle\Omega|\}$. To have an idea of the decomposition into irreducible representations we can use the orthogonality relations[33]. For $N=2$ we have three "chips" leading to

$$3 = 1^2 \oplus 1^2 \oplus 1^2, \tag{2.16}$$

i.e. three one-dimensional irreducible subrepresentations. For $N=3$ we already have 15 elements and the orthogonality relations do not help to find the decomposition. A straightforward but lengthy computation[34] gives

$$15 = 1^2 \oplus 1^2 \oplus 2^2 \oplus 3^2. \tag{2.17}$$

Unfortunately the group given by the "chips" is by far not so well-known as the permutation group so that there are no abstract tools like the Young frames for computing the decomposition other than directly. The parametrisation of $O^{\otimes N}$ invariant states is still possible via the expectation values with the "chips", but for testing positivity one will first have to compute by hand the decomposition into irreducible subrepresentations to boil the problem down to a parametrisation similar to that of multipartite Werner states. Commutative subfamilies of states (for $N \geq 3$) can be obtained in the same way as for the multipartite Werner states, but since the decomposition is not abstractly given we refrain here from presenting examples.

2.4 The power of reduced states

The last section of this chapter is devoted to the behaviour of multipartite symmetric states upon reducing or extending the underlying

[33] Different irreducible representations are orthogonal to each other. In consequence the order of the group is equal to the sum of the squares of the dimensions of the irreducible representations (see [Sim96] Theorem III.1.3).

[34] For simplicity's sake we implemented the "chip$_3$" algebra in Mathematica© to compute the reduction.

system. As one would expect, some symmetry will be left when adding or removing subsystems. The more interesting observation, however, is that when extending the system not only the symmetry but also most of the information will already be fixed by the given reductions as was first pointed out by [LPW02].

2.4.1 Reducing symmetric states

In the special case of multipartite Werner and orthogonal symmetric states the reductions can be easily computed by using the corresponding twirling operation. Due to the cyclicity of the trace it is clear that the reduced states inherit the multipartite Werner symmetry:

$$\begin{aligned}
\mathrm{tr}_N\left\{\rho_N\right\} &= \mathrm{tr}_N\left\{\int_{U(d)} U^{\otimes N}\rho_N U^{*\otimes N} d_H(U)\right\} \\
&= \int_{U(d)} U^{\otimes(N-1)}\rho_{N-1}U^{*\otimes(N-1)}d_H(U) \\
&= \int_{U(d)} U^{\otimes(N-1)}\mathrm{tr}_N\{\rho_N\}U^{*\otimes(N-1)}d_H(U)
\end{aligned} \tag{2.18}$$

and likewise for the orthogonal symmetry. The same holds obviously for the permutation invariance: Removing one subsystem leads to a state invariant under all permutations of $\mathfrak{S}_{N-1}$.

For extremal permutation invariant multipartite Werner states we can even read off the reduced states from the corresponding Young frame. But to see how to read them off we will need one more result related to the branching laws of the $\mathfrak{S}_N$. As we will not need this result later on we restrict ourselves to stating it omitting the proof[35].

Theorem 2.4.1 ([Sim96], VI.4.1): Let $D_{\mathcal{Y}}$ be the irreducible representation of the $\mathfrak{S}_N$ corresponding to the Young frame $\mathcal{Y}$. Then the restriction of $D_{\mathcal{Y}}$ onto $\mathfrak{S}_{N-1}$ can be decomposed into

$$\mathrm{Res}_{\mathfrak{S}_N}^{\mathfrak{S}_{N-1}}\left(D_{\mathcal{Y}}(U)\right) = \bigoplus_{\mathcal{Y}'\lhd\mathcal{Y}} D_{\mathcal{Y}'}(U), \tag{2.19}$$

where $\mathcal{Y}'\lhd\mathcal{Y}$ indicates that the Young frame $\mathcal{Y}'$ can be obtained from $\mathcal{Y}$ by removing one square.

[35] When missing we refer for the proof to the cited number in the respective book.

For the Young projections [36]$p_{\mathcal{Y}}$ of the $\mathfrak{S}_N$ this implies that removing one item (subsystem) leaves a sum of Young projections of the $\mathfrak{S}_{N-1}$:

$$p_{\mathcal{Y}} \xrightarrow{\mathrm{Res}_{\mathfrak{S}_N}^{\mathfrak{S}_{N-1}}} \sum_{\mathcal{Y}' \lhd \mathcal{Y}} p_{\mathcal{Y}'}. \tag{2.20}$$

On the other hand this means that for the normalized Young projections $e_{\mathcal{Y}} = \frac{p_{\mathcal{Y}}}{\dim(\mathcal{Y})}$ we have the following $N-1$-systems reductions:

$$e_{\mathcal{Y}} \xrightarrow{\mathrm{Res}_{\mathfrak{S}_N}^{\mathfrak{S}_{N-1}}} \frac{\sum_{\mathcal{Y}' \lhd \mathcal{Y}} p_{\mathcal{Y}'}}{\sum_{\mathcal{Y}' \lhd \mathcal{Y}} \dim(\mathcal{Y}')} = \frac{\sum_{\mathcal{Y}' \lhd \mathcal{Y}} \dim(\mathcal{Y}') e_{\mathcal{Y}'}}{\dim(\mathcal{Y})}. \tag{2.21}$$

By construction the dimension of a representation does not change upon restriction. Therefore $\dim(\mathcal{Y}) = \sum_{\mathcal{Y}' \lhd \mathcal{Y}} \dim(\mathcal{Y}')$ holds. This result translates directly to the corresponding extremal permutation invariant Werner states:

$$\rho_{\mathcal{Y}} \xrightarrow{\mathrm{tr}_N} \sum_{\mathcal{Y}' \lhd \mathcal{Y}} \lambda_{\mathcal{Y}'} \rho_{\mathcal{Y}'}, \quad \lambda_{\mathcal{Y}'} = \frac{\dim(\mathcal{Y}')}{\sum_{\mathcal{Y}' \lhd \mathcal{Y}} \dim(\mathcal{Y}')}. \tag{2.22}$$

The dimension of an irreducible representation can be read off the corresponding Young frame via the Hook length rule:

Lemma 2.4.2 ([FH91], 4.12): Let $\mathcal{Y}$ be a Young frame of the $\mathfrak{S}_N$, then the dimension of the corresponding irreducible representation is given by

$$\dim(\mathcal{Y}) = \frac{N!}{\prod \text{Hook lengths}}, \tag{2.23}$$

where the Hook length of a box in a Young frame is the number of squares directly below or directly to the right of the box, including the box once.

For example, applying the Hook rule to a Young frame of the $\mathfrak{S}_8$ gives

$$\begin{array}{|c|c|c|c|}\hline & & & \\ \hline & & & \multicolumn{1}{c}{} \\ \cline{1-3} & \multicolumn{3}{c}{} \\ \cline{1-1}\end{array} \quad \xrightarrow{\underline{\text{Hook rule}}} \quad \begin{array}{|c|c|c|c|}\hline 6 & 4 & 3 & 1 \\ \hline 4 & 2 & 1 & \multicolumn{1}{c}{} \\ \cline{1-3} 1 & \multicolumn{3}{c}{} \\ \cline{1-1}\end{array}\,. \tag{2.24}$$

The corresponding dimension can then be calculated to be $\frac{8!}{6\cdot4\cdot4\cdot3\cdot2} = 70$.

Taking the Hook rule together with (2.22) we have derived a graphical method for the computation of the reduced states. We summarize

[36] Note that we distinguish here between the Young projections in group Algebra $\mathcal{A}(\mathfrak{S}_N)$ denoted by a small $p_{\mathcal{Y}}$ and the represented ones denoted by a capital $P_{\mathcal{Y}}$.

this method by giving an example. For this let $N = 6$, then our method gives, for example,

$$\ydiagram{2,2,1,1} \xrightarrow{\mathrm{Res}^{\mathfrak{S}_5}_{\mathfrak{S}_6}} \ydiagram{2,2,1} + \ydiagram{2,1,1,1} \tag{2.25}$$

and

$$\rho_{\ydiagram{2,2,1,1}} \xrightarrow{\mathrm{tr}_6} \frac{5}{9}\rho_{\ydiagram{2,2,1}} + \frac{4}{9}\rho_{\ydiagram{2,1,1,1}}. \tag{2.26}$$

As one might think we can see directly from the branching laws that the reduced states will most often be not again extremal but a mixture of the new extremal ones. There are, however, special situations where extremality is inherited like

$$\ydiagram{2,2} \xrightarrow{\mathrm{Res}^{\mathfrak{S}_3}_{\mathfrak{S}_4}} \ydiagram{2,1}. \tag{2.27}$$

Two situations are in this sense very special as all restrictions from $N - 1$ to 2 remain extremal, namely the totally symmetric and totally antisymmetric states:

$$\boxed{1}\boxed{2}\cdots\boxed{N} \xrightarrow{\mathrm{Res}^{\mathfrak{S}_n}_{\mathfrak{S}_N}} \boxed{1}\boxed{2}\cdots\boxed{n} \quad \text{and} \quad \begin{array}{c}\boxed{1}\\ \boxed{2}\\ \vdots\\ \boxed{N}\end{array} \xrightarrow{\mathrm{Res}^{\mathfrak{S}_n}_{\mathfrak{S}_N}} \begin{array}{c}\boxed{1}\\ \boxed{2}\\ \vdots\\ \boxed{n}\end{array} \tag{2.28}$$

The completely antisymmetric states for $N = d$ have recently been investigated in detail. In that case one has a pure state[37] which can be used to solve the N strangers problem, the secret sharing problem and the liar detection problem [Cab02].

2.4.2 Extending symmetric states

Given a set of density operators it is not always possible to find an extension to one overall state. The most prominent example of this is certainly that three parties cannot be pairwise maximally entangled.

[37] In fact, this is the only pure state in the family of multipartite Werner states.

In subsection 3.3.1 we will study when such an extension from bipartite to tripartite Werner states is possible. This subsection, however, will deal with the special properties that a symmetric extension has if it exists.

Another specialty of the totally antisymmetric state with $d = N$ is that it is completely determined by its two particle reductions:

Lemma 2.4.3: Let $\Psi_-^N \in \mathcal{H}^{\otimes N}$ with $\dim \mathcal{H} = N$ be the totally antisymmetric singlet state

$$|\Psi_-^N\rangle = \frac{1}{\sqrt{N!}} \sum_{i_1,\ldots,i_N} \epsilon_{i_1,\ldots,i_N} |i_1,\ldots,i_n\rangle. \tag{2.29}$$

For any N this state is completely determined by its bipartite reductions, i.e. there is no other state such that all its two-party reduced states are proportional to the projector $P_- = \frac{\mathbb{1}-\mathbb{F}}{2}$ onto the antisymmetric subspace.

Proof. The proof is based on the fact that Fermi-/Bose symmetry can be decided on the level of bipartite reductions. Assume that we have a state ρ with spectral decomposition $\rho = \sum_i \lambda_i |\lambda_i\rangle\langle\lambda_i|$ and bipartite reductions proportional to P_-. Then every eigenvector has to satisfy $\langle\lambda_i|\mathbb{1} \otimes P_+|\lambda_i\rangle = 0$ which implies $(\mathbb{1} \otimes P_-)|\lambda_i\rangle = |\lambda_i\rangle$. Hence, we have $(\mathbb{1} \otimes \mathbb{F})|\lambda_i\rangle = -|\lambda_i\rangle$ (for every $\mathbb{F}$) such that every eigenvector of ρ has to be totally antisymmetric. However, the totally antisymmetric subspace for $d = n$ is one-dimensional, and thus $\rho = |\Psi_-^N\rangle\langle\Psi_-^N|$. ■

Although this situation may seem very special, in [LPW02, LW02] it was shown that for *pure* states it is quite common. In fact, they proved that *almost every* such pure state is completely determined by reductions of not more than two third of the parties. For mixed states, however, the situation is different. The extension is in general not unique and symmetric $N-1$ particle reductions do not even imply the symmetry of the full state. Indeed, $\rho + \epsilon \bigotimes_i^n A_i$ with $\mathrm{tr}[A_i] = 0$ and ρ having full support with ϵ sufficiently small has the same reductions as ρ but need not be symmetric.

One possibility of distinguishing between one state ρ and the various possible extensions of its k particle reductions is to look at the information contained in the states. In [LPW02] a measure was introduced characterizing the extent to which lower order correlations already determine higher ones that can be seen as an analogue to the mutual information for the bipartite case. For a state $\rho \in \mathcal{B}(\mathcal{H}^{\otimes N})$ with

k-party reductions $\rho_K \overset{\text{def}}{=} \mathrm{tr}_{N\setminus K}[\rho]$ where $K \subset N = \{1, \ldots, n\}$, $k = |K|$ the measure proposed therein is then defined as

$$M_k := \sup_{\substack{\tilde{\rho} \\ |K|=k \\ \tilde{\rho}_K = \rho_K}} \left\{ S(\tilde{\rho}) - S(\rho) \right\}, \tag{2.30}$$

where $S(\rho)$ is the von Neumann entropy. The symmetric extension turns out to be among the few optimal ones for Werner states:

Lemma 2.4.4: Let the k-party reduced states of ρ have Werner symmetry, i.e. $\left[U^{\otimes k}, \rho_K\right]_- = 0$, for all $U \in U(d)$, then there exists an optimal state $\tilde{\rho}$ achieving the supremum in (2.30) which has itself Werner symmetry with respect to all N tensor factors.

Proof. Assume that $\tilde{\rho}$ is any state having the reductions $\tilde{\rho}_K = \rho_K$. Then the *twirled* state

$$\mathcal{T}_{U^{\otimes N}}(\tilde{\rho}) = \int_{U(d)} U^{\otimes N} \tilde{\rho} U^{*\otimes N} dU \tag{2.31}$$

has the same k-party reductions as ρ if $\left[U^{\otimes k}, \rho_K\right]_- = 0$ holds:

$$\mathrm{tr}_{N\setminus K}\left\{\mathcal{T}_{U^{\otimes N}}(\tilde{\rho})\right\} = \int_{U \in U(d)} U^{\otimes k} \tilde{\rho}_K U^{*\otimes k} dU = \rho_K. \tag{2.32}$$

Hence $\mathcal{T}_{U^{\otimes N}}(\tilde{\rho})$ is again a valid state for (2.30). Moreover, since $\mathcal{T}_{U^{\otimes N}}(\tilde{\rho})$ is a convex mixture of states having the entropy $S(\tilde{\rho})$, and the von Neumann entropy is concave, we have $S\left(\mathcal{T}_{U^{\otimes N}}(\tilde{\rho})\right) \geq S\left(\tilde{\rho}\right)$. Therefore the optimum in (2.30) is attained for a symmetric state $\mathcal{T}_{U^{\otimes N}}(\tilde{\rho}) = \tilde{\rho}$. ■

In a similar way the symmetric extension turns out to be among the optimal ones in the case of an additional permutation invariance:

Lemma 2.4.5: Let a permutation invariant state ρ have k-party reductions which have in turn Werner symmetry. Then there is an optimal $\tilde{\rho}$, which has also Werner and permutation symmetry.

Proof. Due to Lemma 2.4.4 it only remains to be shown that the twirl operation corresponding to permutation symmetry, i.e.

$$\mathcal{T}_{\mathfrak{S}_N}(\tilde{\rho}) = \frac{1}{N!} \sum_{\pi \in \mathcal{S}_N} V_\pi \tilde{\rho} V_\pi^* \tag{2.33}$$

preserves the reductions $\tilde{\rho}_K$. Following Lemma 2.4.5 we can assume that there is an optimal $\tilde{\rho}$ having Werner symmetry, that is its k-party reductions are completely determined by the expectation values of the permutation operators $x_\sigma(\tilde{\rho}) = \mathrm{tr}[V_\sigma \tilde{\rho}]$, where $\sigma \in \mathcal{S}_k$ and V_σ is the identity on at least $N-k$ sites. Moreover, permutation symmetry requires that $x_\sigma(\tilde{\rho}) = x_{\sigma'}(\tilde{\rho})$ if σ and σ' belong to the same conjugacy class, i.e. if there is a $\pi \in \mathfrak{S}_N$ such that $\pi\sigma\pi^{-1} = \sigma'$. The reductions of the twirled state are then characterized by

$$x_\sigma\left(\mathcal{T}_{\mathfrak{S}_N}(\tilde{\rho})\right) = \frac{1}{N!}\sum_{\pi\in\mathfrak{S}_N} \mathrm{tr}[\tilde{\rho}V_\pi^* V_\sigma V_\pi] = x_\sigma(\tilde{\rho}). \tag{2.34}$$

That is the permutation twirl in (2.33) preserves the reductions in the considered case. ■

Summarizing we can say that the twirling operations not only wipe out the local information[38] but also minimize[39] the information difference between the overall state and its reductions.

[38] Single parties have a completely chaotic reduced state for Werner and orthogonal symmetry.

[39] According to Jaynes' principle (see [Jay57a, Jay57b]) the state fulfilling the additional requirements that has maximal entropy is the most unbiased estimator and thus leads to the minimal information.

Chapter 3

Tripartite Werner states

"Three is a large number."

(David Stove, *The Plato Cult and Other Philosophical Follies*)

In this chapter we will explore the properties introduced in chapter 1 for an example of the states introduced in chapter 2. The simplest non-trivial example is the family of tripartite Werner states. It is the simplest since we will have to deal with only five parameters and it is nontrivial as it already shows the peculiarity of multipartite entanglement and of non-commutativity. We will start by studying the separability properties comparing the analytical results with the strongest separability criteria, namely the positivity of the partial transpose and the cross norm criteria. Afterwards we move on to their entanglement properties. Following chapter 2 we will then turn to the predictive power of their reduced states and finish by taking a closer look at the manifold generated by this state family relating it to the problem of state estimation for this special class. Most of this chapter (though not all) has already been published in [EW01].

As shown in subsection 2.2.1 tripartite Werner states can be written in terms of the permutation operators of the $\mathfrak{S}_3$:

$$\rho \in \mathcal{S}_{U^{\otimes 3}} \Longleftrightarrow \rho = \sum_{\pi \in \mathfrak{S}_3} \mu_\pi V_\pi \tag{3.1}$$

with unitary operators V_π defined as in (2.15). The above equation, however, does not treat the question how to recognize density matrices in terms of the six coefficients μ_π. Hermiticity requires $\mu_{\pi^{-1}} = \overline{\mu_\pi}$, leaving, effectively, six real parameters. One more is fixed by normalization, so that $\mathcal{S}_{U^{\otimes 3}}$ is embedded in a five-dimensional real vector space. In terms of the parameters μ_π positivity is not easy to see. For this reason we will take the second parametrisation presented in 2.2.1 and consisting of the projections onto the irreducible representations P_+, P_- and P_0 and three more operators. Due to the fact that the third irreducible representation is two-dimensional it is isomorphic to the 2×2-matrices. Therefore we can take the remaining three operators R_1, R_2, R_3 as analogue to the Pauli matrices. The new basis is then:

$$\begin{aligned}
R_+ &= P_+ = \frac{1}{6}\left(\mathbb{1} + V_{(12)} + V_{(23)} + V_{(31)} + V_{(123)} + V_{(321)}\right),\\
R_- &= P_- = \frac{1}{6}\left(\mathbb{1} - V_{(12)} - V_{(23)} - V_{(31)} + V_{(123)} + V_{(321)}\right),\\
R_0 &= P_0 = \frac{1}{3}\left(2 \cdot \mathbb{1} - V_{(123)} - V_{(321)}\right),\\
R_1 &= \frac{1}{3}\left(2V_{(23)} - V_{(31)} - V_{(12)}\right),\\
R_2 &= \frac{1}{\sqrt{3}}\left(V_{(12)} - V_{(31)}\right),\\
R_3 &= \frac{i}{\sqrt{3}}\left(V_{(123)} - V_{(321)}\right).
\end{aligned} \tag{3.2}$$

In other words, the six hermitian operators $R_+, R_-, R_0, R_1, R_2, R_3$ are characterized by the commutation relations $R_i R_\pm = R_\pm R_i = 0$, $R_i^2 = R_0$, for $i = 0, 1, 2, 3$, and $R_1 R_2 = iR_3$ with cyclic permutations.

Now every operator $\rho \in \mathcal{S}_{U^{\otimes 3}}$ can be decomposed into the orthogonal parts $R_+\rho$, $R_-\rho$, and $R_0\rho$, and positivity of ρ is equivalent to the positivity of these three operators. This leads to the following lemma:

Lemma 3.0.6: For any operator ρ on $\mathcal{H} \otimes \mathcal{H} \otimes \mathcal{H}$ define the six parameters $r_k(\rho) = \mathrm{tr}[\rho R_k]$, for $k \in \{+, -, 0, 1, 2, 3\}$. Then we have that $r_k(\mathcal{T}_{U^{\otimes 3}}(\rho)) = r_k(\rho)$. Moreover, each $\rho \in \mathcal{S}_{U^{\otimes 3}}$ is uniquely characterized by the tuple $(r_+, r_-, r_0, r_1, r_2, r_3) \in \mathbb{R}^6$, and such a tuple belongs to a density matrix $\rho \in \mathcal{S}_{U^{\otimes 3}}$ if and only if

$$\begin{aligned}
r_+, r_-, r_0 \geq 0, &\qquad r_+ + r_- + r_0 = 1\\
\text{and} &\qquad r_1^2 + r_2^2 + r_3^2 \leq r_0^2.
\end{aligned} \tag{3.3}$$

Proof. The positivity of r_+, r_- and r_0 is given by definition as well as the identity $r_+ + r_- + r_0 = 1$. We then only have to check the positivity of the two-dimensional part which is isomorphic to

$$P_0 \rho P_0 \cong \frac{1}{2} \begin{pmatrix} r_0 + r_3 & r_1 - ir_2 \\ r_1 + ir_2 & r_0 - r_3 \end{pmatrix}. \tag{3.4}$$

For 2×2-matrices positivity is equivalent to positivity of the trace and of the determinant. Since the trace gives $\operatorname{tr}[P_0 \rho P_0] = r_0$, it is already positive and we only have to demand the positivity of the determinant, i.e. $\det P_0 \rho P_0 = r_0^2 - r_1^2 - r_2^2 - r_3^2 \geq 0$. ■

As already mentioned this parametrisation does not depend on the dimension of the underlying Hilbert space except for one case: for $d = 2$ the antisymmetric projection R_- is simply zero, so for qubits we get the additional constraint $r_- = 0$.

Taking $r_0 = 1 - r_+ - r_-$ to be redundant, we get a simple representation of $\mathcal{S}_{U^{\otimes 3}}$ as a convex set in five dimensions. Unfortunately, five-dimensional sets are still not very amenable to graphical representation. In order to visualize the sets we are going to describe analytically, we will therefore use suitable two- and three-dimensional representations. Again, we have the possibility of using sections or projections of $\mathcal{S}_{U^{\otimes 3}}$, and we will emphasize sections which can also be understood as projections.

The simplest example of this is to take the subset $\mathcal{S}_{U^{\otimes 3}, \mathcal{S}_3} \subset \mathcal{S}_{U^{\otimes 3}}$ of states, which also commute with all permutations. The corresponding projection is simply averaging with respect to permutations. Clearly, $\mathcal{S}_{U^{\otimes 3}, \mathcal{S}_3}$ consists of those operators in $\mathcal{S}_{U^{\otimes 3}}$, which are linear combinations of R_+, R_-, R_0 alone. Taking r_+ and r_- as coordinates we get the triangle in figure 3.1. Thus each point in this triangle represents a density operator in $\mathcal{S}_{U^{\otimes 3}, \mathcal{S}_3}$. On the other hand, it represents the set of states in $\mathcal{S}_{U^{\otimes 3}}$ projecting to it on permutation averaging: this will be all states with the given values of r_+ and r_- in the six-tuple, which therefore differ only in the values of r_1, r_2, and r_3. Thus over every point of the triangle in figure 3.1 we should imagine a Bloch sphere of radius r_0.

If more detail is required, we will also use three-dimensional sections and/or projections of a similar nature. For example, if we average only over the permutation $V_{(23)}$, we get the subset $\mathcal{S}_{U^{\otimes 3}}^{(23)} \subset \mathcal{S}_{U^{\otimes 3}}$ with $r_2 = r_3 = 0$ (see the dotted tetrahedron in figure 3.10). Averaging only over cyclic permutations, we get the subset $\mathcal{S}_{U^{\otimes 3}}^{\mathrm{cyc}} \subset \mathcal{S}_{U^{\otimes 3}}$ with $r_1 = r_2 = 0$ (which gives the same tetrahedron as $\mathcal{S}_{U^{\otimes 3}}^{(23)}$ with r_1 substituted by r_3.).

We note for later use that the expectation values r_k are *not* the coef-

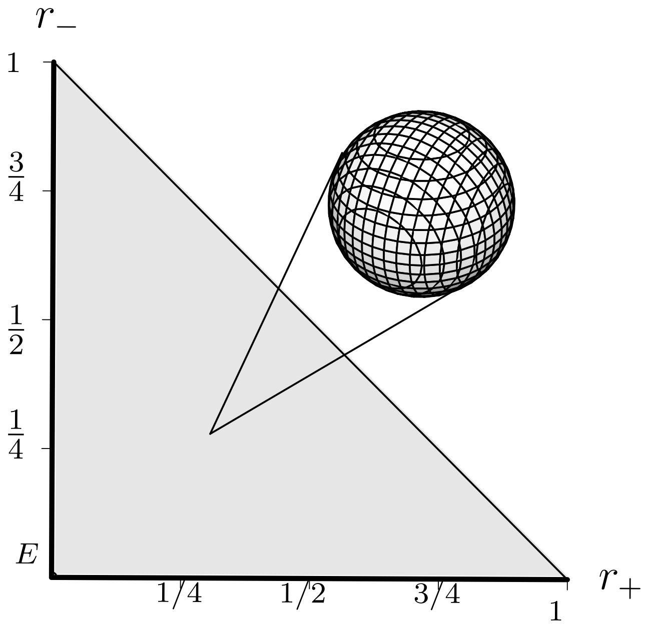


Figure 3.1: Description of $\mathcal{S}_{U^{\otimes 3}}$ in terms of the triangle $\mathcal{S}^P_{U^{\otimes 3}}$ and the corresponding Bloch sphere for each point in $\mathcal{S}^P_{U^{\otimes 3}}$. The sphere represents the two-dimensional representation χ_0 whereas the triangle represents the two one-dimensional ones χ_+ and χ_- (see (1.43)).

ficients in the sum

$$\rho = \sum_{k=+,-,0,1,2,3} c_k R_k. \tag{3.5}$$

These are related to the r_k by the following dimension dependent transformation (which is obtained by observing that $\mathrm{tr}[\mathbb{1}] = d^3$, $\mathrm{tr}\big[V_{(12)}\big] = d^2$, and $\mathrm{tr}\big[V_{(123)}\big] = d$):

$$\begin{aligned} r_+ &= \frac{d}{6}(d^2 + 3d + 2)c_+ \\ r_- &= \frac{d}{6}(d^2 - 3d + 2)c_- \\ r_i &= \frac{2d}{3}(d^2 - 1)c_i \quad \text{for } i = 0, 1, 2, 3. \end{aligned} \tag{3.6}$$

These dimension dependent factors stem from the representation used. In fact, one can easily see that they correspond exactly to the multiplicities in the decomposition given by (2.9). They are equal to the dimension of the Bose subspace $\mathrm{tr}[P_+] = \frac{1}{6}(d^3 + 3d^2 + 2d)$, the dimension of the

Fermi subspace $\mathrm{tr}[P_-] = \frac{1}{6}(d^3 - 3d^2 + 2d)$ and to the dimension of the complement $\mathrm{tr}[P_0] = d^3 - \mathrm{tr}[P_+] - \mathrm{tr}[P_-] = \frac{2}{3}(d^3 - d)$.

With this characterization of tripartite Werner states at hand, we can start exploring their separability properties.

3.1 Separability properties

We now describe the natural separability properties we will chart for these special states.

Of course, we can split the system into just two subsystems and apply the usual separability/entanglement distinctions. A split $1|23$ then corresponds to the grouping of the Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3$ into $\mathcal{H}_1 \otimes (\mathcal{H}_2 \otimes \mathcal{H}_3)$. We call a density operator ρ on this Hilbert space $1|23$-*separable*, or just *biseparable* if the partition is clear from the context, if we can write

$$\rho = \sum_\alpha \lambda_\alpha \, \rho_\alpha^{(1)} \otimes \rho_\alpha^{(23)}, \tag{3.7}$$

with $\lambda_\alpha \geq 0$ and density operators $\rho_\alpha^{(23)}$ on $\mathcal{H}_2 \otimes \mathcal{H}_3$. We will denote the set of such ρ by $\mathcal{B}_1$. This set will be computed in subsection 3.1.2. Furthermore, as they are necessary conditions for biseparability (see [Per96]), we are going to look at those states ρ having a *positive partial transpose* with regard to such a split, denoted by $\rho \in \mathcal{P}_1$, and at those states satisfying the realignment criteria (see [Fan02]). It is clear that $\mathcal{B}_1 \subset \mathcal{P}_1$ holds, but as we will show in section 3.1.4 by computing $\mathcal{P}_1$, this inclusion is strict except for $d = 2$.

As a genuinely "tripartite" notion of separability, we consider states, called *triseparable* (or "three-way classically correlated"), which can be decomposed as

$$\rho = \sum_\alpha \lambda_\alpha \, \rho_\alpha^{(1)} \otimes \rho_\alpha^{(2)} \otimes \rho_\alpha^{(3)}, \tag{3.8}$$

where $\lambda_\alpha \geq 0$, and the $\rho_\alpha^{(i)}$ are density operators on the respective Hilbert spaces. The set of such density operators will be denoted by $\mathcal{T}$. Of course, we may also consider states which are biseparable for all three partitions. It is known from [BDM+99] that this does not imply triseparability, i.e. $\mathcal{T} \subsetneqq (\mathcal{B}_1 \cap \mathcal{B}_2 \cap \mathcal{B}_3)$. Further examples of states showing triple biseparability but not triseparability will be found in subsection 3.1.2. Since we will only be interested in a five-dimensional set $\mathcal{S}_{U^{\otimes 3}}$ of symmetric states, we will from now on use the symbols $\mathcal{T}, \mathcal{B}_1$ and $\mathcal{P}_1$ only for the corresponding subsets of $\mathcal{S}_{U^{\otimes 3}}$.

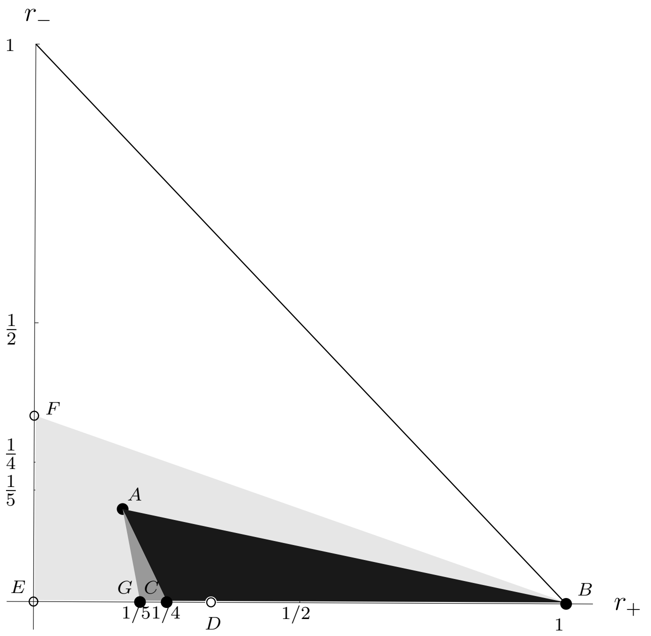


Figure 3.2: Subsets of $\mathcal{S}_{U^{\otimes 3},\mathcal{S}_3}$ with different separability properties. Black: triseparable states, dark grey: biseparable states, light grey: images of biseparable states under permutation averaging. Special points labelled by letters are explained in the text.

An overview of the main results of the separability properties is given in figure 3.2. To keep the picture as simple as possible, we have only depicted the set $\mathcal{S}_{U^{\otimes 3},\mathcal{S}_3}$, i.e. the triangle in figure 3.1. Naturally, this reduction does not allow the representation of our full results, i.e. the detailed structure of the five-dimensional convex sets $\mathcal{T}$, $\mathcal{B}_1$ and $\mathcal{P}_1$, which will be described in the corresponding sections. However, we found this diagram quite useful as a basic map in order not to lose our way in five dimensions.

The shading in figure 3.2 marks different separability properties, and the points labelled with capital letters arise by projecting pure states with special properties with the twirl projection $\mathcal{T}_{U^{\otimes 3}}$. Some of these points (D,E and F) do not lie in the plane $\mathcal{S}_{U^{\otimes 3},\mathcal{S}_3}$, i.e. they have non-zero coordinates (r_1, r_2, r_3). They are represented by white circles, in contrast to the black circles (A,B,C,G and H) representing permutation invariant states in the plane $\mathcal{S}_{U^{\otimes 3},\mathcal{S}_3}$.

The *triseparable* states correspond to the black triangle $\triangle$(ABC). It is easy to see that any triseparable state projected by permutation averaging to $\mathcal{S}_{U^{\otimes 3},\mathcal{S}_3}$ is again triseparable, i.e. the projection of $\mathcal{T}$ onto $\mathcal{S}_{U^{\otimes 3},\mathcal{S}_3}$ coincides with $\mathcal{T} \cap \mathcal{S}_{U^{\otimes 3},\mathcal{S}_3}$. The extreme points of this set are

$$\begin{aligned} A :&|123\rangle \longrightarrow (1/6, 1/6, 0, 0, 0), \qquad B : |111\rangle \longrightarrow (1, 0, 0, 0, 0), \\ C :&(|111\rangle - \sqrt{3}|112\rangle + \sqrt{3}|121\rangle - 3|122\rangle)/4 \longrightarrow (1/4, 0, 0, 0, 0), \end{aligned} \tag{3.9}$$

where the notation $\Psi \longrightarrow (r_+, r_-, r_1, r_2, r_3)$ indicates that the pure state $|\Psi\rangle\langle\Psi|$ is projected to this point by $\mathcal{T}_{U^{\otimes 3}}$. In other words, $\langle\Psi|R_k\Psi\rangle = r_k$ for $k = +, -, 1, 2, 3$. Note that all three vectors given are product vectors, the one for C being the product of three vectors in the "Mercedes star" configuration in the plane, at angle $120°$ from each other.

A quantitative description of the genuinely tripartite entanglement of $\mathcal{S}_{U^{\otimes 3}}$ is given in section 3.2 in terms of the relative entropy, the trace norm distance and violations of tripartite Bell inequalities.

The *biseparable* set $\mathcal{B}_1$ is not permutation invariant, since the partition $1|23$ clearly is not. As a consequence, the permutation average projecting $\mathcal{S}_{U^{\otimes 3}}$ onto $\mathcal{S}_{U^{\otimes 3},\mathcal{S}_3}$ does not map $\mathcal{B}_1$ into itself, and we have to distinguish in our diagram between points (r_+, r_-) such that $(r_+, r_-, 0, 0, 0)$ is biseparable (i.e. the *intersection* $\mathcal{B}_1 \cap \mathcal{S}_{U^{\otimes 3},\mathcal{S}_3}$), and points (r_+, r_-) such that for some suitable (r_1, r_2, r_3) the quintuple $(r_+, r_-, r_1, r_2, r_3)$ represents a point in $\mathcal{B}_1$, (i.e. the *projection* of $\mathcal{B}_1$ onto $\mathcal{S}_{U^{\otimes 3},\mathcal{S}_3}$). In figure 3.2 the intersection is the triangle $\triangle$(GAB), drawn in a darker shade of grey than the triangle $\triangle$ (EFB), which is the projection of the biseparable subset $\mathcal{B}_1$. Note that the shading reflects the inclusion relations, i.e. triseparable states are, in particular, biseparable, and the section of the biseparable set is contained in its projection. Of course, the states in $\mathcal{B}_1 \cap \mathcal{S}_{U^{\otimes 3},\mathcal{S}_3}$ are also biseparable for the other two partitions, since they are permutation invariant. Similarly, the projections of $\mathcal{B}_2$ and $\mathcal{B}_3$ onto $\mathcal{S}_{U^{\otimes 3},\mathcal{S}_3}$ are the same.

Points of special interest for the biseparable set arise from the following vectors:

$$\begin{aligned} D :&|122\rangle \longrightarrow (1/3, 0, 2/3, 0, 0), \\ E :&(|112\rangle - |121\rangle)/\sqrt{2} \longrightarrow (0, 0, -1, 0, 0), \\ F :&(|123\rangle - |132\rangle)/\sqrt{2} \longrightarrow (0, 1/3, -2/3, 0, 0), \\ G :&(|112\rangle - |121\rangle - \sqrt{3}|122\rangle)/\sqrt{5} \longrightarrow (1/5, 0, 0, 0, 0). \end{aligned} \tag{3.10}$$

Here the points B,D,E and F are extreme points of $\mathcal{B}_1$ and span a tetrahedron, which is equal to the subset $\mathcal{B}_1 \cap \mathcal{S}^{(23)}_{U^{\otimes 3}}$ of states invariant under the exchange $2 \leftrightarrow 3$. The point G lies on the line connecting E and D and is the unique extreme point of $\mathcal{B}_1 \cap \mathcal{S}_{U^{\otimes 3},\mathcal{S}_3}$, which is not triseparable. In this sense it represents an extreme case demonstrating the inequality $\mathcal{T} \neq (\mathcal{B}_1 \cap \mathcal{B}_2 \cap \mathcal{B}_3)$.

The set $\mathcal{P}_1$ of states with *positive partial transpose* with respect to the partition $1|23$ contains $\mathcal{B}_1$ strictly, but the difference cannot be seen in this diagram. In fact, we will show in section 3.1.4 that even the 23-invariant subsets of $\mathcal{P}_1$ and $\mathcal{B}_1$ coincide, i.e. $\mathcal{P}_1 \cap \mathcal{S}^{(23)}_{U^{\otimes 3}}$ is spanned by the same four extreme points B,D,E, and F.

As will be seen in section 3.1.4 there is a close connection between the problems of finding $\mathcal{P}_1$ and finding states invariant under averaging over all unitaries of the form $\overline{U} \otimes U \otimes U$. It turns out that the sets of triseparable and biseparable states commuting with such unitaries can be obtained via a simple linear transformation from their counterparts $\mathcal{T} \cap \mathcal{S}_{U^{\otimes 3}}$ and $\mathcal{B}_1 \cap \mathcal{S}_{U^{\otimes 3}}$ computed in this paper. This mapping and a sketch of the results are given in the subsection 3.1.3.

3.1.1 Fully separable states

If a state ρ is triseparable, hence has a decomposition of the form (3.8), we may also find a decomposition in which all factors $\rho^{(i)}_\alpha$ are pure, simply by decomposing each of these density operators into pure ones. Applying to such a decomposition the projection $\mathcal{T}_{U^{\otimes 3}}$, we find that $\rho \in \mathcal{T} \subset \mathcal{S}_{U^{\otimes 3}}$ if and only if ρ is a convex combination of states of the form $\mathcal{T}_{U^{\otimes 3}}(|\Psi\rangle\langle\Psi|)$, where $\Psi = \psi_1 \otimes \psi_2 \otimes \psi_3$ is a normalized product vector. Let us denote by $\mathcal{T}_{\text{pure}} \subset \mathcal{S}_{U^{\otimes 3}}$ the set of such states. Our strategy for determining $\mathcal{T}$ will be to first get $\mathcal{T}_{\text{pure}}$, and then to obtain $\mathcal{T}$ as its convex hull. The resulting characterization of $\mathcal{T}$ is formulated in Theorem 3.1.3.

Given a product vector $\Psi = \psi_1 \otimes \psi_2 \otimes \psi_3$, it is easy to compute the projected state $\mathcal{T}_{U^{\otimes 3}}(|\Psi\rangle\langle\Psi|)$: By Lemma 3.0.6 one just has to compute the expectations of the permutation operators. For example, $\langle\Psi|V_{(12)}\Psi\rangle = \langle\psi_1 \otimes \psi_2 \otimes \psi_3|\psi_2 \otimes \psi_1 \otimes \psi_3\rangle = |\langle\psi_1|\psi_2\rangle|^2$. In this way it is easily seen that the expectations of all permutations are $\{1, a_1, a_2, a_3, a_4 + ia_5, a_4 - ia_5\}$, where the five real parameters are given by

$$\begin{aligned}
a_1 &= |\langle\psi_2|\psi_3\rangle|^2, \\
a_2 &= |\langle\psi_3|\psi_1\rangle|^2, \\
a_3 &= |\langle\psi_1|\psi_2\rangle|^2, \\
a_4 &= \Re e\left(\langle\psi_1|\psi_2\rangle\langle\psi_2|\psi_3\rangle\langle\psi_3|\psi_1\rangle\right), \\
a_5 &= \Im m\left(\langle\psi_1|\psi_2\rangle\langle\psi_2|\psi_3\rangle\langle\psi_3|\psi_1\rangle\right).
\end{aligned} \tag{3.11}$$

Since a pure state in d dimensions (taken up to a factor) is given by $2d-2$ real parameters, these five quantities are a considerable reduction from the $6(d-1)$ parameters determining the three vectors ψ_i. However, they are still not independent, due to the identity

$$f(a_1, a_2, a_3, a_4, a_5) := a_4^2 + a_5^2 - a_1 a_2 a_3 = 0. \tag{3.12}$$

Since we want to determine $\mathcal{T}_{\text{pure}}$ exactly, we also have to find the exact range of these parameters, as the ψ_i vary over all unit vectors. This is done in the following lemma.

Lemma 3.1.1: A tuple $(a_1, a_2, a_3, a_4, a_5) \in \mathbb{R}^5$ arises via equations (3.11) from three unit vectors ψ_1, ψ_2, ψ_3 in a d-dimensional Hilbert space (with $d > 3$), if and only if equation (3.12) is satisfied, $0 \leq a_i \leq 1$ for $i = 1, 2, 3$, and

$$1 - a_1 - a_2 - a_3 + 2a_4 \geq 0. \tag{3.13}$$

If $d = 2$ the lemma holds with last inequality replaced by equality.

Proof. Necessity of equation (3.12), and $0 \leq a_i \leq 1$ is clear. Inequality (3.13) is just the condition that the expectation of antisymmetric projection should be positive. Since this projection vanishes for $d = 2$, it is also clear that equality must hold in this case.

Suppose now that $a_1, \ldots, a_5$ satisfying these constraints are given. We have to reconstruct ψ_1, ψ_2, and ψ_3 satisfying equations (3.11). These equations essentially determine the 3×3-matrix $M_{ij} = \langle \psi_i | \psi_j \rangle$ of scalar products. Of course, we already know the absolute values of its entries (note $M_{ii} = 1$). The phases are irrelevant up to some extent: multiplying any row with a phase, and the corresponding column with its complex conjugate will not change the a_i after equation (3.11), and amounts to multiplying one of the ψ_i with a phase. Hence we may assume that the scalar products $\langle \psi_1 | \psi_2 \rangle$ and $\langle \psi_2 | \psi_3 \rangle$ are positive. The phase of the remaining scalar product $\langle \psi_3 | \psi_1 \rangle$ is then the same as the phase of $a_4 + ia_5$, hence M is essentially uniquely determined by the a_i.

Now a matrix M is a matrix of scalar products if and only if it is positive definite: on the one hand, $\sum_{ij} \overline{u_i} u_j M_{ij} = \| \sum_i u_i \psi_i \|^2 \geq 0$. On the other hand, we can construct a Hilbert space with such scalar products as the space of formal linear combinations of three vectors, with scalar products of basis vectors *defined* by M. Positive definiteness of M then ensures the positivity of the norm in this new Hilbert space. The dimension of this space is the rank of M (number of linearly independent rows/columns). So in the present case the dimension will be 3

(but any larger space will also contain appropriate vectors) or ≤ 2, if M is a singular matrix.

Positive definiteness of M is equivalent to the positivity of all subdeterminants. The diagonal elements are 1, hence positive anyway. Positivity of the three 2×2 subdeterminants is equivalent to $a_i \leq 1$ for $i = 1, 2, 3$. Finally, the full determinant of M, expressed in terms of the a_i gives the expression (3.13). It must be positive, and for $d = 2$ it must vanish, since M is singular. ■

Lemma 3.1.1 describes the set $\mathcal{T}_{\text{pure}}$ of projected pure product states as a compact subset of the hypersurface in $\mathbb{R}^5$ defined by equation (3.12). Computing the convex hull of this set in $\mathbb{R}^5$ is the same as computing the convex hull of $\mathcal{T}_{\text{pure}}$, because the expectations of permutations or the operators R_k from (3.2) are affine functions of the a_i. Explicitly, the expectations $r_k = \langle\Psi|R_k\Psi\rangle$, $k = +, -, 0, 1, 2, 3$, which we have used as our standard coordinates in $\mathcal{S}_{U^{\otimes 3}}$ are

$$\begin{aligned} r_+ &= \tfrac{1}{6}\,(1 + (a_1 + a_2 + a_3) + 2a_4), & r_- &= \tfrac{1}{6}\,(1 - (a_1 + a_2 + a_3) + 2a_4), \\ r_0 &= \tfrac{2}{3}(1 - a_4), & r_1 &= \tfrac{1}{3}(2a_1 - a_2 - a_3), \\ r_2 &= \tfrac{1}{\sqrt{3}}(a_3 - a_2), & r_3 &= \tfrac{2}{\sqrt{3}}a_5. \end{aligned} \tag{3.14}$$

We begin by computing the projection of $\mathcal{T}_{\text{pure}}$ onto the (r_+, r_-)-plane, by determining the possible range of the combinations $m = (a_1 + a_2 + a_3)/3$ and a_4. By choosing phases for the scalar products we can make a_4 vary in the range $|a_4| \leq (a_1 a_2 a_3)^{1/2} = g^{3/2}$, where m and g are the arithmetic and the geometric mean of a_1, a_2, a_3. As is well known, $g \leq m$, and equality holds if $a_1 = a_2 = a_3$. Hence the projection of $\mathcal{T}_{\text{pure}}$ is contained between the parameterized lines

$$r_+(m) = \frac{1}{6}(1 + 3m \pm 2m^{2/3}) \quad \text{and} \quad r_-(m) = \frac{1}{6}(1 - 3m \pm 2m^{2/3}). \tag{3.15}$$

Plotting these curves gives figure 3.3. It is clear that the shape is not convex, and its convex hull is the triangle △(ABC).

A similar plot of the set $\mathcal{T}_{\text{pure}}$ including one more coordinate, r_3, is given in figure 3.4.

Again it is clear that no point on the surface can be an extreme point of the convex hull of the surface, because the surface “curves the wrong way”. This is the intuition behind the following lemma, by which we will show that also in the full five-dimensional case the interior of $\mathcal{T}_{\text{pure}}$ contains no extreme points.

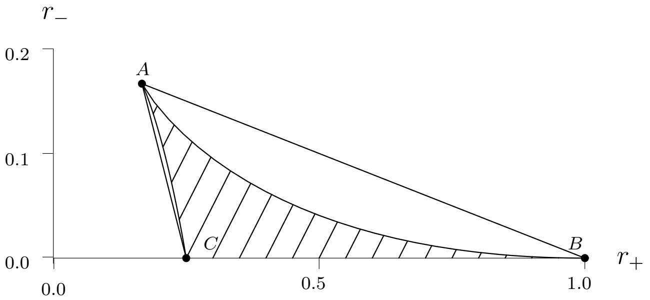


Figure 3.3: Section of the set $\mathcal{T}_{\text{pure}}$ with $\mathcal{S}^P_{U^{\otimes 3}}$ and its convex hull.

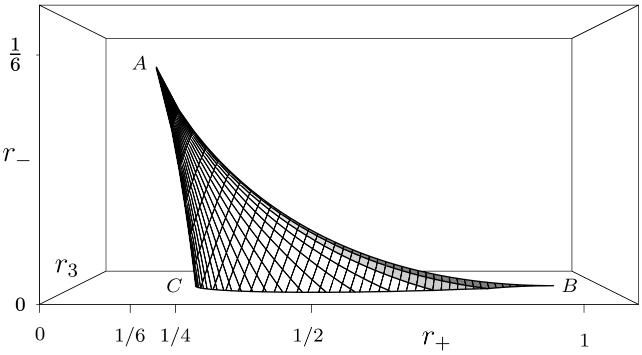


Figure 3.4: Plot of the same section as above making additional use of the coordinate r_3.

Lemma 3.1.2: Let $N_f = \{x \in \mathbb{R}^n \mid f(x) = 0\}$ be the zero surface of a function $f \in \mathcal{C}^2(\mathbb{R}^n, \mathbb{R})$, and $K \subset \mathbb{R}^n$ a compact convex set. Let $\mathcal{U}$ be an open ball around a point $x_h \in N_f$ such that $(\mathcal{U} \cap N_f) \subset K$, and suppose that x_h is hyperbolic in the following sense: $\nabla f(x_h) \neq 0$, and the tangent plane through x_h contains two lines such that the second derivative of f is strictly positive along one and strictly negative along the other. Then x_h is not an extreme point of K.

Proof. Suppose x_h is an extreme point of K. Then there must be a supporting hyperplane, i.e. a hyperplane H through x_h such that K lies entirely in one of the closed subspaces bounded by H. We claim that this implies that f, restricted to H, has to be either non-negative or non-positive in a neighbourhood of x_h.

Suppose to the contrary that there are points $x_+, x_- \in H \cap \mathcal{U}$ such that $f(x_+) > 0 > f(x_-)$. We may then connect x_+ and x_- by a continuous curve lying entirely in $\mathcal{U}$ and also in one of the two open half spaces bounded by H. Since f is continuous, any such a curve must contain a point y with $f(y) = 0$, i.e. $y \in (N_f \cap \mathcal{U}) \subset K$. Since we can choose either side of H for the connection, we find points $y \in K$ on both sides of H, hence H cannot be a supporting hyperplane.

This argument shows, in the first instance, that the only possible supporting hyperplane at x_h is the tangent hyperplane (look at the Taylor approximation of f to first order). Applying the argument with the second order Taylor approximation, we find that hyperbolic points cannot have supporting hyperplanes, hence cannot be extremal. ■

To apply this lemma to the function f from equation (3.12), we have to pick two appropriate tangent lines at any point $\vec{a} = (a_1, a_2, a_3, a_4, a_5)$ on the surface. We parameterize such lines as $\vec{a} + t\vec{b}$, $t \in \mathbb{R}$ so that $f(\vec{a} + t\vec{b}) = f(\vec{a}) + Mt^2$. Two choices with opposite sign of M are

$$\begin{array}{rll} & \vec{b} = (0,0,0,a_5,-a_4), & M = (a_4^2 + a_5^2) \\ \text{and} & \vec{b} = (2a_1, 2a_2, 2a_3, 3a_4, 3a_5), & M = -3(a_4^2 + a_5^2), \end{array} \tag{3.16}$$

where we have used the equation $f(\vec{a}) = 0$ to evaluate the last expression. Hence every point of the surface N_f is hyperbolic.

By Lemma 3.1.2 we therefore only have to consider boundary points of the surface, i.e. points for which at least one of the inequalities in Lemma 3.1.1 is equality.

Let us begin with the equalities $a_i = 0$, for at least one $i \in \{1, 2, 3\}$. Then we have $a_4 = a_5 = 0$ by equation (3.12) and $0 \le a_j + a_k \le 1$ $(j \ne k)$ by equation (3.13). As we are looking for extremal points we are left with the cases $a_j = a_k = 0$ representing the triorthogonal states [EB94] (i.e. point A=$(\frac{1}{6}, \frac{1}{6}, 0, 0, 0)$ in the r_i's) or $a_j + a_k = 1$. All such points satisfy $r_- = 0$, hence they will be in our general discussion of cases with $r_- = 0$. The equalities $a_i = 1$ lead by (3.13) to the inequality $0 \le 2a_4 - (a_j + a_k)$ and therefore to

$$a_4 \ge \frac{1}{2}(a_j + a_k) \ge \sqrt{a_j a_k} = \sqrt{a_i a_j a_k} = \sqrt{a_4^2 + a_5^2} \ge \sqrt{a_4^2} = |a_4| \ge a_4. \tag{3.17}$$

From this we can see $a_5 = 0$, $a_j = a_k$ and $a_4 = a_j = a_k$. Once again this implies $r_- = 0$ so that this remains the only case to be checked.

For $r_- = 0$, we can express the a_i by r_+, r_1, r_2, r_3, and solve equation (3.12) for r_3, obtaining a relation of the form

$$r_3 = \pm h(r_+, r_1, r_2), \tag{3.18}$$

where h is the square root of a third order polynomial. Equation (3.18) describes the surface of a convex set iff h is a concave function. This can be checked by verifying that the Hessian of h is everywhere negative semidefinite. Hence all points in $\mathcal{T}_{\text{pure}}$ with $r_- = 0$ are extremal and are characterized by equation (3.18). This completes the determination of extreme points of $\mathcal{T}$, summarized in the following theorem. It also contains the dual description of $\mathcal{T}$ in terms of inequalities.

Theorem 3.1.3: The subset $\mathcal{T} \subset \mathcal{S}_{U^{\otimes 3}}$ of triseparable states has the following extreme points described here in terms of the expectations $r_k = \operatorname{tr}[\rho R_k]$, $k = +, -, 1, 2, 3$:

1. $3r_3^2 + (1 - 3r_+)^2 = (r_1 + r_+) \cdot (r_1 - \sqrt{3}r_2 - 2r_+) \cdot (r_1 + \sqrt{3}r_2 - 2r_+)$ and $r_- = 0$,
2. The point $A = (1/6, 1/6, 0, 0, 0)$.

A state $\rho \in \mathcal{S}_{U^{\otimes 3}}$ is triseparable if and only if it corresponds to the point A or the following inequalities are satisfied:

(a) $0 \leq r_- < \frac{1}{6}$,

(b) $\frac{1}{4}(1 - 2r_-) \leq r_+ \leq 1 - 5r_-$,

(c) $(3r_3^2 + [1 - 3r_+ - 3r_-]^2)(1 - 6r_-) \leq (r_1 + r_+ - r_-)\left((r_1 - 2[r_+ - r_-])^2 - 3r_2^2\right).$

These inequalities are obtained by projecting the given point onto the hyperplane $r_- = 0$ from point A, and by checking whether the projected point satisfies the inequality $|r_3| \leq h(r_+, r_1, r_2)$ with h from equation (3.18)[40]. To get an idea of the shape of $\mathcal{T}$ we compute the section with $r_+ = 0.27$ and $r_- = 0.1$ (see figure 3.5).

3.1.2 Biseparable states

In this section we are going to compute the set of biseparable states with respect to the partition $1|23$. The technique is exactly the same as in the triseparable case: we first compute the set $\mathcal{B}_{\text{pure}}$ of states of the form $\mathcal{T}_{U^{\otimes 3}}(|\Psi\rangle\langle\Psi|)$ with $|\Psi\rangle\langle\Psi|$ biseparable, i.e. $\Psi = \psi_1 \otimes \psi_{2,3}$. In a second step we get $\mathcal{B}_1$ as the convex hull of $\mathcal{B}_{\text{pure}}$.

We are free to apply to our vector Ψ a $U \otimes U \otimes U$ rotation without changing the projection. In this way we may choose $\psi_1 = |1\rangle$. Now the

[40] Note that this check is very important since we are dealing with a surface of third order which would otherwise lead to an open and thus not necessarily convex set!

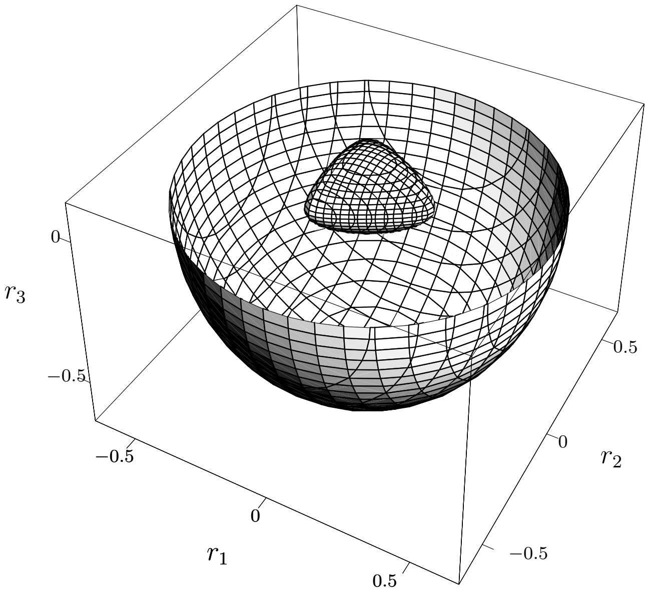


Figure 3.5: Plotting the set $\mathcal{T}$ for the section $r_+ = 0.27$, $r_- = 0.1$ gives a heart-shaped surface with trigonal symmetry which is contained in the respective Bloch sphere.

rotated state Ψ' is of the form $\Psi' = \sum_{i,j} \psi_{ij}|1ij\rangle$. The expectations of permutations of such a vector, like $\langle\Psi'|V_{(12)}\Psi'\rangle = \sum_{i,j,k,l} \overline{\psi_{ij}}\psi_{kl}\langle 1ij|k1l\rangle = \sum_j |\psi_{1j}|^2$ then depend linearly on the following real parameters:

$$\begin{aligned} c_0 &= |\psi_{11}|^2, \qquad c_1 = \sum_{j>1} |\psi_{1j}|^2, \qquad c_2 = \sum_{i>1} |\psi_{i1}|^2, \\ c_3 &= \sum_{i,j>1} \overline{\psi_{ij}}\psi_{ji}, \qquad c_4 + ic_5 = \sum_{j>1} \overline{\psi_{1j}}\psi_{j1}. \end{aligned} \tag{3.19}$$

From this we obtain the following r_k:

$$\begin{array}{ll} r_+ = \frac{1}{6}(1 + 5c_0 + c_1 + c_2 + c_3 + 4c_4), & r_- = \frac{1}{6}(1 - c_0 - c_1 - c_2 - c_3), \\ r_0 = \frac{2}{3}(1 - c_0 - c_4), & r_1 = \frac{1}{3}(-c_1 - c_2 + 2c_3 + 4c_4), \\ r_2 = \frac{c_1 - c_2}{\sqrt{3}}, & r_3 = \frac{2c_5}{\sqrt{3}}. \end{array} \tag{3.20}$$

As in the tripartite case we need to determine the exact range of the parameters c_i. Let us assume $d > 2$ for the moment. By the definitions of c_0, c_1 and c_2 we have

$$c_0, c_1, c_2 \geq 0. \tag{3.21}$$

These parameters fix the weights of the blocks $(i = 1, j = 1)$, $(i = 1, j > 1)$, and $(i > 1, j = 1)$ in the normalization sum $\sum_{i,j=1}^{d} |\psi_{ij}|^2 = 1$. $c_4 + ic_5$ can be read as the scalar product of two $(d-1)$-dimensional vectors $\varphi_1 = (\psi_{12}, \dots, \psi_{1d})$ and $\varphi_2 = (\psi_{21}, \dots, \psi_{d1})$ with norm squares $\|\varphi_1\|^2 = c_1$ and $\|\varphi_2\|^2 = c_2$. By the Cauchy-Schwarz inequality we have:

$$c_4^2 + c_5^2 = |\langle\varphi_1|\varphi_2\rangle|^2 \leq \|\varphi_1\|^2 \|\varphi_2\|^2 = c_1 c_2, \tag{3.22}$$

and any value of $c_4 + ic_5$ consistent with this can actually occur.

We arrange the remaining ψ_{ij} $(i, j > 1)$ into a $(d-1)^2$-dimensional vector $\widetilde{\Psi} = (\psi_{22}, \dots, \psi_{2d}, \psi_{32}, \dots, \psi_{dd})$ with $\|\widetilde{\Psi}\|^2 = 1 - c_0 - c_1 - c_2$. On this $(d-1)^2$-dimensional vector space, let U denote the operator swapping ψ_{ij} and ψ_{ji}. Then $c_3 = \langle\widetilde{\Psi}|U\widetilde{\Psi}\rangle$ is the expectation of an hermitian operator with eigenvalues ± 1. Hence

$$|c_3| \leq \|\widetilde{\Psi}\|^2 = 1 - c_0 - c_1 - c_2, \tag{3.23}$$

and all $c_3 \in \mathbb{R}$ satisfying this inequality can occur.

Together with the obvious modifications in the case $d = 2$, when there is only one index $i > 1$, we get the following lemma:

Lemma 3.1.4: A tuple $(c_0, c_1, c_2, c_3, c_4, c_5) \in \mathbb{R}^6$ arises via equations (3.19) from a unit vector Ψ in a d^2-dimensional Hilbert space, if and only if equations (3.21), (3.22) and (3.23) are satisfied, and, in the case $d = 2$, equality holds in (3.22) and (3.23).

Let Γ denote the set of tuples $(c_0, c_1, c_2, c_3, c_4, c_5)$ satisfying these constraints. The r_k depend linearly on the c_i, although the mapping is not one-to-one. Nevertheless any extreme point of $\mathcal{B}_1$ must be the image of an extreme point of the convex hull of Γ.

Hence we can proceed by first determining the extreme points of Γ. Since the positive variables c_0, $|c_3|$ and the sum $(c_1 + c_2)$ are only constrained by inequality (3.23), every point in Γ is a convex combination of tuples in which only one of these is equal to 1, and the other two vanish. This gives the extreme points

1. $c_0 = 1 \Leftrightarrow \vec{r} = (1, 0, 0, 0, 0) \equiv B$,
2. $c_3 = +1 \Leftrightarrow \vec{r} = (\frac{1}{3}, 0, \frac{2}{3}, 0, 0) \equiv D$,
3. $c_3 = -1 \Leftrightarrow \vec{r} = (0, \frac{1}{3}, -\frac{2}{3}, 0, 0) \equiv F$,

and furthermore some points with $(c_1 + c_2) = 1$, $c_0 = c_3 = 0$. Eliminating $c_2 = 1 - c_1$ we can write inequality (3.22) as $c_4^2 + c_5^2 + (c_1 - 1/2)^2 \leq 1/4$.

This is a ball with extreme points parameterized by

$$\begin{array}{lll} c_0 = 0, & c_1 = \frac{1+\cos(\vartheta)}{2}, & c_2 = \frac{1-\cos(\vartheta)}{2}, \\ c_3 = 0, & c_4 = \frac{\sin(\vartheta)\cos(\varphi)}{2}, & c_5 = \frac{\sin(\vartheta)\sin(\varphi)}{2}, \end{array} \tag{3.24}$$

with $\varphi, \vartheta \in [0, 2\pi]$. By mapping this description of Γ to the r_k-parameterization we come to the following theorem:

Theorem 3.1.5: The subset $\mathcal{B}_1 \subset \mathcal{S}_{U^{\otimes 3}}$ of biseparable states with respect to the partition $1|23$ has the following extreme points described here in terms of the expectations $r_k = \mathrm{tr}[\rho R_k]$, $k = +, -, 1, 2, 3$:

1. The sphere given by $\frac{1}{4}(3r_1+1)^2 + 3r_2^2 + 3r_3^2 = 1$ with $r_+ = (r_1+1)/2$ and $r_- = 0$ except for the point $(\frac{2}{3}, 0, \frac{1}{3}, 0, 0)$, which is decomposable as $(\frac{2}{3}, 0, \frac{1}{3}, 0, 0) = \frac{1}{2}(B + D)$
2. The point $F = (0, \frac{1}{3}, -\frac{2}{3}, 0, 0)$
3. The point $D = (\frac{1}{3}, 0, \frac{2}{3}, 0, 0)$
4. The point $B = (1, 0, 0, 0, 0)$.

A state $\rho \in \mathcal{S}_{U^{\otimes 3}}$ is biseparable with respect to the partition $1|23$ if and only if it corresponds to the points F, B or D or if the following inequalities are satisfied:

(a) $0 \leq r_- < \frac{1}{3}$,

(b) $-1 < \frac{1+r_1-r_--2r_+}{1-3r_-} < 1$,

(c) if $-1 < \frac{1+r_1-r_--2r_+}{1-3r_-} \leq 0$ then

$$3r_2^2 + 3r_3^2 + (1 + 2r_1 + r_- - r_+)^2 \leq (2 + r_1 - 4r_- - 2r_+)^2,$$

(d) if $0 \leq \frac{1+r_1-r_--2r_+}{1-3r_-} < 1$ then

$$3r_2^2 + 3r_3^2 + (1 - 3r_- - 3r_+)^2 \leq (r_1 + 2r_- - 2r_+)^2.$$

Here again we omit the computation of these inequalities from the known extreme points. They can be obtained by projecting from the three points F, B and D onto the sphere of extremal points.

The projection of the set $\mathcal{B}_1$ onto $\mathcal{S}^P_{U^{\otimes 3}}$ comes to be equal to the projection of the set of pure $\mathcal{B}_1$-states and was already shown in figure 3.2

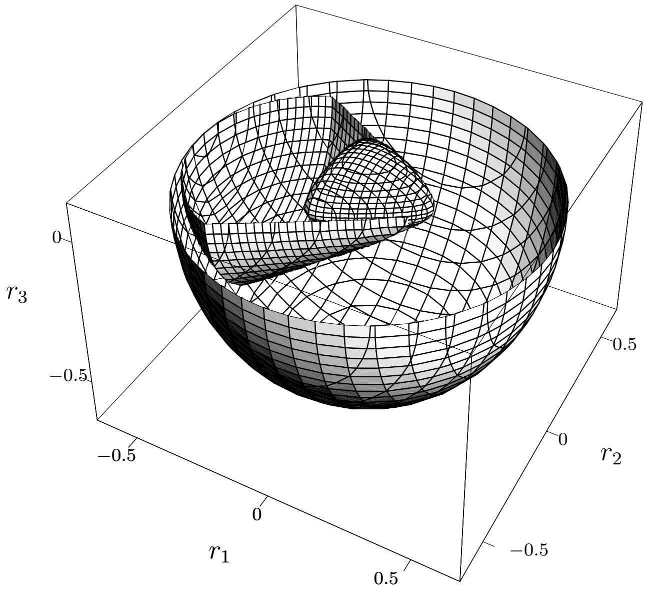


Figure 3.6: Plot of the set $\mathcal{B}_1$ for $r_+ = 0.27$ and $r_- = 0.1$ embedded in the respective Bloch sphere together with $\mathcal{T}$.

together with the section $\mathcal{B}_1 \cap \mathcal{S}^P_{U^{\otimes 3}}$. To compare $\mathcal{B}_1$ with $\mathcal{T}$ we plot again the section with $r_+ = 0.27$ and $r_- = 0.1$ (see figure 3.6).

To make the inclusion $\mathcal{T} \subsetneq (\mathcal{B}_1 \cap \mathcal{B}_2 \cap \mathcal{B}_3)$ we mentioned earlier more evident we can compute the sets $\mathcal{B}_2$ and $\mathcal{B}_3$ to build their intersection with $\mathcal{B}_1$. Due to the permutation symmetry of the three subsystems we can rotate $\mathcal{B}_1$ by $\pm\frac{2\pi}{3}$ in the r_1–r_2–plane, instead. This leads to figure 3.7. One can clearly see that there is much room left between the threefold biseparable states and the triseparable ones, especially for $r_1 = r_2 = 0$.

3.1.3 Partially transposed permutations

Before analyzing the power of the separability criteria we will shortly analyze the algebra of partially transposed permutation operators because we will need it for the analysis.

When ρ is a linear combination of permutation operators the partially transposed density operator

$$\Theta_1(\rho) = \sum_\pi \mu_\pi \Theta_1(V_\pi) \tag{3.25}$$

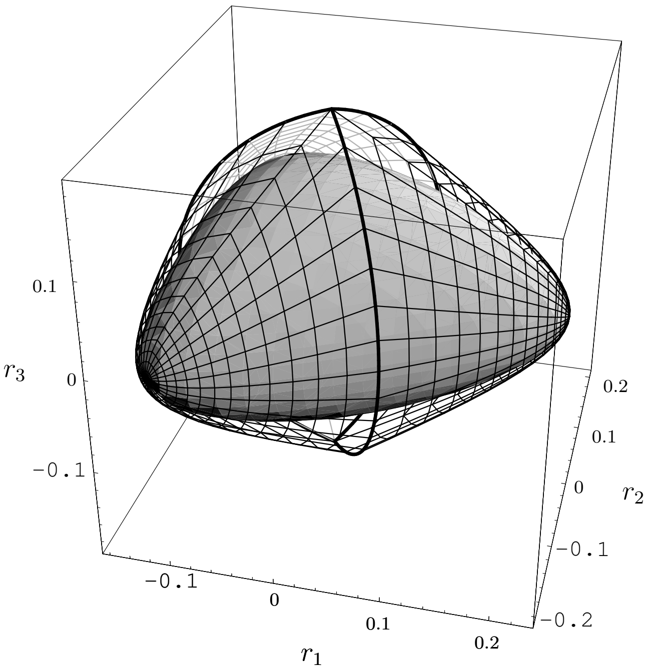


Figure 3.7: The intersection $\mathcal{B}_1 \cap \mathcal{B}_2 \cap \mathcal{B}_3$ is shown as a mesh on a transparent surface allowing the set $\mathcal{T}$ to be seen. This plot is again computed for the section $r_+ = 0.27$ and $r_- = 0.1$. The thick lines indicate the intersection of two of the biseparable sets.

is likewise a linear combination of the six operators $\Theta_1(V_\pi)$, and we have to decide for which coefficients μ_π such an operator is positive. Since partial transposition is *not* a homomorphism, it would appear that the linear combinations of the $\Theta_1(V_\pi)$ can be a fairly arbitrary space of operators, and deciding positivity could be quite difficult. However, it turns out that these linear combinations do form an algebra[41], so after the introduction of the right basis, deciding positivity is just as easy as determining the state space of the tripartite Werner states.

The abstract reason for this "happy coincidence" is that the operators $\Theta_1(V_\pi)$ span the set of fixed points of an averaging operation in much the same way as the permutations span the set of fixed points of

[41] Note that the algebra generated by partially transposed permutation operators is a subalgebra of the "chip"-algebra since it does not contain the permutations any more.

$\mathcal{T}_{U^{\otimes 3}}$. The corresponding averaging operator is

$$\mathcal{T}_{\overline{U}\otimes U^{\otimes 2}}\rho = \int dU\ (\overline{U}\otimes U\otimes U)\rho\,(\overline{U}\otimes U\otimes U)^*. \tag{3.26}$$

Its range consists of all operators commuting with all unitaries of the form $\overline{U}\otimes U\otimes U$, hence it is an algebra. The following lemma describes the relation between $\mathcal{T}_{\overline{U}\otimes U^{\otimes 2}}$ and $\mathcal{T}_{U^{\otimes 3}}$:

Lemma 3.1.6: Let A be any hermitian operator, then

1. $\mathcal{T}_{U^{\otimes 3}}A = A \Leftrightarrow \mathcal{T}_{\overline{U}\otimes U^{\otimes 2}}\Theta_1(A) = \Theta_1(A)$
2. $\Theta_1\left(\mathcal{T}_{\overline{U}\otimes U^{\otimes 2}}A\right) = \mathcal{T}_{U^{\otimes 3}}\Theta_1\left(A\right)$.

Proof. For any hermitian operator A one has:

$$\begin{aligned}\mathcal{T}_{\overline{U}\otimes U^{\otimes 2}}A = A &\Leftrightarrow \left[\overline{U}\otimes U\otimes U, A\right]_- = \mathbf{0}\\ &\Leftrightarrow \left[U\otimes U\otimes U, \Theta_1(A)\right]_- = \mathbf{0}\\ &\Leftrightarrow \mathcal{T}_{U^{\otimes 3}}\Theta_1(A) = \Theta_1(A).\end{aligned} \tag{3.27}$$

Furthermore we can compute directly:

$$\begin{aligned}\mathcal{T}_{U^{\otimes 3}}\Theta_1(A) &= \int dU(U\otimes U\otimes U)\Theta_1(A)(U\otimes U\otimes U)^*\\ &= \int dU\Theta_1\big((\overline{U}\otimes U\otimes U)A(\overline{U}\otimes U\otimes U)^*\big)\\ &= \Theta_1\big(\mathcal{T}_{\overline{U}\otimes U^{\otimes 2}}A\big),\end{aligned} \tag{3.28}$$

finishing the proof of the lemma. ■

In order to decide positivity of partial transposes we need a concrete form of the algebra spanned by the partial transposes of the permutation operators. For example, we get the chip

$$\Theta_1\left(V_{(12)}\right) = \sum_{ijk}\Theta_1\Big(|ijk\rangle\langle jik|\Big) = \sum_{ijk}|jjk\rangle\langle iik| = (|\Phi\rangle\langle\Phi|)\otimes\mathbb{1}, \tag{3.29}$$

where $\Phi = \sum_i |ii\rangle$ is a maximally entangled vector of norm d. The partial transposes of the other permutations are computed similarly. We can express all of them in terms of the first two:

$$X = \Theta_1\left(V_{(12)}\right) \qquad \text{and} \qquad V = \Theta_1\left(V_{(23)}\right) = V_{(23)} \tag{3.30}$$

as

$$\begin{array}{ll}\Theta_1(\mathbb{1}) = \mathbb{1}, & \Theta_1\big(V_{(13)}\big) = VXV, \\ \Theta_1\big(V_{(123)}\big) = XV, & \Theta_1\big(V_{(321)}\big) = VX.\end{array} \tag{3.31}$$

Then these operators satisfy the relations $X^* = X$, and $V^* = V$, and

$$X^2 = dX\ , \qquad V^2 = \mathbb{1}\ , \qquad XVX = X. \tag{3.32}$$

Due to these relations the set of linear combinations of the operators $\{\mathbb{1}, X, VXV, V, XV, VX\}$ is closed under adjoints and products. Positivity of such linear combinations, and hence the positivity of all partial transposes of operators in $\mathcal{S}_{U^{\otimes 3}}$ can therefore be decided by studying the abstract algebra generated by two hermitian elements X and V satisfying (3.32). As a six-dimensional non-commutative C*-algebra it is isomorphic to the algebra generated by the permutations[42] $\mathcal{A}(\mathfrak{S}_3)$, i.e. a sum of two one-dimensional and a two-dimensional matrix algebra. But of course, the partial transpose operation mapping one into the other is not a homomorphism.

From these considerations it is clear that all we have to do now is to find a basis of the algebra generated by X and V analogous to the basis (3.2). This computation is equivalent to finding the corresponding irreducible representations and can be quite painful, so we recommend the use of a symbolic algebra package like Mathematica©. The result is

$$\begin{aligned}
S_+ &= \frac{\mathbb{1}+V}{2}\Big(\mathbb{1} - \frac{2X}{d+1}\Big)\frac{\mathbb{1}+V}{2}, \\
S_- &= \frac{\mathbb{1}-V}{2}\Big(\mathbb{1} - \frac{2X}{d-1}\Big)\frac{\mathbb{1}-V}{2}, \\
S_0 &= \frac{1}{d^2-1}\Big(d(X+VXV) - (XV+VX)\Big), \\
S_1 &= \frac{1}{d^2-1}\ \Big(d(XV+VX) - (X+VXV)\Big), \\
S_2 &= \frac{1}{\sqrt{d^2-1}}\ \Big(X - VXV\Big), \\
S_3 &= \frac{i}{\sqrt{d^2-1}}\ \Big(XV - VX\Big).
\end{aligned} \tag{3.33}$$

These operators satisfy exactly the same relations as the R_k from (3.2) and we will therefore denote the corresponding expectation values by

[42] Note that this isomorphism is just a lucky coincidence. In fact there are examples of abelian algebras that are no longer commutative after the partial transposition (see [VW01]).

$s_k(\rho) := \mathrm{tr}[\rho S_k]$. The two projections $S_\pm$ correspond to the two one-dimensional representations of the algebra, i.e. to the two realizations of the relations by c-numbers, namely $X = 0, V = 1$ and $X = 0, V = -1$.

Since the two algebras are isomorphic, we can find an affine mapping translating the r_k coordinates into the $\underset{\smile}{s_k}$. A characterization of the separability classes ($\widetilde{\mathcal{T}}$, $\widetilde{\mathcal{B}}_1$, and $\widetilde{\mathcal{P}}_1$) of $\widetilde{\mathcal{T}_{U^{\otimes 3}}}$ can thus be deduced from those of $\mathcal{T}_{U^{\otimes 3}}$ without any computation due to this affine mapping.

The intimate relation between the two twirls emerged already in Lemma 3.1.6 where we stated the existence of an isomorphism between the two algebras spanning the eigenspaces of $\mathcal{T}_{U^{\otimes 3}}$ and $\mathcal{T}_{\overline{U}\otimes U^{\otimes 2}}$. This isomorphism establishes an affine mapping ι between the two eigenspaces that we used for computing $\mathcal{P}_1$. Due to the inclusion $\mathcal{T} \subsetneq \mathcal{B}_1 \subsetneq \mathcal{P}_1$ it is clear that the same mapping transports the sets $\mathcal{T}$ and $\mathcal{B}_1$ to their counterparts $\widetilde{\mathcal{T}}$ and $\widetilde{\mathcal{B}}_1$. The mapping ι can be computed by fixing the ordering $\{\mathbb{1}, X, V, VXV, XV, VX\}$ for the second algebra and concatenating the transformations 3.2 and 3.33 getting $\vec{s} = \iota \cdot \vec{r}$ with

$$\iota = \begin{pmatrix} \frac{d-1}{d+1} & 0 & \frac{d+2}{2d+2} & \frac{d+2}{2d+2} & 0 & 0 \\ 0 & \frac{d+1}{d-1} & \frac{d-2}{2d-2} & \frac{2-d}{2d-2} & 0 & 0 \\ \frac{2}{d+1} & -\frac{2}{d-1} & \frac{1}{d^2-1} & -\frac{d}{d^2-1} & 0 & 0 \\ \frac{2}{d+1} & \frac{2}{d-1} & -\frac{d}{d^2-1} & \frac{1}{d^2-1} & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{\sqrt{3}}{\sqrt{d^2-1}} & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{\sqrt{3}}{\sqrt{d^2-1}} \end{pmatrix}. \tag{3.34}$$

With this mapping we can directly compute the $\mathcal{T}_{\overline{U}\otimes U^{\otimes 2}}$-projection of the states A to G:

$$\begin{aligned}
A :& |123\rangle \longrightarrow (1/2, 1/2, 0, 0, 0), \\
B :& |111\rangle \longrightarrow \left(\frac{d-1}{d+1}, 0, \frac{2}{d+1}, 0, 0\right), \\
C :& (|111\rangle - \sqrt{3}|112\rangle + \sqrt{3}|121\rangle - 3|122\rangle)/4 \\
& \qquad\qquad\qquad \longrightarrow \left(\frac{4+5d}{8+8d}, \frac{3d-6}{8d-8}, \frac{d+2}{4-4d^2}, 0, 0\right), \\
D :& |122\rangle \longrightarrow (1, 0, 0, 0, 0), \\
E :& (|112\rangle - |121\rangle)/\sqrt{2} \longrightarrow \left(0, \frac{d-2}{d-1}, \frac{1}{1-d}, 0, 0\right), \\
F :& (|123\rangle - |132\rangle)/\sqrt{2} \longrightarrow (0, 1, 0, 0, 0), \\
G :& (|112\rangle - |121\rangle - \sqrt{3}|122\rangle)/\sqrt{5} \longrightarrow \left(\frac{3}{5}, \frac{2d-4}{5d-5}, \frac{2}{5-5d}, 0, 0\right).
\end{aligned} \tag{3.35}$$

Applying the transformation to the extremal points and inequalities of Theorems 3.1.3, 3.1.5 and 3.1.10 (see section 3.1.4) then yields a characterization of $\widetilde{\mathcal{T}}$, $\widetilde{\mathcal{B}}_1$ and $\widetilde{\mathcal{P}}_1$.

We omit the results of these transformations here and give the picture corresponding to figure 3.2. In contrast to what can be seen in figure 3.2, the projection of $\widetilde{\mathcal{T}}$ onto the s_+–s_-–plane differs from its section with it, as one can see in figure 3.9.

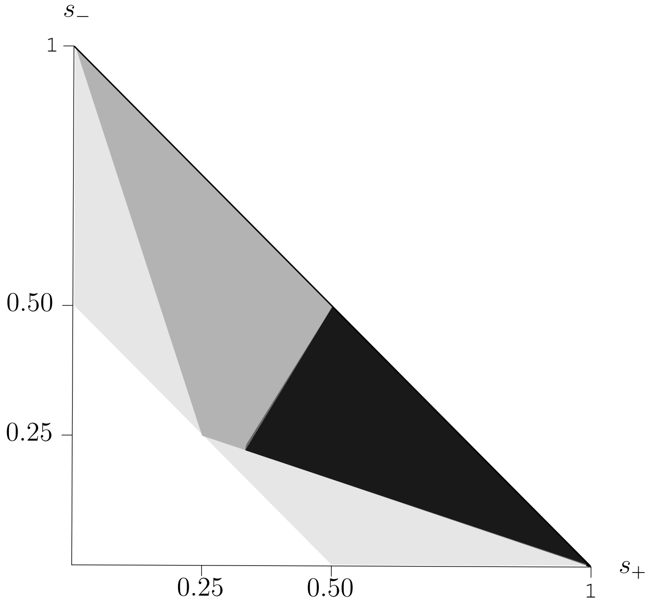


Figure 3.8: Sections and projections of $\widetilde{\mathcal{T}}$ and $\widetilde{\mathcal{B}}_1$ with/onto the s_+–s_-–plane for $d = 3$. Black: section with $\widetilde{\mathcal{T}}$, dark grey: projection of $\widetilde{\mathcal{T}}$, light grey: section with $\widetilde{\mathcal{B}}_1$.

3.1.4 States having a positive partial transpose

The positivity of the partial transpose serves as a necessary condition for separability[43], which is even sufficient in $2 \otimes 2$ and $2 \otimes 3$ dimensions (the Peres criterion [Per93]). Moreover, it is a necessary condition for undistillability, and here it comes much closer to sufficiency even in general situations. Both aspects play a role in the analysis of tripartite states. Therefore, in this subsection we describe the subset $\mathcal{P}_1 \subset \mathcal{S}_{U^{\otimes 3}}$ of states with positive 1-transpose.

[43] Actually, states that have a positive partial transpose show classical behaviour with respect to certain aspects although they might be entangled (see [Wol02]).

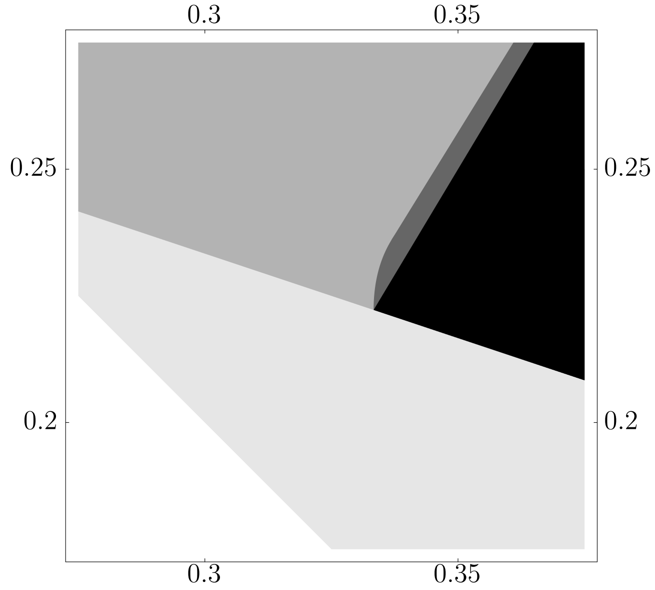


Figure 3.9: Zoomed region of figure 3.8.

Since the dimensions of this bipartite system are $d \otimes d^2$, positive partial transpose does not automatically imply biseparability, i.e. the inclusion $\mathcal{B}_1 \subset \mathcal{P}_1$ may be strict. However, since we are considering a special class of states, it is also possible that in this class equality holds. This does happen, for example, in the case of bipartite Werner states [HH99]. In the tripartite case we will see that $\mathcal{B}_1 = \mathcal{P}_1$ for $d = 2$, but not for higher dimensions, although the two sets come to be remarkably close (see figure 3.11). However, the exact description of $\mathcal{P}_1$ is also important for distillation questions.

Before coming to the general case we start with the simpler situation of states that are invariant under permutation of the subsystems B and C which form a three-dimensional object. In fact the $V_{(23)}$-invariance implies the conditions $\mathrm{tr}\big[\rho V_{(23)}\big] = 1$, $\mathrm{tr}\big[\rho V_{(12)}\big] = \mathrm{tr}\big[\rho V_{(31)}\big]$ and $\mathrm{tr}\big[\rho V_{(123)}\big] = \mathrm{tr}\big[\rho V_{(321)}\big]$. Therefore we have $r_2 = r_3 = 0$. In the same way we obtain for a $V_{(23)}$-invariant state $\rho \in \Theta_1 \mathcal{S}_{U^{\otimes 3}}$ the conditions $s_2 = 0$ and $s_3 = 0$. Positivity of a $V_{(23)}$-invariant state in $\mathcal{S}_{U^{\otimes 3}}$ now requires $r_+ \geq 0$, $r_- \geq 0$ and $|r_1| \leq r_0 = 1 - r_+ - r_-$ (see (3.3)) giving rise to a tetrahedron bounded by the hyperplanes

$$\begin{array}{llll} (h_1) & r_+ = 0, & (h_2) & r_- = 0, \\ (h_3) & r_1 = 1 - r_+ - r_-, & (h_4) & r_1 = r_+ + r_- - 1, \end{array} \qquad (3.36)$$

and having the extreme points $P_1 = (0,0,1)$, $P_2 = (0,0,-1)$, $P_3 = (0,1,0)$, and $P_4 = (1, 0, 0)$. The same computation can be done on the partially transposed side leading to the tetrahedron confined by the hyperplanes

$$\begin{array}{llll} (h_1') & s_+ = 0, & (h_2') & s_- = 0, \\ (h_3') & s_1 = 1 - s_+ - s_- & (h_4') & s_1 = s_+ + s_- - 1. \end{array} \tag{3.37}$$

Using Lemma 3.1.6 we can express the s_k by the r_k of the corresponding $\mathcal{S}_{U^{\otimes 3}}$-state. Multiplying by positive constants one gets an easier description of these hyperplanes:

$$\begin{array}{ll} (h_1') & 2(1 + r_1 - r_- - 2r_+) + d(1 + r_1 - r_- + r_+) = 0, \\ (h_2') & 2(-1 + r_1 + 2r_- + r_+) + d(1 - r_1 + r_- - r_+) = 0, \\ (h_3') & 1 - r_1 - 5r_- - r_+ = 0, \\ (h_4') & 1 + r_1 - r_- - 5r_+ = 0. \end{array} \tag{3.38}$$

Its four extremal points are now $Q_1 = (\frac{2+d}{3}, 0, \frac{1-d}{3})$, $Q_2 = (0, \frac{2-d}{3}, -\frac{1+d}{3})$, $Q_3 = (0, \frac{1}{3}, -\frac{2}{3})$ and $Q_4 = (\frac{1}{3}, 0, \frac{2}{3})$. Of course, these points have no reason to correspond to positive states, and, indeed, only Q_3 and Q_4 lie inside the state space, whereas Q_1 and Q_2 are outside the state space for all d.

As we are looking for those $V_{(23)}$-invariant $\mathcal{S}_{U^{\otimes 3}}$-states that have positive partial transpose, i.e. that lie in $\mathcal{P}_1$, we have now to look at the intersection of these two tetrahedra. The resulting object is again a tetrahedron as one can see in figure 3.10. This is due to the fact that the extremal points P_i and Q_i for $i = 1, 2, 3, 4$ lie on just two straight lines, namely $\overline{P_1 Q_4 P_4 Q_1}$ and $\overline{Q_2 P_2 Q_3 P_3}$. The intersection of the two tetrahedra is hence again a tetrahedron, spanned by the extremal points P_2, P_4, Q_3 and Q_4 (called E, B, F, and D in (3.9) and (3.10), and is thus dimension independent. But it is easily verified from Theorem 3.1.5 that these four points are precisely the extreme points of the $V_{(23)}$-invariant part of $\mathcal{B}_1$. Since $\mathcal{B}_1 \subset \mathcal{P}_1$, we have shown the following:

Lemma 3.1.7: A $V_{(23)}$-invariant $\mathcal{S}_{U^{\otimes 3}}$-state has a positive partial transpose if and only if it is biseparable.

As we will see below, the assumption of $V_{(23)}$-invariance is essential, i.e. the conclusion does not hold for general $\mathcal{S}_{U^{\otimes 3}}$-states. In order to see how $V_{(23)}$-invariance helps, we conclude this subsection with a direct proof of the above lemma for $d = 2$.

Proof. If ρ is a $V_{(23)}$-invariant $\mathcal{S}_{U^{\otimes 3}}$-state, then we can decompose it into the following sum

$$\rho = \frac{1}{4}\big(\mathbb{1} + V_{(23)}\big)\rho\big(\mathbb{1} + V_{(23)}\big) + \frac{1}{4}\big(\mathbb{1} - V_{(23)}\big)\rho\big(\mathbb{1} - V_{(23)}\big) =: \rho^+ + \rho^-. \tag{3.39}$$

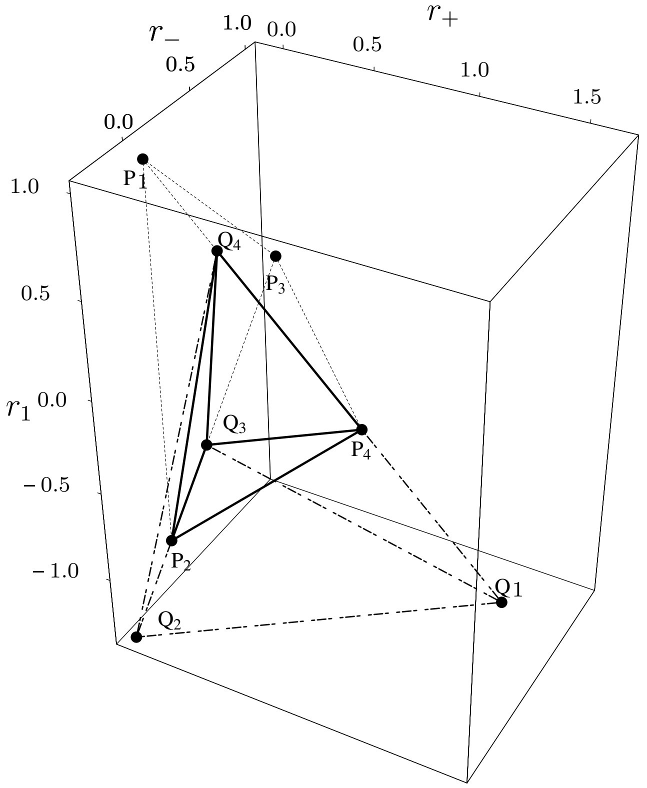


Figure 3.10: The two positivity tetrahedra bounded by the h_i (dotted) and the h_i' (dashed) and the intersection tetrahedron (solid lines) for $d = 3$.

It is now clear that ρ has a positive partial transpose iff both ρ^+ and ρ^- each have a positive partial transpose. ρ^+ denotes the $V_{(23)}$-symmetric part of ρ, ρ^- the antisymmetric part. Thus we know that ρ^+ is a 2×3 density operator and ρ^- a 2×1. For these systems the Peres criterion holds strictly [HHH96], i.e. states have a positive partial transpose iff they are separable or in our case biseparable over the $1|23$ split. Biseparability of ρ^+ and ρ^- is equivalent to the biseparability of ρ, which proves the lemma. ∎

For a general linear combination of the operators S_k the positivity conditions give the following result:

Lemma 3.1.8: Let $\rho \in \mathcal{S}_{U^{\otimes 3}}$ be a density operator with expectations $r_k = \mathrm{tr}[\rho R_k]$, $k = +, -, 1, 2, 3$. Then the partial transpose of ρ with respect to the first tensor factor is positive,i.e. $\rho \in \mathcal{P}_1$, if and only if

$$\begin{array}{llll} (a) & 0 \leq r_-, & (b) & 0 \leq r_1 - r_+ - r_- + 1, \\ (c) & 0 \leq 1 - r_1 - 5r_- - r_+, & (d) & 0 \leq -1 - r_1 + r_- + 5r_+, \\ (e) & r_2^2 + r_3^2 \leq R_1, & (f) & r_2^2 + r_3^2 \leq R_2, \end{array} \tag{3.40}$$

where

$$\begin{aligned} R_1 &:= (1 - r_1 - 5r_- - r_+)(-1 - r_1 + r_- + 5r_+)/3, \\ R_2 &:= (1 - r_1 - r_- - r_+)(1 + r_1 - r_- - r_+). \end{aligned} \tag{3.41}$$

Proof. Recall that averaging with respect to $V_{(23)}$ projects $\mathcal{P}_1$ to the section of $\mathcal{P}_1$ with $r_2 = r_3$. Therefore, the inequalities describing the tetrahedron discussed in the last subsection are optimal. These are the first four inequalities. We therefore only have to describe the admissible set of (r_2, r_3), given (r_+, r_-, r_1). There are two conditions to consider, one from the positivity of ρ, and one from the positivity of $\Theta_1(\rho)$. As shown in the first subsection, both these requirements have a very similar form, namely the positivity of an element in an abstract algebra with two one-dimensional summands and one summand isomorphic to the 2×2-matrices. Now in both cases one can readily see that (r_+, r_-, r_1) fix the weights of the one-dimensional parts, as well as the trace and the expectation of the first Pauli matrix for the 2×2-part. This leaves a condition of the form $r_2^2 + r_3^2 \leq R$ in both cases. The two conditions are given in the lemma, where $R_2 = (1 - r_+ - r_-)^2 - r_1^2$ expresses the requirement $\rho \geq 0$. The condition (3.40e) is obtained from $\Theta_1(\rho) \geq 0$ by expressing $\Theta_1(\rho)$ in the basis S_k, and applying the same criterion to the expectations s_k. ■

According to this lemma the set $\mathcal{P}_1$ can be visualized as follows: firstly, one has to fix a point (r_+, r_-) in the permutation invariant triangle (see figure 3.2). The possible choices of (r_1, r_2, r_3) can then be seen from figure 3.6. Apart from the heart-shaped tripartite set in the center this figure contains three quadratic surfaces: the Bloch sphere and the two surfaces bounding $\mathcal{B}_1$. Comparing condition (3.40d) of Theorem 3.1.5 and the expression for R_1 given in the above lemma, we find that both constraints are given by the same hyperboloid, the one wrapped around the tripartite set in figure 3.6. Hence in that figure we can readily find $\mathcal{P}_1$ by extending this hyperboloid all the way to the Bloch sphere and taking the intersection. This is shown in figure 3.11, in the section $r_3 = 0$.

Figure 3.11 shows the generic situation with $r_- \neq 0$. When $r_- = 0$, in particular for systems of three qubits, the boundary ellipsoid of $\mathcal{B}_1$,

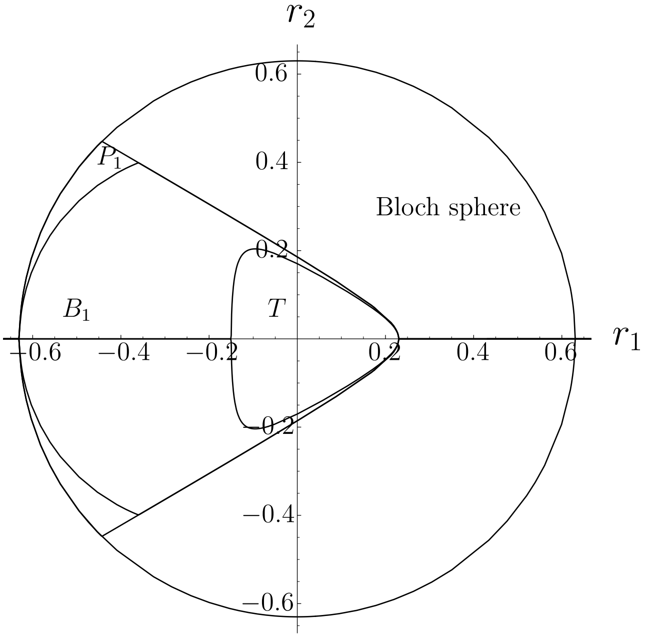


Figure 3.11: Plot of the Bloch sphere, $\mathcal{T}$, $\mathcal{B}_1$ and $\mathcal{P}_1$ for $r_+ = 0.27, r_- = 0.1$ and $r_3 = 0$.

described by condition (c) of Theorem 3.1.5, coalesces with the Bloch sphere. This leads to another instance where the Peres-Horodecki criterion for separability holds:

Corollary 3.1.9: The intersections of $\mathcal{B}_1$ and $\mathcal{P}_1$ with the plane $r_- = 0$ coincide. In particular, for 3-qubit $\mathcal{S}_{U^{\otimes 3}}$-states, biseparability is equivalent to the positivity of the partial transpose.

We conclude this subsection by the explicit determination of the extreme points of $\mathcal{P}_1$. From figure 3.11 it might appear that all points on the quadratic surfaces bounding $\mathcal{P}_1$ might be extremal. But this is misleading, because we also have to take into account the possibility of decompositions with different values of (r_+, r_-). In fact, for the inequalities arising from $\rho \geq 0$ it is evident that generically such decompositions are possible: given any $(r_+, r_-, r_1, r_2, r_3)$, which lies on the Bloch sphere in figure 3.11, we can just change the weights of the three blocks in the block decomposition of ρ according to $(\lambda_+ r_+, \lambda_- r_-, \lambda_0 r_1, \lambda_0 r_2, \lambda_0 r_3)$, as long as the λ_α are positive, and the normalization given by $\lambda_+ r_+ + \lambda_- r_- + \lambda_0(1 - r_+ - r_-) = 1$ is respected. This leaves a two-dimensional affine manifold through $(r_+, r_-, r_1, r_2, r_3)$. Hence, unless other conditions constraining $\mathcal{P}_1$ prevent the indicated decompositions, no such point will be extremal. Of course, the second constraint (3.40e) has the same structure, because the algebra of partial transposes is isomorphic to the algebra generated by the states. Hence in figure 3.11 only the points in the intersection of the hyperboloid and the Bloch sphere remain as candidates for extreme points. This is analogous to the extreme points of $\mathcal{B}_1$, which also consist of the intersection of two quadratic surfaces in figure 3.11. For $\mathcal{P}_1$ we get

Theorem 3.1.10: The subset $\mathcal{P}_1 \subset \mathcal{S}_{U^{\otimes 3}}$ of $\mathcal{S}_{U^{\otimes 3}}$-states with positive 1-transpose has the following extreme points, described here in terms of the expectations $r_k = \mathrm{tr}[\rho R_k]$, $k = +, -, 1, 2, 3$:

1. The points P_2, Q_3, P_4, and Q_4, which also span the $V_{(23)}$-invariant part of $\mathcal{P}_1$.

2. the remaining extreme points of $\mathcal{B}_1$, which form a sphere in the $r_- = 0$ plane (see Theorem 3.1.5).

3. The points for which $(r_+, r_-, r_1, 0, 0)$ lie in the interior of the $V_{(23)}$-invariant tetrahedron, and for which the inequalities (3.40e) and (3.40f) are both satisfied with equality.

Proof. Let us first discuss the periphery of the tetrahedron. Every face of the tetrahedron corresponds to a face of $\mathcal{P}_1$, namely the face of points projecting to it upon $V_{(23)}$-averaging. In Lemma 3.1.8 this corresponds to the subsets for which one of the linear inequalities (3.40a) to (3.40d) is equality. We will show first that each of these faces is actually contained in $\mathcal{B}_1$. Indeed, when (3.40b), (3.40c) or (3.40d) are equalities, one of the factors in R_1 or R_2 vanishes, forcing $r_2 = r_3 = 0$, reducing our claim to Lemma 3.1.7. When (3.40a) is equality, i.e. $r_- = 0$, the claim is contained in corollary 3.1.9.

Now a point of $\mathcal{P}_1$ contained in one of these faces can only have decompositions in the same face, hence in $\mathcal{B}_1$, hence for such a point extremality in $\mathcal{P}_1$ and extremality in $\mathcal{B}_1$ are equivalent.

What remains to be done is to show item 3 of the theorem, i.e. to characterize the extreme points of $\mathcal{P}_1$, whose $V_{(23)}$-averages fall in the interior of the tetrahedron. From the arguments preceding the theorem it is clear that points for which only one of the inequalities (e) and (f) of (3.40) are equalities cannot be extremal, since the surfaces defined by these equations contain straight lines. Therefore, the condition stated in the theorem is necessary for a point to be extremal. It remains to be shown that none of the points with $R_1 = R_2$ can be decomposed in a proper convex combination.

Let us denote by M_1 (resp. M_2) the set of those points in the interior of the tetrahedron such that $R_1 \leq R_2$ (respectively $R_2 \leq R_1$). The intersection $M_* = M_1 \cap M_2$ of these sets is described by the condition $R_1 = R_2$, or explicitly

$$r_1^2 + 3r_- + r_1 r_- - 2r_-^2 + 3r_+ - r_1 r_+ - 8r_- r_+ - 2r_+^2 = 1. \tag{3.42}$$

This is a one-sheet hyperboloid, generated by two sets of straight lines shown in figure 3.11. Consider a line segment

$$u \mapsto (\hat{r}_+, \hat{r}_-, \hat{r}_1) + u(t_+, t_-, t_1) \tag{3.43}$$

through one of the points $\hat{p} = (\hat{r}_+, \hat{r}_-, \hat{r}_1) \in M_*$ of the hyperboloid. Consider the radius functions $\sqrt{R_i}$, evaluated as a function of the parameter u. If such a function is affine (has a vanishing second derivative) we can set $(r_1(u), r_2(u)) = (\cos\alpha, \sin\alpha)\sqrt{R_i}$ with arbitrary α, to get a straight line in the corresponding hypersurface in five dimensions. We then call (t_+, t_-, t_1) an *affine direction* for R_i. Along other directions, R_i is strictly concave, so no decomposition along the segment (3.43) is possible. For both radius functions, the set of affine directions is a two-dimensional plane, and thus best described by its normal vector. That is $\vec{t} = (t_+, t_-, t_1)$ is an affine direction for R_i if $\vec{t} \cdot \vec{A}_i = 0$, where

$$\vec{A}_1 = \begin{pmatrix} 2 - 3\hat{r}_1 - 12\hat{r}_- \\ -2 - 3\hat{r}_1 + 12\hat{r}_+ \\ -1 + 3\hat{r}_- + 3\hat{r}_+ \end{pmatrix}, \quad \vec{A}_2 = \begin{pmatrix} -\hat{r}_1 \\ -\hat{r}_1 \\ -1 + \hat{r}_- + \hat{r}_+ \end{pmatrix}. \tag{3.44}$$

Assuming that a convex decomposition along (3.43) is possible, we thus arrive at a threefold case distinction:

- The line segment lies entirely in M_1.
  Then it must be tangent to the hyperboloid M_* and also an affine direction for R_1. The vector $\vec{t}$ is uniquely determined up to a factor by these conditions. However, that does not mean that the corresponding line segment lies in M_1, and, in fact, one can show that it *never* does. Hence this case is ruled out.

- The line segment lies entirely in M_2.
  This is ruled out analogously.

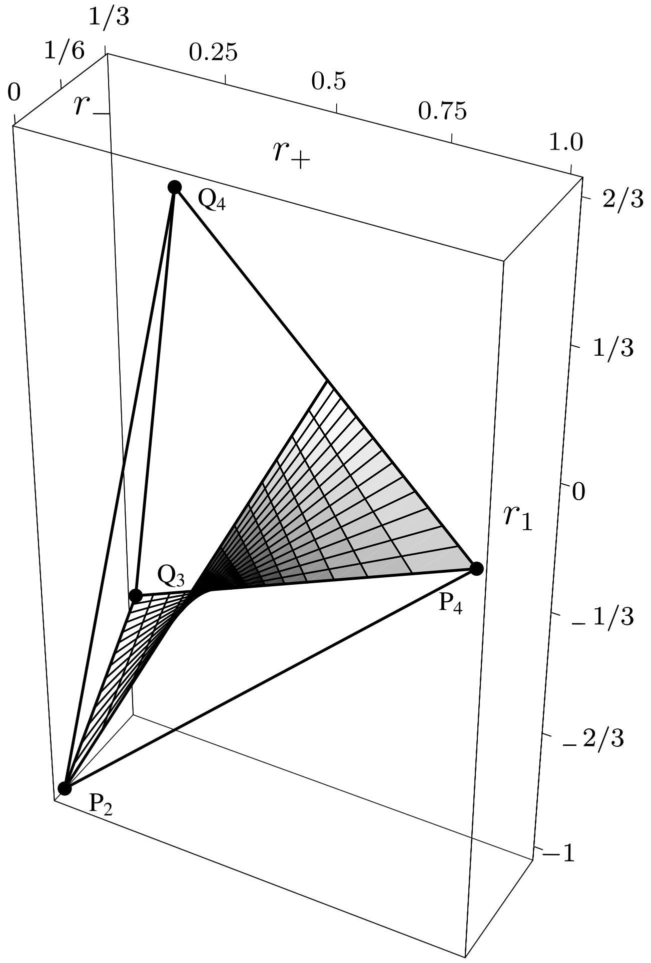


Figure 3.12: Section of the intersecting tetrahedron with the separating one-leaf hyperboloid.

- The line segment crosses from M_1 into M_2.
Then $\vec{t}$ must be affine for both radius functions. Again, this determines $\vec{t}$ up to a factor. But for a proper decomposition we must also have that the slopes of $\sqrt{R_1}$ and $\sqrt{R_2}$ match at $u = 0$. One can show that this never happens inside the tetrahedron we discuss, so this case is also ruled out.

We conclude that no point on M_* allows a convex decomposition inside $\mathcal{P}_1$, and the theorem is proved. ■

3.1.5 The realignment criteria

As already mentioned in subsection 1.2.2 the positivity of the partial transpose belongs to the class of separability criteria given by matrix reorderings. For tripartite systems there are, besides the three partial transposes, six other criteria (see [Fan02]) of the form

$$\|\Theta_i\left(\mathbb{F}_{ij}\rho\right)\|_1 \leq 1 \qquad \text{with} \quad i \neq j, \quad i,j \in \{1,2,3\}. \tag{3.45}$$

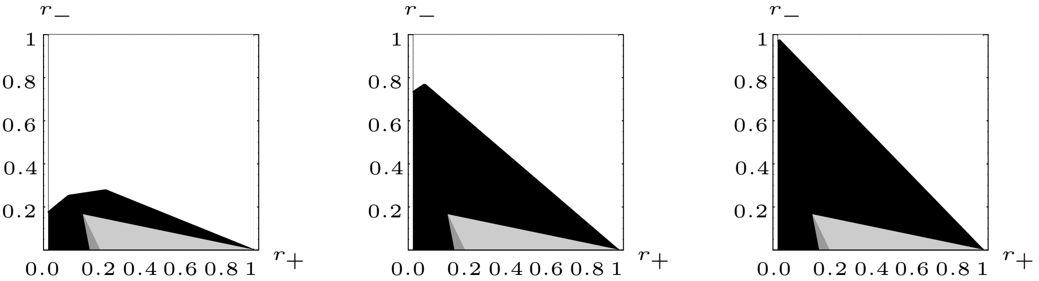


Figure 3.13: The black region depicts the states fulfilling the matrix reordering criterion, the dark grey area shows biseparable states (which is identical to the ppt area for permutation invariant states), the light grey area corresponds to fully separable states. The dimensions are from left to right: $d = 3$, $d = 13$ and $d = 137$.

Fortunately the partial transpose of $\mathbb{F}\rho$ is still in the "chip" algebra (see 2.3.1) so that the tracenorm can be computed analytically for general partially transposed tripartite Werner states. However, since the resulting expression is dimension dependent in contrast to the other sets described so far, we refrain from writing down the long general expression as it does not give much insight. As an example we compute it, instead, for arbitrary permutation invariant tripartite Werner states. In this case the six different criteria coincide and give one single expression. The partially transposed states are linear combinations of the fifteen "chips" that form a basis for the commutant of $O^{\otimes 3}$-symmetric operators. As such they can be represented by two complex numbers, one 2×2 and one 3×3-matrix (see the decomposition in (2.17)). The trace norm can then be computed for each matrix singularly and summed up, weighted by the respective multiplicities. Finally we obtain the inequality

$$\begin{aligned}d + 4r_- + 3dr_- - 4r_+ + 3dr_+ + \sqrt{x} \\ + (d+1)|2(1 + r_- - r_+) + d(-1 + 5r_- + r_+)| \\ + (d-1)|2(1 - r_- + r_+) - d(-1 + r_- + 5r_+)| \\ + |d + 4r_- + 3dr_- - 4r_+ + 3dr_+ - \sqrt{x}| \\ \leq 4(d^2 - 1),\end{aligned} \tag{3.46}$$

with

$$\begin{aligned}x = 8(3r_- + 3r_+ - 1) \\ + d^2(9 + 25r_-^2 - 2r_-(9 + 7r_+) + r_+(25r_+ - 18)) \\ + 8d(r_- - r_+)(1 + 3r_- + 3r_+).\end{aligned} \tag{3.47}$$

To get a better picture of the strength of this criterion we plotted the region fulfilling inequality (3.46) in figure 3.13 for the dimensions $d = 3$, $d = 13$ and $d = 137$. The realignment criterion seems to become weaker with growing dimension. In all cases it turned out to be strictly weaker than the Peres criterion, as one can see comparing the region fulfilling the reordering criterion and the biseparable/separable region.

3.2 Entanglement monotones and Bell violations

In the tripartite case the difficulties in quantifying entanglement begin already with the pure states, for which no canonical form as simple as the Schmidt decomposition exists. One can, however, extend the standard definition of the relation "more entangled than" to tripartite states. It is clear what local quantum operations should be in the multipartite case, and we can describe classical communication between many partners in much the same way as in the bipartite case. Once we fix the rules of classical communication (e.g. "each partner may broadcast its results to all the others"), we will say that ρ is more entangled than σ, ($\rho \succ \sigma$), whenever we can reach σ from ρ by a sequence of local operations and classical communication (LOCC).

A full characterization of this partial order relation is only known in the case of bipartite pure states (Nielsen's Theorem [Nie99]). Even in the mixed bipartite case there is no straightforward way of deciding whether one of two given density operators is more entangled than the other. Hence we cannot hope to give such a characterization in the tripartite case. Nevertheless, the entanglement ordering is one of the features one would like to explore and to chart in $\mathcal{S}_{U^{\otimes 3}}$. There are various ways of approaching this. For example, we may start from some state $\rho \in \mathcal{S}_{U^{\otimes 3}}$, apply many LOCC operations to it, and see where we end up. We can always assume the operation to end up in $\mathcal{S}_{U^{\otimes 3}}$, because the twirl operation is itself a LOCC operation, which involves the random choice of U by any one of the partners, the broadcasting of U to the other two partners, and the unitary transformation by U at each of the sites. For an initial survey, we may even study the relation in the permutation invariant triangle $\mathcal{S}_{U^{\otimes 3},\mathcal{S}_3}$, even though the permutation of sites is definitely *not* a local operation. But if the initial state is permutation invariant, and T is any LOCC operation, involving certain specified tasks for Alice, Bob and Charly, the three may just throw dice to decide who is to take which role. With this procedure they effectively get the permutation average of the output state of T. With such studies, we get sufficient conditions for $\rho \succ \sigma$.

The first method of characterizing the amount of entanglement contained in a state was to look at the strength of the violation of Bell type inequalities. Although Bell violations are nowadays known to be *not* an entanglement monotone[44], we will take a quick glance at the violations of various Bell type inequalities by tripartite Werner states.

3.2.1 Relative entropy and trace norm distance

In order to get necessary conditions the only approach is to find functionals on the state space, which are monotone with respect to entanglement ordering. Luckily, one of the ideas for getting such monotones can be transferred from the bipartite case. Obviously, the triseparable subset is invariant under LOCC operations, so the distance to $\mathcal{T}$ is an entanglement monotone, provided the distance functional has appropriate properties. One needs only one condition for a function Δ to define an appropriate "distance" $\Delta(\rho, \sigma)$ between arbitrary states of the same tripartite system:

$$\Delta(T\rho, T\sigma) \leq \Delta(\rho, \sigma) \text{ for any LOCC operation } T. \qquad (3.48)$$

[44] In fact, the Bell violation can be raised if Alice and Bob apply an LOCC filtering operation where Bob chooses his observable depending on the outcome of Alice's measurement.

Then for the functional

$$E_\Delta(\rho) = \inf\{\Delta(\rho, \sigma) | \sigma \in \mathcal{T}\} \tag{3.49}$$

we get the inequalities

$$\begin{aligned} E_\Delta(T\rho) &\leq \inf\{\Delta(T\rho, \sigma) | \sigma = T\sigma'; \sigma' \in \mathcal{T}\} \\ &= \inf\{\Delta(T\rho, T\sigma') | \sigma' \in \mathcal{T}\} \\ &\leq \inf\{\Delta(\rho, \sigma') | \sigma' \in \mathcal{T}\} = E_\Delta(\rho). \end{aligned} \tag{3.50}$$

Hence E_Δ is, indeed, a decreasing functional with respect to the ordering $\succ$. Note that the only property of $\mathcal{T}$ needed to show this is that it is mapped into itself under LOCC operations. Any other set with that property (e.g. $\mathcal{B}_1$ or $\mathcal{P}_1$) will also lead to an entanglement monotone.

Two natural choices for Δ satisfy requirement (3.48), and both of them satisfy it with respect to arbitrary operations T (not just LOCC operations): firstly the trace norm distance: $\Delta_1(\rho, \sigma) = \|\rho - \sigma\|_1$, and secondly the relative entropy $\Delta_S(\rho, \sigma) = S(\rho, \sigma)$, leading to entanglement monotones we denote by E_1 and E_S, respectively. In both cases, the actual computation of the distance for $\rho, \sigma \in \mathcal{S}_{U^{\otimes 3}}$ is greatly simplified by the observation that we may consider both ρ and σ as states (positive normalized linear functionals) on the algebra generated by the permutation operators, and that both the trace norm and the relative entropy are naturally defined for such functionals [OP93]. Moreover, as the twirl is a conditional expectation, the relative entropy of states in $\mathcal{S}_{U^{\otimes 3}}$ is independent of the algebra over which it is computed (see Theorem 1.13, [OP93]). Now the six-dimensional algebra generated by the permutations is independent of the dimension d, so that if we parameterize ρ and σ by the expectations of R_k as before, we find that the entanglement monotones E_Δ are independent of dimension. The expression for the relative entropy involves, apart from the abelian summands, the logarithm of a 2×2-matrix, which can also be written explicitly in terms of the parameters r_k and s_k for the two states

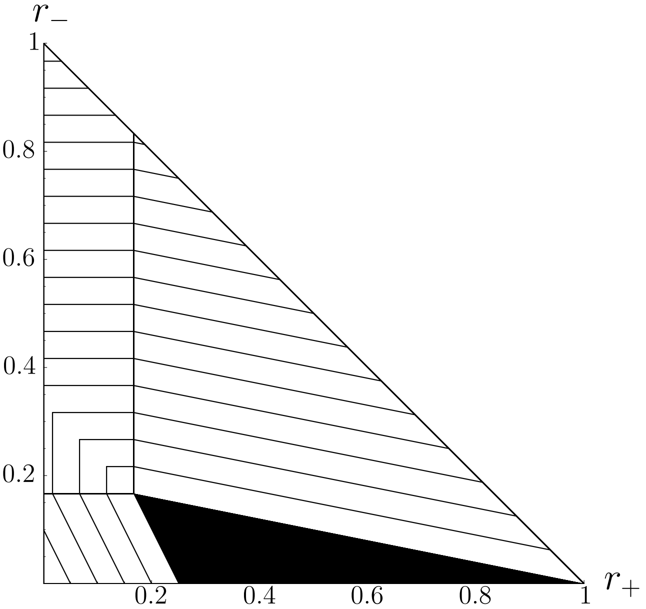


Figure 3.14: Contour lines over $\mathcal{S}_{U^{\otimes 3},\mathcal{S}_3}$ for E_1.

involved:

$$\begin{aligned}S(\rho;\sigma) =& r_+\log(r_+) + r_-\log(r_-) - r_+\log(s_+) - r_-\log(s_-)\\ &+ \frac{r_0+\sqrt{r_1^2+r_2^2+r_3^2}}{2}\log\frac{r_0+\sqrt{r_1^2+r_2^2+r_3^2}}{2}\\ &+ \frac{r_0-\sqrt{r_1^2+r_2^2+r_3^2}}{2}\log\frac{r_0-\sqrt{r_1^2+r_2^2+r_3^2}}{2}\\ &- \frac{1}{2}\left(r_0+\frac{r_1s_1+r_2s_2+r_3s_3}{\sqrt{s_1^2+s_2^2+s_3^2}}\right)\log\left[\frac{s_0+\sqrt{s_1^2+s_2^2+s_3^2}}{2}\right]\\ &- \frac{1}{2}\left(r_0-\frac{r_1s_1+r_2s_2+r_3s_3}{\sqrt{s_1^2+s_2^2+s_3^2}}\right)\log\left[\frac{s_0-\sqrt{s_1^2+s_2^2+s_3^2}}{2}\right].\end{aligned} \tag{3.51}$$

The variational problem (3.49) can then be solved numerically for arbitrary states in $\mathcal{S}_{U^{\otimes 3}}$.

For states in $\mathcal{S}_{U^{\otimes 3},\mathcal{S}_3}$ the distance functions give even simpler expressions:

$$\begin{aligned}S(\rho;\sigma) = r_+\log(r_+) + r_-\log(r_-) + r_0\log(r_0)&\\ - r_+\log(s_+) - r_-\log(s_-) - r_0\log(s_0)&\end{aligned} \tag{3.52}$$

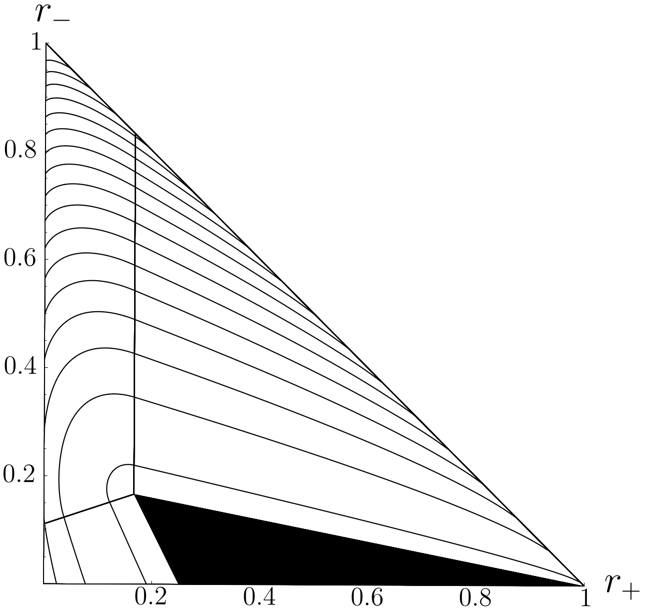


Figure 3.15: Contour lines over $\mathcal{S}_{U^{\otimes 3},\mathcal{S}_3}$ for E_S.

and

$$\|\rho - \sigma\|_1 = |r_+ - s_+| + |r_- - s_-| + 2|r_0 - s_0|. \qquad (3.53)$$

The contour lines over $\mathcal{S}_{U^{\otimes 3},\mathcal{S}_3}$ of the resulting entanglement monotones are plotted in figure 3.14 for E_1, and in figure 3.15 for the relative entropy of tripartite entanglement E_S. Note that the two necessary conditions for $\rho \succ \sigma$ expressed in these diagrams complement each other. In order not to complicate these graphs we have not drawn the simplest sufficient condition for entanglement ordering: from any state ρ, any state lying on a straight line segment ending in $\mathcal{T}$ is less entangled than ρ.

As a second section of interest we chose the plane $r_- = 0 = r_1 = r_2$, which is relevant to qubit systems. Qualitatively, it gives the same picture of level lines wrapped around the tripartite set (see figure 3.16).

For a maximally entangled state the entropic distance to the separable regime is bounded from above by $\log d$ regardless of the number of tensor factors (see (1.32) and (1.33)). Since both monotones are dimension independent for tripartite Werner states this can be seen as a hint on the "classicality" of these states. In fact, this implies that the ratio of the entanglement contained in a tripartite Werner state to the maximal entanglement possible goes to zero for growing dimensions.

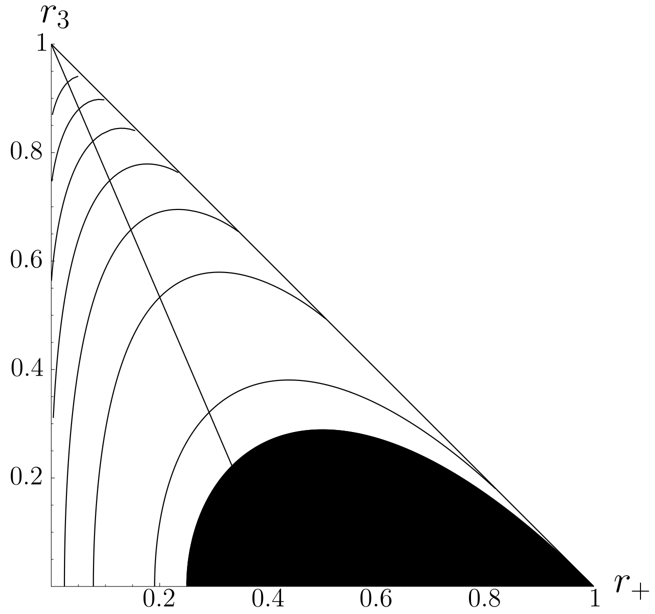


Figure 3.16: Contour lines over the r_3–r_+–plane for E_S.

3.2.2 Bell inequalities for dichotomic observables

The first method of testing the entanglement properties of a state was to check whether it violates Bell type inequalities (see [Pop95]). These inequalities were introduced by Bell in [Bel64] as a key experiment between quantum mechanics and alternative theories involving local hidden variables. Although they test the existence of a local classical model able to reproduce the observed correlations, they can be used to check separability. In fact, states violating Bell type inequalities are necessarily entangled. However, the converse is not true (see [Wer89]), i.e. there are entangled states that *admit* a local classical model and thus do *not* violate these inequalities. Nevertheless, due to their historical role, we will investigate them briefly for bipartite and tripartite Werner states.

We start by recalling the CHSH[45] version of Bell's inequality. In this formulation two parties (Alice and Bob) are given two ±1-valued (dichotomic) observables[46] each (A_1, A_2 and B_1, B_2) as possible measure-

[45] CHSH stands for the authors Clause, Horne, Shimony and Holt of [CHSH69].

[46] The widespread belief that an observable is represented by a hermitian operator can be recovered from the POVM formalism. For a two-outcome POVM $\{A, \mathbb{1} - A\}$ we just have to look at the difference of the outcomes $X = 2A - \mathbb{1}$ to get a hermitian

ments. The existence of a local classical model is then equivalent to the following inequality:

$$|\mathrm{tr}[\rho B_{\mathrm{Bell}}]| \leq 1, \quad \text{with} \quad B_{\mathrm{Bell}} = \frac{A_1}{2} \otimes (B_1 + B_2) + \frac{A_2}{2} \otimes (B_1 - B_2). \tag{3.54}$$

Actually the existence of a local classical model is (by definition) equivalent to the satisfaction of a *complete set* of Bell inequalities. However, for bipartite systems Fine [Fin82] showed that one such complete set is given by the CHSH inequality and a second inequality which is satisfied trivially. The maximal violation of the CHSH inequality is known to be $\sqrt{2}$, which is attained for the maximally entangled states of two qubits like the antisymmetric Werner state of two qubits. Interestingly, the violation due to Werner states vanishes for higher dimensions:

Lemma 3.2.1: Bipartite Werner states $\rho_W(f)$ violate Bell inequalities for dichotomic observables only for $d = 2$. The maximal violation is given by

$$\beta(f) = \max\left\{\sqrt{2}\frac{df-1}{d^2-1}, 1\right\} \tag{3.55}$$

where f is the Flip expectation value $f = \mathrm{tr}[\rho_W(f)\mathbb{F}]$.

Proof. For the proof we basically need only two facts: First, whenever two observables of the same site commute, a joint probability distribution for all the observables exists and the system can be regarded as classical, i.e. no violation will be possible. Secondly, using the partial trace we have $\mathrm{tr}_A\left[(\mathbb{1} \pm \mathbb{F})\, A \otimes B\right] = \mathrm{tr}[A] \cdot B \pm A \cdot B$. Since the maximal violation

$$\beta(f) = \sup_{-\mathbb{1} \leq A_i, B_j \leq \mathbb{1}} \mathrm{tr}\left[\rho_W(f)\left(\frac{A_1}{2} \otimes (B_1 + B_2) + \frac{A_2}{2} \otimes (B_1 - B_2)\right)\right] \tag{3.56}$$

is the supremum of an affine functional on the convex set of observables, it is clear that it will be attained at the boundary given by $A_i^2 = B_j^2 = \mathbb{1}$. Computing the trace in (3.56) for a bipartite Werner state $\rho_W(f) = \frac{1+f}{2(d^2+d)}(\mathbb{1} + \mathbb{F}) + \frac{1-f}{2(d^2-d)}(\mathbb{1} - \mathbb{F})$ first over subsystem A we get

$$\beta(f) = \frac{1}{2} \sup_{-\mathbb{1} \leq A_i, B_j \leq \mathbb{1}} \mathrm{tr}\left[\{\hat{A}_1(f) + \hat{A}_2(f)\} \cdot B_1 + \{\hat{A}_1(f) - \hat{A}_2(f)\} \cdot B_2\right] \tag{3.57}$$

operator $-\mathbb{1} \leq X \leq \mathbb{1}$.

with

$$\begin{aligned}\hat{A}_i =&\frac{1+f}{2(d^2+d)}(\mathrm{tr}[A_i]\cdot\mathbb{1}+A_i)+\frac{1-f}{2(d^2-d)}(\mathrm{tr}[A_i]\cdot\mathbb{1}-A_i)\\ =&\frac{d-f}{d^3-d}\mathrm{tr}[A_i]\cdot\mathbb{1}+\frac{df-1}{d^3-d}A_i.\end{aligned}\tag{3.58}$$

At this point the variation over the observables of site B can be done separately and it is clear that the optimum will be achieved for $B_1 = \mathrm{sign}\left[\hat{A}_1(f)+\hat{A}_2(f)\right]$ and $B_2 = \mathrm{sign}\left[\hat{A}_1(f)-\hat{A}_2(f)\right]$ leading to

$$\beta(f) = \frac{1}{2}\sup_{-\mathbb{1}\leq A_i\leq\mathbb{1}} \mathrm{tr}\left[|\hat{A}_1(f)+\hat{A}_2(f)|+|\hat{A}_1(f)-\hat{A}_2(f)|\right].\tag{3.59}$$

To complete the proof we just need to look at the optimal observables B_i resulting from this variation. Up to signs and relabelling we have the following cases:

$\mathrm{tr}[A_1]>0$, $\mathrm{tr}[A_2]>0$: In this case we have that due to

$$d-f+(df-1)=(d-1)(1+f)\geq 0\tag{3.60}$$

both $\hat{A}_i \geq \mathbf{0}$. Therefore the optimal B_1 is the identity which obviously commutes with all B_2. In this case we will get no violation, that is $\beta(f)=1$.

$\mathrm{tr}[A_1]<0$, $\mathrm{tr}[A_2]>0$: Similarly we have that the optimal B_2 is equal to the identity and therefore again $\beta(f)=1$.

$\mathrm{tr}[A_1]=0$, $\mathrm{tr}[A_2]>0$: Since the optimal observables must satisfy $A_i^2 = \mathbb{1}$ they have whole-numbered traces. $\mathrm{tr}[A_1]=0$ can thus happen only in even dimensions where $\mathrm{tr}[A_2]>0$ is equivalent to $\mathrm{tr}[A_2]\geq 2$ as all the eigenvalues are ± 1. This, in turn, leads to $\hat{A}_1\geq\mathbf{0}$ and $\hat{A}_2\geq\mathbf{0}$ and moreover to $B_1=B_2=\mathbb{1}$.

$\mathrm{tr}[A_1]=\mathrm{tr}[A_2]=0$: Here we have $\hat{A}_i=\frac{df-1}{d^3-d}A_i$ and for the moduli:

$$\begin{aligned}|\hat{A}_1\pm\hat{A}_2|^2 &= \left(\frac{df-1}{d^3-d}\right)^2|A_1\pm A_2|^2\\ &= \left(\frac{df-1}{d^3-d}\right)^2(2\mathbb{1}\pm[A_1,A_2]_+).\end{aligned}\tag{3.61}$$

The anticommutator $[A_1, A_2]_+ \overset{\text{def}}{=} 2C$ commutes with the identity so that the variation boils down to optimizing the function

$$\beta'(A_1, A_2) = \operatorname{tr}\left[\sqrt{\mathbb{1} + C} + \sqrt{\mathbb{1} - C}\right]. \tag{3.62}$$

The supremum can then be calculated with functional calculus to be attained at $C = 0$ leading to

$$\frac{1}{2} \sup_{A_1, A_2} \beta'(A_1, A_2) = \frac{df - 1}{d^2 - 1}\sqrt{2}. \tag{3.63}$$

To get the maximal violation we have to take the maximum over all possible values finishing the proof. ■

Although this lemma demonstrates the existence of a local classical model for all Werner states for dimensions $d > 2$ we have to keep in mind that it applies only to the case of two dichotomic observables per site. Complete sets of Bell inequalities are not known yet for the case of non-dichotomic observables or more than two dichotomic observables per site. However, numerical computations for a few known Bell inequalities for bipartite systems with more than two dichotomic observables per site suggest that this remains true.

For tripartite systems there are obviously more Bell type inequalities than the well known CHSH inequality. A complete set of such inequalities has been derived for arbitrary many parties in [WW01]. For tripartite systems the set contains, up to a relabelling of the observables, of the sites and of the outcomes, only five inequivalent inequalities given by the following Bell operators:

$$\begin{gathered} A_1 \otimes B_1 \otimes C_1, \\ \tfrac{1}{4} \textstyle\sum_{i,j,k} A_i \otimes B_j \otimes C_k - A_1 \otimes B_1 \otimes C_1, \\ \tfrac{1}{2}[A_1 \otimes (B_1 + B_2) + A_2 \otimes (B_1 - B_2)] \otimes C_1, \\ \tfrac{1}{2}[A_1 \otimes B_1 \otimes (C_1 + C_2) + A_2 \otimes B_2 \otimes (C_1 - C_2)], \\ \tfrac{1}{2}[A_1 \otimes B_1 \otimes C_2 + A_1 \otimes B_2 \otimes C_1 + A_2 \otimes B_1 \otimes C_1 - A_2 \otimes B_2 \otimes C_2]. \end{gathered} \tag{3.64}$$

Unfortunately, the iteration used in Lemma 3.2.1 does not lead to an analytical solution for tripartite Werner states for any of these Bell inequalities. Nevertheless it can be used to implement a very fast numerical search. In figure 3.17 we have plotted a line showing which tripartite permutation symmetric Werner states violate the Mermin inequality (the fifth in (3.64)). This line has been evaluated pointwise

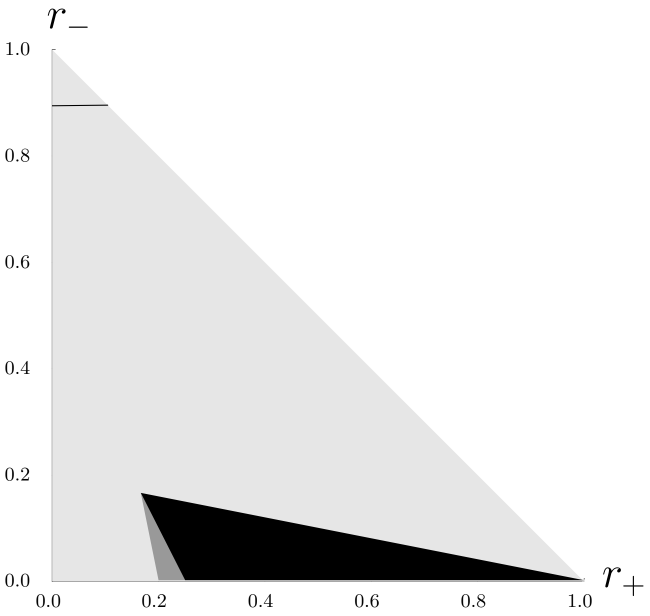


Figure 3.17: States above the black line violate the Mermin inequality for $d = 3$.

via a seesaw-like search using the above optimization over single sites recursively. Although the Mermin inequality is not the one showing the largest violation by tripartite Werner states for $d = 3$, it is the Bell inequality which *always*[47] shows a quantumly possible maximal violation of $2^{\frac{N-1}{2}}$, where N is the number of involved parties. The overall behaviour for tripartite Werner states is almost the same for the four latter inequalities (the first one is trivial) so that figure 3.17 can be taken as representative. Just like in the bipartite case numerical investigations show that the Bell violations vanish for $d > 3$.

3.3 The power of reduced states

As already stated in section 2.4 the two party reduced density matrices inherit the symmetry. In fact, in our case they are bipartite Werner states. In the first part of this section we will therefore check whether three bipartite Werner states are commensurable in the sense that they can be interpreted as the reduced density operators of one common tripartite ancestor.

[47] That is, for any N, and two dichotomic obervables per site.

In the second part of this section we will have a short look at the information measure introduced in [LPW02] for the special case of permutation invariant tripartite Werner states.

3.3.1 Embedding bipartite Werner states

In section 2.1 we had already seen that such a bipartite Werner state is fully characterized by its Flip expectation. For our tripartite states this corresponds to looking at the expectation values with the three transpositions $V_{(12)}$, $V_{(23)}$ and $V_{(31)}$. To characterize the set of commensurable triples of bipartite Werner states, we can use the techniques used for the characterization of the separability properties. That is we can compute the three expectation values for the set of extreme points and compute the convex hull afterwards. We recall that the extreme points of the state space $\mathcal{S}_{U^{\otimes 3}}$ are the two projections P_+ and P_- and the Bloch sphere with radius 1. For the two projections $P_\pm$ the expectations are easy:

$$\begin{aligned} \operatorname{tr}\big[V_{(12)}P_+\big] = \operatorname{tr}\big[V_{(23)}P_+\big] = \operatorname{tr}\big[V_{(31)}P_+\big] = 1, \\ \operatorname{tr}\big[V_{(12)}P_-\big] = \operatorname{tr}\big[V_{(23)}P_-\big] = \operatorname{tr}\big[V_{(31)}P_-\big] = -1. \end{aligned} \tag{3.65}$$

For the Bloch sphere we can use the spherical coordinates $r_1 = \cos\varphi\cos\psi$, $r_2 = \sin\varphi\cos\psi$ and $r_3 = \sin\psi$ to get the following parametrisation:

$$\begin{aligned} f_1 &= \frac{1}{2}\left(-\cos\varphi\cos\psi + \sqrt{3}\sin\varphi\cos\psi\right), \\ f_2 &= \cos\varphi\cos\psi, \\ f_3 &= \frac{1}{2}\left(-\cos\varphi\cos\psi - \sqrt{3}\sin\varphi\cos\psi\right), \end{aligned} \tag{3.66}$$

which depicts a tilted circle in the space given by the coordinates f_1, f_2 and f_3 (see figure 3.18).

In very much the same way we can check whether the overall tripartite state given by the three flip expectations is itself fully or only biseparable leading to figures 3.18 and 3.19. Especially the shape showing triseparable states is interesting as it reflects the separability properties of the reductions too. Taking a closer look at this shape one can see that it is bounded from below by the three inequalities $f_i \geq 0$, i.e. it is bounded by the fact that no restriction is allowed to be entangled and thus to have a negative flip expectation. The curvature of the upper boundary is a remnant of the heart-shaped set of triseparable states.

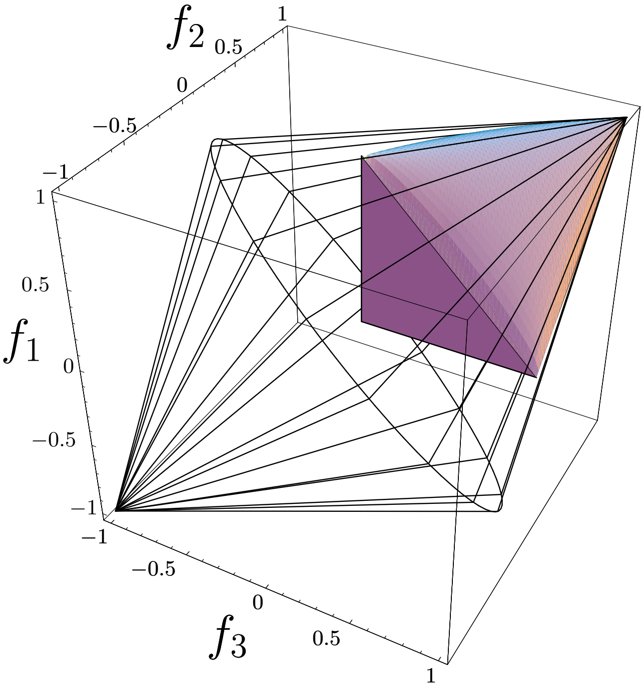


Figure 3.18: The set of commensurable triples is drawn as a mesh containing the set of triples leading to a triseparable tripartite Werner state.

As one would expect it this figure shows the trigonal symmetry of rotations by $\frac{2\pi}{3}$ about the diagonal corresponding to a relabelling of the sites. Similarly the biseparable shape in figure 3.19 can be seen as limited by the constraint that the state has to be separable over one split and thus the shape to be confined by only two inequalities, $f_1 \geq 0$ and $f_3 \geq 0$ in our case, breaking the trigonal symmetry.

As usual we could characterize all these shapes by computing the defining inequalities. However, as this computation does not give more insight than the pictures, we refrain from doing it and recall that they can be easily derived by projecting recursively from one set of extremal points to the others.

3.3.2 The Popescu information measure

Conversely to subsection 3.3.1 we can go back to subsection 2.4.2 and ask how much information is already contained in the bipartite reductions. Or, in other words, how much information of a tripartite Werner

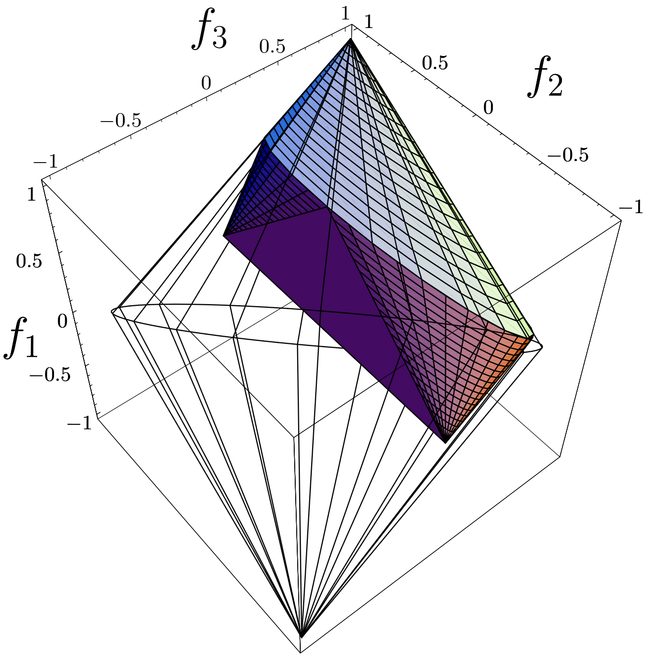


Figure 3.19: Analogously to figure 3.18 the mesh shows the set of commensurable triples whereas the interior shape shows triples giving biseparable states.

state is contained in the three flip expectations?

In section 2.4.2 we have seen that the state with least bipartite information inherits both symmetries, the Werner symmetry (see (2.4.4)) and the permutation invariance (see (2.4.5)). In the following we will utilize these two observations in order to calculate M_2 for permutation invariant tripartite Werner states. The three bipartite reduced states coincide due to the permutation invariance and are thus characterized by only one flip expectation value $f = \mathrm{tr}[\rho_K \mathbb{F}] = r_+ - r_-$.

The above observations now tell us that for every permutation invariant tripartite Werner state the optimal state $\tilde{\rho}$ is again from this set and lies in addition on the line $r_+ - r_- = f$. Hence, the set of all proper $\tilde{\rho}$ can be parameterized by a single parameter λ. It is now straightforward to write down the entropy and to solve the variation with respect to λ numerically.

However, since not much insight is coming out of writing down the formulas which are rather lengthy due to the logarithm (the solution is the root of a polynomial with not whole-numbered exponents) we

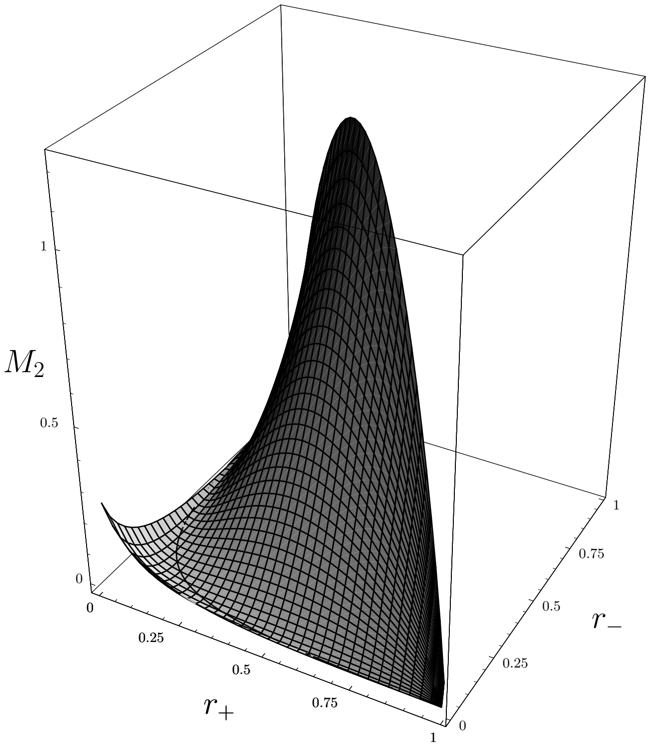


Figure 3.20: The measure M_2 as a function of r_+, r_- for permutation invariant tripartite Werner states (plotted for $d = 3$). Note that for all states lying on the black curve including the states corresponding to the projectors onto totally symmetric respectively antisymmetric subspaces (i.e. $r_\pm = 1$) we have $M_2 = 0$.

refrain from that and present, in figure 3.20, the obtained result .

Note that for the states corresponding to the projectors onto totally symmetric respectively antisymmetric subspaces (i.e. $r_\pm = 1$) we have $M_2 = 0$ (as for all states lying on the thin black curve). For $d = 3$ the antisymmetric state is pure (it is the spin-1 singlet state) and it is completely determined by its bipartite reductions. This is, however, a general feature of the n-party singlet states in $d = n$ dimensions (see Lemma (2.4.3)).

3.4 Inner geometry and state estimation

Another question that arises naturally when dealing with a family of states characterized by only few parameters is: Once one such state has been prepared, how well can one determine the corresponding parameters via measurements on a certain number of copies of the state? This question is well known in classical statistics under the keyword parameter estimation. In our context it is closely related to the question: How well can two states be distinguished statistically?

In [Woo81] Wootters, in a natural way, introduced a statistical distance between two pure states by investigating the maximum number of intermediate, mutually distinguishable pure states in a finite number of trials. His astonishing result was that this statistical distance coincides with the usual geometrical distance measure in a Hilbert space given by its inner product:

$$d_W(\psi, \tilde{\psi}) = \cos^{-1} |\langle \psi | \tilde{\psi} \rangle|. \tag{3.67}$$

A generalization to mixed state was then presented in [BC94], which involved maximizing the Fisher information as optimization of the measurements. The distance measure proposed therein turned out to be the distance given by the Bures metric[48] d_B (up to a factor) for neighboured states ρ and $\rho + d\rho$. Topologically this distance measure is equivalent to the trace norm distance even for arbitrary von Neumann-algebras (e.g. infinite dimensional systems). In fact in [Had86] it was already shown that all norms of the form[49]

$$d_q(\psi_1, \psi_2) = \sup_{\left\{\{p_i\} | p_i^2 = p_i \wedge \sum_i p_i = \mathbb{1}\right\}} \left(\sum_{k=1}^{d} |\langle \psi_1 | p_k | \psi_1 \rangle^{\frac{1}{q}} - \langle \psi_2 | p_k | \psi_2 \rangle^{\frac{1}{q}} |^q \right)^{\frac{1}{q}} \tag{3.68}$$

are uniformly equivalent. Now any such distance function d_x induces a volume element via its metric tensor g_{ij}^x, which has a density with respect to the Lebesgue measure given by:

$$\mu_x = \sqrt{|\det g_{ij}^x|}. \tag{3.69}$$

To have something like an "a priori" probability for a state to lie in a certain region Γ of the state space, we can thus take the relative

[48] The Bures metric was introduced in [Bur69] in the context of state spaces of von Neumann-algebras.

[49] Note that this family contains the trace norm distance for $q = 1$ and the Bures metric for $q = 2$.

volume of Γ with respect to the given metric. In the following we will investigate these relative volumes for tripartite Werner states. We will concentrate on the Bures metric alone for two reasons: Firstly, it is connected to the problem of statistical distinguishability and secondly, the metric induced by the trace norm is completely flat contrary to the Bures metric, which leads to a riemannian metric.

For finite dimensional density matrices the Bures metric reduces to the following distance function which is closely related to Uhlmann's transition probability for density operators (see [Uhl76]):

$$d_B^2(\rho, \sigma) = 2 - 2\mathrm{tr}\left[\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right], \tag{3.70}$$

which for symmetric states can be computed on the algebra itself since the dimension dependence drops out like for the entanglement monotones in subsection 3.2.1. The corresponding metric tensor can then be derived by

$$g_{ij}^B \mathrm{d}\rho^i \mathrm{d}\rho^j = \frac{1}{2}\frac{\mathrm{d}^2}{\mathrm{d}t^2} d_B^2(\rho, \rho + t\mathrm{d}\rho)\bigg|_{t=0}. \tag{3.71}$$

We start applying these ideas to bipartite Werner states. Any bipartite Werner state can be written as

$$\rho_W = r_+\rho_+ + r_-\rho_- \qquad \text{with} \qquad r_+ + r_- = 1, \tag{3.72}$$

where $\rho_\pm = P_\pm/\mathrm{tr}[P_\pm]$. The advantage of this representation is, of course, that it is in a sense already the spectral decomposition of ρ_W. Taking the two neighboured states $\rho \equiv (r_+, 1 - r_+)$ and $\rho + t\mathrm{d}\rho \equiv (r_+ + t\mathrm{d}r_+, 1 - r_+ - t\mathrm{d}r_+)$ we get

$$d_B^2(\rho, \rho + t\mathrm{d}\rho) = 2 - 2\sqrt{r_+(r_+ + t\mathrm{d}r_+)} - 2\sqrt{(1 - r_+)(1 - r_+ - t\mathrm{d}r_+)} \tag{3.73}$$

and, after normalization, the density

$$\mu_B = \frac{1}{\pi\sqrt{r_+(1 - r_+)}}. \tag{3.74}$$

An "a priori" probability for a bipartite Werner state to be separable can then be calculated by integrating this density over the parameter range corresponding to separable states. As derived in Lemma (2.1.1), this is the set of states with positive flip expectation value $f \in [0, 1]$. With $f = r_+ - r_-$ and $r_- = 1 - r_+$ we obtain:

$$p_{\mathrm{bip,sep}} = \int_0^{\frac{1}{2}} \frac{1}{\pi\sqrt{r_+(1 - r_+)}}\mathrm{d}r_+ = \frac{1}{2}. \tag{3.75}$$

For bipartite Werner states we therefore have a 50% a priori probability of their being separable and likewise of their being entangled.

In the same way we can compute the Bures distance for permutation invariant tripartite Werner states

$$\begin{aligned} d_B^2(\rho, \rho + t\mathrm{d}\rho) =& 2 - 2\sqrt{r_+(r_+ + t\mathrm{d}r_+)} - 2\sqrt{(1-r_+)(1-r_+ - t\mathrm{d}r_+)} \\ & - 2\sqrt{(1-r_+-r_-)(1-r_+-r_- - t\mathrm{d}r_+ - t\mathrm{d}r_-)} \end{aligned} \tag{3.76}$$

and the normalized density

$$\mu_B = \frac{1}{2\pi\sqrt{r_+ r_-(1-r_+-r_-)}}. \tag{3.77}$$

Integrating over the separable and biseparable triangles as given in figure 3.2 we get the “a priori” probabilities

$$p_{\text{trip,perm,sep}} = \frac{\pi}{40}\left(-16 + 6\sqrt{6} + 5\log\frac{3(6-\sqrt{6})}{6+\sqrt{6}}\right) \approx 0.170502 \tag{3.78}$$

and

$$p_{\text{trip,perm,bisep}} = \frac{\pi}{10}\left(1 - 5\sqrt{5} + 4\sqrt{6} - 10\log\frac{(5+\sqrt{5})(6-\sqrt{6})}{(5-\sqrt{5})(6+\sqrt{6})}\right) \approx 0.179607, \tag{3.79}$$

which is remarkably close to the result for triseparable states. Since for permutation invariant tripartite Werner states ppt is equivalent to biseparability, there is nothing to calculate in that case.

Turning now to general tripartite Werner states the situation is a little bit more complex due to the lack of commutativity. Fortunately, we can compute the distance on the algebra so that we can represent the state by

$$\rho \equiv r_+ \oplus r_- \oplus \begin{pmatrix} r_0 + r_3 & r_1 - ir_2 \\ r_1 + ir_2 & r_0 - r_3 \end{pmatrix}, \tag{3.80}$$

boiling the problem down to computing the Bures distance for 2×2-matrices. This was already done by [Hüb92] so that we can directly write down the Bures distance as

$$\begin{aligned} d_B^2(\rho, \rho + t\mathrm{d}\rho) &= 2 - 2\sqrt{r_+(r_+ + dr_+)} - 2\sqrt{r_-(r_- + dr_-)} \\ & - 2\sqrt{2r_0(r_0 + \mathrm{d}r_0) + 2\vec{r}\cdot(\vec{r} + \vec{\mathrm{d}r}) + \sqrt{r_0^2 - \vec{r}^2}\sqrt{(r_0 + \mathrm{d}r_0) - (\vec{r} + \vec{\mathrm{d}r})^2}} \end{aligned} \tag{3.81}$$

with $r_0 = 1 - r_+ - r_-$, $\mathrm{d}r_0 = -\mathrm{d}r_+ - \mathrm{d}r_-$, $\vec{r} = (r_1, r_2, r_3)$ and finally $\vec{\mathrm{d}r} = (\mathrm{d}r_1, \mathrm{d}r_3, \mathrm{d}r_3)$. Again we can normalize the resulting density to be:

$$\mu_B = \frac{2}{\pi^3(1 - r_+ - r_-)\sqrt{r_+ r_-((1 - r_+ - r_-)^2 - r_1^2 - r_2^2 - r_3^2)}}. \tag{3.82}$$

Although all the preceding expressions were free of dimension, there is one last dimension dependency hidden. In fact, for $d = 2$ there are no antisymmetric states or equivalently the alternating representation does not show up, i.e. $P_- = 0$ for $d = 2$. Three qubit Werner states can be parameterized with four parameters only. For the distance we need just to set $r_- = 0$, but for the volume element we have to make an analogous computation to arrive at the density

$$\mu_B^{d=2} = \frac{3}{4\pi^2(1 - r_+)\sqrt{r_+((1 - r_+)^2 - r_1^2 - r_2^2 - r_3^2)}}. \tag{3.83}$$

Unfortunately, this time an analytic integration over the various separable sets fails. To have a rough estimate on the corresponding "a priori" probabilities we computed, therefore, 600 Monte-Carlo integrations with 100.000.000 samples each. Since the obtained averages and variances stem from the same distribution, we can invoke the central limit theorem to see that the averages are normally distributed. With a simple calculation of the error propagation we obtain the results shown in table 3.21.

class	average	error
PPT	12.0520×10^{-3}	0.0060×10^{-3}
bipartite	7.0610×10^{-3}	0.0028×10^{-3}
tripartite	1.3685×10^{-3}	0.0016×10^{-3}

Figure 3.21: A priori probabilities for arbitrary tripartite Werner states calculated via Monte Carlo integrations.

The obtained a priori probabilities confirm the intuition from figures 3.11 and 3.6 that separable states are more or less concentrated in the vicinity of the permutation invariant states.

Chapter 4

Quantum data hiding

> “The most exciting phrase to hear in science, the one that heralds new discoveries, is not Eureka! (I found it!) but rather, ’hmm...that’s funny’.”
>
> (Isaac Asimov)

Having introduced and characterized two families of symmetric multipartite states, in this chapter we will present an application of them. We will use them to construct a protocol called *quantum data hiding*. Quantum data hiding makes use of the difficulty in distinguishing two symmetric states via LOCC operations only[50] to establish an encryption protocol similar to but stronger than quantum secret sharing.

We begin by re-presenting the idea due to [TDL01]. We then enlarge their results on bipartite quantum data hiding giving a geometric interpretation of quantum data hiding and show that the protocol remains secure even when using separable states. In section 4.2 we will generalize the protocol to multipartite systems and give a construction scheme for the corresponding hiding states as well as various examples. Section 4.3 will then deal with the optimal quantum data hiding for two qubits.

The construction scheme for multipartite quantum data hiding has

[50] Note that distinguishability heavily depends on the class of operations used to make the distinction.

been published in [EW02]. A longer, rigorous version can be found in [EW] including most of this chapter.

4.1 Hiding classical bits

As we have already seen in Lemma 2.4.5, twirling is a very effective way of wiping out local information and at the same time best for maximizing the information difference between the overall state and its reduced states. It was therefore natural to use symmetric states in order to "hide" information. In [TDL01, TDL02] Terhal et al. introduced a protocol serving this purpose in the following way: Assume that one person (say Donald Duck) has an important piece of information. Unfortunately, he has to leave without taking this classical information with him. To store the information (one bit for simplicity) he decides to prepare, according to the value of the secret bit, one out of two states of a bipartite quantum system[51]. After the preparation procedure he hands one subsystem to Huey and one to Dewey. The nephews will stay in separate rooms, being able to communicate in a classical way only (i.e. without the possibility of exchanging their systems). Obviously, they are curious to know the information and will try to extract it. Donald's task is therefore to prepare the systems in such a state that the nephews will not be able to infer the bit unless they manage to come together and join their systems. This application is long-known in classical information theory as Shamir's secret sharing [Sha79]. The first quantum version of it was termed *quantum secret sharing* [HBB99]. However, quantum data hiding is the stronger protocol since it guarantees the security of the hidden bit even in the case that all parties are allowed to communicate classically unlike in quantum secret sharing where one "bad" party is excluded from communication.

The crucial part for Donald is to model the set of operations his nephews will be able to apply to their subsystems. Unfortunately, the LOCC class is mathematically hard to characterize (see subsection 1.1.2). Therefore we will follow [TDL01] and take the class of operations having a positive partial transpose since it is a strict overset of the LOCC operations and easier to characterize. In fact, for PPT-measurements we have:

[51] For simplicity's sake we will assume that the dimensions of the single subsystems are equal. This is not a real restriction since we can always embed lower dimensional systems into higher dimensional ones.

Lemma 4.1.1: Let $T\colon \rho \mapsto s \times T_s(\rho)$ be a PPT-instrument with the "subchannels" $T_s(\rho) = K_s \rho K_s^*$ and the corresponding POVM-elements $M_s = K_s^* K_s$. Then all POVM-elements are PPT themselves:

$$\forall s: \quad \Theta_2(M_s) \geq \mathbf{0}. \tag{4.1}$$

Proof. Let ρ be a density operator, then $\Theta_2(\Theta_2(\rho)) = \rho \geq \mathbf{0}$. Since all the T_s are PPT we have that $\Theta_2(T_s(\Theta_2(\rho))) \geq \mathbf{0}$ holds and therefore

$$0 \leq \mathrm{tr}[\Theta_2(T_s(\Theta_2(\rho)))] = \mathrm{tr}[T_s(\Theta_2(\rho))] \overset{\text{def}}{=} \mathrm{tr}[\Theta_2(\rho) M_s] = \mathrm{tr}[\rho \Theta_2(M_s)] \tag{4.2}$$

for all positive ρ and thus $\Theta_2(M_s) \geq \mathbf{0}$. ■

For our purpose of hiding only one bit of information we can summarize whatever operation the parties perform in a two outcome positive operator valued measure (POVM) $\{M_0, M_1\} \equiv \{A, \mathbb{1} - A\}$. The conditional probabilities of obtaining the outcome i when the bit j is encoded is then given by

$$p_{ij} = \mathrm{tr}[M_i \rho_j]. \tag{4.3}$$

As any experiment where these two probabilities sum up to 1 can be implemented by simple coin tossing the interesting quantity is the amount of information beyond it:

$$|1 - p_{00} - p_{11}| = |1 - \mathrm{tr}[A\rho_0] - \mathrm{tr}[(\mathbb{1} - A)\rho_1]| = |\mathrm{tr}[A(\rho_1 - \rho_0)]|. \tag{4.4}$$

The task in quantum data hiding is now to find a pair of states $\{\rho_0, \rho_1\}$ such that this quantity becomes arbitrarily small for all analyzing operators A representing LOCC measurements:

$$|\mathrm{tr}[(\rho_1 - \rho_0)A]| \leq \varepsilon \tag{4.5}$$

and at the same time arbitrarily close to unity for arbitrary analyzing operators:

$$|\mathrm{tr}[(\rho_1 - \rho_0)A]| \geq 1 - \delta. \tag{4.6}$$

The quantities ε and δ are called *hiding quality* and *recovery accuracy*. The proof that this is always possible even for multipartite configurations will be given in section 4.2. Furthermore we will see in that section that both, ε and δ, behave like the inverse of the dimension of the single subsystems. The security of this scheme is therefore achieved only in the limit of high dimensions (asymptotic security).

4.1.1 A geometrical interpretation

It is clear that the set of admissible analyzing operators will determine the set of hiding states and vice versa. Therefore we first give a geometric interpretation of this reciprocity to have a better intuition before calculating simple examples of quantum data hiding.

The relationship between hiding states and analyzing operators can be formulated in terms of the duality between base norm spaces and order unit spaces (see [Nag73]). In this subsection we will show that the hiding quality $|\mathrm{tr}[(\rho_0 - \rho_1)\, A]|$ corresponds exactly to a base norm, and give simple examples to illustrate it.

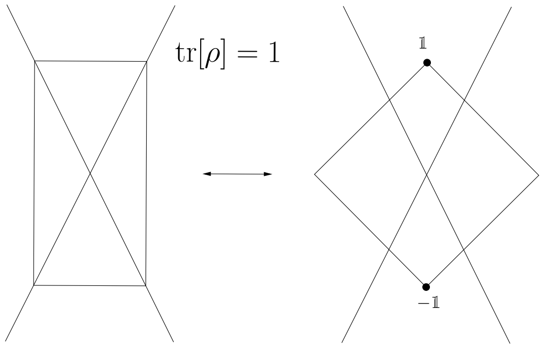


Figure 4.1: The left cone represents the positive (upper half) and negative operators (lower half). The basis is given by the combination of the intersections $\mathrm{tr}[\rho] = 1$ and $\mathrm{tr}[\rho] = -1$. The cone at the right is the dual cone to the cone of positive operators and depicts the order unit space of selfadjoint operators and the corresponding unit ball. These cones are dual in the sense that to each edge of one unit ball there are corresponding faces in the other.

We start by noting that the set

$$E_+(\mathcal{P}) = \{A | \Theta_2(A) \geq \mathbf{0}\} \tag{4.7}$$

has the structure of a positive cone, since with every A which is in $E_+(\mathcal{P})$, $\lambda \cdot A$ with $\lambda \in \mathbb{R}_+$ is in $E_+(\mathcal{P})$ too. Together with the order unit $\mathbb{1}$ the cone $E_+(\mathcal{P})$ spans an order unit space denoted by $E(\mathcal{P})$. The POVMs the parties can implement can then be written as the elements belonging to the double cone:

$$E_1(\mathcal{P}) = \left\{ F \left| \frac{\mathbb{1} \pm F}{2} \in E_+(\mathcal{P}) \right. \right\} \tag{4.8}$$

which is equivalent to F being in the unit ball:

$$F \in B(\mathcal{P}) = \{F \in E(\mathcal{P}) | \|\Theta_S(F)\| \leq 1 \forall S\} \, . \tag{4.9}$$

Associated to $E_+(\mathcal{P})$ there is its *dual cone*[52], i.e. the cone of linear forms that are positive on $E_+(\mathcal{P})$:

$$E_+(\mathcal{P})^* = \{B | \mathrm{tr}[B^* A] \geq 0 \forall A \in E_+(\mathcal{P})\}. \tag{4.10}$$

Furthermore the cone $E_+(\mathcal{P})^*$ has a base given by

$$K(E_+(\mathcal{P})^*) = \{B \in E_+(\mathcal{P})^* | \mathrm{tr}[B] = 1\} \tag{4.11}$$

(K for short) and a base norm given by

$$\|\sigma\|_\sharp^* = \inf\{\lambda_+ + \lambda_- | \sigma = \lambda_+ \sigma_+ - \lambda_- \sigma_-, \lambda_\pm \geq 0\} \tag{4.12}$$

with $\sigma_\pm \in K$. $E_+(\mathcal{P})^*$ equipped with $\| \cdot \|_\sharp$ is a base norm space $E(\mathcal{P})^*$. Since the dual of this base norm space is the order unit space $E(\mathcal{P})$ we have that $E(\mathcal{P})$ has the norm dual to (4.12):

$$\|A\|_\sharp = \sup\{|\mathrm{tr}[B^* A]| | B \in \mathrm{co}(K \cup -K)\} \tag{4.13}$$

where co denotes the convex hull of the respective set. Alternatively we can write this norm as

$$\|A\|_\sharp = \sup_{\sigma \in E(\mathcal{P})^*} \frac{|\langle \sigma | A \rangle|}{\|\sigma\|_\sharp^*} \tag{4.14}$$

with $\langle \sigma | A \rangle$ denoting the Hilbert-Schmidt scalar product $\mathrm{tr}[\sigma^* A]$. By the polarity correspondence (see [Roc72]) we get

$$\|\sigma\|_\sharp^* = \sup_{A \in E(\mathcal{P})} \frac{|\langle \sigma | A \rangle|}{\|A\|_\sharp}. \tag{4.15}$$

Writing the POVM element A in terms of elements of the unit ball ($A = \frac{\mathbb{1}+F}{2}$) we can rewrite this norm for elements of the unit ball to recover the hiding quality:

$$\sup_{F \in E_1(\mathcal{P})} |\mathrm{tr}[(\rho_0 - \rho_1) \, F]| = \frac{1}{2} \|\rho_0 - \rho_1\|_\sharp^*. \tag{4.16}$$

[52] This algebraic duality can be interpreted as duality with respect to the Hilbert-Schmidt scalar product.

4.1.2 Hiding bits in Werner/isotropic states

To give some intuition of these objects we compute, as an example, the hiding quality of bipartite Werner states and of isotropic states. As was already shown in [TDL01, TDL02], the optimal bipartite hiding states with Werner symmetry are the normalized symmetric and antisymmetric projectors[53] (see subsection 4.2.4):

$$\rho_0 = \frac{\mathbb{1} + \mathbb{F}}{d^2 + d} \qquad \text{and} \qquad \rho_1 = \frac{\mathbb{1} - \mathbb{F}}{d^2 - d}, \tag{4.17}$$

where $\mathbb{F}$ is the Flip operator defined by $\mathbb{F}(\varphi \otimes \psi) = \psi \otimes \varphi$ for all $\varphi, \psi \in \mathbb{C}^d$. The POVM element A can be written as $A = \frac{\mathbb{1}+F}{2}$ with $F \in E_1(\mathcal{P})$, i.e.

$$-\mathbb{1} \leq F \leq \mathbb{1}, \qquad -\mathbb{1} \leq \Theta_{\{2\}}(F) \leq \mathbb{1}. \tag{4.18}$$

Furthermore, for symmetric states it suffices to consider operators A bearing the same symmetry. In fact, since we are looking at expectation values only, if we take symmetric states, i.e. states being invariant under some twirling operation $\mathcal{T}$, we can restrict ourselves to operators A having the same symmetry:

$$\mathrm{tr}[A(\rho_1 - \rho_0)] = \mathrm{tr}[A\mathcal{T}(\rho_1 - \rho_0)] = \mathrm{tr}[\mathcal{T}(A)(\rho_1 - \rho_0)], \tag{4.19}$$

or in other words: to each operator A we can find a symmetric partner $\mathcal{T}(A) = \lambda\mathbb{1} + \mu\mathbb{F}$ leading to the same conditional probabilities[54]. The constraints of (4.18) turn then into

$$|\lambda \pm \mu| \leq 1, \quad |\lambda| \leq 1 \text{ and } |\lambda + \mu \cdot d| \leq 1. \tag{4.20}$$

In these parameters we get for the hiding quality:

$$|\mathrm{tr}[(\rho_0 - \rho_1)A]| = \frac{1}{2}\|\rho_0 - \rho_1\|_\sharp^* = |\mu|. \tag{4.21}$$

Figure 4.2 shows a plot of the sets of operators F satisfying (4.18). In contrast to the positivity constraint the ppt range is dimension dependent and converges to the interval $[-1, 1]$ of the abscissa. The optimization of $|\mu|$ can now be done by inspection. There are, of course, two

[53] Actually they build the *only* pair of orthogonal states in the bipartite Werner family.

[54] To obtain the last equality one needs the unimodularity of the Haar measure involved in the twirling operation, the interchangeability of the trace and the integration for finite dimensions and the cyclicity of the trace.

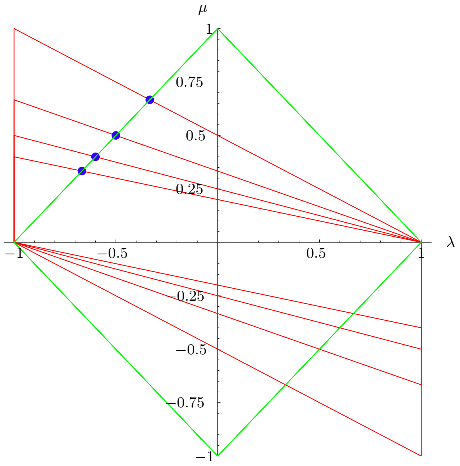


Figure 4.2: Positive and ppt operators of Werner symmetry. The ppt range and the optimal POVM are displayed for the dimensions 2, 3, 4 and 5.

equivalent solutions, due to the absolute value, which correspond to the interchange of A and $\mathbb{1} - A$. The optimum converges together with the ppt region towards a multiple of the identity which has no resolution power, i.e. the chosen states hide the bit in the limit of $d \to \infty$.

For the isotropic states ($\rho_0 = |\Omega\rangle\langle\Omega|$, $\rho_1 = \frac{\mathbb{1}-|\Omega\rangle\langle\Omega|}{d^2-1}$) the calculation is more or less the same up to the fact that the two sets of operators (positive and ppt) swap their rôles (cf. figure 4.3). Contrary to the Werner picture the parallelogram describes the positive operators and remains fixed whereas the rhombus is stretched by the dimension. With $A = \lambda\mathbb{1} + \mu|\Omega\rangle\langle\Omega|$ the hiding quality is again equal to $|\mu|$. The optimal POVM converges to the projector onto the maximally entangled state. Hiding is therefore not possible since we have that $\varepsilon \geq \frac{d}{d+1}$.

4.1.3 Separable hiding states

As we will see in section 4.2.3, it is possible to enhance the hiding quality by taking more copies or higher dimensional systems. Therefore, we are no longer restricted to taking orthogonal hiding states. In fact, even separable non-orthogonal states can hide a classical bit, although this might need more resources (=Hilbert space dimensions) as we need more copies of them to achieve a given hiding quality.

To make this result easier to read we will not compute the hiding quality in detail but use a simpler though weaker bound. This bound arises if we omit the positivity constraint enlarging the set of allowed POVMs:

$$\begin{aligned}\varepsilon &= \sup_{\substack{\mathbb{1}\geq A\geq \mathbf{0}\\ \mathbb{1}\geq\Theta_2(A)\geq\mathbf{0}}} |\mathrm{tr}[(\rho_0-\rho_1)\,A]| = \frac{1}{2}\sup_{\substack{\|A\|\leq 1\\ \|\Theta_2(A)\|\leq 1}} |\mathrm{tr}[(\rho_0-\rho_1)\,A]| \\ &\leq \frac{1}{2}\sup_{\|\Theta_2(A)\|\leq 1} |\mathrm{tr}[(\rho_0-\rho_1)]A| = \frac{1}{2}\sup_{\|\Theta_2(A)\|\leq 1} |\mathrm{tr}[\Theta_2\,(\rho_0-\rho_1)]\Theta_2(A)| \\ &= \frac{1}{2}\|\Theta_2\,(\rho_0-\rho_1)\,\|_1.\end{aligned} \tag{4.22}$$

A very simple bipartite hiding scheme with separable states was already presented in [EW02]. As hiding states we used

$$\widehat{\rho}_1 = \rho_+^{\otimes K}, \qquad \widehat{\rho}_0 = \left(\frac{\rho_+ + \rho_-}{2}\right)^{\otimes K}, \tag{4.23}$$

which are clearly separable [Wer89]. For the best possible analyzer $A = P_+^{\otimes K}$ we can compute the recovery accuracy to be $\delta = 2^{-K}$ and use (4.22) to estimate the hiding quality ε:

$$\begin{aligned}2\varepsilon \leq \|\Theta_2(\widehat{\rho}_0-\widehat{\rho}_1)\|_1 &= \|\left(\frac{P_1}{d^2+d}+\frac{(1+d)P_0}{d^2+d}\right)^{\otimes K} - \left(\frac{P_1}{d^2-1}\right)^{\otimes K}\|_1 \\ &= \mathrm{tr}\left[\left(\frac{P_0}{d}+\frac{P_1}{d^2+d}\right)^{\otimes K} - \left(\frac{P_1}{d^2+d}\right)^{\otimes K}\right] \\ &\quad + \mathrm{tr}\left[\left(\left|\left(\frac{1}{d^2+d}\right)^K - \left(\frac{1}{d^2-1}\right)^K\right|\right)P_1^{\otimes K}\right] \\ &= 1 + \left(\left(\frac{1}{d^2-1}\right)^K - 2\left(\frac{1}{d^2+d}\right)^K\right)\left(d^2-1\right)^K \\ &= 2\left(1-\left(1-\frac{1}{d}\right)^K\right)\end{aligned} \tag{4.24}$$

with $P_0 = |\Omega\rangle\langle\Omega|$ and $P_1 = \mathbb{1} - P_0$. This simple example shows that any finitely distinguishable pair can be used if one can afford enough copies, i.e. a big enough Hilbert space.

4.1.4 Robustness of symmetric quantum data hiding

Since the security is crucial for such hiding protocols it is important to know how they behave in the presence of prior entanglement. One

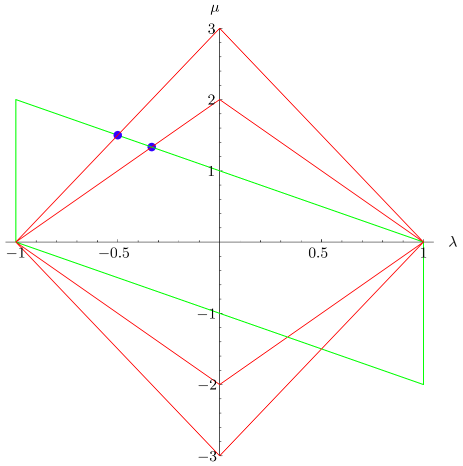


Figure 4.3: Positive and ppt operators of isotropic symmetry. The optimal POVM is figured for dimensions 2 and 3.

could think that for breaking a protocol hiding one classical bit one e-bit might be enough. Fortunately, this is not true as a simple application of (4.22) shows.

As an example we can take any bipartite hiding protocol with the hiding states ρ_0 and ρ_1. Furthermore we allow the two parties to share a maximally entangled state Ω of dimension D, getting a scheme with the states $\rho_i \otimes |\Omega\rangle\langle\Omega|$. By virtue of (4.22) we get:

$$2\varepsilon \leq \|\Theta_2\left((\rho_0 - \rho_1) \otimes |\Omega\rangle\langle\Omega|\right)\|_1 = D\|\Theta_2\left(\rho_0 - \rho_1\right)\|_1. \tag{4.25}$$

The behaviour of this new protocol is thus the same but for the dimension of the entanglement resource. To break the hiding scheme it would be therefore necessary to have $D = d$, that is one would have to enable the parties to teleport their particles.

4.2 Hiding bits in multipartite states

Hiding quantum data among more than two parties (e.g. with a third or a fourth nephew[55]) naturally leads to more complicated configurations. Let us assume that the classical bit has been encoded into the choice of

[55] In some comics like *Donald Duck: Medaling Around* (story W WDC 261-01) by Carl Barks a fourth nephew, afterwards called Fooey or Phooey, has been drawn by accident in some panels.

one out of two states of an N-partite system, where all the single site Hilbert spaces have the same dimension d. After the encoder has made his choice he passes the N particles to N different parties that may try to recover the hidden bit performing some measurements and communicating classically. Moreover some of the parties can have quantum lines of communication, i.e. they can be regarded as having more than one of the particles. The idea is that the parties that can exchange quantum information are stored in one lab and the different labs communicate via classical information exchange (phone lines etc.). The different subsets belonging to different labs altogether form a *partition* $\mathcal{P}$ of the N sites which fully describes the communication possible. This partition determines what can be called the local operations with classical communication ($\mathcal{P}$-LOCC operations) of the setup.

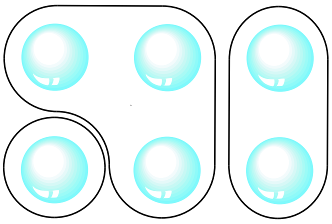


Figure 4.4: The partition $\mathcal{P} = \{(4)(36)(125)\}$ for a six-partite system. Parties belonging to the same block can communicate quantumly whereas the blocks can communicate only classically.

Again we will not use $\mathcal{P}$-LOCC operations to demonstrate the security of the protocol but the corresponding lager class of $\mathcal{P}$-PPT observables. A $\mathcal{P}$-PPT observable will be described similarly to (4.1) by a dichotomic POVM $\{M_0, M_1\} \equiv \{A, \mathbb{1} - A\}$:

Lemma 4.2.1: Let S be any of the subsets of a partition $\mathcal{P}$. A $\mathcal{P}$-PPT instrument $T: \rho \mapsto i \times T_i(\rho)$ with "subchannels" $T_i(\rho) = K_i \rho K_i^*$ and corresponding POVM-elements $M_i = K_i^* K_i$ fulfills

$$\Theta_S(M_i) \geq \mathbf{0} \qquad \text{for all } S \subset \mathcal{P}. \tag{4.26}$$

Proof. The proof is identical to the proof of Lemma 4.1.1 if one takes the splits $S|\complement S$ for all $S \subset \mathcal{P}$ instead of $1|2$. ■

In the protocol we present (see [EW02]) the encoder is allowed to choose a set $\mathbb{P}$ of hiding partitions $\mathcal{P}$ for which he wants the bit to be hidden, and conversely the bit to be recoverable for any partition $\mathcal{P} \notin \mathbb{P}$.

The set $\mathbb{P}$ is completely arbitrary up to the fact that choosing a finer partition $\mathcal{P}$, i.e. allowing less quantum communication lines, makes it harder to recover the bit. The power of our scheme is summarized in the following theorem:

Theorem 4.2.2: Consider any set $\mathbb{P}$ of hiding partitions containing with each partition all finer ones. Then, for any given security $\varepsilon \geq 0$ and accuracy of recovery $\delta \geq 0$, we can find a pair of hiding states ρ_0, ρ_1 such that:

1. For all partitions $\mathcal{P} \in \mathbb{P}$ and all analyzing operators A which are admissible for $\mathcal{P}$ we have
$$|\mathrm{tr}[(\rho_1 - \rho_0)A]| \leq \varepsilon.$$
2. For all partitions $\mathcal{P} \notin \mathbb{P}$ there is an analyzing operator A which is admissible for $\mathcal{P}$ such that
$$|\mathrm{tr}[(\rho_1 - \rho_0)A]| \geq 1 - \delta.$$

The proof of this theorem will be carried out in detail in the next three sections. This scheme is fairly general but we remark that the hiding and recovery qualities will determine the resources needed to implement it. As we will prove in section 4.2.2 the qualities will behave like the inverse of the single Hilbert space dimension.

4.2.1 Multipartite symmetric hiding states

As hiding states we will use the multipartite Werner states introduced in chapter 2. In subsection 4.2.4 we will see that even permutation invariant multipartite Werner states already serve our purpose of hiding a classical bit.

Besides the fact that these states are easy to characterize a second advantage is that for symmetric states it suffices to consider operators A bearing the same symmetry. The second ingredient (the POVM) will now have the same symmetry as the states used:

$$A = \sum_{\pi} a_\pi V_\pi, \qquad \pi \in \mathfrak{S}_N. \tag{4.27}$$

In contrast to the plain positivity $A \geq \mathbf{0}$, the positivity condition $\Theta_S(A) \geq \mathbf{0}$ written in terms of the coefficients a_π is heavily dimension dependent, as we will show in this subsection. We start by exploring the consequences of the plain positivity and then turn to the positivity of partially transposed As.

Let us consider the matrix M given by

$$d^{-N}\mathrm{tr}[V_\pi^* V_\sigma] = \delta_{\pi,\sigma} + d^{-1}M_{\pi,\sigma}. \tag{4.28}$$

Since $\mathrm{tr}[V_\pi] = d^c$, where c is the number of cycles in π including those of length 1 (alternatively this can be seen as the number of closed loops, cf. figure 2.7), M is up to a factor a doubly stochastic matrix and thus invertible, so we can invert the linear relation

$$\mathrm{tr}[V_\pi^* A] = \sum_\sigma \mathrm{tr}[V_\pi^* V_\sigma a_\sigma] = d^N \left((\mathbb{1} + d^{-1}M)a\right)_\pi. \tag{4.29}$$

Applying the inequality $\|M{\cdot}a\|_{\mathrm{m}ax} \leq \|M\|{\cdot}\|a\|_{\mathrm{m}ax}$ to the maximum Norm $\|a\|_{\mathrm{m}ax} := \max_\pi |a_\pi|$ we get by summing the Neumann series [Bha97] for the inverse of $\mathbb{1} + d^{-1}M$:

$$\max_\pi |a_\pi| \leq \frac{\max_\pi \left| d^{-N}\mathrm{tr}[V_\pi^* A]\right|}{1 - \|M\|/d}. \tag{4.30}$$

As M is doubly stochastic (up to a factor) $\|M\|$ is simply the sum of the components of one of its rows or columns. A closer look at M reveals that each row or column consists of all permutations but the identity which has been subtracted in (4.28). The sum of one such row is thus proportional to the dimension of the Bose projector:

$$\begin{aligned}\|M\| &= d\left(d^{-N}N!\mathrm{tr}[P_+] - 1\right)\\ &= d\left(d^{-N}\frac{(d+N-1)!}{(d-1)!} - 1\right)\\ &= d\left(\frac{d+N-1}{d}\cdot\ldots\cdot\frac{d}{d} - 1\right)\\ &= d\left(\left(1+\frac{N-1}{d}\right)\cdot\ldots\cdot\left(1+\frac{1}{d}\right) - 1\right)\\ &\leq d\left(e^{\frac{N-1}{d}}\cdots e^{\frac{1}{d}} - 1\right)\\ &= d\left(e^{\frac{N(N-1)}{2d}} - 1\right)\end{aligned} \tag{4.31}$$

due to the relation $1 + x \leq e^x$ which holds for all nonnegative x. This leads to

$$\begin{aligned} \max_{\pi} |a_\pi| &\le \frac{1}{1 - \|M\|/d} \\ &= \frac{1}{2 - e^{\frac{N(N-1)}{2d}}} \\ &= 1 - \frac{N(N-1)}{2} \cdot d^{-1} + \mathcal{O}(d^{-2}), \end{aligned} \tag{4.32}$$

where we used the estimate $|\mathrm{tr}[V_\pi A]| \le \|V_\pi\|_1 \|A\|$ with

$$\|V_\pi\|_1 \overset{\text{def}}{=} \mathrm{tr}\Big[\sqrt{V_\pi^* V_\pi}\Big] = d^N \tag{4.33}$$

and $\|A\| \le 1$. From this we see that the positivity constraint $\mathbf{0} \le A \le \mathbb{1}$ already bounds the coefficients of A by 1.

For the partially transposed operators these bounds are even tighter. This is best seen if we take a permutation σ that does not leave all the subsets of $\mathcal{P}$ invariant. In that case we have

$$\|\Theta_S(V_\sigma)\|_1 = \mathrm{tr}\Big[\sqrt{\Theta_S(V_\sigma^*)\Theta(V_\sigma)}\Big] = d^{N - l_S(\sigma)}, \tag{4.34}$$

where $l_S(\sigma)$ is the number of repeated indices in either ket or bra of the "chip" $\Theta_S(V_\sigma)$.

4.2.2 Tailoring the hiding property

In this subsection we will make use of these tighter bounds to show how to construct states suitable for hiding.

In fact, for a permutation that is not *adapted* to $\mathcal{P}$ (4.28) gives:

$$\begin{aligned} d^{-N}|\mathrm{tr}[AV_\sigma]| &= d^{-N}|\mathrm{tr}[\Theta_S(A)\Theta_S(V_\sigma)]| \\ &\le d^{-N}\|\Theta_S(V_\sigma)\|_1 \|\Theta_S(A)\| \\ &\le d^{-l_S(\sigma)} \end{aligned} \tag{4.35}$$

because of $\|\Theta_S(A)\| \le 1$, and as for (4.30) we get

$$|a_\sigma| \le d^{-l_S(\sigma)} + \mathcal{O}(d^{-1}). \tag{4.36}$$

But this means that only those symmetric operators will distinguish asymptotically between the two given symmetric states that respect all S, since for all σ with $l_S(\sigma) > 0$ for any S we have that $|a_\sigma| \to 0$ for $d \to \infty$.

As a first consequence of these bounds consider the case where no quantum communication is allowed at all, i.e. $\mathcal{P} = (\{1\}\{2\}\ldots\{N\})$. The only permutation leaving $\mathcal{P}$ invariant is the identity which has the same expectation for ρ_0 and ρ_1. Hence $|\mathrm{tr}[(\rho_0 - \rho_1)A]|$ decays as $\mathcal{O}(d^{-1})$ and the bit is asymptotically hidden.

The idea of our construction scheme is now to choose ρ_0 and ρ_1 exactly in this way, namely such that $\mathrm{tr}[\rho_0 V_\pi] = \mathrm{tr}[\rho_1 V_\pi]$ for all π which are adapted to *any* of the targeted hiding partitions $\mathcal{P} \in \mathbb{P}$. Although this ensures that the classical bit is hidden it does not guarantee that the resolution achievable is arbitrarily good. Fortunately, it will suffice to have $\mathrm{tr}[(\rho_0 - \rho_1)V_\pi] \neq 0$ for one permutation adapted to any targeted revealing partitions. No matter how small this resolution quality is, as we will show in section 4.2.3, we can improve it to an arbitrarily good resolution quality just by using multiple copies of the hiding states.

4.2.3 Tailoring the resolution property

As already mentioned in the preceding subsection, our construction so far does not guarantee perfect distinction ($\delta = 0$) for the partitions meant to be revealing (see examples 4.2.4.1.3.2 and 4.2.4.1.3.3). In fact, the difficulty of guaranteeing good recovery for all partitions $\mathcal{P} \notin \mathbb{P}$ remains. One part of this can be achieved easily, namely by satisfying condition 2 of the theorem for *some* $\delta < 1$, uniformly in d. For that we only need to take $\mathrm{tr}[(\rho_1 - \rho_0)V_\pi] \neq 0$, whenever π is adapted to any $\mathcal{P} \in \mathbb{P}$. For if $\mathcal{P} \notin \mathbb{P}$ we can use a permutation π with cycle decomposition $\mathcal{P}$, or rather a combination of V_π, V_π^*, and $\mathbb{1}$ as analyzing operator. This is then a local measurement, which does not even require communication, apart from the need to bring correlation data together.

Taking $\mathrm{tr}[(\rho_1 - \rho_0)V_\pi] \neq 0$ for a prescribed set of permutations is always possible, even with the constraint that ρ_0 and ρ_1 both have to be positive: we only need to take $\rho_{0,1} \propto \mathbb{1} \pm \epsilon \cdot \delta\rho$ with sufficiently small ϵ, and $\mathrm{tr}[\delta\rho_1\, V_\pi]$ zero or non-zero as desired. At the same time, this shows that we can work with separable $\rho_{0,1}$ (see subsection 4.1.3).

The recovery probability achieved in this way will be rather low. However, we can boost it by taking multiple copies of ρ_i, i.e. we choose $\widehat{\rho}_i = \rho_i^{\otimes K}$ $(i = 0, 1)$ for large K as our hiding states. By construction, if $\mathcal{P} \notin \mathbb{P}$, we can find an admissible observable $X = \sum_\alpha \xi_\alpha F_\alpha$, with $F_\alpha \geq 0$ and $\sum_\alpha F_\alpha = \mathbb{1}$ such that $\mathrm{tr}[\rho_0 X] < \mathrm{tr}[\rho_1 X]$. As analyzing measurement F to discriminate $\widehat{\rho}_0$ and $\widehat{\rho}_1$ we can therefore take a *statistical* *measurement* of X:

$$F = \sum_{\substack{\alpha_1,\dots,\alpha_K \\ \frac{1}{K}\sum_i \xi_{\alpha_i} > \check{x}}} F_{\alpha_1} \otimes \cdots \otimes F_{\alpha_K} \tag{4.37}$$

with $\check{x}$ being the mean value of X. This observable is measured on all of the K copies giving the outcomes X_α, and when the mean of these K results is $\leq \check{x}$ the partners decide on "1" as the value of the hidden bit.

The large deviation estimates [Ell] assure us that the probability of getting the wrong answer:

$$\begin{aligned} p_{1|0} = \operatorname{tr}[\widehat{\rho}_0 F] = \mathbb{P}\left(\frac{1}{K}\sum_{\alpha=1}^{K} X_\alpha \geq \check{x}\right) &= \sum_{\substack{x_1,\dots,x_K \\ \sum_\alpha x_\alpha \geq K\check{x}}} p(x_1)\cdots p(x_K) \\ \overset{\lambda\geq 0}{\leq} \sum_{x_1,\dots,x_K} p(x_1)\cdots p(x_K)\cdot e^{\lambda\sum_\alpha (x_\alpha - \check{x})} &= \left(\sum_x p(x) e^{\lambda(x-\check{x})}\right)^K \end{aligned} \tag{4.38}$$

is exponentially small in K.

Since the function $f(\lambda) = \sum_x p(x)e^{\lambda(x-\xi)}$ is convex in λ and the first order derivative is negative at $\lambda = 0$, ($f'(0) = \frac{1}{K}\sum_i x_{\alpha_i} - \check{x}$) it is clear that for positive λ we have $f(\lambda) < f(0) = 1$, giving an overall exponential decay for the probability of guessing wrong.

What remains to be checked, however, is that this statistically enhanced detection scheme with its larger local Hilbert spaces does not allow new, unwanted detection possibilities for the hiding partitions $\mathcal{P} \in \mathbb{P}$. Fortunately, this is not the case. Admissible analyzing operators now have the form

$$A = \sum_{\vec{\pi}=(\pi_1,\dots,\pi_K)} a(\pi_1,\dots,\pi_K) V_{\pi_1} \otimes \cdots \otimes V_{\pi_K}. \tag{4.39}$$

By arguments completely analogous to the single copy case in section 4.2.1, we have:

$$\begin{aligned} \left|\operatorname{tr}\left[\left(V^*_{\sigma_1} \otimes \cdots \otimes V^*_{\sigma_K}\right) A\right]\right| &= \left|\operatorname{tr}\left[\left(\Theta_S\left(V^*_{\sigma_1}\right) \otimes \cdots \otimes \Theta_S\left(V^*_{\sigma_K}\right)\Theta_S\left(A\right)\right)\right]\right| \\ &\leq \|\Theta_S\left(V^*_{\sigma_1}\right) \otimes \cdots \otimes \Theta_S\left(V^*_{\sigma_K}\right)\|_1 \cdot \underbrace{\|\Theta_S\left(A\right)\|}_{\leq 1} \\ &\leq \prod_{i=1}^{K} \|\Theta_S\left(V_{\sigma_1}\right)\|_1 = \prod_{i=1}^{K} d^{N-l_S(\sigma_1)}. \end{aligned} \tag{4.40}$$

On the other hand we have:

$$\begin{aligned} |\mathrm{tr}\big[\big(V_{\sigma_1}^* \otimes \cdots \otimes V_{\sigma_K}^*\big)\, A\big]| &= |\sum_{\vec{\pi}} \mathrm{tr}\big[\big(V_{\sigma_1}^* V_{\pi_1} \otimes \cdots \otimes V_{\sigma_K}^* V_{\pi_K}\big)\, a(\vec{\pi})\big]| \\ &= d^{N \cdot K} \left(\left(\mathbb{1}^{\otimes K} + \frac{M_K}{d} \right) a(\vec{\pi}) \right)_{\vec{\sigma}} \end{aligned} \tag{4.41}$$

where M_K is defined analogously to (4.28). Putting (4.40) and (4.41) together we obtain again:

$$\max_{\vec{\sigma}} |a(\vec{\sigma})| \leq \frac{\max_{\vec{\sigma}} \prod_{i=1}^{K} d^{-l_S(\sigma_i)}}{1 - \frac{\|M_K\|}{d}} \tag{4.42}$$

which goes to zero for $d \to \infty$, whenever not all σ_i are adapted to the chosen partition $\mathcal{P}$. Using the shorthand notation $R_i(\pi) = \mathrm{tr}[\sigma_i V_\pi]$ we finally get

$$\mathrm{tr}[(\widehat{\rho}_0 - \widehat{\rho}_1)\, A] = \sum_{\vec{\pi}} a(\vec{\pi}) \left(\prod_{i=1}^{K} R_0(\pi_i) - \prod_{i=1}^{K} R_1(\pi_i) \right). \tag{4.43}$$

Now if all π_i are adapted to $\mathcal{P}$, then the difference in the bracket is zero. If not, there must be some π_i which is not adapted to $\mathcal{P}$ and the whole expression goes to zero due to (4.42), i.e. multiple copies of symmetric hiding states are again hiding.

Effectively we used one-site Hilbert spaces of dimension d^K, which is again in keeping with the "1/dimension" behaviour of errors in the theorem. For hiding the classical bit we can thus first choose K large to make δ small, and subsequently d large, in order to get $\varepsilon = K/d + \mathcal{O}(d^{-2})$ small.

4.2.4 Examples

The main novelty when going from bipartite to multi-partite protocols is the possibility that the parties may conspire. In order to reveal the hidden bit they can come together in groups allowing quantum communication to the members of the group and classical communication to the rest. Excluding the trivial case where all parties come back together we show in this subsection how different coalitions can turn into different degrees of concealment.

4.2.4.1 Permutation invariant examples

To make the construction of our first examples even simpler we will restrict ourselves to permutation invariant partitions $\mathcal{P}$. This will enable us to read the desired hiding states directly off the character table of the $\mathfrak{S}_N$.

4.2.4.1.1 Weakest concealment The weakest concealment is at the same time the easiest to realize. We could use, for instance, the normalized symmetric and antisymmetric projections to encode the classical bit and the information a single party could gain on it would tend asymptotically to zero. On the other hand, this concealment is the weakest possible as a coalition of any two single parties would suffice to detect the bit with certainty without any further communication with the remaining parties. The two conspiring partners only have to test their bipartite system with the symmetric/antisymmetric projectors of their twofold tensor product. In this case the discrimination would be perfect even when the two conspiring partners do not communicate at all with the rest of the parties.

4.2.4.1.2 Strongest concealment As the strongest form of concealment we could try to hide the bit in such a way that it is asymptotically secure against all possible coalitions (besides the trivial one joining all parties).

Let us fix two states ρ_0, ρ_1 and take their difference $\delta\rho = \rho_1 - \rho_0$. In order to hide our bit against a coalition corresponding to a partition $\mathcal{P}$ we must have $\mathrm{tr}[\delta\rho V_\pi] = 0$ for all permutations adapted to $\mathcal{P}$. This means that in order to hide the bit against all possible coalitions we have to use states such that $\delta\rho$ is orthogonal to all conjugacy classes up to the one of the N-cycle. This tells us already how to construct our states. In fact, all we have to do is to take a look at the character table of the $\mathfrak{S}_N$, that is the table of coefficients of the irreducible representations written in terms of conjugacy classes (see figure 4.5). The hiding states can now be chosen as linear combinations of the projections onto the irreducible representations such that their coefficients are equal on every conjugacy class but the one of the N-cycle.

4.2.4.1.3 Fourpartite examples To make it clearer we apply the receipt given above to the case of $N = 4$.

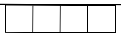
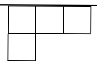
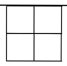
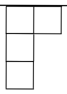
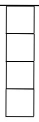
	Young frame	(1^4)	$(2,1^2)$	(2^2)	$(3,1)$	(4^1)
A		1	1	1	1	1
B		3	1	-1	0	-1
C		2	0	2	-1	0
D		3	-1	-1	0	1
E		1	-1	1	1	-1

Figure 4.5: The character table of $\mathfrak{S}_4$.

The two states we want to construct have to be orthogonal, which means that no irreducible representation can be in both linear combinations. Furthermore the coefficients of the two linear combinations written in conjugacy classes must be equal up to the last one belonging to the 4-cycle. Now we can associate to each projector onto an irreducible representation a state by normalizing it. A linear combination on the level of the character table then corresponds to taking the linear combination of the states weighted by the dimension of the respective irreducible representation[56]. The two linear combinations we can use for our purpose are

$$\begin{array}{rr|rrrrr} & A & 1 & 1 & 1 & 1 & 1 \\ + & D & 3 & -1 & -1 & 0 & 1 \\ \hline = & & 4 & 0 & 0 & 1 & 2 \end{array} \quad \text{and} \quad \begin{array}{rr|rrrrr} & B & 3 & 1 & -1 & 0 & -1 \\ + & E & 1 & -1 & 1 & 1 & -1 \\ \hline = & & 4 & 0 & 0 & 1 & -2 \end{array}$$

corresponding to the states

$$\rho_0 = \frac{\rho_A + 3\rho_D}{4} \quad \text{and} \quad \rho_1 = \frac{3\rho_B + \rho_E}{4}. \tag{4.44}$$

[56] This can be computed using the trace of the group algebra: Let P_y be the projectors onto the irreducible representations labelled by the Young frames. To each row in figure 4.5 corresponds one such projector. The addition of two projections P_{y_1} and P_{y_2} corresponds to the state $\frac{P_{y_1}+P_{y_2}}{\mathrm{tr}[P_{y_1}+P_{y_2}]}$. Since the trace of such a projection taken with the trace of the group algebra gives exactly the dimension of the representation we get: $\mathrm{tr}[P_{y_1} + P_{y_2}] = d_{y_1} + d_{y_2}$ and thus

$$\frac{P_{y_1} + P_{y_2}}{\mathrm{tr}[P_{y_1} + P_{y_2}]} = \frac{d_{y_1}}{d_{y_1} + d_{y_2}} \rho_{y_1} + \frac{d_{y_2}}{d_{y_1} + d_{y_2}} \rho_{y_2}.$$

Since these states are orthogonal by construction we can take, as a perfect analyzer, the projector onto one of the states, e.g. $A = P_A + P_D$.

Knowledge of the character table of the $\mathfrak{S}_N$ is therefore all one needs to construct permutation invariant $U^{\otimes N}$-invariant states suitable for hiding a classical bit against all possible (non-trivial) coalitions.

To show that this procedure is valid also for intermediate cases of concealment we keep $N = 4$ and construct in the same manner the examples we presented in [EW02].

4.2.4.1.3.1 Two pairs. One of the remaining possibilities for $N = 4$ is to allow the parties to form two pairs, e.g. $\mathcal{P} = (\{1,2\},\{3,4\})$. These pairs may communicate only classically between them but can exchange quantum information within the two pairs. Applying the above technique to this case we have to build two linear combinations of irreducible representations such that the coefficients of the (1^4), the $(2,1^2)$, the (2^2) and perhaps even of the (4^1) conjugacy class are equal. Again the computation is quite easy at this point:

$$\begin{array}{r|rrrrr} A & 1 & 1 & 1 & 1 & 1 \\ +\quad E & 1 & -1 & 1 & 1 & -1 \\ \hline = & 2 & 0 & 2 & 2 & 0 \end{array} \qquad \text{and} \qquad \begin{array}{r|rrrrr} C & 2 & 0 & 2 & -1 & 0 \end{array}$$

leading to the states

$$\rho_0 = \frac{\rho_A + \rho_E}{2} \quad \text{and} \quad \rho_1 = \rho_C. \tag{4.45}$$

With these states we are able to hide (asymptotically good) a classical bit against the formation of two pairs. As a perfect analyzer we can use $A = \frac{1}{3}(\mathbb{1} + R + L)$, where R (L) is the right (left) shift of the three-partite system.

4.2.4.1.3.2 The 3:1 split. Another possibility for $N = 4$ is to hide the bit against a coalition of any three of the four parties, partitions like $\mathcal{P} = (\{1,2,3\},\{4\})$. To this end we take the following linear combinations:

$$\begin{array}{r|rrrrr} A & 1 & 1 & 1 & 1 & 1 \\ +\quad C & 2 & 0 & 2 & -1 & 0 \\ \hline = & 3 & 1 & 3 & 0 & 1 \end{array} \qquad \text{and} \qquad \begin{array}{r|rrrrr} B & 3 & 1 & -1 & 0 & -1 \end{array}$$

and the corresponding states

$$\rho_0 = \frac{\rho_A + 2\rho_C}{3} \quad \text{and} \quad \rho_1 = \rho_B. \tag{4.46}$$

No 3:1 split can separate them but any two pairs can (though not perfectly) with the analyzer $A = \frac{1}{3}(\mathbb{1} + T \otimes T)$, where $T \otimes T$ denotes the tensor product of the transpositions in the two pairs.

4.2.4.1.3.3 The 2:1:1 split. The last possibility for $N = 4$ is to hide against single pairs but not allowing the remaining two parties to join into a second pair, e.g. $\mathcal{P} = (\{1, 2\}, \{3\}, \{4\})$. The usual computation then gives

$$\begin{array}{rr|rrrrr} & C & 2 & 0 & 2 & -1 & 0 \\ + & E & 1 & -1 & 1 & 1 & -1 \\ \hline = & & 3 & -1 & 3 & 0 & -1 \end{array} \quad \text{and} \qquad D \,|\, 3 \quad -1 \quad -1 \quad 0 \quad 1$$

and the corresponding states

$$\rho_0 = \frac{2\rho_C + \rho_E}{3} \quad \text{and} \quad \rho_1 = \rho_D. \tag{4.47}$$

with the best possible (imperfect) analyzer $A = (\mathbb{1} + V_{(12)(34)})/2$.

We conclude this subsection by stressing that the setups of two pairs and one triplet are not comparable in terms of allowed amount of quantum communication since two pairs can reveal a bit hidden for triplets and vice versa. The hiding strength can thus not be measured on a one parameter scale.

4.2.4.2 Beyond permutation invariance

All the examples given in the preceding subsection were easy to construct because of their high symmetry. Of course, the invariance under all permutations is not necessary for our scheme to work. In fact, when dropping the permutation invariance we still have enough freedom to keep the complete concealment scale.

In the case of $N = 4$ we could, for example, choose as hiding partitions $\mathbb{P} = \{(123)(4), (12)(3)(4), (13)(2)(4), (23)(1)(4), (1)(2)(3)(4))\}$ which fixes six out of 24 coefficients of $\delta\rho$. The set of revealing partitions $\complement\mathbb{P} = \{(1234), (124)(3), (134)(2), (234)(1), (12)(34), (13)(24), (14)(23), (14)(2)(3), (24)(1)(3), (34)(1)(2)\}$ then consists of all those partitions where the fourth party communicates quantumly with at least one other party (see 4.2.6). By choosing the remaining coefficients of $\delta\rho$ properly we can still implement the full concealment scale for the remaining 3 parties in the following sense:

- *The weakest concealment:* Every 2:1:1 partition in $\complement\mathbb{P}$ can analyze.

- *Single pairs:* No 2:1:1 partition in $\mathbb{CP}$ can analyze but all other can.

- *Two pairs:* No 2:2 and no 2:1:1 partition in $\mathbb{CP}$ can analyze but all other can.

- *Triplets:* No 3:1 and no 2:1:1 partition in $\mathbb{CP}$ can analyze but all other can.

- *The strongest concealment:* No partition in $\mathbb{CP}$ can analyze but (1234) can.

Of course, even this remaining symmetry is not necessary and was just used for keeping the examples simple.

4.2.5 Hiding bit sequences

The estimates of section 4.2.3 can be used to prove that the symmetric hiding of whole bit strings is secure. However, using the weaker bound (4.22) one can already show the security of such schemes at least for separable single bit hiding states.

Suppose the bit strings are encoded in the hiding states $\rho_I = \rho_{i_1} \otimes \cdots \otimes \rho_{i_L}$, where $\{\rho_0, \rho_1\}$ build a separable bipartite hiding scheme with security ε. The weaker bound then gives:

$$\begin{aligned}
\tilde{\varepsilon} \leq \frac{1}{2}\|\Theta_2\left(\rho_I - \rho_J\right)\|_1 &= \|\Theta_2\left(\bigotimes_{l=1}^{L}\rho_{i_l} - \bigotimes_{l=1}^{L}\rho_{j_l}\right)\|_1 \\
&\leq \|\Theta_2\left(\bigotimes_{l=1}^{L}\rho_{i_l} - \bigotimes_{l=1}^{L-1}\rho_{i_l}\otimes\rho_{j_L}\right)\|_1 \\
&\qquad + \|\Theta_2\left(\bigotimes_{l=1}^{L-1}\rho_{i_l}\otimes\rho_{j_L} - \bigotimes_{l=1}^{L}\rho_{i_l}\right)\|_1 \\
&= \|\Theta_2\left(\bigotimes_{l=1}^{L}\rho_{i_l} - \bigotimes_{l=1}^{L-1}\rho_{i_l}\otimes\rho_{j_L}\right)\|_1 + \varepsilon
\end{aligned}$$

and by iteration

$$\leq d_H\left(I,J\right)\cdot\varepsilon \tag{4.48}$$

where $d_H(I,J)$ denotes the Hamming distance between the bit strings I and J. The separability of the single bit hiding schemes may not be necessary but it improves the bound as we do not gather factors from the trace norm of their partial transpose which can reach d in the worst case. The security of hidden bit strings thus scales with at most the length of the strings for separable schemes.

4.2.6 Hiding quantum data

In [DHT03] the inventors of quantum data hiding have extended the notion of data hiding to quantum data. In this new protocol Alice and Bob are given $2n$ particles each encoding $2n$ classical bits and additionally one of the two (say Bob) has an n-qubit string which has been unitarily rotated depending on the encoded bit string such that it is locally undistinguishable from the chaotic state. Now, whenever Alice and Bob are able to recover the encoded bit string Bob can invert the rotation and get the original qubit string back. This is equivalent to using a hidden classical key to lock away a quantum secret (or a banana).

In contrast to usual quantum data hiding this protocol singles out one party which will be given the secret qubit string. When going to a multipartite setting with a set $\mathbb{P}$ of hiding partitions there may be partitions $\mathcal{P}$ which are not in $\mathbb{P}$ and which do not allow the exchange of quantum information with the privileged party. In this case, as pointed out by [DHT03], the conspiring parties may recover the hidden key but not the quantum secret since it is out of reach for them. Fortunately, there are setups where this situation does not occur. In fact, the crucial point of hiding quantum data is that the secret-keeping party should not be allowed to be part of a conspiracy, i.e. to communicate quantumly with others. In this case (see subsection 4.2.4.2) every partition not in the hiding set will correspond to a coalition capable of revealing the quantum secret. Nonetheless, all the different degrees of security for the hidden classical key are still possible.

4.3 Optimal bit-hiding in a pair of qubits

In all the preceding cases the security of the quantum data hiding protocol was achieved in the limit of an infinite single site dimension. This is obviously a big problem for experimentalists which cannot implement such a limit. It is therefore natural to ask for an optimal protocol for a fixed dimension. In [But02] a characterization of optimal quantum data hiding protocols for two qubits has been investigated in detail. In this section we will give a short derivation of some of the results obtained therein showing that optimal quantum data hiding for qubits cannot be done perfectly well but still with a non-zero gain.

It is clear that a quantum data hiding protocol does not depend on the hiding states but only on the difference $\delta\rho$. The optimal *hiding strength* of the protocol can be described with a norm similar to (4.16):

$$\|\delta\rho\|_{\text{hide}} = \sup_{\mathbf{0}\leq F, \Theta_2(F)\leq \mathbb{1}} |\text{tr}[\delta\rho \cdot F]| \tag{4.49}$$

Hiding states that optimize the hiding strength lead to a difference $\delta\rho$ that minimizes this norm. Conversely, the hiding states can be best distinguished if their difference $\delta\rho$ has a large tracenorm $\|\delta\rho\|_1$. In fact, if we write $\delta\rho = \delta\rho_+ - \delta\rho_-$ we have that:

$$\begin{aligned}\|\delta\rho\|_{\text{hide}} &= \sup_{\mathbf{0}\leq F, \Theta_2(F)\leq \mathbb{1}} |\text{tr}[\delta\rho_+ \cdot F] - \text{tr}[\delta\rho_- \cdot F]| \\ &\leq \max\left\{ \sup_{\mathbf{0}\leq F, \Theta_2(F)\leq \mathbb{1}} |\text{tr}[\delta\rho_+ \cdot F]|, \sup_{\mathbf{0}\leq F, \Theta_2(F)\leq \mathbb{1}} |\text{tr}[\delta\rho_- \cdot F]| \right\} \\ &= \frac{\|\delta\rho\|_1}{2}.\end{aligned} \tag{4.50}$$

Therefore, to achieve a hiding strength of 1, one needs orthogonal hiding states.

For an optimal protocol for quantum data hiding it is natural to demand that the ratio of hiding strength to trace norm distance (analysability) is minimal:

$$\gamma_{\text{opt}} = \inf_{\delta\rho} \frac{2 \cdot \|\delta\rho\|_{\text{hide}}}{\|\delta\rho\|_1}, \tag{4.51}$$

where the factor of two appears as a normalization. Hence, orthogonal hiding states can (or at least could) achieve an optimal hiding quality of unity. However, since we are dealing with a finite dimensional Hilbert space, it is clear that both norms, $\|\cdot\|_{\text{hide}}$ and $\|\|_1$, are topologically equivalent. In other words: There exist constants $c_\pm$ such that for all differences $\delta\rho$ we have $\|\delta\rho\|_1 \leq c_+ \cdot \|\delta\rho\|_{\text{hide}}$ and $\|\delta\rho\|_{\text{hide}} \leq c_- \cdot \|\delta\rho\|_1$. The optimal hiding quality γ_{opt} is thus bounded from below by $\frac{1}{c_+} \leq \gamma_{\text{opt}}$. A perfect hiding is thus not possible for finite dimensions. Nevertheless, it is interesting to know the tightest bounds on the optimal hiding quality.

A lower bound on the optimal hiding quality can be obtained using the norm of *complete boundedness* (see [Pau86]) defined on operations:

$$\|T\|_{\mathrm{cb}} = \sup_{1\le d\le\infty} \|T\otimes \mathrm{id}_d\| = \|T\otimes \mathrm{id}_{d'}\|, \tag{4.52}$$

with $T\colon \mathcal{B}(\mathbb{C}^{d'}) \to \mathcal{B}(\mathbb{C}^{d'})$. For the partial transposition $\Theta_2\colon \mathcal{B}(\mathbb{C}^{d}) \to \mathcal{B}(\mathbb{C}^{d})$ the cb-norm gives:

$$\begin{aligned} \|\Theta_2\|_{\mathrm{cb}} &= \|\Theta_2\otimes \mathrm{id}_d\| = \sup_{\|A\|\le 1} \|\Theta_2(A)\| \\ &= \sup_{\substack{\|A\|=1\\ \|\psi\|=1}} |\mathrm{tr}[\Theta_2(A)\cdot|\psi\rangle\langle\psi|]| = \sup_{\substack{\|A\|=1\\ \|\psi\|=1}} |\mathrm{tr}[A\cdot\Theta_2(|\psi\rangle\langle\psi|)]| \\ &= \sup_{\|\psi\|=1} \|\Theta_2(|\psi\rangle\langle\psi|)\|_1. \end{aligned} \tag{4.53}$$

The last variation can be done by making use of the Schmidt decomposition of ψ. It finally leads to

$$\|\Theta_2\|_{\mathrm{cb}} = d. \tag{4.54}$$

Therefore, the set of POVM elements $\{\|A\|, \|\Theta_2(A)\| \le 1\}$ in (4.50) can be restricted to $\|A\| \le \frac{1}{2}$ to get a lower bound on the optimal hiding strength:

$$\begin{aligned} \|\delta\rho\|_{\mathrm{hide}} &= \sup_{0\le A,\Theta_2(A)\le\mathbb{1}} |\mathrm{tr}[\delta\rho\cdot A]| = \sup_{\|A\|,\|\Theta_2(A)\|\le 1} |\mathrm{tr}\left[\delta\rho\cdot\frac{\mathbb{1}+A}{2}\right]| \\ &= \frac{1}{2}\sup_{\|A\|,\|\Theta_2(A)\|\le 1} |\mathrm{tr}[\delta\rho\cdot A]| \ge \frac{1}{2}\sup_{\|A\|\le\frac{1}{2}} |\mathrm{tr}[\delta\rho\cdot A]| \\ &= \frac{1}{4}\sup_{\|A\|\le 1} |\mathrm{tr}[\delta\rho\cdot A]| = \frac{\|\delta\rho\|_1}{4}, \end{aligned} \tag{4.55}$$

and furthermore a lower bound on the optimal hiding quality: $\gamma_{\mathrm{opt}} \ge \frac{1}{2}$.

In order to obtain an upper bound we now turn to one last example of quantum data hiding.

4.3.1 Hiding a bit in a pair of Bell-diagonal qubits

In the early days of quantum information a special basis for two-qubit systems was given strong consideration. It was the so-called Bell basis, a basis consisting of maximally entangled pure states, i.e. states violating Bell's inequality maximally:

$$\begin{aligned} |\Phi_+\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right), & |\Phi_-\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right), \\ |\Psi_+\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right), & |\Psi_-\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right). \end{aligned} \tag{4.56}$$

States that are diagonal in this special basis played a major rôle in early entanglement theory. They can be obtained by averaging over the discrete abelian group (twirling)

$$\{\mathbb{1} \otimes \mathbb{1}, \sigma_x \otimes \sigma_x, \sigma_y \otimes \sigma_y, \sigma_z \otimes \sigma_z\}. \tag{4.57}$$

This group is a discrete subgroup of $\{U \otimes U | U \in \mathcal{U}(2)\}$. It is thus not surprising that the set of Bell-diagonal states contains the Werner-symmetric states. Since the set of (4.57) is a self-dual hermitian operator basis, the Bell-symmetric operators can be written as

$$\mathcal{T}_{\text{Bell}}(A) = \sum_{i=0}^{3} \lambda_i \sigma_i \otimes \sigma_i \tag{4.58}$$

with $\sigma_0 = \mathbb{1}$, $\sigma_1 = \sigma_x$ etc. The coefficients λ_i fix the spectrum of Bell-diagonal operators: $\text{spec}(A) = \{\alpha, \beta, \gamma, \delta\}$ with $\alpha \overset{\text{def}}{=} \lambda_0 - \lambda_1 - \lambda_2 - \lambda_3$, $\beta \overset{\text{def}}{=} \lambda_0 + \lambda_1 + \lambda_2 - \lambda_3$, $\gamma \overset{\text{def}}{=} \lambda_0 + \lambda_1 - \lambda_2 + \lambda_3$, $\delta \overset{\text{def}}{=} \lambda_0 - \lambda_1 + \lambda_2 + \lambda_3$ and similarly of their partial transpose: $\text{spec}(\Theta_2(A)) = \{\alpha', \beta', \gamma', \delta'\}$ with $\alpha' \overset{\text{def}}{=} \lambda_0 + \lambda_1 - \lambda_2 - \lambda_3$, $\beta' \overset{\text{def}}{=} \lambda_0 - \lambda_1 + \lambda_2 - \lambda_3$, $\gamma \overset{\text{def}}{=} \lambda_0 - \lambda_1 - \lambda_2 + \lambda_3$, $\delta \overset{\text{def}}{=} \lambda_0 + \lambda_1 + \lambda_2 + \lambda_3$. With these parameters the locality constraints for Bell-diagonal POVMs read:

$$\begin{aligned} &0 \leq \alpha, \beta, \gamma, \delta \leq 1 \\ &0 \leq x - \alpha, x - \beta, x - \gamma, -x\delta \leq 1 \quad \text{with} \quad x = \frac{1}{2}(\alpha + \beta + \gamma + \delta). \end{aligned} \tag{4.59}$$

Since the group is abelian it is not surprising that the convex set determined by the positivity constraints (inequalities (4.59)) is a polytope. The functional we want to maximize is convex in the POVM so that it suffices to compute the values of the extreme points of the polytope. The extreme points can be calculated by hand or using, for example, the Avis-Fukuda algorithm[57] (see [AF92]). Either way it turns out that there are only eight extremal POVMs A_i:

[57] We used the Mathematica© implementation VertexEnum.m due to K. Fukuda and I. Mizukoshi, available at www.mathsource.com.

i	spec(A_i)	$(\lambda_{i,0},\lambda_{i,1},\lambda_{i,2},\lambda_{i,3})$
1	$(0,0,0,0)$	$(0,0,0,0)$
2	$(0,0,1,1)$	$(\frac{1}{2},0,0,\frac{1}{2})$
3	$(0,1,0,1)$	$(\frac{1}{2},0,\frac{1}{2},0)$
4	$(0,1,1,0)$	$(\frac{1}{2},\frac{1}{2},0,0)$
5	$(1,0,0,1)$	$(\frac{1}{2},-\frac{1}{2},0,0)$
6	$(1,0,1,0)$	$(\frac{1}{2},0,-\frac{1}{2},0)$
7	$(1,1,0,0)$	$(\frac{1}{2},0,0,-\frac{1}{2})$
8	$(1,1,1,1)$	$(1,0,0,0)$

With a Bell-diagonal difference $\delta\rho = \sum_{i=1}^{3} d_i\sigma_i \otimes \sigma_i$ we get for the hiding strength

$$\begin{aligned} \|\delta\rho\|_{\text{hide}} &= \max_{A_i} |\mathrm{tr}[\delta\rho \cdot A_i]| = \max_i |\sum_{j,k} \lambda_{i,j} d_k \mathrm{tr}[\sigma_j\sigma_k]\mathrm{tr}[\sigma_j\sigma_k]| \\ &= 4\max_i |\sum_{j=1}^{3} d_j\lambda_{i,j}| = 2\max_{i=1,2,3} |d_i|. \end{aligned} \tag{4.60}$$

The trace-norm of the difference $\delta\rho$ evaluates to

$$\|\delta\rho\|_1 = |d_1+d_2+d_3| + |d_1+d_2-d_3| + |d_1-d_2+d_3| + |-d_1+d_2+d_3|. \tag{4.61}$$

Without loss of generality we can assume $0 \le d_1 \le d_2 \le d_3$. Now, if $d_3 \ge d_1 + d_2$ holds, we have that $\|\delta\rho\|_1 = 4d_3$. Otherwise we have $\|\delta\rho\|_1 = 2(d_1 + d_2 + d_3) \le 6d_3$. For the optimal hiding quality for Bell-diagonal states we finally obtain

$$\gamma_{\text{Bell}} = \inf_{\delta\rho = \mathcal{T}_{\text{Bell}}(\delta\rho)} \frac{2\|\delta\rho\|_{\text{hide}}}{\|\delta\rho\|_1} \ge \frac{2\cdot 2\cdot d_3}{6\cdot d_3} = \frac{2}{3}. \tag{4.62}$$

This value is achieved already for the Werner states used in subsection 4.1.2. Since the Bell-diagonal states build a larger state space than the Werner states this optimum is not necessarily unique any more. In fact, any difference with $d_i \in \{-\frac{1}{3}, \frac{1}{3}\}$ turns out to be optimal.

4.3.2 Beyond symmetry

So far we have obtained the bounds $\frac{1}{2} \le \gamma_{\text{opt}} \le \frac{2}{3}$ by making use of special symmetric two-qubit states. However, it may well be that the optimal states for quantum data hiding are not symmetric. Fortunately, there are two more observations that help to extend the obtained results to a larger set of two-qubit states: Firstly, the states need not be symmetric. It suffices to have a Bell-diagonal difference $\delta\rho$ to apply the above result. Secondly, the optimal hiding quality is the quotient of two unitarily invariant norms. Therefore, the result on Bell-diagonal states extends naturally to those states that are Bell-diagonal up to local unitary rotations. In this subsection we will show that this set of states is quite large. Unfortunately, it will not enable us to prove the following conjecture:

Conjecture 4.3.1: Werner states are optimal for quantum data hiding, i.e. $\gamma_{\text{opt}} = \frac{2}{3}$.

To see which differences are Bell-diagonal up to local unitary rotations we make use of the self-duality of the operator basis $\{\sigma_i \otimes \sigma_j\}$. Any operator $A \in \mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ can be represented by its coefficient matrix with respect to this operator basis:

$$\langle i|R_A j\rangle \overset{\text{def}}{=} \operatorname{tr}[A\sigma_i \otimes \sigma_j]. \tag{4.63}$$

This R-matrix bears a few interesting properties: it is diagonal for Bell-diagonal operators, it is real-valued for selfadjoint operators, the partial transposition acts by inverting the sign of the third column, local unitary rotations $U \otimes V$ act as orthogonal rotations:

$$R_{(U\otimes V)A(U^*\otimes V^*)} = O_U \cdot R_A \cdot O_V, \tag{4.64}$$

with

$$O_U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & u_{11} & u_{12} & u_{13} \\ 0 & u_{21} & u_{22} & u_{23} \\ 0 & u_{31} & u_{32} & u_{33} \end{pmatrix}, \quad \text{and} \quad O_V = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & v_{11} & v_{12} & v_{13} \\ 0 & v_{21} & v_{22} & v_{23} \\ 0 & v_{31} & v_{32} & v_{33} \end{pmatrix}. \tag{4.65}$$

The coefficients of the reduced states can be readily read off the R-matrix. The first row contains the coefficients of Bob's reduced state, the first column contains those of Alice. A Bell-diagonal difference $\delta\rho$ corresponds to an R-matrix of the form

$$R_{\delta\rho_{\text{Bell}}} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & d_1 & 0 & 0 \\ 0 & 0 & d_2 & 0 \\ 0 & 0 & 0 & d_3 \end{pmatrix}. \tag{4.66}$$

On the other hand, due to the existence of the singular value decomposition (see [Bha97]) we know that any real-valued matrix of the form

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & a_{11} & a_{12} & a_{13} \\ 0 & a_{21} & a_{22} & a_{23} \\ 0 & a_{31} & a_{32} & a_{33} \end{pmatrix} \tag{4.67}$$

can be decomposed into two orthogonal rotations and a diagonal matrix of the form (4.66). Therefore, the result on Bell-diagonal states extends to all those state pairs that have identical restrictions, i.e. $\rho_0^A = \rho_0^A$ and $\rho_0^B = \rho_1^B$.

This observation is very interesting since it is intuitive that states that differ already at the level of the reduced states cannot lead to a better hiding quality. Furthermore the conjecture 4.3.1 is also in line with the observations of section 2.4, where we had seen that the symmetric overall state minimizes the information difference to the reduced states. Nevertheless, it seems quite intuitive we were unfortunately not able to prove conjecture 4.3.1 yet. Even sophisticated numerical investigations (see [But02]) were not able to disprove it.

Chapter 5

Shared Fidelity

> **Marriage** – We affirm the sanctity of the marriage covenant that is expressed in love, mutual support, personal commitment, and *shared fidelity* between a man and a woman.
>
> (The United Methodist Church)

In section 3.3.1 we encountered another purely quantum feature: Quantum systems can be *stressed* even without closed loops. In contrast to the classical situation, a common tripartite extension of two bipartite quantum systems having a common reduction may fail to exist. In particular, one party, say Alice, cannot be maximally entangled with Bob *and* Charly. In fact, if she were, she could teleport an unknown state to both of her friends and establish, therefore, a perfect quantum cloning machine, which is, however, prohibited by the linearity of quantum mechanics [WZ82].

However, we can ask for the maximal bipartite entanglement Alice can simultaneously share with several other parties (see [CKW00] and [DW01]). In this final chapter we address the question how one party could maximize its bipartite entanglement with N other parties along the lines between the various parties. This can be done in several different ways. First we have to fix a functional E which quantifies bipartite entanglement. Then we may either maximize the entanglement

$\mathcal{E}_{min}$ along the worst line

$$\mathcal{E}_{min} = \sup_{\rho} \min_{\{i,j\}} E(\rho_{ij}) \tag{5.1}$$

or optimize the average entanglement $\mathcal{E}_{av}$:

$$\mathcal{E}_{av} = \sup_{\rho} \frac{1}{\#\text{lines}} \sum_{i} E(\rho_{ij}), \tag{5.2}$$

where ρ is the density matrix of the whole system and ρ_{ij} denotes its bipartite reduction with respect to the systems i and j.

We will in the following choose E to be the *fully entangled fraction*

$$E(\rho_{ij}) = \sup_{U \in U(d)} \langle \psi_+^U | \rho_{ij} | \psi_+^U \rangle, \tag{5.3}$$

that is the maximal *fidelity* between ρ_{ij} and a maximally entangled state $|\psi_+^U\rangle = (\mathbb{1} \otimes U)|\psi_+\rangle$, with $|\psi_+\rangle = \frac{1}{\sqrt{d}} \sum_j |jj\rangle$. This choice for E makes the stated problems feasible since $\mathcal{E}_{av}$ reduces to an operator norm and in this case turns out to be equal to $\mathcal{E}_{min}$. However, we have to note that the fully entangled fraction is no entanglement monotone since it can increase under local operations and classical communication.

We will start by studying the optimal way to share fidelity among three parties and by proving that the optimum is attained for the choice of standard local bases for the reference states and equal weights in averaging. The second part will show the intimate relation between shared fidelity and cloning fidelity. In the last part of this chapter we investigate the optimal way of sharing fidelity among maximally connected clusters of parties (web-states).

5.1 Optimal fidelity sharing in tripartite systems

Even for tripartite systems there are restrictions on the shared fidelity. In fact, one can achieve that the parties AB and AC share a maximally entangled reduced state. But then it is known that BC cannot share a maximally entangled state. In this case the system is *frustrated* (see for example [Wer94]). These limitations will be the object of this section.

When talking about the fidelity of one single bipartite reduction it is clear that we can choose the local bases in such a way to measure the fidelity with respect to a maximally entangled state in its standard form $|\Psi_+\rangle = \frac{1}{\sqrt{d}}\sum_{i=1}^{d}|ii\rangle$. However, if we are interested in the optimal average shared fidelity, we have to optimize over all three reduced states at the same time. The freedom to choose the local bases freely is then restricted to two subsystems. As a general set of reference states we will therefore use $|\Psi_+\rangle\langle\Psi_+|$ for the reductions on BC and AC and $(\mathbb{1}\otimes U)|\Psi_+\rangle\langle\Psi_+|(\mathbb{1}\otimes U^*)$ with some unitary operator U for AB.

Furthermore it is still open which way to average may be best. We will therefore optimize over all convex combinations $\{\lambda_1, \lambda_2, \lambda_3\}$, too. In these terms the optimal average shared fidelity we are interested in is

$$f_{\max} = \sup_{\rho, U, \{\lambda_1,\lambda_2,\lambda_3\}} \mathrm{tr}[\rho F] = \sup_{U,\{\lambda_1,\lambda_2,\lambda_3\}} \|F\|, \tag{5.4}$$

with the fidelity operator

$$\begin{aligned} F = \lambda_1 \mathbb{1}_1 \otimes |\Psi_+\rangle\langle\Psi_+|_{23} + \lambda_2 \mathbb{1}_2 \otimes |\Psi_+\rangle\langle\Psi_+|_{31} \\ + \lambda_3 \mathbb{1}_3 \otimes \{(\mathbb{1}\otimes U)|\Psi_+\rangle\langle\Psi_+|(\mathbb{1}\otimes U^*)\}_{12}\,. \end{aligned} \tag{5.5}$$

To keep the notation compact we write the tensor factor the operators act on as an index and refrain from writing out correctly the reshuffled tensor factors.

The main result of this section is the following

Lemma 5.1.1: The maximal shared fidelity is attained when all local bases are equal to the standard computational basis and all weights are equal leading to $f_{\max} = \frac{1}{3}(1 + \frac{1}{d})$.

Proof. Instead of computing the norm (5.4) we begin by describing the manifold of possible triples

$$\vec{f} = \begin{pmatrix} \mathrm{tr}[\rho \mathbb{1}_1 \otimes |\Psi_+\rangle\langle\Psi_+|_{23}] \\ \mathrm{tr}[\rho \mathbb{1}_2 \otimes |\Psi_+\rangle\langle\Psi_+|_{31}] \\ \mathrm{tr}[\rho \mathbb{1}_3 \otimes \{(\mathbb{1}\otimes U)|\Psi_+\rangle\langle\Psi_+|(\mathbb{1}\otimes U^*)\}_{12}]) \end{pmatrix} \tag{5.6}$$

of fidelities that are commensurable for a chosen unitary operator U. The gradient of the plane which is given by the maximal average fidelity $f_{\max} = \lambda_1 f_1 + \lambda_2 f_2 + \lambda_3 f_3$ points in direction of the coefficient vector $\vec{\lambda} = (\lambda_1, \lambda_2, \lambda_3)$. For the variation of (5.4) we will therefore first optimize the direction in order to maximize the fidelity and perform the variation over the unitary operators afterwards.

The manifold we want to characterize is given by

$$K = \{x \in \mathbb{R}^3 | x_i = \mathrm{tr}[\rho P_i]\}, \tag{5.7}$$

where the P_i are the projections $P_1 = \mathbb{1}_1 \otimes |\Psi_+\rangle\langle\Psi_+|_{23}$, $P_2 = \mathbb{1}_2 \otimes |\Psi_+\rangle\langle\Psi_+|_{31}$ and $P_3 = \mathbb{1}_3 \otimes \{(\mathbb{1} \otimes U)|\Psi_+\rangle\langle\Psi_+|(\mathbb{1} \otimes U^*)\}_{12}$. Since a direct characterization is difficult we first characterize its polar (see [Roc72]):

$$\begin{aligned} K^\circ &\overset{\text{def}}{=} \{\xi \in \mathbb{R}^3 | \forall \vec{x} \in K \colon \vec{\xi} \cdot \vec{x} \leq 1\} = \{\vec{\xi} | \forall \rho \colon \sum_i \xi_i \mathrm{tr}[\rho P_i] \leq 1\} \\ &= \{\vec{\xi} | \sum_i \xi_i P_i \leq \mathbb{1}\} \end{aligned} \tag{5.8}$$

Obviously the fidelity operator is the sum of positive operators and thus itself positive. Therefore there must be operators V such that $F = VV^*$. Furthermore, any operator has the same norm as its Gram operator, i.e.

$$\|F\| = \|VV^*\| = \|V^*V\|. \tag{5.9}$$

We use $V \colon \mathbb{C}^d \oplus \mathbb{C}^d \oplus \mathbb{C}^d \to \mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d$ with

$$\begin{aligned} V(\oplus_i \varphi_i) = \sqrt{\lambda_1}|\varphi_1\rangle_1 \otimes |\Psi_+\rangle_{23} + \sqrt{\lambda_2}|\varphi_2\rangle_2 \otimes |\Psi_+\rangle_{31} + \\ \sqrt{\lambda_3}|\varphi_3\rangle_2 \otimes |\Psi_+\rangle_{12}. \end{aligned} \tag{5.10}$$

With this operator we can rewrite the polar as:

$$\begin{aligned} K^\circ &= \{\vec{\xi} | \forall \Phi = V(\oplus_i \varphi_i) \colon \langle \Phi | \sum_i \xi_i P_i \Phi \rangle \leq \langle \Phi | \Phi \rangle\} \\ &= \{\vec{\xi} | (W - W \mathrm{diag}[\xi] W) \geq \mathbf{0}\} = \{\vec{\xi} | \mathrm{diag}[\xi] \leq W^{-1}\} \end{aligned} \tag{5.11}$$

with the Gram operator $W = V^*V$. It can be seen as a 3×3 matrix of $d \times d$-blocks given by $W_{ij} = \langle V(\varphi_i) | V(\varphi_j) \rangle$ leading to

$$W = \begin{pmatrix} \lambda_1 \mathbb{1} & \frac{\sqrt{\lambda_1 \lambda_2}}{d} \mathbb{1} & \frac{\sqrt{\lambda_1 \lambda_3}}{d} U^T \\ \frac{\sqrt{\lambda_1 \lambda_2}}{d} \mathbb{1} & \lambda_2 \mathbb{1} & \frac{\sqrt{\lambda_2 \lambda_3}}{d} U \\ \frac{\sqrt{\lambda_1 \lambda_3}}{d} \overline{U} & \frac{\sqrt{\lambda_2 \lambda_3}}{d} U^* & \lambda_3 \mathbb{1} \end{pmatrix}. \tag{5.12}$$

Expression (5.11) for the polar can be simplified by scaling the ξ_i. In fact, we can write $W = \Lambda W' \Lambda$ with $\Lambda^* = \Lambda = \mathrm{diag}[(\sqrt{\lambda_1}, \sqrt{\lambda_2}, \sqrt{\lambda_3})]$ and for the polar:

$$K^\circ = \{\vec{\xi} | \Lambda \cdot \mathrm{diag}[\xi] \cdot \Lambda \leq W'^{-1}\} = \{\vec{\xi} | \mathrm{diag}[\lambda_i \xi_i] \leq W'^{-1}\} \tag{5.13}$$

with W' being the matrix

$$W' = \begin{pmatrix} \mathbb{1} & \frac{1}{d}\mathbb{1} & \frac{1}{d}U^T \\ \frac{1}{d}\mathbb{1} & \mathbb{1} & \frac{1}{d}U \\ \frac{1}{d}\overline{U} & \frac{1}{d}U^* & \mathbb{1} \end{pmatrix}. \tag{5.14}$$

Applying the unitary transformation $\mathbb{1} \oplus \mathbb{1} \oplus U^T$ to W' we get

$$\tilde{W} = \begin{pmatrix} \mathbb{1} & \frac{1}{d}\mathbb{1} & \frac{1}{d}\mathbb{1} \\ \frac{1}{d}\mathbb{1} & \mathbb{1} & \frac{1}{d}U\overline{U} \\ \frac{1}{d}\mathbb{1} & \frac{1}{d}U^T U^* & \mathbb{1} \end{pmatrix}. \tag{5.15}$$

As these blocks commute, they can be diagonalized independently:

$$\begin{pmatrix} \mathbb{1} & \frac{1}{d}\mathbb{1} & \frac{1}{d}\mathbb{1} \\ \frac{1}{d}\mathbb{1} & \mathbb{1} & \frac{1}{d}U\overline{U} \\ \frac{1}{d}\mathbb{1} & \frac{1}{d}U^T U^* & \mathbb{1} \end{pmatrix} \to \begin{pmatrix} \mathbb{1} & \frac{1}{d}\mathbb{1} & \frac{1}{d}\mathbb{1} \\ \frac{1}{d}\mathbb{1} & \mathbb{1} & \frac{1}{d}\tilde{U} \\ \frac{1}{d}\mathbb{1} & \frac{1}{d}\tilde{U}^* & \mathbb{1} \end{pmatrix} \tag{5.16}$$

with some diagonal unitary operator $\tilde{U}$. Furthermore, a matrix with purely diagonal blocks can be written as the direct sum of matrices. In our case we have $\tilde{W} = \oplus_j w_j$ with

$$\begin{pmatrix} \mathbb{1} & \frac{1}{d}\mathbb{1} & \frac{1}{d}\mathbb{1} \\ \frac{1}{d}\mathbb{1} & \mathbb{1} & \frac{1}{d}\tilde{U} \\ \frac{1}{d}\mathbb{1} & \frac{1}{d}\tilde{U}^* & \mathbb{1} \end{pmatrix} = \bigoplus_{j=1}^{d} \begin{pmatrix} 1 & \frac{1}{d} & \frac{1}{d} \\ \frac{1}{d} & 1 & \frac{1}{d}e^{i\alpha_j} \\ \frac{1}{d} & \frac{1}{d}e^{-i\alpha_j} & 1 \end{pmatrix}, \tag{5.17}$$

where the $e^{i\alpha_j}$ are the eigenvalues of the diagonal unitary operator $\tilde{U}$. For the polar we get:

$$K^\circ = \{\vec{\xi} | \mathrm{diag}[\lambda_i \xi_i] \leq \tilde{W}^{-1}\} = \{\vec{\xi} | \forall j \colon \mathrm{diag}[\lambda_i \xi_i] \leq w_j^{-1}\}. \tag{5.18}$$

Positivity of the matrix $w_j^{-1} - \mathrm{diag}[\lambda_i \xi_i]$ is equivalent to the inequalities

$$\begin{aligned} 0 &\leq \frac{1}{\det[w_j]}(1 - \frac{1}{d^2}) - \tilde{\xi}_i, \\ 0 &\leq d^3(1-\tilde{\xi}_i)(1-\tilde{\xi}_k) + 2\cos(\alpha_j)\tilde{\xi}_i\tilde{\xi}_k + d(\tilde{\xi}_i + \tilde{\xi}_k - 3\tilde{\xi}_i\tilde{\xi}_k), \\ 0 &\leq d^3(1-\tilde{\xi}_1)(1-\tilde{\xi}_2)(1-\tilde{\xi}_3) - 2\cos(\alpha_j)\tilde{\xi}_1\tilde{\xi}_2\tilde{\xi}_3 \\ &\qquad - d(\tilde{\xi}_1\tilde{\xi}_2 + \tilde{\xi}_2\tilde{\xi}_3 + \tilde{\xi}_3\tilde{\xi}_1 - 3\tilde{\xi}_1\tilde{\xi}_2\tilde{\xi}_3), \end{aligned} \tag{5.19}$$

with $\tilde{\xi}_i \overset{\text{def}}{=} \lambda_i \xi_i$. The sought-after set of commensurable fidelity triplets is given by those vectors pointing from the origin to the surface given by the inequalities of (5.19) and can be plotted for some choice of d and α_j (see figure 5.1). It describes a convex shape with a trigonal rotational symmetry around the diagonal in $(1,1,1)$-direction proving that the optimum will be found in that direction. As we pointed out already, the direction of the optimal vector is that of the gradient and is given by $(\lambda_1, \lambda_2, \lambda_3)$. Therefore, the optimum lies at $\lambda_1 = \lambda_2 = \lambda_3$.

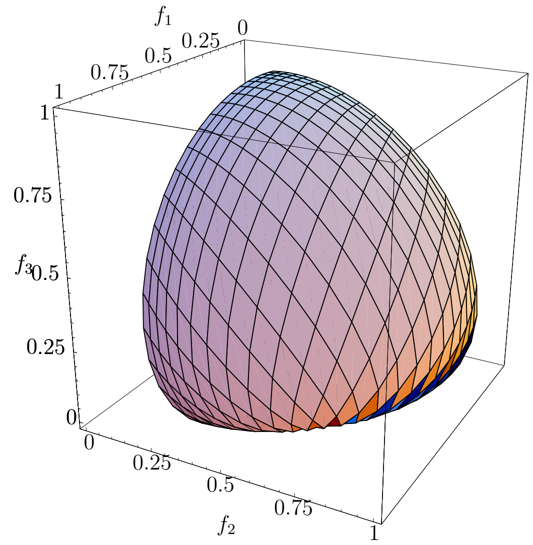


Figure 5.1: The surface of commensurable triples of single fidelities for $d = 2$ and $\alpha = 0$.

To end our computation of the norm of W we can restrict ourselves to one single block and compute its eigenvalues analytically:

$$\operatorname{spec}\left[\frac{1}{3}\begin{pmatrix} 1 & \frac{1}{d} & \frac{1}{d} \\ \frac{1}{d} & 1 & \frac{1}{d}e^{i\alpha} \\ \frac{1}{d} & \frac{1}{d}e^{-i\alpha} & 1 \end{pmatrix}\right] = \frac{1}{3}\left\{1 + \frac{2\cos(\frac{\alpha}{3})}{d}, 1 - \frac{\cos(\frac{\alpha}{3}) \pm \sqrt{3}\sin(\frac{\alpha}{3})}{d}\right\}. \tag{5.20}$$

Optimizing over the phase α leads then to $\alpha = 0$ and $f_{\max} = \frac{1}{3}(1+\frac{2}{d})$. ■

The final result tells us that the optimal average shared fidelity can be achieved by using standard local bases and by weighing all single fidelities equally. This leads then to an optimum of $f_{\max} = \frac{1}{3}(1 + \frac{2}{d})$ attained for any state of the form

$$V(\varphi \oplus \varphi \oplus \varphi) = \frac{1}{\sqrt{3}}\left(|\varphi\rangle_1 \otimes |\Psi_+\rangle_{23} + |\varphi\rangle_2 \otimes |\Psi_+\rangle_{31} + |\varphi\rangle_2 \otimes |\Psi_+\rangle_{12}\right), \tag{5.21}$$

with some $\varphi \in \mathbb{C}^d$. Once these two assumptions are proved to be valid, one can calculate the optimal value and the optimal state much easier via the operator norm in (5.4) and (5.9). In fact, under these assumptions we can optimize the shared fidelity even for more complex configurations than tripartite systems as we will see in the following two sections.

5.2 From shared fidelity to quantum telecloning

One configuration which is of special interest is the $1 : N$-star configuration. It is closely connected to the $1 : N$-cloner and will lead us to a state which implements an optimal $1 : N$-telecloner. In this special configuration one party is singled out since all other parties are connected to this one and to this one only (see the starducks configuration in figure 5.2).

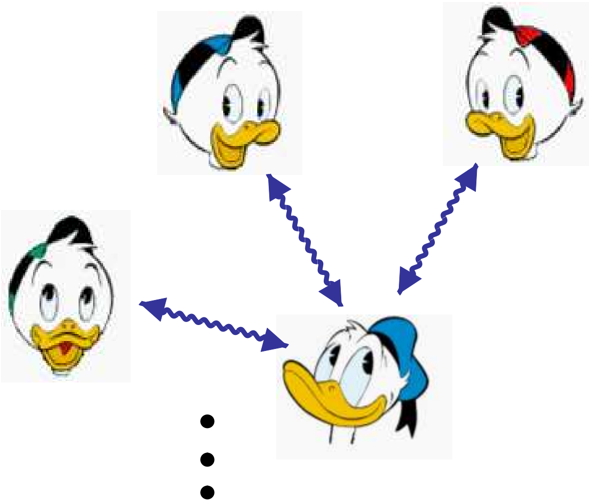


Figure 5.2: The starducks configuration (not to be confused with Starbucks®). [The ducks are copyright of Disney Corporation.]

Now assuming that standard bases and equal weights have been chosen, the corresponding fidelity operator is

$$F_{1:\mathrm{N}} = \frac{1}{N} \sum_{i=2}^{N+1} |\Psi_+\rangle\langle\Psi_+|_{1i} \otimes \mathbb{1}_{N+1/\{1,i\}}. \tag{5.22}$$

Similarly to (5.10) we take the operator $V \colon \bigoplus_{i=1}^{N+1} (\mathbb{C}^d)^{\otimes(N-1)} \to \bigotimes_{i=1}^{N+1} \mathbb{C}^d$ to be

$$V(\bigoplus_{i=1}^{N+1} |\varphi_i\rangle) = \sum_{i=2}^{N+1} |\psi_+\rangle_{1i} \otimes |\varphi_i\rangle, \qquad \text{with } |\varphi_i\rangle \in (\mathbb{C}^d)^{\otimes(N-1)}. \tag{5.23}$$

In order to optimize the fidelity we can use (5.9) and evaluate the supremum of $\|V(\bigoplus_{i=2}^{N+1} \varphi_i)\|^2$ over the set of vectors satisfying the normalization condition $\sum_{i=2}^{N+1} \|\varphi_i\|^2 = 1$. For this we will make use of the identity

$|\psi_+\rangle_{2j} \otimes |\varphi_i\rangle \equiv \mathbb{F}_{2j}\left(|\psi_+\rangle_{12} \otimes |\varphi_i\rangle\right)$ with the Flip operators $\mathbb{F}_{ij}$ interchanging the i-th and j-th tensor factors of vectors. Then we can compute:

$$\begin{aligned}
\|V^*V\| &= \sup \sum_{i,j=2}^{N+1} \mathrm{tr}[(|\psi_+\rangle\langle\psi_+|_{12} \otimes |\varphi_j\rangle\langle\varphi_i|)\, \mathbb{F}_{2i}\mathbb{F}_{2j}] \\
&\overset{(*)}{=} \frac{1}{d} \sup \sum_{i,j=2}^{N+1} \mathrm{tr}[(\mathbb{1}_2 \otimes |\varphi_j\rangle\langle\varphi_i|)\, \mathbb{F}_{2i}\mathbb{F}_{2j}] \\
&= 1 + \frac{1}{d} \sup \left[\sum_{k=3}^{N+1} 2\Re(\langle\varphi_2|\varphi_k\rangle) + \sum_{i\neq j=3}^{N+1} \langle\varphi_i|\mathbb{F}_{ij}\varphi_j\rangle \right] \\
&\leq 1 + \frac{1}{d} \sup \sum_{i\neq j=2}^{N+1} \|\varphi_i\|\|\varphi_j\|,
\end{aligned} \tag{5.24}$$

where we traced out the first tensor factor in $(*)$ and made use of the "magic formula" for flip operators $\mathrm{tr}[(A \otimes B)\mathbb{F}] = \mathrm{tr}[AB]$. This variational problem is again symmetric under interchanging the labels so that one can see (or compute by using Lagrangian multipliers) that the maximum will be attained at $\|\varphi_i\| = \|\varphi_j\|$. In fact, the inequality turns into an equality, if the optimal states satisfy $|\varphi_k\rangle = |\varphi_2\rangle$ and $|\varphi_i\rangle = \mathbb{F}_{i,j}|\varphi_j\rangle$. Hence, a state is optimal if and only if it corresponds to vectors $|\varphi_i\rangle = |\varphi\rangle \in \mathbb{C}^{d(N-1)}$, which are totally symmetric with respect to a permutation of the $(N-1)$ tensor factors. Furthermore, if $\varphi \in P_{\mathrm{Bose}}(\mathbb{C}^d)^{\otimes(N-1)}$ we obtain the optimal value $f_{\max} = \frac{1}{N}\left(1 + \frac{N-1}{d}\right)$ for any state of the form

$$|\Phi_\varphi\rangle = \frac{1}{\sqrt{\mathrm{f}_{\max}}} \sum_{i=2}^{N+1} |\psi_+\rangle_{1i} \otimes |\varphi\rangle \qquad \text{and any } \varphi \in P_{\mathrm{Bose}}(\mathbb{C}^d)^{\otimes(N-1)}. \tag{5.25}$$

As we will see in the following subsections all these states implement an optimal $1 : N$-telecloner.

5.2.1 Cloning via teleportation

In this subsection we resume the idea of cloning a state via teleportation presented in [MJPV99]. To make N clones out of one original pure state we will teleport the original to N distant parties that will receive one clone each.

The tool we need for this purpose is the duality between channels and states as introduced in [Jam72] (see also subsection 1.1.3). Consider a channel $T\colon \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H}^{\otimes N})$, which can be interpreted as a 1 to

N cloner. Then T corresponds to a state τ on $\mathcal{H}^{\otimes(N+1)}$ and vice versa via the relations:

$$\tau = (\mathbb{1} \otimes T)(|\psi_+\rangle\langle\psi_+|), \quad \text{and} \quad \mathrm{tr}\left[\tau \bigotimes_{i=1}^{N+1} A_i\right] = \frac{1}{d}\mathrm{tr}\left[T(A_1^T) \bigotimes_{i=2}^{N+1} A_i\right] \qquad (5.26)$$

where the matrix transposition is taken in the basis corresponding to the maximally entangled state $|\psi_+\rangle$. These equations lead to

$$\mathrm{tr}\left[\big(A_0 \otimes \tau\big)|\psi_+\rangle\langle\psi_+|_{01} \otimes \bigotimes_{k=2}^{N+1} A_k\right] = \frac{1}{d^2}\mathrm{tr}\left[T(A_0) \bigotimes_{k=2}^{N+1} A_k\right]. \qquad (5.27)$$

This tells us now how to implement the cloner T *probabilistically* given the state τ: Donald, who is assumed to posses the first particle of τ and the state to be cloned (acting on system '0'), measures in a basis containing $|\psi_+\rangle$. Whenever the outcome of his measurement corresponds to $|\psi_+\rangle$, he tells his N 'nephews' that they have succeeded[58].

However, if the state corresponding to such a $1 : N$-cloner commutes with a group of local unitaries $[\tau, \overline{U} \otimes U^{\otimes N}] = 0$ and is thus an element of the well-known "chip" algebra of chapter 2, we obtain a trace preserving implementation if Donald measures in a maximally entangled basis

$$|\psi_+\rangle_{ij} = \big(U_{ij} \otimes \mathbb{1}\big)|\psi_+\rangle, \qquad (5.28)$$

where the U_{ij}, $i, j = 1, \ldots d$ form a basis of unitaries (see [Wer01a]), and the 'nephews' undo the unitary operations corresponding to the respective measurement result. In this case the cloner fulfills

$$T(UAU^*) = U^{\otimes N} T(A) U^{*\otimes N} \qquad \forall U \in U(d), \qquad (5.29)$$

i.e. it does not prefer any original state and is thus a *covariant* cloner. Then all the unitaries we have to insert in the l.h.s. of (5.27) cancel and we have a trace preserving implementation of the channel T by a standard teleportation scheme.

By now, we see that the states $|\Phi_\varphi\rangle$ which share the fidelity in an optimal way can be used as $1 : N$-telecloner. In the upcoming subsection we will show that the telecloner thus obtained is already an optimal cloner.

[58] Note that this works analogously when cloning M copies of the original state to N parties.

5.2.2 Optimal telecloning

In order to prove optimality we have to relate the optimal fidelity sharing states $|\Phi_\varphi\rangle$ with the telecloning states τ. To this end we first symmetrize the state $|\Phi_\varphi\rangle$:

$$\begin{aligned}\tau_\varphi &\overset{\text{def}}{=} \int dU(\overline{U} \otimes U^{\otimes N})|\Phi_\varphi\rangle\langle\Phi_\varphi|(\overline{U} \otimes U^{\otimes N})^* \\ &= \int dU|\Phi_{\varphi(U)}\rangle\langle\Phi_{\varphi(U)}|,\end{aligned} \tag{5.30}$$

where $\varphi(U) = U^{\otimes(N-1)}\varphi$ and the integration is an averaging over unitaries with respect to the Haar measure. Note that τ_φ again leads to the optimal value for the shared fidelity $f_{\max}$ as it has support in the subspace spanned by the vectors $|\Phi_\varphi\rangle$. The averaging can be seen as applying an additional local unitary to each of the N outputs in the teleportation protocol.

Before stating what we intend by *optimal* we have to define the *figure of merit* we want to optimize. There are different figures of merit that compare the outputs of a cloning machine with its input. Fortunately, for the cloning of pure states they all lead to the same optimal universal cloner, which is mathematically given by tensoring the input with a sufficiently large multiple of the identity and then projecting onto the Bose subspace (see [Wer98, KW99]).

In the following we will use the *cloning fidelity*

$$\mathcal{F} \overset{\text{def}}{=} \inf_{\|\psi\|=1} \operatorname{tr}\left[T\left(|\psi\rangle\langle\psi|\right)|\psi\rangle\langle\psi|^{\otimes N}\right] \tag{5.31}$$

in order to test the quality of the output. The symmetry of τ_φ, i.e. the covariance property of the respective channel T, ensures that the trace in (5.31) does not depend on ψ. Hence, we can drop the infimum and choose ψ to be real in the distinguished basis. Using (5.26) we have

$$\begin{aligned}\mathcal{F} = d\operatorname{tr}\left[\tau_\varphi(|\psi\rangle\langle\psi|)^{\otimes(N+1)}\right] &= d\int dU|\langle\Phi_{\varphi(U)}|\psi^{\otimes(N+1)}\rangle|^2 \\ = c^2N^2\int dU|\langle\varphi|(U\psi)^{\otimes(N-1)}\rangle|^2 &= c^2N^2\langle\varphi|\sigma|\varphi\rangle,\end{aligned} \tag{5.32}$$

with $\sigma \overset{\text{def}}{=} \int dU\left(U|\psi\rangle\langle\psi|U^*\right)^{\otimes(N-1)}$.

Obviously, σ is a multipartite Werner state (see chapter 2) and therefore commutes with the Bose projection P_{Bose}, i.e. it is supported by the Bose subspace $P_{\text{Bose}}\mathcal{H}^{\otimes(N-1)}$ and commutes with all unitaries of the form $U^{\otimes(N-1)}$. The latter, however, act irreducibly on the symmetric subspace, which means that σ itself has to be a multiple of the projector P_{Bose} onto the Bose subspace. Since $\text{tr}[\sigma] = 1$, the missing factor is just the dimension $\dim_+[N-1, d]$ of the symmetric subspace (for $N-1$ tensor factors each of dimension d) and we have

$$\mathcal{F} = \frac{c^2 N^2}{\dim_+[N-1, d]} \langle\varphi|P_{\text{Bose}}|\varphi\rangle = \frac{d}{\dim_+[N, d]} \langle\varphi|P_{\text{Bose}}|\varphi\rangle, \tag{5.33}$$

where $\dim_+[M, d] = \binom{d+M-1}{M}$.

Furthermore, if φ lies in the Bose subspace and therefore leads to the optimal value for $f_{\max}$, the fidelity in (5.33) is, in fact, the optimal universal cloning fidelity derived in [Wer98].

5.3 Shared fidelity for entangled webs

As our last application of symmetric states we study the case of optimal fidelity sharing between maximally connected parties (complete graphs). Such states may be of interest since the overall state is robustly entangled against disposal of particles as described in [Dür01]. It is intuitive that due to the high number of connections the optimization should be more difficult than in the previous cases. However, maximally connected graphs (webs) have a high symmetry which we will exploit for the optimization.

The fidelity operator testing the average fidelity for maximally connected parties is

$$F = \sum_{i,j=1}^{N} \mathbb{1}_{N/\{i,j\}} \otimes |\psi_+\rangle\langle\psi_+|_{ij}. \tag{5.34}$$

Again the computation of its norm via the Gram operator (5.9) is quite cumbersome. Therefore we will exploit the fact that the fidelity operator is nonnegative, i.e. all entries of the matrix F are nonnegative ($F_{ij} \geq 0$). This enables us to make use of results on nonnegative matrices like the Perron-Frobenius Theorem (see [HJ95]) for proving:

Lemma 5.3.1: The maximal average fidelity for a maximally connected set of N parties is:

for even N: $f_{\max}^{\text{even}} = \frac{1}{N-1}(1 + \frac{N-2}{d})$ and is attained for the state

$$|\psi_{\text{even}}\rangle = P_{\text{Bose}}\big(|\Psi_+\rangle_{12} \otimes \cdots \otimes |\Psi_+\rangle_{N-1,N}\big).$$

for odd N: $f_{\max}^{\text{odd}} = \frac{1}{N}(1+\frac{N-1}{d})$ and is attained for any state

$$|\psi_{\text{odd}}\rangle = P_{\text{Bose}}(|\Psi_+\rangle_{12} \otimes \cdots \otimes |\Psi_+\rangle_{N-2,N-1} \otimes |i\rangle_N),$$

with $i \in \{1,\ldots,d\}$.

That is, the larger the number of parties, the smaller the optimal shared fidelity between pairs of parties becomes. This result is in line with [KBI00]. However, before proving this lemma we resume those results on nonnegative matrices we will need (see chapters 6 and 8 of [HJ95] and [FHW79]). The entries of the matrix $F \in \mathcal{B}(\mathbb{C}^{d\otimes N})$ are labelled by N-tuples $(i_1, i_2, \ldots, i_N)$. Two such tuples $(i_1, i_2, \ldots, i_N)$ and $(j_1, j_2, \ldots, j_N)$ are said to be *connected* by F if the corresponding matrix element does not vanish: $F_{\vec{i},\vec{j}} \overset{\text{def}}{=} \langle i_1, i_2, \ldots, i_N|F|j_1, j_2, \ldots, j_N\rangle \neq 0$ or if there is a connecting *path* between them: $F_{\vec{i},\vec{z}}F_{\vec{z},\vec{k}}\cdots F_{\vec{y},\vec{j}} \neq 0$. The entries of F can therefore be grouped into maximally connected subsets[59]. These connected components are called Perron-Frobenius blocks. Each such block contains only positive entries so that we can apply Perron's Theorem which states that any positive matrix (i.e. having positive entries) has a unique maximal eigenvalue with a corresponding eigenvector with purely positive entries (see Theorem 8.2.11 of [HJ95]).

Proof. In order to characterize the Perron-Frobenius blocks of F we start by describing its connected components by looking at the single summands $P_{ij} \overset{\text{def}}{=} \mathbb{1}_{N/\{i,j\}} \otimes |\psi_+\rangle\langle\psi_+|_{ij}$ of F. Now, if all entries of the tuples $(i_1, i_2, \ldots, i_N)$ and $(j_1, j_2, \ldots, j_N)$ are different we have that $\langle(i_1, i_2, \ldots, i_N)|F|(j_1, j_2, \ldots, j_N)\rangle = 0$. Therefore, for two such tuples to be connected there must be at least two identical entries in each tuple, namely at the positions i and j. Denoting by $\sim$ the relation "connected to" we have

$$\begin{aligned}(1,1,\alpha,\beta,\text{rest}) \sim (\alpha,\alpha,\alpha,\beta,\text{rest}) &\sim (\beta,\alpha,\beta,\beta,\text{rest}) \\ \sim (\alpha,\alpha,\beta,\alpha,\text{rest} &\sim (1,1,\beta,\alpha,\text{rest})\end{aligned} \tag{5.35}$$

and

$$(1,1,\alpha,\text{rest}) \sim (\alpha,\alpha,\alpha,\text{rest}) \sim (\alpha,1,1,\text{rest}). \tag{5.36}$$

Pairs of equal entries can therefore be substituted by other pairs of equal entries. Furthermore, equations (5.35) and (5.36) tell us that

[59] Note that since F is a positive semidefinite matrix it is symmetric. Therefore we need not distinguish the directions of the connections.

the connected components are invariant under permutation. In fact, they depend only on the parities $\mathcal{P} \overset{\text{def}}{=} \{\alpha | \#\{i|\alpha_i = \alpha\} \text{ is odd}\}$ of the tuples. The greatest eigenvalue of the single Perron-Frobenius blocks will depend on $p = |\mathcal{P}|$ and N. For this we only need to look at tuples of the form $(1, 2, 3, \ldots, p, x, x, y, y, \ldots)$. Such tuples are represented by the vector $|\tilde{\phi}\rangle \overset{\text{def}}{=} |e_1\rangle \otimes |e_2\rangle \otimes \cdots \otimes |e_p\rangle \otimes |\psi_+\rangle \otimes \cdots \otimes |\psi_+\rangle$. For this vector one can easily compute that $P_{kl}|\tilde{\phi}\rangle = \lambda_{kl} U_{\pi_{kl}} |\tilde{\phi}\rangle$ holds with the following eigenvalues λ_{kl} and permutation operators $U_{\pi_{kl}}$:

1. If (k, l) is one of the pairs: $\lambda_{kl} = 1$, $\pi_{kl} = id$ and $\#\{k, l\} = \frac{N-p}{2}$.

2. If (k, l) connects two different pairs, say (j, k) and (l, m): $\lambda_{kl} = \frac{1}{d}$, $\pi = (km)$ and $\#\{k, l\} = 4 \begin{pmatrix} \frac{N-p}{2} \\ 2 \end{pmatrix}$.

3. If (k, l) connects $q \in \{1, \ldots, p\}$ with a pair, say (l, m): $\lambda_{kl} = \frac{1}{d}$, $\pi = (qm)$ and $\#\{k, l\} = p(N - p)$.

4. If (k, l) connects q_1 and q_2 with $q_1, q_2 \in \{1, \ldots, p\}$: $\lambda_{kl} = 0$.

Furthermore, since $F \equiv \sum_\pi V_\pi^* F V_\pi$ commutes with the Bose projection:

$$\begin{aligned} P_{\text{Bose}} F &= \frac{1}{N!} \sum_{\sigma,\pi} V_\sigma V_\pi^* F V_\pi = \frac{1}{N!} \sum_{\sigma,\pi} V_{\sigma\circ\pi^{-1}} F V_\pi \\ &= \frac{1}{N!} \sum_{\sigma,\sigma'} V_{\sigma'^{-1}} F V_{\sigma'\circ\sigma} = F P_{\text{Bose}}, \end{aligned} \tag{5.37}$$

we can use $|\phi\rangle \overset{\text{def}}{=} P_{\text{Bose}}|\tilde{\phi}\rangle$ as Perron-Frobenius vector of F. This is indeed an eigenvector of F:

$$\begin{aligned} F|\phi\rangle &= \frac{1}{N!} \sum_\pi F V_\pi |\tilde{\phi}\rangle = P_{\text{Bose}} F |\tilde{\phi}\rangle \\ &= \sum_{k,l} P_{\text{Bose}} P_{k,l} |\tilde{\phi}\rangle = \sum_{k,l} \lambda_{kl} P_{\text{Bose}} V_{\pi_{kl}} |\tilde{\phi}\rangle = \left(\sum_{k,l} \lambda_{kl} \right) |\phi\rangle, \end{aligned} \tag{5.38}$$

namely to the eigenvalue $\Lambda = \sum_{k,l} \lambda_{kl}$ with purely positive entries. Perron's Theorem then ensures that Λ is the unique greatest eigenvalue of F. To finish the optimization we only have to maximize Λ by varying the parity p. The eigenvalue is

$$\Lambda = \frac{N-p}{2} \left(1 + \frac{N+p-2}{d} \right) = x \left(1 + \frac{2}{d}(N - x - 1) \right) \tag{5.39}$$

with $x = \frac{N-p}{2}$. Its maximum is achieved for $p = 0$ if N is even and for $p = 1$ if N is odd, which finishes the proof. ■

We finish by giving an example. If we take the web state for $N = 4$ (see figure 5.3), then our lemma directly gives that

$$|\phi_3\rangle = \frac{1}{\sqrt{3+\frac{6}{d}}}(|\psi_+\rangle_{12} \otimes |\psi_+\rangle_{34} + |\psi_+\rangle_{13} \otimes |\psi_+\rangle_{24} + |\psi_+\rangle_{14} \otimes |\psi_+\rangle_{23}) \quad (5.40)$$

is one of the states that give an optimal shared fidelity of $\frac{1}{3}(1+\frac{2}{d})$.

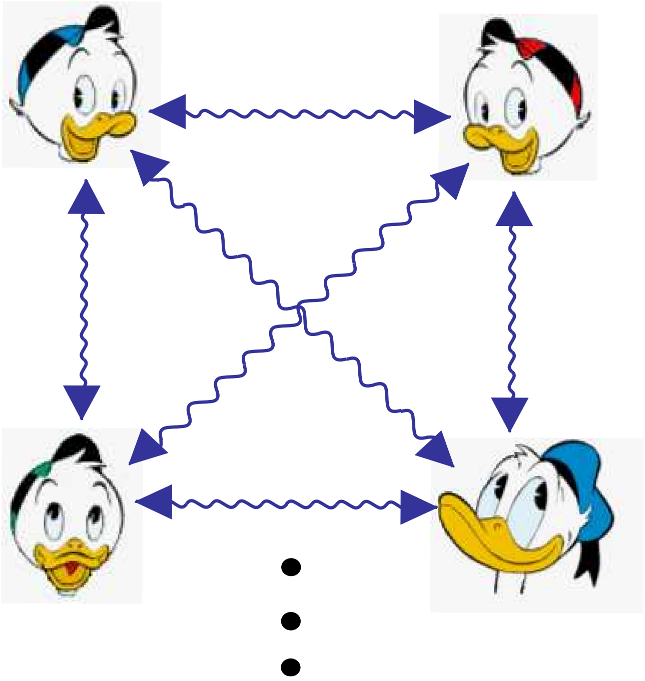


Figure 5.3: The four-duck web configuration. [The ducks are copyright of Disney Corporation.]

Summary

This dissertation describes the application of symmetry to multipartite quantum systems from the viewpoint of quantum information theory. It is written in the framework of abstract quantum information theory, i.e. without distinguishing the physical nature of the d-level systems considered. The results are mathematically rigorous and aim at investigating entanglement properties as well as operational properties of states of multipartite systems.

In the following we give a chapter by chapter summary of the obtained results.

Chapter 2: Multipartite symmetric states. The parametrization of multipartite states is crucial when investigating multipartite entanglement and protocols. To avoid an exponential number of parameters we introduce families of symmetric multipartite states with a dimension independent number of parameters. Results of representation theory are used to give a parametrization and to construct commutative subsets of these families of states. Furthermore we investigate reductions of these states to smaller numbers of subsystems as well as their extensions to larger numbers of subsystems. For the two basic examples considered later – multipartite Werner states and multipartite orthogonally invariant states – we derive graphical notations to simplify the computations.

Chapter 3: Tripartite Werner states. In this chapter we pick up the multipartite Werner states for $N = 3$ and analyze them in detail. We investigate the case of $N = 3$ since it is the simplest nontrivial example of multipartite Werner states. They are simpler than higher-partite states, showing at the same time all peculiarities of noncommutativity. We fully characterize their separability properties and analyze the strength of the known separability criteria. Furthermore we investigate their entanglement properties in terms of the relative

entropy of entanglement, the entanglement monotone induced by the trace norm distance and the maximal violation of Bell inequalities. As a third aspect we analyze the possibility of embedding bipartite Werner states as reduced tripartite Werner states and investigate the predictive power of these reductions. We finish by exploring the inner geometry of the manifold given by the statistical distance of two neighbouring tripartite Werner states.

Chapter 4: Quantum data hiding. As an application of the multipartite Werner states introduced in the preceding chapters we extend the protocol called quantum data hiding to multipartite systems. Using the graphical notations derived in chapter 2 we prove that this protocol is at least asymptotically secure in the limit of large system dimension. A constructive scheme for the hiding states is given making use of the multipartite Werner states. We show by example that the hiding strength cannot be measured by one single parameter. Furthermore we show that even separable states can be used for quantum data hiding and analyze the security in presence of prior shared entanglement and for hiding whole bit sequences. We finish by arguing that Werner symmetry could already be optimal for quantum data hiding in fixed dimensions.

Chapter 5: Shared fidelity. In the last chapter we show that multipartite symmetric states sometimes arise naturally when asking "symmetric questions", i.e. questions that are invariant under the relabelling of the parties. To this end we investigate to what extent single parties can be entangled to others in terms of fidelity. In fact, as a purely quantum feature, multipartite quantum systems can already be frustrated even in absence of closed loops. We start by analyzing, for a tripartite setup, what the optimal reference set of maximally entangled states is, and which way of averaging leads to the best average shared fidelity. We then turn to the $1:N$ configuration and show that the states optimizing the average shared fidelity correspond to optimal telecloners. As a last example we investigate entangled webs, i.e. states of maximally connected sets of parties. We derive the optimal states in terms of average shared fidelity for an arbitrary number of parties.

Bibliography

[AF92] D. Avis and K. Fukuda. A pivoting algorithm for convex hulls and vertex enumeration of arrangements and polyhedra. *Discrete Comp. Geom.*, 8:295–313, 1992.

[AGR81] A. Aspect, P. Grangier, and G. Roger. Experimental tests of realistic local theories via Bell's theorem. *Phys. Rev. Lett.*, 47:460–463, 1981.

[BBC$^+$93] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, 1993.

[BC94] S. L. Braunstein and C. M. Caves. Statistical distance and the geometry of quantum states. *Phys. Rev. Lett.*, 72:3439–3443, 1994.

[BDM$^+$99] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal. Unextendible product bases and bound entanglement. *Phys. Rev. Lett.*, 82:5385–5388, 1999.

[BDSW96] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed-state entanglement and quantum error correction. *Phys. Rev. A*, 54:3824–3851, 1996.

[Bel64] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195–200, 1964.

[Ben80] P. Benioff. The computer as a physical system: A microscopic quantum mechanical hamiltonian model of computers as represented by Turing machines. *J. Stat. Phys.*, 22:563–591, 1980.

[Bha97] R. Bhatia. *Matrix Analysis*, volume 169 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, Heidelberg, Berlin, 1997.

[BR79] O. Bratteli and D. W. Robinson. *Operator Algebras and Quantum Statistical Mechanics I*. Text and Monographs in Physics. Springer-Verlag, New York; Heidelberg; Berlin, 1979.

[Bur69] D. Bures. An extension of Kakutani's theorem on infinite product measures to the tensor product of seminfinite W*-algebras. *Trans. Amer. Math. Soc.*, 135:199–212, 1969.

[But02] M. Butkus. Verstecken von klassischer Information in zweigeteilten Quantensystemen. Master's thesis, Technische Universität Braunschweig, 2002.

[Cab02] A. Cabello. N-particle n-level singlet states: Some properties and applications. *Phys. Rev. Lett.*, 89:100402, 2002.

[CHSH69] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880, 1969.

[CKW00] V. Coffman, J. Kundu, and W. K. Wootters. Distributed entanglement. *Phys. Rev. A*, 61:052306, 2000.

[Deu85] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proc. R. Soc. Lond. A*, 400:97, 1985.

[DHR02] M. Donald, M. Horodecki, and O. Rudolph. The uniqueness theorem for entanglement measures. *J. Math. Phys.*, 43:4252–5272, 2002.

[DHT03] D. P. DiVincenzo, P. Hayden, and B. Terhal. Hiding quantum data. *Foundations of Physics*, David Mermin Festschrift (special issue), 2003.

[Dür01] W. Dür. Multipartite entanglement that is robust against disposal of particles. *Phys. Rev. A*, 63:020303, 2001.

[DW01] K. A. Dennison and W. K. Wootters. Entanglement sharing among quantum particles with more than two orthogonal states. *Phys. Rev. A*, 65:010301, 2001.

[EAP02] J. Eisert, K. Audenaert, and M. B. Plenio. Remarks on entanglement measures and non-local state distinguishability. *LANL preprint*, quant-ph:0212007, 2002.

[EB94] A. Elby and J. Bub. Triorthogonal uniqueness theorem and its relevance to the interpretation of quantum mechanics. *Phys. Rev. A*, 49:4213–4216, 1994.

[Ell] R. S. Ellis. *Entropy, Large Deviations and Statistical Mechanics*. Springer-Verlag, New York, N.Y.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, 1935.

[EVWW01] T. Eggeling, K. G. H. Vollbrecht, R. F. Werner, and M. M. Wolf. Distillability via protocols respecting the positivity of partial transpose. *Phys. Rev. Lett.*, 87:257902, 2001.

[EW01] T. Eggeling and R. F. Werner. Separability properties of tripartite states with $U \otimes U \otimes U$ symmetry. *Phys. Rev. A*, 63:042111, 2001.

[EW02] T. Eggeling and R. F. Werner. Hiding classical data in multipartite quantum states. *Phys. Rev. Lett.*, 89:097905, 2002.

[EW] T. Eggeling and R. F. Werner. On quantum data hiding. in preparation.

[Fan02] H. Fan. A note on separability criteria for multipartite states. *LANL preprint*, quant-ph:0210168, 2002.

[Fey86] R. P. Feynman. Quantum mechanical computers. *Foundations of Physics*, 16:507–531, 1986.

[FH91] W. Fulton and J. Harris. *Representation Theory*, volume 129 of *Graduate texts in mathematics*. Springer, New York, Berlin, Heidelberg, 3rd printing, 1st edition, 1991.

[FHW79] F.-J. Fritz, B. Huppert, and W. Willems. *Stochastische Matrizen*. Springer-Verlag, Berlin, Heidelberg, New York, 1979.

[Fin82] A. Fine. Hidden variables, joint probability, and the Bell inequalities. *Phys. Rev. Lett.*, 48:291–295, 1982.

[Fuc02] C. A. Fuchs. Quantum mechanics as quantum information (and only a little more). *LANL preprint*, quant-ph:0205039, 2002.

[Gro96] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing.*, pages 212–219, New York, NY, USA, 1996. ACM Press.

[Had86] N. Hadjisavvas. Metrics on the set of states of a W^*-algebra. *Lin. Alg. Appl.*, 84:281–287, 1986.

[HBB99] M. Hillery, V. Bužek, and A. Berthiaume. Quantum secret sharing. *Phys. Rev. A*, 59:1829–1834, 1999.

[HH99] M. Horodecki and P. Horodecki. Reduction criterion of separability and limits for a class of distillation protocols. *Phys. Rev. A*, 59:4206–4216, 1999.

[HHH96] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A*, 223:1, 1996.

[HHH02] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed quantum states: linear contractions approach. *LANL preprint*, quant-ph:0206008, 2002.

[HJ95] R. A. Horn and C. R. Johnson. *Matrix Analysis*. Cambridge University Press, Cambridge, UK, 1995.

[Hol82] A. S. Holevo. *Probabilistic and statistical aspects of quantum theory*, volume 1 of *Statistics and Probability*. North-Holland Publishing Company, Amsterdam, 1982.

[Hor94] R. Horodecki. Informationally coherent quantum systems. *Phys. Lett. A*, 187:145–150, 1994.

[Hor97] P. Horodecki. Separability criterion and inseparable mixed states with positive partial transposition. *Phys. Lett. A*, 232:333–339, 1997.

[Hüb92] M. Hübner. Explicit computation of the Bures distance for density matrices. *Phys. Lett. A*, 163:239–242, 1992.

[Jam72] A Jamiołkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Rep. Math. Phys.*, 3:275–278, 1972.

[Jay57a] E. T. Jaynes. Information theory and statistical mechanics. *Phys. Rev.*, 106:620–630, 1957.

[Jay57b] E. T. Jaynes. Information theory and statistical mechanics ii. *Phys. Rev.*, 108:171–190, 1957.

[KBI00] M. Koashi, V. Bužek, and N. Imoto. Entangled webs: Tight bound for symmetric sharing of entanglement. *Phys. Rev. A*, 62:050302, 2000.

[Kra83] K. Kraus. *States, Effects and Operations*, volume 190 of *Lecture Notes in Physics*. Springer-Verlag, New York; Heidelberg; Berlin, 1983.

[KW99] M. Keyl and R. F. Werner. Optimal cloning of pure states, judging single clones. *J. Math. Phys.*, 40:3283–3299, 1999.

[Lin76] G. Lindblad. On the generators of quantum dynamical semigroups. *Commun. Math. Phys.*, 48:119–130, 1976.

[LPW02] N. Linden, S. Popescu, and W. K. Wootters. Almost every pure state of three qubits is completely determined by its two-particle reduced density matrices. *Phys. Rev. Lett.*, 89:207901, 2002.

[Lud76] G. Ludwig. *Einführung in die Grundlagen der Theoretischen Physik*, volume 3, Quantenmechanik. Friedr. Vieweg & Sohn Verlagsgesellschaft, Braunschweig, 1976.

[LW02] N. Linden and W. K. Wootters. The parts determine the whole in a generic pure quantum state. *Phys. Rev. Lett.*, 89:277906, 2002.

[MJPV99] A. Murao, D. Jonathan, M. B. Plenio, and V. Vedral. Quantum telecloning and multipartite entanglement. *Phys. Rev. A*, 59:156–161, 1999.

[Nag73] R. J. Nagel. *Foundations of Quantum Mechanics and Ordered Linear Spaces*, volume 29 of *Lecture notes in physics*, chapter 3. Order Unit and Base Norm Spaces, pages 23–29. Springer, Berlin, Heidelberg, New York, 1973.

[NC00] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, UK, 2000.

[Nie99] M. A. Nielsen. Conditions for a class of entanglement transformations. *Phys. Rev. Lett.*, 83:436–439, 1999.

[NK01] M. A. Nielsen and J. Kempe. Separable states are more disordered globally than locally. *Phys. Rev. Lett.*, 86:5184–5187, 2001.

[OP93] M. Ohya and D. Petz. *Quantum Entropy and Its Use*. Springer-Verlag, New York, Berlin, Heidelberg, 1993.

[Pau86] V. I. Paulsen. *Completely bounded maps and dilations*. Longman Scientific & Technical, Longman House, Burnt Mill, Harlow, England, 1986.

[Ped79] G. K. Pedersen. *C*-Algebras and their Automorphism Groups*. Academic Press, London, 1979.

[Per93] A. Peres. *Quantum Theory: Concepts and Methods*, volume 57 of *Fundamental Theories of Physics*. Kluwer Academic Publishers, Dordrecht, Boston, London, 1993.

[Per96] A. Peres. Separability criterion for density matrices. *Phys. Rev. Lett.*, 77:1413–1415, 1996.

[Pol74] J. J. Pollitt. *The Ancient View of Greek Art*. Yale University Press, New Haven and London, 1974.

[Pop95] S. Popescu. Bell's inequalities and density matrices: Revealing "Hidden" nonlocality. *Phys. Rev. Lett.*, 74:2619–2622, 1995.

[Rai99] E. M. Rains. Bound on distillable entanglement. *Phys. Rev. A*, 60:179–184, 1999.

[Roc72] R. T. Rockafellar. *Convex Analysis*. Princeton University Press, Princeton, NJ, 2nd edition, 1972.

[Rud00] O. Rudolph. A separability criterion for density operators. *J. Phys. A*, 33:3951–3955, 2000.

[SBG01] C. Simon, V. Bužek, and N. Gisin. No-signaling condition and quantum dynamics. *Phys. Rev. Lett.*, 87:170405, 2001.

[Sch07] E. Schmidt. Zur Theorie der linearen und nichtlinearen Integralgleichungen. *Math. Ann.*, 63:433, 1907.

[Sch35] E. Schrödinger. Die gegenwärtige Situation in der Quantenmechanik (2). *Die Naturwissenschaften*, 23(49):823–828, 1935.

[Sha48] C. E. Shannon. A mathematical theory of communication. *Bell System Tech. J.*, 27:379–423,623–656, 1948.

[Sha79] A. Shamir. How to share a secret. *Comm. ACM*, 22:612–613, 1979.

[Sho94] P. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In S. Goldwasser, editor, *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, pages 124–134, Los Alamitos, CA, 1994. IEEE Computer Society Press.

[Sim96] B. Simon. *Representations of Finite and Compact Groups*, volume 10 of *Graduate Studies in Mathematics*. American Mathematical Society, Rhode Island, NY, 1996.

[TDL01] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung. Hiding bits in Bell states. *Phys. Rev. Lett.*, 86:5807, 2001.

[TDL02] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung. Quantum data hiding. *IEEE Trans. Inf. Th.*, 48:580–598, 2002.

[Uhl76] A. Uhlmann. The transition probability in the state space of a *-algebra. *Rep. Math. Phys.*, 9:273–279, 1976.

[VC01] G. Vidal and I. Cirac. Irreversibility in asymptotic manipulation of entanglement. *Phys. Rev. Lett.*, 86:5803–5806, 2001.

[Vid00] G. Vidal. Entanglement monotones. *J. Mod. Opt.*, 47:355, 2000.

[VP98] V. Vedral and M. B. Plenio. Entanglement measures and purification procedures. *Phys. Rev. A*, 57:1619–1633, 1998.

[VW01] K. G. H. Vollbrecht and R. F. Werner. Entanglement measures under symmetry. *Phys. Rev. A*, 64:062307, 2001.

[VW02] K. G. H. Vollbrecht and M. M. Wolf. Conditional entropies and their relation to entanglement criteria. *J. Math. Phys.*, 43:4299–4306, 2002.

[Wer89] R. F. Werner. Quantum states with Einstein-Rosen-Podolsky correlations admitting a hidden-variable model. *Phys. Rev. A*, 40:4277–4281, 1989.

[Wer94] R. F. Werner. Finitely correlated pure states. In M. Fannes, C. Maes, and A. Verbeure, editors, *On Three Levels: Micro-, Meso-, and Macro-Approaches in Physics.*, volume 324 of *NATO ASI Seires B: Physics*, pages 193–202, New York, NY, 1994. Plenum Press.

[Wer98] R. F. Werner. Optimal cloning of pure states. *Phys. Rev. A*, 58:1827–1832, 1998.

[Wer01a] R. F. Werner. All teleportation and dense coding schemes. *J. Phys. A*, 35:7081–7094, 2001.

[Wer01b] R. F. Werner. *Quantum information – an introduction to basic theoretical concepts and experiments.*, chapter Quantum Information Theory – an Invitation. Springer-Verlag, New York, 2001.

[Wig31] E. P. Wigner. *Gruppentheorie und ihre Anwendung auf die Quantenmechanik der Atomspektren*, volume 85 of *Die Wissenschaft*. Friedr. Vieweg & Sohn Akt.-Ges., Braunschweig, 1931.

[Wol02] M. M. Wolf. *Partial Transposition in Quantum Information Theory*. PhD thesis, Technische Universität Braunschweig, 2002.

[Woo81] W. K. Wootters. Statistical distance and Hilbert space. *Phys. Rev. D*, 23:357–362, 1981.

[WW01] R. F. Werner and M. M. Wolf. All multipartite Bell correlation inequalities for two dichotomic observables per site. *Phys. Rev. A*, 64:032112, 2001.

[WZ82] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–3, 1982.

Publication list

[EW00] T. Eggeling, R. F. Werner: *Separability properties of tripartite states with $U \otimes U \otimes U$-symmetry,* Phys. Rev. A **63**, 042111 (2000).

[ES01] T. Eggeling, D. M. Schlingemann, R. F. Werner: *Semicausal operations are semilocalizable,* Europhys. Lett. **57**(6), 782 (2001).

[EV01] T. Eggeling, K. G. H. Vollbrecht, R. F. Werner, M. M. Wolf: *Distillability via protocols respecting the positivity of partial transpose,* Phys. Rev. Lett. **87**, 257902 (2001).

[EW02] T. Eggeling, R. F. Werner: *Hiding classical data in multipartite quantum systems,* Phys. Rev. Lett. **89**, 097905 (2002).

[EW03] T. Eggeling, R. F. Werner: *On quantum data hiding,* in preparation.

[EWW03] T. Eggeling, R. F. Werner, M. M. Wolf: *From optimal entanglement sharing to optimal cloning,* in preparation.

[ES03] T. Eggeling, P. B. Slater: *A priori probabilities for tripartite Werner states*, in preparation.

Acknowledgements

I am greatly indebted to my advisor Prof. Dr. R. F. Werner for introducing me to quantum information theory and for sharing his vast knowledge of mathematics.

Thank-yous go to

... Dr. Dirk “the intertwiner” Schlingemann for teaching me the beauty of representation theory.

... Dr. Michael “it’s only finite dimensional” Keyl for being a helpful guide in the forest of infinite dimensions.

... My office mates, colleagues and friends Karl␣Gerd Vollbrecht and Michael Wolf for innumerable stimulating discussions and the fun we had.

... Ole Krüger for being an example of discipline and thoroughness.

... Frank Klose for being a good friend.

... Dr. Eberhard “I’ve seen that before...” Gerbracht, Dr. Uwe “I’m almost there” Schomäcker, Martin Neumann, Michael Reimpell, Martin Butkus, Verena Grützun, Andreas “how goes?” Friedrich, Cornelia “Conny” Schmidt, Dennis Kretschmann and all the others that influenced me in one way or another...

... The staff of the Institute for Mathematical Physics for making everyday life so enjoyable.

... The Deutsche Forschungsgemeinschaft for its financial support without which this thesis would not exist.

Special thanks go to my parents for their love and support and to Simone for her ♡ and patience.