universität wien

MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

„Bound Entanglement Detection via Mutually Unbiased Bases“

verfasst von / submitted by

Eva Kilian, BSc

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Science (MSc)

Wien, 2018 / Vienna, 2018

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	A 066876
Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet:	Masterstudium Physik
Betreut von / Supervisor:	Mag. Dr. Beatrix Hiesmayr, Privatdoz.

Abstract

Recently bipartite bound entanglement has been experimentally detected for the first time [1]. Bipartite bound entanglement is a curious type of entanglement since it needs maximally entangled states to be generated, but no maximally entangled states can, hereafter, be distilled.

This thesis studies bound entanglement of a family of states ρ_M that forms the magic simplex. Detection of entanglement is known to belong to the NP-hard mathematical problems. Detecting bound versus free entanglement adds complexity since the PPT criterion (positivity under partial transposition) fails.

In this thesis, we have considered so-called MUB-Witnesses. These are observables that are formed by sets of mutually unbiased bases (MUBs) to detect bound entanglement within the magic simplex in different dimensions. We have found that the ordering of MUB vectors forming the witness is crucial to detect bound entanglement which is relevant when designing a dedicated experiment.

Zusammenfassung

Kürzlich wurde gebundene Zweiteilchenverschränkung erstmals nachgewiesen [1]. Gebundene Zweiteilchenverschränkung ist eine sonderbare Art der Verschränkung, da sie maximal verschränkter Zustände bedarf um erzeugt zu werden, jedoch anschließend keine maximal verschränkten Zustände mehr distilliert werden können.
Diese Arbeit betrachtet gebundene Verschränkung einer Zustandsfamilie ρ_M im magischen Simplex. Der Nachweis von Verschränkung fällt in die Gruppe der NP-harten mathematischen Probleme. Gebundene im Gegensatz zu freier Verschränkung zu detektieren ist aufgrund des Versagens des PPT (positive partielle Transposition) Kriteriums zusätzlich umso komplexer.
In dieser Arbeit haben wir sogenannte MUB-Verschränkungszeugen betrachtet. Diese sind Observablen, welche mithilfe von Sets gegenseitig unvoreingenommener Basen (engl. mutually unbiased bases, kurz MUBs genannt) konstruiert werden um gebundene Verschränkung im magischen Simplex und in unterschiedlichen Dimensionen zu detektieren. Wir zeigen, dass die Reihenfolge der MUB Vektoren welche den Verschränkungszeugen formen entscheidend ist um gebundene Verschränkung zu detektieren, was für das Design eines neuen Experiments von besonderer Wichtigkeit ist.

Acknowledgements

First and foremost, I want to thank Mag. Dr. Beatrix Hiesmayr for her patience in explaining when I did not understand, her subtle guidance when I was in need for direction and her spirit of encouragement, enabling me to dare and follow my own interests, even when I felt their consideration required a level of comprehension that was far beyond my own. I want to thank her for her support in visiting conferences and workshops on quantum information and for always making time for talks and brisk discussions when they were needed.

Secondly I want to extend the warmest gratitude to my friends Markus Rademacher, Julia Holzer and Nikola Mandl, who've provided me with welcomed distractions whenever my own frustration about non-compliant software or a broken computer exceeded my level of patience or tolerance.

And lastly, I want to thank my family for not trying to change my mind about going into physics and the support that they have given me over the years. Even as a child, you have encouraged me to ask questions just as well as you have taught me not to quit, irrespective of how hard it proved to get the answers to them. It was your utmost dedication that has brought me to this point and I'm forever thankful to you all.

Contents

1 Introductory Remarks **1**

2 Mathematical Foundations **3**
2.1 Discrete and Algebraic Structures . . . 3
2.1.1 From Commutative Rings to Finite Fields . . . 3
2.1.2 Vector Spaces over Fields: The Hilbert Space . . . 6
2.2 State Representation and Quantum Operations in Hilbert Space . . . 8
2.2.1 Representation of Pure and Mixed Quantum States . . . 8
2.2.2 Bloch Decomposition . . . 10
2.2.3 Quantum Operations . . . 10
2.2.4 The Class of LOCC . . . 12
2.2.5 The Weyl Operator Basis . . . 14

3 Entangled Systems **15**
3.1 Separability and Entanglement of Bipartite Systems . . . 15
3.1.1 Pure State Separability via Schmid's Decomposition . . . 18
3.1.2 Mixed State Separability via Positive Maps . . . 19
3.2 Multipartite Entanglement . . . 21
3.3 Bound Entanglement . . . 22

4 Mutually Unbiased Bases **23**
4.1 The Notion of Mutual Unbiasedness . . . 23
4.2 Constructions of MUBs from Finite Fields . . . 23
4.2.1 Odd Prime Powers . . . 24
4.2.2 Even Prime Powers (= Powers of 2) . . . 25
4.3 Constructions of MUBs using the Generalized Pauli Group . . . 28

5 Entanglement Witnesses **30**
5.1 Mathematical Definition . . . 30
5.2 Witnesses from Mutually Unbiased Bases . . . 31

6 Geometry of Bipartite Systems **34**
6.1 The Magic Simplex . . . 34
6.2 Bound Entanglement Detection via MUB Witnesses . . . 37
6.2.1 Starting with $3 \otimes 3$ . . . 38
6.2.2 MUB-Witnesses for Bound Entanglement in $4 \otimes 4$ . . . 42
6.2.3 MUB-Witnesses for Bound Entanglement in $5 \otimes 5$ . . . 46
6.3 D-Dimensional Witness Generalization . . . 49
6.4 Bound Entanglement Detection via MUB Witnesses in Higher Dimensions . . . 52
6.5 Lower Bound on the MUB Criterion . . . 52

7 Conclusion **54**

References **55**

1 Introductory Remarks

Entanglement is generally a vital resource in the field of quantum information. Quantum cryptography as well as quantum computation heavily rely on the distillability of maximally entangled states from any general, arbitrary entangled state.

In his seminal paper [2], Peres has mathematically proven that states fulfilling the partial transposition criterion do not possess this property of distillability. The Horodecki family [3–6] generalized this concept by exploiting positive but not completely positive maps. Within the last two decades, the natural conclusion of their findings has amounted to the notion that for systems of dimension $d_{tot} > 6$, there can exist mixed entangled states which do remain positive under partial transposition [7] and are therefore undistillable. This realization leads to a classification of two intrinsically distinct types of entanglement: distillable entanglement which is sometimes also referred to as free entanglement and undistillable or so-called *bound* entanglement. The existence of the latter is especially interesting: bound entangled states may require pure maximally entangled states for their generation, which, however, cannot be extracted from them afterwards. The origin or physical meaning of this irreversibility is not currently known. Some classes of bound entangled states have been shown to violate Bell inequalities [8–10]. In Ref. [1], the bipartite PPT type of bound entanglement has been experimentally detected for the first time. It is still an open question whether there exist bound entangled states that are negative with respect to the partial transpose criterion. Numerical indication of the existence of such states was for example claimed in Ref. [11], while a bipartite two-parameter family of such NPT and possibly undistillable entangled states was discussed in Ref. [12].

Let us name here some examples: bound entangled states can be used as a resource for secure key generation [13], quantum steering [14], communication complexity reduction [15] and entanglement activation [4].

The focus of this thesis is set onto detections of bound entanglement in a certain family of states that lie within a reduced subspace referred to as the magic simplex which exhibits a $U \otimes U^*$ symmetry. This will be done by employing entanglement witnesses constructed via mutually unbiased bases. These bases are maximally incompatible in the sense that all outcomes of systems prepared in one complete orthonormal eigenbasis are equally likely when measured in another basis that is mutually unbiased to it. Furthermore, MUBs have the advantage of being easily implementable in the lab, at least with respect to measurements on lower-dimensional systems. The MUB criterion employed in this thesis and derived in publication [16] provides an upper bound for all separable states and, therefore, a violation of the bound witnesses entanglement. All states will be investigated within the magic simplex $\mathcal{W}$ that is defined in chapter 6.1.

The second chapter provides the mathematical framework utilized in this thesis. A brief description of the most readily employed discrete and algebraic structures will be concluded by the basic mathematical representation of the physical systems under in-

vestigation as well as some of their transformations.

The third chapter introduces in more detail the notion of separability and entanglement of quantum systems. It introduces the positive partial transpose criterion, the distillability of quantum states and bound entanglement.

In chapter four mutual unbiasedness of sets of bases is introduced. Two different methods to construct such sets are described.

Chapter five defines the concept of an entanglement witness and utilizes mutually unbiased bases in order to construct such a witness.

Last but not least, chapter 6 deals with the characterization of a special class of $U \otimes U^*$ states within the magic simplex. With the help of the MUB witness we show explicitly how bound entangled states within some cuts of the magic simplex, i.e. for some class of states, can be detected and visualize its geometry.

2 Mathematical Foundations

This chapter is partly inspired by the publications [17–20].

2.1 Discrete and Algebraic Structures

In order to establish an adequate understanding of the theoretical considerations of this thesis, this chapter will provide the reader with a selection of the discrete and algebraic structures that are most readily used throughout the following pages.
More detailed information on the mentioned concepts from discrete algebraics can be taken from [17, 18].

2.1.1 From Commutative Rings to Finite Fields

Possibly introduced by David Hilbert, the term *commutative ring* refers to a set of the two operations multiplication and addition. It is defined in the following way:

Definition 2.1 (Commutative ring)**.** The set of multiplicative and additive operations that is a *commutative ring* $\mathcal{R}$, fulfills the following axioms:

1. $a + b = b + a, \quad \forall\ a, b \in \mathcal{R}$
2. $a + (b + c) = (a + b) + c, \quad \forall\ a, b, c \in \mathcal{R}$
3. There is an element $0 \in \mathcal{R}$ such that $0 + a = a, \quad \forall\ a \in \mathcal{R}$
4. For each $a \in \mathcal{R}$, there is $a' \in \mathcal{R}$ with $a' + a = 0$
5. $ab = ba, \quad \forall\ a, b \in \mathcal{R}$
6. $a(bc) = (ab)c, \quad \forall\ a, b, c \in \mathcal{R}$
7. There is a unit element $1 \in \mathcal{R}$, such that $1a = a, \quad \forall\ a \in \mathcal{R}$
8. $a(b + c) = ab + ac, \quad \forall\ a, b, c \in \mathcal{R}$

It shall be noted here, that the first four axioms - which are commutativity, associativity, additive identity and inverse - constitute an abelian group under the operation addition. Note here that in order to be an abelian group under multiplication, there would have to exist a multiplicative inverse for every element.

One of the simplest examples of a commutative ring would be the set of integers $\mathbb{Z} = \{...-3, -2, -1, 0, 1, 2, 3...\}$. It is closed under the operations addition and multiplication.

Definition 2.2 (Characteristic of a ring)**.** If there exists a positive integer m such that $m \cdot r = 0$ for all $r \in \mathcal{R}$, the *characteristic* m of the ring $\mathcal{R}$ is the least such positive integer m. Otherwise, the characteristic of $\mathcal{R}$ equals zero.

Stated differently, the characteristic of $\mathcal{R}$ can be obtained by adding up the multiplicative identity element for the m smallest possible times until the additive identity element is reached. As an example, by extension of this reasoning to for instance the commutative ring of integers, it becomes clear that $\mathbb{Z}$ bears characteristic 0.

Definition 2.3 (Fields)**.** *Fields* are commutative rings for which every element $a \in \mathcal{R}$ is invertible and $1 \neq 0$.

This means, that every non-zero element a of a field $\mathbb{F}$ has a multiplicative inverse b such that the product $a \cdot b = 1$ and an additive inverse c such that $a + c = 0$.

The set of integers $\mathbb{Z}$ can again be taken as an example. As $\mathbb{Z}$ lacks multiplicative inverses for all integers except 1 & -1, e.g. $3 \cdot b \neq 1, \forall b \in \mathbb{Z}$, it is not a field.

Definition 2.4 (Finite fields)**.** *Finite fields*[1] are fields as defined in 2.3, containing a finite number of field elements. The order of a field is defined by the number of its elements.

The simplest kind of finite fields are those of prime order. Their elements may be represented by integers. To avoid any confusion beforehand: There exist no finite fields that are not of order p or p^n, p being a prime number and n denoting a positive integer. For a proof of this fact see [17, p. 300ff.]. In prime field arithmetics, the operations for multiplication and addition are carried out modulo p.

$$\begin{aligned} a + b &= c \mod p, \qquad \forall \quad a, b, c \in \mathbb{F}_p \\ a \cdot b &= c' \mod p, \qquad \forall \quad a, b, c' \in \mathbb{F}_p \end{aligned}$$

The smallest prime field of this type is $\mathbb{F}_2$ with the elements $\{0, 1\}$. The operation tables of $\mathbb{F}_3$ may serve as an illustration of prime field arithmetics for the reader.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Table 1: The operation tables for multiplication and addition for elements of $\mathbb{F}_3$

If and only if it is of order p, the ring $\mathbb{Z}/p\mathbb{Z}$[2] of integers modulo p is an isomorphism of a finite prime field $\mathbb{F}_p$, because only then, every nonzero field element has a multiplicative inverse.

[1] synonymous to Galois Fields

[2] $p\mathbb{Z}$ is an ideal in the ring of integers $\mathbb{Z}$ and denotes the set of all integers that are divisible by p

Definition 2.5. *Field extensions* $\mathbb{F}_q$ of finite prime fields $\mathbb{F}_p$ are finite fields of order $q = p^n$, n being a positive integer and $n \geq 2$. Their elements may explicitly be represented by irreducible polynomials of the form

$$A(x) = \sum_{i=0}^{n-1} a_i \alpha^i, \qquad a_i \in \mathbb{F}_p \; . \tag{2.1}$$

As an example, the operation tables of the prime field extension $\mathbb{F}_4$=$\mathbb{F}_{2^2}$ which can be represented by $\{a_0 + a_1\alpha : a_0, a_1 \in \mathbb{F}_2\}$ are:

$+$	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

$\cdot$	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

Table 2: The operation tables for multiplication and addition for elements of $\mathbb{F}_4$

The elements α and α^2=-$\alpha^2 = (\alpha+1)$ are given by the roots of the irreducible polynomial $x^2 + x + 1$. Operations on integer elements are taken mod $p = 2$, so that the resulting elements $\{0, 1\}$ belong to the field $\mathbb{F}_2$.

Definition 2.6 (Field theoretic trace)**.** Let $\alpha \in L = \mathbb{F}_{q^n}$ and $K = \mathbb{F}_q$. The *field theoretic trace* of α over K is then defined as

$$Tr_{L/K}(\alpha) = \sum_{i=0}^{n-1} \alpha^{q^i} = \alpha + \alpha^q + ... + \alpha^{q^{n-1}} \; . \tag{2.2}$$

As it will become important in the later chapters, the notion of an ideal over a commutative ring shall be defined here as well.

Definition 2.7 (Ideal)**.** An ideal I in a commutative ring $\mathcal{R}$ is a subset of $\mathcal{R}$. It has the following properties:

1. The additive inverse 0 is an element of the ideal I
2. If $a, b \in I$, then their sum $a + b$ is also in I
3. If $a \in I$ and $r \in \mathcal{R}$, then $r \cdot a \in I$

As an example, consider the ring $\mathcal{R} = \mathbb{Z}$ of integers. Then $I = 2\mathbb{Z}$ would be an ideal in $\mathcal{R}$, as every even number times any element r of the ring $\mathcal{R}$ would again yield an even number and therefore be contained in I.

2.1.2 Vector Spaces over Fields: The Hilbert Space

Definition 2.8 (Vector Space over Field)**.** A vector space V over a field k is an abelian group with respect to addition, that is equipped with scalar multiplication. The elements of V are referred to as vectors, whereas the constituents of the field k are called scalars. The elements $a, b \in k$ and $u, v, w \in V$ are subject to the operations of vector addition $V \times V \to V$ denoted by $(u, v) \mapsto u + v$ and scalar multiplication $k \times V \to V$ denoted by $(a, v) \mapsto av$. A vector space over a field satisfies the following axioms:

1. $a(u + v) = au + av$
2. $(a + b)v = av + bv$
3. $(ab)v = a(bv)$
4. $1v = v$, with 1 being the multiplicative identity in k
5. $(u + v) + w = u + (v + w)$
6. $(u + v) = v + u$
7. $\exists\ 0 \in V$ with $0 + v = v$
8. $\forall\ v \in V\ \exists\ v' \in V$ with $v + v' = 0$

A vector space together with an inner product is then referred to as product space. Product spaces are commonly used especially in physics, for the inner product introduces a notion of distance.

The prevalent quantum mechanical formalism uses Hilbert spaces to describe physical systems. The following definitions will be given with respect to infinite Hilbert spaces, but they also hold for finite dimensional Hilbert spaces with obvious modifications.

Definition 2.9 (Hilbert Space)**.** A Hilbert space is a complete (with respect to its metric) linear vector space over the field of complex numbers $\mathbb{C}$, that is equipped with the usual operations of vector addition and scalar multiplication, as well as an inner product.

The inner product obeys the following laws:

$$\langle u|v\rangle \geq 0 \qquad \forall\, u, v \in V \qquad (\langle u|v\rangle = 0 \text{ only if } v = 0) \tag{2.3}$$

$$\langle \alpha u + \beta v|w\rangle = \alpha\langle u|w\rangle + \beta\langle v|w\rangle \qquad \forall\, \alpha, \beta \in \mathbb{C},\ \forall\, u, v, w \in V \tag{2.4}$$

$$\langle u|v\rangle = \overline{\langle v|u\rangle} \tag{2.5}$$

The real-valued norm

$$||u|| = \sqrt{\langle u|u\rangle} \tag{2.6}$$

introduces the distance

$$D(u,v) = ||u-v|| = \sqrt{\langle u-v|u-v\rangle}. \tag{2.7}$$

Furthermore, the Schwarz inequality holds.

$$|\langle u,v\rangle| \leq ||u|| \cdot ||v|| \tag{2.8}$$

Due to properties (2.4) and (2.5) of the inner product, the parallelogram identity holds.

$$||u+v||^2 + ||u-v||^2 = 2||u||^2 + 2||v||^2 \tag{2.9}$$

Linear operators are linear maps between normed vector spaces. A certain kind of linear operators on Hilbert Space, the Hilbert-Schmidt and trace class operators, will become increasingly relevant when ascribing states to physical systems. The density matrix formalism will employ Hilbert-Schmidt operators.

Definition 2.10 (Hilbert-Schmidt Space)**.** A linear vector space of operators with a Hilbert-Schmidt inner product defined by $\langle A|B\rangle = Tr(A^\dagger B)$ is called the *Hilbert-Schmidt* space.

In the finite dimensional case, the Hilbert-Schmidt space becomes a useful tool because it contains all linear operators [21].

Definition 2.11 (Hilbert-Schmidt Operators)**.** Suppose a bounded[3] linear operator B $\in \mathcal{B}(\mathcal{H})$ with an orthonormal basis $\varepsilon_B = \{e_i\}_{i=1}^{\infty} \subset \mathcal{H}$. If

$$\sum_{i=1}^{\infty} ||Be_i||^2 < \infty \tag{2.10}$$

then this operator is a Hilbert-Schmidt operator [22].

Say the set $\mathcal{J}_2$ is the set of all Hilbert Schmidt operators on a given Hilbert space. For any B, $C \in \mathcal{J}_2$ the scalar product is given by

$$\langle B|C\rangle = \sum_{i=1}^{\infty} \langle Be_i|Ce_i\rangle = \sum_{i=1}^{\infty} \langle e_i|B^\dagger Ce_i\rangle \ . \tag{2.11}$$

If a Hilbert-Schmidt operator belongs to the trace class[4], $A \in \mathcal{J}_1$, then the scalar product can be expressed via the trace defined as $\mathrm{Tr}(A) := \sum_{i=1}^{\infty} \langle e_i|Ae_i\rangle$ and therefore

$$\langle Ae_i|A'e_i\rangle = \sum_{i=1}^{\infty} \langle e_i|A^\dagger A'e_i\rangle = \mathrm{Tr}(A^\dagger A') \ . \tag{2.12}$$

[3]A linear operator $B : V_1 \to V_2$ is bounded when $\exists a \geq 0 : ||Bu||_2 \leq a||u||_1$, $\forall u \in V_1$

[4]An operator $A \in \mathcal{B}(\mathcal{H})$ is of the trace class, if $Tr(|A|) < \infty$

2.2 State Representation and Quantum Operations in Hilbert Space

2.2.1 Representation of Pure and Mixed Quantum States

In the standard quantum mechanical formalism, a quantum state is associated with a vector or an operator on a Hilbert space $\mathcal{H}_n$ of dimension d_n.

For two vectors $|\psi_1\rangle = \sum_i \alpha_i |u_i\rangle$, $|\psi_2\rangle = \sum_i \beta_i |u_i\rangle \in \mathcal{H}_n$ with $\{|u_i\rangle\}$ forming a basis in $\mathcal{H}_n$, the inner product $\langle\psi_1|\psi_2\rangle$ is given by

$$\langle\psi_2|\psi_1\rangle = \sum_i \beta_i^* \alpha_i \ . \tag{2.13}$$

The outer product is denoted as

$$|\psi_2\rangle\langle\psi_1| = \sum_i \beta_i \alpha_i^* |u_i\rangle\langle u_i| \ . \tag{2.14}$$

A composite system of two quantum states $|\psi_1\rangle = \sum_i \alpha_i |u_i\rangle \in \mathcal{H}_1$, $|\psi_2\rangle = \sum_j \beta_j |v_j\rangle \in \mathcal{H}_2$ can be governed by employing the tensor product

$$|\psi_1\rangle \otimes |\psi_2\rangle = \sum_{i,j} \alpha_i \beta_j |i\rangle \otimes |j\rangle \ . \tag{2.15}$$

There is an important distinction to be made regarding the quantitative knowledge one possesses about a physical state.

Systems one has maximal information about, meaning that one knows with certainty which state they are in after a measurement has been performed, are referred to as pure states[23]. Such states can be represented by a single vector in a Hilbert space. In the density matrix formalism, it is common to work in the Hilbert-Schmidt space $\tilde{\mathcal{H}}_1 \otimes \tilde{\mathcal{H}}_2 \otimes ... \otimes \tilde{\mathcal{H}}_n$ of operators on the finite dimensional Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes ... \otimes \mathcal{H}_n$, where general properties of density matrices are:

1. $\langle A\rangle = Tr(\rho A)$

2. $\rho^\dagger = \rho$

3. $Tr(\rho) = 1$

Pure states can then be expressed as $\rho = |\psi\rangle\langle\psi|$. Furthermore, one has the following relation for pure states

$$\rho^2 = |\psi\rangle \overbrace{\langle\psi|\psi\rangle}^{=1}\langle\psi| = \rho \; . \tag{2.16}$$

Stated differently and for the bipartite case, any state $\rho \in \mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ that cannot be written as the convex sum and therefore probabilistic mixture of $\rho = \alpha\rho_1 + (1-\alpha)\rho_2$, $\alpha \in [0,1]$ of two states $\rho_1 \in \mathcal{H}_1$, $\rho_2 \in \mathcal{H}_2$ is called pure. This definition can trivially be extended to the n-partite case. However, a probabilistic mixture of this kind is not to be confused with superposition of states. A pure state can for example also be given by a superposition of again two pure product states

$$|\Psi\rangle = \frac{1}{\sqrt{2}} \left(|\psi_1\rangle \otimes |\psi_2\rangle + |\phi_1\rangle \otimes |\phi_2\rangle \right) \; . \tag{2.17}$$

Product states like $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ are states that can be written as a tensor product of their respective subsystem states. Measurements on one subsystem of a product state do not influence the state on the other subsystem, therefore the information contained in product states is precisely that of their subsystem states. Pure product states of the above form are separable, whereas states in the form of (2.17) are entangled.

Mixed states on the other hand are states one has only partial or possibly even no knowledge about. An example of such a state would be represented by an operator

$$\rho = \sum_i p_i |\phi_i\rangle\langle\phi_i| \tag{2.18}$$

in the form of a probability distribution over orthogonal states $|\phi_i\rangle$, each $|\phi_i\rangle$ occuring with probability p_i and more than one eigenvalue differing from zero.

Just as in the case of pure states, mixed product states

$$\rho = \rho_1 \otimes \rho_2 \otimes ... \rho_{n-1} \otimes \rho_n \tag{2.19}$$

do not exhibit correlations. Then again, any general mixed state that is also separable can be expressed by a convex sum over such product states and will generally exhibit classical correlations[5]

$$\rho_{sep} = \sum_i p_i \rho_1^i \otimes \rho_2^i \otimes ... \rho_{n-1}^i \otimes \rho_n^i, \qquad \sum_i p_i = 1 \; . \tag{2.20}$$

Mixed states that cannot be decomposed into such convex sums over product states are entangled.

[5]classical, as the states are defined via classical probabilities

2.2.2 Bloch Decomposition

Independent of whether it is mixed or not, any density matrix in a d-dimensional Hilbert-Schmidt space can be decomposed via the Bloch vector decomposition [24]

$$\rho = \frac{1}{d}\mathbb{I} + \vec{b} \cdot \vec{\Gamma} \, . \tag{2.21}$$

The components $b_i = \langle \Gamma_i \rangle = Tr(\rho \Gamma_i)$ constitute the Bloch vector $\vec{b} \in \mathbb{R}^{d^2-1}$ with $|\vec{b}| \leq \frac{\sqrt{d-1}}{d}$. The reverse however, is not necessarily true, as not every operator that can be written in the above form has to be a density matrix. There are points on the Bloch hypersphere which are not referring to a positive ρ and therefore do not correspond to physical states.

In the bipartite case, a density matrix $\rho \in \tilde{\mathcal{H}}_1^d \otimes \tilde{\mathcal{H}}_2^d$ can be decomposed in an analogous way

$$\rho = \frac{1}{d}\mathbb{I} \otimes \mathbb{I} + \sum_i a_i \Gamma_i \otimes \mathbb{I} + \sum_i b_i \mathbb{I} \otimes \Gamma_i + \sum_{ij} c_{ij} \Gamma_i \otimes \Gamma_j \, . \tag{2.22}$$

The family of isotropic states, which bears similarity to the class of states that will be investigated in this thesis, is invariant under local unitary transformations of the form $(U \otimes U^*)$ and can be represented by a mixture of the maximally mixed and maximally entangled pure states, the terms $a_i \Gamma_i \otimes \mathbb{I}$ and $b_i \mathbb{I} \otimes \Gamma_i$ vanish

$$\rho_{iso} = \frac{1}{d}\mathbb{I} \otimes \mathbb{I} + \sum_i c_{ii} \Gamma_i \otimes \Gamma_i \, . \tag{2.23}$$

2.2.3 Quantum Operations

A quantum operation can be defined as a map $\Lambda : \tilde{\mathcal{H}}_1 \mapsto \tilde{\mathcal{H}}_2$ from the set of density matrices $\rho_1 \in \tilde{\mathcal{H}}_1$ on a Hilbert-Schmidt space $\tilde{\mathcal{H}}_1$ to the set of density matrices $\rho_2 \in \tilde{\mathcal{H}}_2$. An axiomatic approach for embedding physical quantum operations into a mathematical formalism ascribes three properties to such a map Λ (see [19, 25]):

1. The map is trace non-increasing: $0 \leq Tr(\Lambda(\rho)) \leq 1$
2. The map is convex linear: $\Lambda\left(\sum_i p_i \rho_i\right) = \sum_i p_i \Lambda(\rho_i)$
3. The map is completely positive, i.e $\Lambda(A)$ is positive for any operator A. Even upon the inclusion of another auxiliary system R, the map $(\mathbb{I} \otimes \Lambda)(A) \geq 0$ for any A on the combined system, where $\mathbb{I}$ is the identity map on R.

Trace preserving quantum operations $Tr(\Lambda(\rho)) = Tr(\rho) = 1$ are referred to as *deterministic quantum operations*. Such operations can be described by combinations of the following processes:

1. **Unitary transformations** of a state $\rho_1 \in \tilde{\mathcal{H}}_1$ via the map $\Lambda : \tilde{\mathcal{H}}_1 \mapsto \tilde{\mathcal{H}}_1$:

$$\Lambda(\rho_1) \equiv U\rho_1 U^\dagger \tag{2.24}$$

2. Extending the system $\rho_1 \in \tilde{\mathcal{H}}_1$ by **adding an ancilla** $\rho_2 \in \tilde{\mathcal{H}}_2$, where $\Lambda : \tilde{\mathcal{H}}_1 \mapsto \tilde{\mathcal{H}}_1 \otimes \tilde{\mathcal{H}}_2$:

$$\Lambda(\rho_1) \equiv \rho_1 \otimes \rho_2 \tag{2.25}$$

3. **Partially tracing** out a system employing $\Lambda : \tilde{\mathcal{H}}_1 \otimes \tilde{\mathcal{H}}_2 \mapsto \tilde{\mathcal{H}}_1$:

$$\Lambda(\rho_1 \otimes \rho_2) \equiv Tr_2(\rho_1 \otimes \rho_2) = \rho_1 \tag{2.26}$$

Then there are *probabilistic quantum operations* where $Tr(\Lambda(\rho)) < 1$ and Λ does not completely describe the processes that affect the system.

4. **Selective measurements** on a system $\rho \in \tilde{\mathcal{H}}$, with p_i denoting the probability of measuring the i^{th} of k possible outcomes related to measurement operators A_i:

$$\Lambda(\rho_1) \equiv \rho_i = \frac{A_i \rho A_i^\dagger}{Tr(A_i \rho A_i^\dagger)} \qquad with \quad p_i = Tr(A_i \rho A_i^\dagger) \tag{2.27}$$

Generally, the measurement operators A_i corresponding to k outcomes i satisfy $\sum_i^k A_i^\dagger A_i \leq \mathbb{I}$, following directly from the trace-non-increasing relation. The map Λ in the case of selective measurements is not trace preserving and cannot be obtained by using (1)-(3).

Non-selective measurements on the other hand, are those that satisfy $Tr(\Lambda(\rho)) = 1$. If no selection takes place, the post measurement state ρ' can be written in the form of a convex sum over the possible outcomes i

$$\rho' = \sum_i A_i \rho A_i^\dagger \ . \tag{2.28}$$

By adding an ancilla to a system, letting it evolve unitarily and finally tracing over it, one can easily obtain a state in the form (2.28). To prove this claim, let $\rho' = Tr_2(U(\rho \otimes |\phi\rangle\langle\phi|)U^\dagger)$. Tracing out system 2 leads to

$$\begin{aligned} \rho' &= Tr_2(U(\rho \otimes |\phi\rangle\langle\phi|)U^\dagger) && (2.29)\\ &= \sum_\varphi \langle\varphi|U|\phi\rangle \rho \langle\phi|U^\dagger|\varphi\rangle && (2.30)\\ &= \sum_\varphi A_\varphi \rho A_\varphi^\dagger \,, \ A_\varphi = \langle\varphi|U|\phi\rangle \ . && (2.31) \end{aligned}$$

Formally, the operators A_φ are known as the Kraus operators and the description seen in (2.28) is an operator sum representation of a completely positive map.

Theorem 2.1 (Operator Sum Representation)**.** *The map Λ is completely positive, convex linear and trace non-increasing for a set $\{A_i\}$ mapping the input to the output Hilbert space and satisfying $\sum_i A_i A_i^\dagger \leq \mathbb{I}$, if and only if*

$$\Lambda(\rho) = \sum_i A_i \rho A_i^\dagger \ . \tag{2.32}$$

An elaborate proof of this theorem can be found in [19, p.368ff]. Conversely, all completely positive maps can be written in this form.

2.2.4 The Class of LOCC

Operations on quantum systems as the ones described in chapter 2.2.3 can act locally or globally.

Local operations [26] are those whose action on the subsystems of a joint system leaves them to evolve independently of each other. Such operations can be represented by the tensor product of maps acting on the corresponding subsystems. They satisfy the trace preserving condition and may be expressed via the operator sum representation in the following form for bipartite systems

$$\Lambda_{loc}(\rho) = \sum_{ij} A_i \otimes B_j \rho A_i^\dagger \otimes B_j^\dagger \qquad \text{with} \qquad \sum_{ij} A_i^\dagger A_i \otimes B_j^\dagger B_j = \mathbb{I}_{\mathcal{H}_1 \otimes \mathcal{H}_2} \ . \tag{2.33}$$

A generalization to multipartite systems is straightforward. Any correlations that exist prior to the action of local operations remain unchanged. As an example, product states $\rho = \rho_1 \otimes \rho_2$ remain product states under local operations.

$$\Lambda_{loc}(\rho) = (\sum_i A_i \rho_1 A_i^\dagger) \otimes (\sum_j B_j \rho_2 B_j^\dagger) \tag{2.34}$$

States that are separable before the action of local operations also remain separable after.

$$\Lambda_{loc}(\sum_i p_i \rho_1^i \otimes \rho_2^i) = \sum_i p_i (\sum_i A_i \rho_1^i A_i^\dagger) \otimes (\sum_j B_j \rho_2^i B_j^\dagger) \tag{2.35}$$

While local operations cannot solely invoke classical or quantum correlations, global operations on the other hand, for example in the form of global unitaries in the case of interacting systems, can cause in- and decreases of correlations.

It shall be mentioned here, that operations $U = U_1 \otimes U_2$ on a generally entangled state ρ are local symmetries of ρ if they leave the state $\rho' = (U_1 \otimes U_2)\rho(U_1 \otimes U_2)^\dagger = \rho$. As an example, the set of isotropic states are left invariant by transformations of the form

$U = U \otimes U^*$.

The concept of local operations and classical communication (LOCC) can be illustrated with respect to two parties A and B, each of them having access to one subsystem ρ_A, ρ_B of a joint system $\rho_{AB} = \rho_A \otimes \rho_B$.

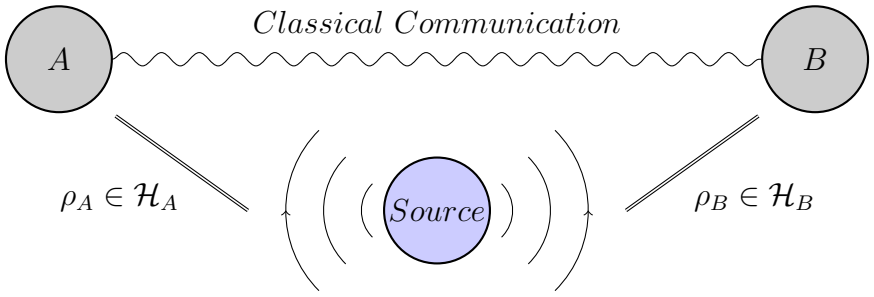

Figure 2.2.1: Schematic illustration of an LOCC scenario

LOCC now allow not only for local operations to be performed on systems ρ_A and ρ_B, but also for the exchange of information between two parties A and B via classical channels. Therefore party A could in principle condition its local operations on the classically communicated outcomes of measurements performed by B. Consequently, classical correlations can be created between subsystems by means of LOCC. Quantum correlations on the other hand, cannot.

The operator sum representation for LOCC[27] is denoted as

$$\Lambda_{LOCC}(\rho_{AB}) = \sum_i S_i \rho S_i^\dagger \,, \qquad S_i = \sum_i A_i \otimes B_i \tag{2.36}$$

with

$$A_i = A_{rn}(r(n-1), ..., r2, r1) \cdots A_{r3}(r2, r1) A_{r1} \tag{2.37}$$

$$B_i = B_{r(n-1)}(r(n-2), ..., r2, r1) \cdots B_{r4}(r3, r2, r1) B_{r2}(r1) \,. \tag{2.38}$$

The set $A_{r1} \otimes \mathbb{I}$ denotes the set of operation elements conducted by party A in round $r1$. The conducted operations are reported to party B. Party B can conduct his local operations dependent on the measurements reported in $r1$ and so on.

2.2.5 The Weyl Operator Basis

A useful unitary orthonormal basis that will readily be worked with throughout this thesis is the Weyl operator basis [24] that is given by the d^2 operators

$$W_{kl} = \sum_{n=0}^{d-1} e^{\frac{2\pi i(k\cdot n)}{d}} |n\rangle\langle (n+l) \bmod d| \,, \quad m,n = 0,...,d-1 \tag{2.39}$$

$$\mathrm{Tr}(W_{mn}^{\dagger} W_{kl}) = d \cdot \delta_{mk}\delta_{nl} \,. \tag{2.40}$$

As the Weyl operators are unitary operators, they preserve the eigenvalue spectrum and do not change the purity of the state they act on. The Weyl operators can be utilized to construct a basis of maximally entangled qudits in $\mathcal{H}_d$ [28]. This can be achieved via the local operation $(W_{kl} \otimes \mathbb{I})|\Omega_{00}\rangle$, which describes the application of the W_{kl} to one subsystem of a maximally entangled state $|\Omega_{00}\rangle = |\Phi_d^+\rangle = \frac{1}{\sqrt{d}} \sum_{s=0}^{d-1} |s\rangle \otimes |s\rangle$. This method of construction will prove to be very useful in defining the magic simplex in chapter 6.1.

The Weyl operators are related to identity and the Pauli matrices. In the case of $d = 2$, these relations are:

$$W_{00} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbb{I}_2 \tag{2.41}$$

$$W_{01} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_x \tag{2.42}$$

$$W_{10} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \sigma_z \tag{2.43}$$

$$W_{11} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = i\sigma_y \,. \tag{2.44}$$

3 Entangled Systems

Based on the concepts already derived in chapter 2.1, this chapter will offer a mathematical definition of entangled quantum systems using the Dirac notation and the density matrix formalism. Within the scope of this thesis, it suffices to consider bipartite quantum systems living in finite dimensional Hilbert spaces $\mathcal{H}_d$. Therefore, the definitions and considerations of the following chapters will be restricted mostly to such systems with finite degrees of freedom. Other theoretical concepts are taken from [24, 29, 30].

3.1 Separability and Entanglement of Bipartite Systems

Generally, bipartite systems of dimension $d = d_1 \times d_2$ can be represented by an operator $\rho \in \tilde{\mathcal{H}}_1 \otimes \tilde{\mathcal{H}}_2$ on the d-dimensional Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$ of the form

$$\rho = \sum_{i=1}^{d} p_i |\psi_i\rangle\langle\psi_i| \ . \tag{3.1}$$

These quantum states are operators over a factorization algebra M^d which are subject to the general properties of density matrices as denoted in chapter 2.2.1 equations $(1)-(3)$. The squared norm induced on $\tilde{\mathcal{H}}_1 \otimes \tilde{\mathcal{H}}_2$ by the scalar product is given by

$$||A||^2 = Tr(AA^\dagger), \qquad \forall A \in \tilde{\mathcal{H}}_1 \otimes \tilde{\mathcal{H}}_2 \ . \tag{3.2}$$

A given state ρ of the above form is then separable with respect to a factorization $M^d = M^{d_1} \otimes M^{d_2}$ if it can be rewritten via tensor products on its subspaces.

$$\rho = \sum_{i=1}^{d} p_i \rho_1^i \otimes \rho_2^i \tag{3.3}$$

Any state that cannot be written in this form is entangled with respect to the specific factorization $M^{d_1} \otimes M^{d_2}$. Separable states constitute a convex set Ω_{sep}. Given any two separable states ρ_1, ρ_2 their mixture $\rho = \alpha\rho_1 + (1-\alpha)\rho_2$ is also in Ω_{sep}.

Theorem 3.1 (Pure State Factorization)**.** *Let ρ be a pure state denoted as $\rho = |\psi\rangle\langle\psi|$. Then there exists a factorization $M^d = A_1 \otimes A_2$ with respect to which the state is separable as well as there exists another factorization $M^d = B_1 \otimes B_2$ with respect to which it appears maximally entangled.*

The proof for theorem 3.1 employs unitary operations on the given density matrix.

Proof. By use of unitary operators $U \in M^d$, the state vector $|\psi\rangle$ of a pure state can be transformed into any product vector $|\psi_1\rangle \otimes |\psi_2\rangle$ via $U|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$. Then again, U can also be chosen such that its action yields a maximally entangled state, for example $U|\psi\rangle = \frac{1}{\sqrt{d}} \sum_i |\psi_{1i}\rangle \otimes |\psi_{2i}\rangle$, with $d = min(d_1, d_2)$. □

A similar theorem can be found for the mixed case, but only with some restrictions. The necessity of these restrictions is illustrated by the fact that the maximally mixed state $\rho_{max} = \frac{1}{d}\mathbb{I}_d$ is separable with respect to any factorization.

Theorem 3.2 (Factorization in Mixed States)**.** *There exists a factorization $M^d = A_1 \otimes A_2$ for any mixed state ρ, such that it is separable with respect to that factorization. A factorization $M^d = B_1 \otimes B_2$ with respect to which ρ seems entangled exists only beyond a certain bound of mixedness.*

The proof given in [30] uses unitary transformations of an initially separable state to the Weyl state.

Proof. Suppose a mixed state $\rho = \sum_{\alpha=1}^{d} \rho_\alpha |\chi_\alpha\rangle\langle\chi_\alpha|$. One can find an orthonormal basis $|\phi_i\rangle \otimes |\psi_j\rangle$ with $i = 1, ..., d_1$ and $j = 1, ..., d_2$ of separable pure states, where the sets $\{|\phi_i\rangle\}$, $\{|\psi_j\rangle\}$ denote ONBs in $\mathcal{H}_1$, $\mathcal{H}_2$. Then a unitary operation $U|\chi_\alpha\rangle = |\phi_{i,\alpha}\rangle \otimes |\psi_{j,\alpha}\rangle$ can be performed, such that the state ρ is transformed into a separable state

$$U\rho U^\dagger = \sum_{\alpha=1}^{d} \rho_\alpha |\phi_{i,\alpha}\rangle\langle\phi_{i,\alpha}| \otimes |\psi_{j,\alpha}\rangle\langle\psi_{j,\alpha}| \; . \tag{3.4}$$

Supposing $d_1 = d_2 = d$ for simplicity, another orthonormal basis $|\chi_{kl}\rangle = \sum_j e^{\frac{2\pi i}{d} jl} |\phi_j\rangle \otimes |\psi_{j+k}\rangle$ of maximally entangled states can be found. That this basis is in fact orthonormal can be checked via the scalar product.

$$\langle\chi_{kl}|\chi_{mn}\rangle = \sum_{ij} e^{\frac{2\pi i}{d}(in-jl)} \overbrace{\langle\phi_j|\phi_i\rangle}^{\delta_{ij}} \langle\psi_{j+k}|\psi_{i+m}\rangle \tag{3.5}$$

$$= \sum_{j} e^{\frac{2\pi i}{d} j(n-l)} \overbrace{\langle\psi_{j+k}|\psi_{j+m}\rangle}^{\delta_{km}} \tag{3.6}$$

$$= \delta_{km} \overbrace{\sum_{j} e^{\frac{2\pi i}{d} j(n-l)}}^{\delta_{ln}} \tag{3.7}$$

$$= \delta_{km}\delta_{ln} \tag{3.8}$$

In the pure bipartite case, maximal entanglement can for instance be seen by considering the partial trace over the first system.

$$\rho_2 = Tr_1(|\chi_{kl}\rangle\langle\chi_{kl}|) = Tr_1(\sum_j |\phi_j\rangle\langle\phi_j| \otimes |\psi_{j+k}\rangle\langle\psi_{j+k}|) \tag{3.9}$$

$$= \frac{1}{d}\sum_j |\psi_{j+k}\rangle\langle\psi_{j+k}| \tag{3.10}$$

$$= \frac{1}{d}\mathbb{I}_d \tag{3.11}$$

If the partial trace over the first system leaves ρ_2 to be the maximally mixed state, then the initial pure state ρ is maximally entangled. Measurements on both systems would reveal maximal correlation of the outcomes.

Applying now a unitary transformation of the initial state vectors to maximally entangled state vectors yields the Weyl state.

$$U\rho U^\dagger = \sum_{j,k} \rho_k |\phi_j\rangle\langle\phi_j| \otimes |\psi_{j+k}\rangle\langle\psi_{j+k}| \tag{3.12}$$

As the set of entangled states is not convex, the Weyl state is not necessarily entangled. □

Definition 3.1 (Absolutely separable states)**.** States that are separable with respect to any splitting of a composite system into two systems are referred to as *absolutely separable states*. Such states remain separable under any global unitary transformation $\rho' = U\rho U^\dagger$.

3.1.1 Pure State Separability via Schmid's Decomposition

The entanglement of pure states can be classified via the Schmidt decomposition[25, p.236ff]. By Schmidt's Theorem, pure states can be written in a specific way.

Theorem 3.3 (Schmidt's Theorem)**.** *Given a Hilbert space $\mathcal{H}_{12}$. Every pure state in this space $\mathcal{H}_{12} = \mathcal{H}_1 \otimes \mathcal{H}_2$ can be written as*

$$|\psi\rangle = \sum_{i=1}^{d} \sqrt{\lambda_i} |a_i\rangle \otimes |b_i\rangle \tag{3.13}$$

with $\{|a_i\rangle\}_{i=1}^{d_1}$ and $\{|b_i\rangle\}_{i=1}^{d_2}$ representing orthonormal bases in H_1 and H_2 respectively and $d \leq min(d_1, d_2)$.

Proof. This Schmidt decomposition can be obtained by expressing any such state $|\psi\rangle \in \mathcal{H}_{12}$ in arbitrary bases

$$|\psi\rangle = \sum_{i=1}^{d_1} \sum_{j=1}^{d_2} C_{ij} |\hat{a}_i\rangle \otimes |\hat{b}_j\rangle \ . \tag{3.14}$$

Written in an arbitrary basis, the state $|\psi\rangle \in \mathcal{H}_{12}$ is now associated with the complex valued matrix C. Assuming $d_1 \leq d_2$ and introducing the states $|\hat{\phi}_i\rangle = \sum_j C_{ij} |\hat{b}_j\rangle$, $|\psi\rangle$ can be rewritten as

$$|\psi\rangle = \sum_{i=1}^{d} |\hat{a}_i\rangle |\hat{\phi}_i\rangle \ . \tag{3.15}$$

Partially tracing over subsystem 2 of $\rho = |\psi\rangle\langle\psi|$ leads to

$$\rho_1 = \mathrm{Tr}_2(\rho) = \sum_{i,j=1}^{d_1} \langle\hat{\phi}_j|\hat{\phi}_i\rangle |\hat{a}_i\rangle\langle\hat{a}_j| \ . \tag{3.16}$$

Now there can always be found a local unitary basis transformation to another basis $|a_i\rangle \in \mathcal{H}_1$ such that ρ_1 takes a diagonal form with real, non-negative coefficients λ_i.

$$\rho_1 = \sum_{i=1}^{d_1} \lambda_i |a_i\rangle\langle a_i| \tag{3.17}$$

Comparing (3.16) and (3.17) and using the diagonal basis $\{|a_i\rangle\}$ from the start yields the relations

$$\langle\hat{\phi}_j|\hat{\phi}_i\rangle = \lambda_i \delta_{ij} \tag{3.18}$$

$$|\hat{\phi}_i\rangle = \sqrt{\lambda} |\hat{b}_j\rangle \ . \tag{3.19}$$

Losing the hat notation, this leads to the Schmidt decomposition as given in (3.3). □

Another brief derivation of the Schmidt decomposition can be carried out using singular value decomposition (SVD)[26]. It empolys the identities $\mathbb{I}_1 = \sum_i U^\dagger|\hat{a}_i\rangle\langle\hat{a}_i|U \in \mathcal{H}_1$ and $\mathbb{I}_2 = \sum_i V^\dagger|\hat{b}_i\rangle\langle\hat{b}_i|V \in \mathcal{H}_2$, where U and V are local unitary opertions on the respective subspaces. Inserting the identities into (3.14) the state $|\psi\rangle$ can be rewritten as

$$|\psi\rangle = \sum_{ij} [\mathcal{U}C\mathcal{V}]_{ij}\, U^\dagger|\hat{a}_i\rangle \otimes V^\dagger|\hat{b}_j\rangle \ . \tag{3.20}$$

The matrices $\mathcal{U}$ and $\mathcal{V}$ are defined as

$$\mathcal{U}_{ij} = \langle\hat{a}_i|U|\hat{a}_j\rangle \tag{3.21}$$

$$\mathcal{V}_{ij} = \langle\hat{b}_j|V|\hat{b}_i\rangle \ . \tag{3.22}$$

Now due to SVD, there exist two unitary matrices $\mathcal{U}$ and $\mathcal{V}$ for every complex valued matrix C such that $S = \mathcal{U}C\mathcal{V}$ becomes diagonal. Then S represents the singular value decomposition of C and the non-negative and real valued elements S_i are referred to as singular values. Any state can then be represented by its Schmidt coefficients $\lambda_i = S_i^2$ using the Schmidt basis $|a_i\rangle \otimes |b_i\rangle = U^\dagger|\hat{a}_i\rangle \otimes V^\dagger|\hat{b}_i\rangle$. This yields again the Schmidt decomposition as denoted in equation (3.3).

The Schmidt coefficients λ_i are subject to the properties

$$\sum_i \lambda_i = 1 \tag{3.23}$$

$$\lambda_i \geq 0 \ . \tag{3.24}$$

As the Schmidt basis is formed by separable states, the classification in terms of entanglement of the state $|\psi\rangle$ is contained solely in the Schmidt coefficients. The Schmidt rank refers to the number r of non-vanishing coefficients of $|\psi\rangle$. Only if $r = 1$, the total state is separable. If $r > 1$, the pure bipartite state is entangled. Local unitary operations do not change the Schmidt coefficients. Governing the Schmidt rank can be achieved in employing the partial trace on one, preferrably the smaller dimensionate, subsystem and computing its spectrum.

In the case of pure states, the degree of mixing in the reduced density matrices can be related to the notion of separability of the total state. A maximally mixed reduced state corresponds to a maximally entangled total state and a pure reduced states is related to a separable composite system.

3.1.2 Mixed State Separability via Positive Maps

In his seminal paper [2], Asher Peres was among the first to introduce the concept of employing a positive map, in his case partial transposition of a subsystem, in order to

decide upon the separability of a given quantum system. The Horodeckis [5, 6] later generalized his concepts to the use of positive but not completely positive maps, providing a sufficient criterion for characterizing the separability of arbitrary mixed states.

The starting basis is to use the insights on the general representation of separable states already provided in equation (3.3). Now a map $\Lambda : \tilde{\mathcal{H}}_1 \to \tilde{\mathcal{H}}_2$ is positive if and only if $\Lambda(A) \geq 0$ for all positive operators $A \in \tilde{\mathcal{H}}_1$. As already mentioned in chapter 2.2.3, if the extension $\mathbb{I} \otimes \Lambda_A(A)$ remains positive for any A, the map is completely positive.

For any positive map Λ on a subsystem of a separable state it holds

$$(\mathbb{I} \otimes \Lambda)\rho_{sep} = \sum_i p_i \rho_1^i \otimes \Lambda(\rho_2^i) \geq 0 \; . \tag{3.25}$$

The idea in using positive maps as a separability criterion now hinges on the notion that for inseparable states, the extended maps might yield $(\mathbb{I} \otimes \Lambda)\rho_{ent} \leq 0$.

Although the extended linear map $\mathbb{I} \otimes \Lambda$ is not completely positive, the assumption of positivity of Λ results in a positive spectrum of $\Lambda(\rho_2^i)$ and lastly $(\mathbb{I} \otimes \Lambda)\rho_{sep} \geq 0$ in the case of separable states. Concluding, for any separable state it holds that $(\mathbb{I} \otimes \Lambda)\rho_{sep} \geq 0$.

The converse assumption that extended linear maps upon which ρ remains positive imply the separability of ρ does however not hold in general. There can exist entangled states for which $(\mathbb{I} \otimes \Lambda)\rho_{ent} \geq 0$.

Introduced by Peres, partial transposition of a subsystem represents one example of a positive but not completely positive map that consitutes a readily used separability criterion, referred to as the PPT[6] criterion. States that are not positive under partial transposition are certainly entangled. It turns out to be a necessary and sufficient criterion for the characterization of states in $d_1 \otimes d_2$ with respect to separability if $d_1 d_2 \leq 6$. Sufficiency in these cases follows from the fact that in these low dimensions, all positive maps are decomposable as $\Lambda_{Dec} = \Lambda_1^{CP} + \Lambda_2^{CP} \circ T$. It can be shown that no other decomposable maps besides transposition can reveal entanglement which is not already found via transposition.

In $d_1 d_2 > 6$, the PPT criterion is only necessarily able to distinguish separable from entangled states. It is however not sufficient and there exist entangled states with remain positive under partial transposition. These states are referred to as *PPT bound entangled states*.

[6] positive partial transpose

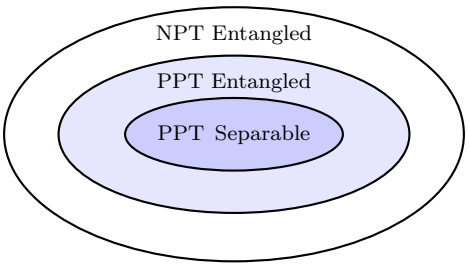

Figure 3.1.1: Separability under PPT ($d_1 d_2 > 6$)

For the detection of such states that are PPT and entangled see chapter 5.

3.2 Multipartite Entanglement

In the multipartite case, the notion of separability is similar to that introduced in the bipartite case, but now distinctions between full n-party separability and partial separability arise. Both notions will be explained using definitions from [6, 31], where the interested reader can find more detailed information.

Definition 3.2 (k-separability)**.** An n-partite pure state is k-separable iff it can be expressed via product states of k subsystems.

$$|\psi_{k-sep}\rangle = \sum_{i=1}^{k} |\psi_i\rangle^{\otimes k} \tag{3.26}$$

A mixed state is k-separable iff it can be decomposed into k-separable pure states.

$$\rho_{k-sep} = \sum_i p_i |\psi^i_{k-sep}\rangle\langle\psi^i_{k-sep}| \tag{3.27}$$

A k-separable mixed state can be separable with respect to certain partitions. A state that is not $2-separable$ is genuine multipartite entangled.

PPT criteria do not sufficiently characterize separability of m-partite systems. However, there are a multitude of criteria that can be used to gain more information on the inseparability of n-partite quantum states. One particularly useful criterion for detecting genuine multipartite entanglement that can be found and is also proven in [31] relies on permutations on copies of a state ρ and states that:

Theorem 3.4. *It holds for every k-separable state that*

$$\sqrt{\langle\psi_{n-sep}|\rho^{\otimes 2} P_{tot}|\psi_{n-sep}\rangle} - \sum_{\{\alpha\}} \left(\prod_{i=1}^{k} \langle\psi_{n-sep}| P^{\dagger}_{\alpha i} \rho^{\otimes 2} P_{\alpha i} |\psi_{n-sep}\rangle \right)^{\frac{1}{2k}} \leq 0 \,. \tag{3.28}$$

The operators $P_{\alpha i}$ permute the two copies gained by $\rho^{\otimes 2}$ of all subsystems constituting the i^{th} subset of partition α and P_{tot} denotes the total permutation operator.

An advantage this criterion may provide is that it does not rely on the computation of eigenvalues. Due to its expression in terms of density matrices, it also qualifies as a simplified method for experimental realizations because it limits the measurements needed for full state-tomography to $2^n - 1$ for any fixed $|\psi_{n-sep}\rangle$ and is therefore also independent of the dimension of the subsystems.

3.3 Bound Entanglement

In quantum physical experiments imperfect preparation methods and decoherence significantly contribute to the fact that in reality, one is predominantly and inevitably dealing with mixed states. As many quantum information theoretic purposes exploit the use of pure maximally entangled states, e.g. the Bell-type state $|\Omega_{00}\rangle = \frac{1}{\sqrt{d}} \sum_{s=0}^{d-1} |ss\rangle$, the aim of noise reduction in experimental setups prompts the search for protocols of purifying arbitrary entangled states, in the sense of gaining states that are close to maximally entangled pure states. Fidelity [25] provides such a measure of closeness of two states.

$$\mathcal{F}(\rho_1, \rho_2) = \left(Tr\big(\sqrt{\sqrt{\rho_1}\rho_2\sqrt{\rho_1}}\big) \right)^{\frac{1}{2}} \tag{3.29}$$

In the case of $\rho_1 = |\psi\rangle\langle\psi|$ being a pure state, it reduces to

$$\mathcal{F}(\rho_1, \rho_2) = \langle\psi|\rho_2|\psi\rangle \ . \tag{3.30}$$

The procedure of achieving the purification of entangled mixed states via LOCC is referred to as *distillation of entanglement* [6, 32]. The basic idea is the following: Suppose two observers, each in possession of n quantum systems that originate from entangled pairs, prepared in a state ρ. Both parties are allowed to perform LOCC on their particles, such that they then obtain some number $k(n) < n$ copies of ρ denoted by $\sigma^{\otimes k}$ which are in a state close to pure maximally entangled states, such that $\langle\psi^{\otimes k}|\sigma^{\otimes k}|\psi^{\otimes k}\rangle \to 1$. The question is then how many k pure maximally entangled states can be distilled employing certain entanglement purification protocols.

The ratio $R_P = lim_{n\to\infty}\frac{k(n)}{n}$ denotes the rate of distillation of a protocol P. The supremum of these rates over all possible protocols P is referred to as *distillable entanglement* E_D. If no entanglement can be distilled, then $E_D = 0$.

Contrary to formerly common assumptions, it has been shown that there exist mixed entangled states which cannot be brought into a pure maximally entangled form via means of LOCC [1, 7]. These states are called *bound entangled*. Interestingly, all states that are distillable have been shown [7] to violate PPT. For PPT entangled states, this evidently implies their non-distillability. The question of whether there exist NPT bound entangled states is still open [11, 12]

4 Mutually Unbiased Bases

4.1 The Notion of Mutual Unbiasedness

In his seminal publication [33], Schwinger was among the first to put emphasis on the complementarity of unitary operators.

He establishes that two unitary operators A and B representing parameters of a physical system of d degrees of freedom are called complementary, if:

1. they both are generators of complete, orthonormal operator bases, having d non-degenerate, usually complex eigenvalues.

$$\text{Orthonormality :} \qquad \langle v_{a,i}|v_{a,j}\rangle = \delta_{ij} = \langle v_{b,i}|v_{b,j}\rangle \tag{4.1}$$

$$\text{Completeness Relation :} \qquad \sum_{i=1}^{d} |v_{a,i}\rangle\langle v_{a,i}| = \sum_{i=1}^{d} |v_{b,i}\rangle\langle v_{b,i}| = 1 \tag{4.2}$$

$$\text{Nondegeneracy of eigenvalues :} \qquad \lambda_{a,i} \neq \lambda_{a,j} \tag{4.3}$$

2. all normalized vectors $|v_{a,i}\rangle, |v_{b,i}\rangle$ of the two operator bases are maximally incompatible, such that the probability $p(v_{a,i}, v_{b,j})$ for a≠b becomes $\frac{1}{d}$.

$$\begin{aligned} \text{Mutual Unbiasedness :} \qquad p(v_{a,i}, v_{b,j}) &\overset{a\neq b}{=} |\langle v_{a,i}|v_{b,j}\rangle|^2 \\ &\overset{a\neq b}{=} \delta_{a,b}\delta_{i,j} + \frac{1}{d}(1-\delta_{a,b}) \\ &\overset{a\neq b}{=} \frac{1}{d} \end{aligned} \tag{4.4}$$

This definition of complementarity is generally not restricted to unitary operators. It becomes clear from the mathematical description of mutual unbiasedness, that all outcomes of systems prepared in - say an eigenstate of A - are equally likely when the prepared system is measured in any eigenbasis of operator B. Therefore, the probabilities p($v_{a,i}$,$v_{b,j}$) are independent of the choice of quantum numbers i,j. The properties ascribed to A and B are maximally incompatible [34].

4.2 Constructions of MUBs from Finite Fields

The construction of mutually unbiased bases from finite fields will be outlined with respect to the works of Klappenecker and Roetteler [35] and Wootters and Fields [36]. The derivations of the construction methods involving finite fields are split into two parts, one for odd and one for even prime powers. This is due to the limited use of Weil sums (see Lemma 4.1), whose properties can only be exploited for the purpose of MUB constructions in dimensions of odd prime powers. Even prime power MUBs will be assembled by using exponential sums over Galois rings.

4.2.1 Odd Prime Powers

The following lemma is presumed without proof [35].

Lemma 4.1 (Weil Sums)**.** *Let the finite field $\mathbb{F}_q$ be of odd characteristic, the polynomial $p(x)$ be of degree 2 and $\chi(\theta) : \mathbb{F}_q \to \mathbb{C}^\times$ be a non-trivial additive character of $\mathbb{F}_q$ of the form*

$$\chi(\theta) = \omega_p^{tr(\theta)}, \quad \omega_p = e^{2\pi i/p} \tag{4.5}$$

where tr() denotes the absolute trace with respect to the prime field $\mathbb{F}_p$. Then the Weil sum, provided it is not degenerate, is given by

$$\left| \sum_{x \in \mathbb{F}_q} \chi(p(x)) \right| = \sqrt{q} \, . \tag{4.6}$$

Theorem 4.2. *For a finite field $\mathbb{F}_q$ of odd characteristic, $x \in \mathbb{F}_q$, q bases B_a=$\{v_{a,b} | b \in \mathbb{F}_q\}$ of q+1 complete mutually unbiased bases (with inclusion of the standard basis) are obtained by the following set of vectors*

$$v_{a,b} = q^{-\frac{1}{2}} \omega_p^{tr(ax^2+bx)} \, . \tag{4.7}$$

A proof for this construction can be made by considering the definition of mutual unbiasedness of two vectors $v_{a,b}$, $v_{c,d}$.

Proof. See the absolute of the scalar product of two vectors.

$$\left| \langle v_{a,b} | v_{c,d} \rangle \right| = \left| \frac{1}{q} \sum_{x \in \mathbb{F}_q} \omega_p^{tr((a-c)x^2+(b-d)x)} \right| = \begin{cases} 1 & \text{if } a = c, \quad b = d \\ 0 & \text{if } a = c, \quad b \neq d \\ q^{-\frac{1}{2}} & \text{if } a \neq c \end{cases} \tag{4.8}$$

□

As the coefficient of each vector $v_{a,b}$ is equal to the absolute of $q^{-\frac{1}{2}}$, all bases B_a are mutually unbiased with respect to the standard basis. They are also mutually unbiased to each other, as for $b = d$, the absolute yields $q^{-\frac{1}{2}}$. Furthermore, all q vectors of the same basis ($a = c$) are pairwise orthogonal to each other. As the norm of each $v_{a,b}$ is equal to 1, the bases B_a are orthonormal bases.

An explicit example for the construction of odd-dimensional MUBs will be illustrated here for q=5.

$$B_0 = (v_{0,0}, v_{0,1}, v_{0,2}, v_{0,3}, v_{0,4}) = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 \\ 1 & \omega^2 & \omega^4 & \omega & \omega^3 \\ 1 & \omega^3 & \omega & \omega^4 & \omega^2 \\ 1 & \omega^4 & \omega^3 & \omega^2 & \omega \end{pmatrix} \tag{4.9}$$

The vectors $v_{0,i}$ are represented by the columns of matrix B_0. The other bases are given below.

$$B_1 = \{v_{1,0}, v_{1,1}, v_{1,2}, v_{1,3}, v_{1,4}\} = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ \omega & \omega^2 & \omega^3 & \omega^4 & 1 \\ \omega^4 & \omega & \omega^3 & 1 & \omega^2 \\ \omega^4 & \omega^2 & 1 & \omega^3 & \omega \\ \omega & 1 & \omega^4 & \omega^3 & \omega^2 \end{pmatrix} \tag{4.10}$$

$$B_2 = \{v_{2,0}, v_{2,1}, v_{2,2}, v_{2,3}, v_{2,4}\} = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ \omega^2 & \omega^3 & \omega^4 & 1 & \omega \\ \omega^3 & 1 & \omega^2 & \omega^4 & \omega \\ \omega^3 & \omega & \omega^4 & \omega^2 & 1 \\ \omega^2 & \omega & 1 & \omega^4 & \omega^3 \end{pmatrix} \tag{4.11}$$

$$B_3 = \{v_{3,0}, v_{3,1}, v_{3,2}, v_{3,3}, v_{3,4}\} = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ \omega^3 & \omega^4 & 1 & \omega & \omega^2 \\ \omega^2 & \omega^4 & \omega & \omega^3 & 1 \\ \omega^2 & 1 & \omega^3 & \omega & \omega^4 \\ \omega^3 & \omega^2 & \omega & 1 & \omega^4 \end{pmatrix} \tag{4.12}$$

$$B_4 = \{v_{4,0}, v_{4,1}, v_{4,2}, v_{4,3}, v_{4,4}\} = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ \omega^4 & 1 & \omega & \omega^2 & \omega^3 \\ \omega & \omega^3 & 1 & \omega^2 & \omega^4 \\ \omega & \omega^4 & \omega^2 & 1 & \omega^3 \\ \omega^4 & \omega^3 & \omega^2 & \omega & 1 \end{pmatrix} \tag{4.13}$$

4.2.2 Even Prime Powers (= Powers of 2)

The construction of mutually unbiased bases for $q = 2^m$ is different, because Lemma 3.1 does not hold for powers of 2.

$$\left| \sum_{x \in \mathbb{F}_{2^m}} e^{\frac{2\pi i}{2} tr(ax^2 + bx)} \right| = 0, \qquad \forall a, b \in \mathbb{F}_{2^m}$$

Therefore, the properties of Weil sums cannot be exploited in this case.

Furthermore, the construction now relies upon the use of irreducible polynomials of degree n over Galois rings GR(4,n), instead of the simple Galois fields $\mathbb{F}_{p^m}$ used previously. A closer look at the exponent of expression 4.7 reveals why.

$$v_{a,b} = 2^{-\frac{m}{2}} e^{\frac{2\pi i}{2} tr(ax^2+bx)} \tag{4.14}$$

The square roots of unity in the exponent are real and therefore do not fully characterize the complex state space, which leads to wrong arithmetics in field extensions of $\mathbb{F}_2$. Taking the fourth root of unity instead solves this problem of constructing MUBs for powers $m > 1$ of $p = 2$.

The set $\mathcal{T}_n$ of a Galois ring GR(q,n)=$\mathbb{Z}_q[x]/\langle h(x)\rangle$[7] denotes the Teichmüller set of representatives. It is a subset of the ring, with ξ being a root of $h(x)$. Any element r$\in$ GR(4,n) has a unique expression of the form $r = a + 2b$ with $a \neq 0$, where $a, b \in \mathcal{T}_n = \{0, 1, \xi, \xi^2, ..., \xi^{2^n-2}\}$. This has been proven in [37, p.82f].

Lemma 4.3 (Exponential Sum over GR(4,n))**.** *The exponential sum* $\Gamma(r)$ *which is now a function from* GR(4,n)$\to \mathbb{C}$ *is*

$$\Gamma(r) = \sum_{x \in \mathcal{T}_n} e^{\frac{2\pi i}{4} tr(rx)} \ . \tag{4.15}$$

$$\tag{4.16}$$

Its absolute value yields

$$|\Gamma(r)| = \begin{cases} 0 & if \quad r \neq 0 \quad \text{and} \quad r \in 2\mathcal{T}_n \\ 2^n & if \quad r = 0 \\ 2^{\frac{n}{2}} & \text{otherwise} \ . \end{cases} \tag{4.17}$$

Lemma 4.3 provides the basis for the construction of MUBs in even prime power dimensions.

Theorem 4.4. *Assume a and b to be elements of the the Teichmüller set $\mathcal{T}_n$ of the finite Galois ring* GR(4,n)*. Let B_a be a basis comprised of the set of vectors $\{v_{a,b} | b \in \mathcal{T}_n\}$ given by*

$$v_{a,b} = 2^{-\frac{n}{2}} e^{\frac{2\pi i}{4} tr((a+2b)x)}, \qquad x \in \mathcal{T}_n \ . \tag{4.18}$$

Then the standard basis and the bases B_a constitute a set of $q+1=2^n+1$ complete mutually unbiased bases in $\mathbb{C}^{2^n}$.

[7] $\langle h(x)\rangle$ denotes the principal ideal of $\mathbb{Z}[x]$ generated by the irreducible polynomial $h(x)$, for more information see [18]

Again, a proof can be made by considering the absolute of the scalar product of $\left|\langle v_{a,b}|v_{c,d}\rangle\right|$, this time using lemma 4.3.

Proof.

$$\left|\langle v_{a,b}|v_{c,d}\rangle\right| = \left|\frac{1}{q}\sum_{x\in\mathbb{F}_q}\omega_p^{tr((a-c)+(b-d)x)}\right| = \begin{cases} 1 & \text{if } a=c, \quad b=d \\ 0 & \text{if } a=c, \quad b\neq d \\ 2^{-\frac{n}{2}} & \text{if } a\neq c \end{cases} \tag{4.19}$$

□

The simplest example for such a construction of MUBs would be made considering $q = 2^2$. The polynomial $x^2 + x + 1$ is then an irreducible polynomial (in 2) of degree n. Its roots are contained in $\mathcal{T}_2 = \{0, 1, 3 + 3\xi, \xi\}$. One obtains the following sets of MUBs B_a:

$$B_0 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{pmatrix} \tag{4.20}$$

$$B_1 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & 1 \\ -i & i & i & -i \\ -i & i & -i & i \end{pmatrix} \tag{4.21}$$

$$B_{3+3\xi} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ -i & -i & i & i \\ -i & i & i & -i \\ -1 & 1 & -1 & 1 \end{pmatrix} \tag{4.22}$$

$$B_\xi = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ -i & -i & i & i \\ -1 & 1 & 1 & -1 \\ -i & i & -i & i \end{pmatrix} \tag{4.23}$$

$$\tag{4.24}$$

4.3 Constructions of MUBs using the Generalized Pauli Group

A pair of mutually unbiased bases can be obtained by performing the discrete Fourier transformation on vectors of the computational basis via

$$|\hat{j}\rangle = \frac{1}{\sqrt{d}} \sum_k \omega^{-jk} |k\rangle, \qquad \omega = e^{\frac{2\pi i}{d}} \ . \tag{4.25}$$

It can be checked, that the two bases are then mutually unbiased by construction

$$\langle \hat{j}|k\rangle = \frac{1}{\sqrt{d}} \omega^{jk} \ . \tag{4.26}$$

In analogy to the Pauli matrices, one can construct cyclic unitary operators X and Z which then satisfy [34]

$$X|\hat{j}\rangle = |\hat{j}\rangle\omega^j, \qquad X^d = 1 \ , \tag{4.27}$$

$$Z|k\rangle = |k\rangle\omega^k, \qquad Z^d = 1 \ . \tag{4.28}$$

Explicitly and in the computational basis, these operators can be expressed via

$$X = \sum_{k=0}^{d-1} |(k+1 \mod d)\rangle\langle k| \tag{4.29}$$

$$Z = \sum_{k=0}^{d-1} \omega^k |k\rangle\langle k| \ . \tag{4.30}$$

They are subject to the Weyl commutation rule.

$$X^m Z^n = \omega^{-nm} Z^n X^m \tag{4.31}$$

The operators $Y^{lmn} = \omega^l X^m Z^n$ constitute the generalized Pauli group [38], also known as Heisenberg-Weyl group of unitary operators. It is a (non-abelian) group with respect to matrix multiplication and its elements are defined by the phases ω^l and the generalized Pauli operators X^m, Y^n. The group law is given by

$$Y_{lmn} Y_{kij} = Y_{l+k+ni,m+i,n+j} \ . \tag{4.32}$$

For d being any prime, the following operators of the Pauli group are complementary and can be used for the construction of mutually unbiased bases

$$X, Z, XZ^2, ..., XZ^{d-1} \ . \tag{4.33}$$

Calculating the eigenbases of all these operators will then yield a complete set of $d+1$ mutually unbiased bases.

In the case of $d = p^m$, it is possible to extend the method of construction via generalized Pauli matrices by employing again finite field arithmetics. The tensor products of the operators X and Z can be considered to act on parts $\mathbb{C}_p$ on the Hilbert space $\mathcal{H} = \mathbb{C}_p^1 \otimes \cdots \otimes \mathbb{C}_p^m$. One can then re-define the shifts in (4.27) and (4.28) as m shifts modulo p with $l = (0, 1, ..., d-1)$.

$$V_l^0 = X^l = \sum_{k=0}^{d-1} |k \oplus l\rangle\langle k| \tag{4.34}$$

$$V_0^l = Z^l = \sum_{k=0}^{d-1} \omega^{(k \odot l)} |k\rangle\langle k| \tag{4.35}$$

Here, the operations $\oplus$ and $\odot$ denote addition and multiplication of finite field elements and are chosen for reasons of clarity. For $l = 1$, these operators are p-periodic and equivalent to those derived for the prime case. A set of $d+1$ mutually unbiased bases can be found via construction of $d+1$ commuting sets - containing d elements - from the d^2 unitary operators

$$V_i^j = V_0^j V_i^0 = \sum_{k=0}^{d-1} \omega^{(k \oplus i) \odot j} |k \oplus i\rangle\langle k| \ . \tag{4.36}$$

5 Entanglement Witnesses

5.1 Mathematical Definition

In the most general sense, entanglement witnesses [29] are linear or non-linear functionals of a density matrix ρ, who serve as a distinctive operational measure of separability. Although they are not always easy to construct, they are mathematically precisely defined.

Definition 5.1. Assuming an arbitrary entangled state $\rho_{ent} \in \mathcal{H}_d$, a hermitian operator $W \in \mathcal{H}_d$ is called an entanglement witness iff

$$\mathrm{Tr}\left(W\rho_{ent}\right) < 0 \tag{5.1}$$

$$\mathrm{Tr}\left(W\rho\right) \geq 0 \qquad \forall \rho \in \Omega_{sep}\ . \tag{5.2}$$

Proving 5.2 for all states in Ω_{sep} is generally an NP-hard problem and therefore typically not a trivial endeavor, depending on the families of states that are considered.

The set of entangled states in $\mathcal{H}_d$ that are detected by an entanglement witness W is defined by

$$E_W = \left\{\rho \in \Omega\left(\mathcal{H}_d\right) | \mathrm{Tr}\left(W\rho\right) < 0\right\}\ . \tag{5.3}$$

Witnesses and PNCP (positive but not completely positive) maps are related via the Choi-Jamiolkowski isomorphism [25, p.244ff, 6], which establishes an association of a linear map Λ with a Hilbert space $\mathcal{H}_d \otimes \mathcal{H}_d$.

$$W_\Lambda = \left[\mathbb{I} \otimes \Lambda\right] P_d^+ \tag{5.4}$$

The operator P_d^+ denotes the Bell projector $P_d^+ = |\Phi_d^+\rangle\langle\Phi_d^+|$. Decomposable witnesses $W_{dec} = aP + bQ^\Gamma$ - with $Q, P \geq 0$ and Γ denoting the partial transposition of a subsystem - which are associated with decomposable maps are not able to detect PPT bound entanglement, as they define the set of all states satisfying PPT. Indecomposable witnesses related to indecomposable PNCP maps may be used to detect bound entanglement.

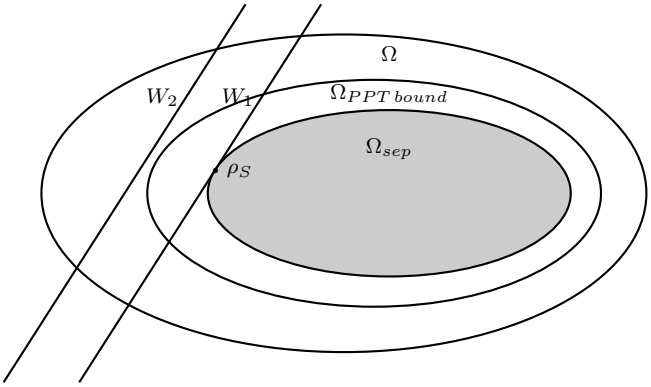

Figure 5.1.1: Entanglement witnesses and geometrical optimality

A witness W_1 is finer than $W_2 = (1-\epsilon)W_1 + \epsilon P$ with $0 \leq \epsilon < 1$ and $P \geq 0$ if it detects all the entangled states that are detected by W_2.

Generally, a witness W_1 is referred to as optimal, if no other witness W_2 can be found such that W_2 is finer than W_1. Witness W_1 in figure 5.1.1 is optimal in a geometrical sense, as it defines a plane that is tangential to the set Ω_{sep} and there exists one separable state ρ_S such that $\mathrm{Tr}\,(W\rho_S) = 0$. There exists no positive operator P that can be substracted from W_1 in order to make it finer, such that $W_1' = (1-\epsilon)W_1 - \epsilon P$ is still an entanglement witness.

There exist a variety of methods on how to construct optimal entanglement witnesses. For more information, the interested reader is recommended to [39].

5.2 Witnesses from Mutually Unbiased Bases

As already described previously, mutually unbiased bases are maximally complementary in the sense that any outcome of a measurement on a state prepared in a basis which is mutually unbiased to the measurement basis is purely random.

Mutually unbiased bases can be related to separability of a state [16]. In the case of bipartite systems on $\mathcal{H}_d \otimes \mathcal{H}_d$, $\mathcal{H}_1$ and $\mathcal{H}_2$ shall denote two d-dimensional subsystems. Measurements on those subsystems then yield d different outcomes $\{0, 1, ..., d-1\}$.
A correlation function for two observables a on $\mathcal{H}_1$ corresponding to an orthonormal basis $\{|i_a\rangle\}$ and b on $\mathcal{H}_2$ with the set $\{|i_b\rangle\}$ can then be defined as

$$C_{ab} = \sum_{i=0}^{d-1} \sum_{j=0}^{d-1} P_{ab}(i,j) \tag{5.5}$$

where $P_{ab}(i,j)$ represents the joint probability of obtaining outcomes i and j from a measurement on a and b respectively. Generally, the following the joint probability is expressed as

$$P_{ab}(i,j) = \langle i_a| \otimes \langle j_b|\rho|j_b\rangle \,.\otimes |i_a\rangle \tag{5.6}$$

Fully correlated observables will give $C_{ab} = 1$, while completely uncorrelated observables will yield $C_{ab} = \frac{1}{d}$. In order to establish a link between these correlation functions and the separability of a state, measurement in at least another combination of bases a' and b' has to be considered. If one would only measure both observables in one set of bases, the correlation C_{ab} would yield equal values for a classically correlated separable state $\rho_{cc}^{sep} = \sum_i |\lambda_i|^2 |i_a\rangle\langle i_a| \otimes |i_b\rangle\langle i_b|$ and a pure entangled state $|\psi^{ent}\rangle = \sum_i \lambda_i |i_a\rangle \otimes |i_b\rangle$, namely $C_{ab} = 1$. This illustrates that a distinction between separable and entangled would not be possible in this case.

One can then define [16] the quantity $I_m = \sum_{k=1}^{m} C_{kk}$ as the sum over all correlations C_{kk} measured with respect to m mutually unbiased bases B_k.

Theorem 5.1 (MUB Criterion)**.** *For all separable states and a set of m MUBs, the following upper bound can be achieved*

$$I_m = \sum_{k=1}^{m} C_{kk} \leq 1 + \frac{m-1}{d} \,. \tag{5.7}$$

Proof. Suppose first a pure product state $|\psi\rangle = |a\rangle \otimes |b\rangle$, $|\psi\rangle \in \mathcal{H}_d \otimes \mathcal{H}_d$. Then for I_m it follows

$$I_m = \sum_{k=1}^{m} C_{kk} = \sum_{k=1}^{m} \sum_{i=0}^{d-1} |\langle i_k|a\rangle|^2 |\langle i_k|b\rangle|^2 \,. \tag{5.8}$$

For any real, non-negative number n one can employ the inequality of arithmetic and geometric means $(x_1 + x_2 + ... + x_n)/n \geq \sqrt[n]{x_1 \cdots x_n}$, yielding

$$I_m \leq \frac{1}{2} \sum_{k=1}^{m} \sum_{i=0}^{d-1} \left(|\langle i_k|a\rangle|^4 + |\langle i_k|b\rangle|^4 \right) . \tag{5.9}$$

Using the definition of mutual unbiasedness $|\langle i_a|i_b\rangle|^2 = \frac{1}{d}$, one can now infer that for pure product states it holds

$$I_m \leq 1 + \frac{m-1}{d} \,. \tag{5.10}$$

As every mixed separable state can be represented by a convex combination of pure product states and I_m is linear, it is by the argument of linearity that the criterion also holds for such mixed states.

□

For $d+1$ complete sets of MUBs, it holds

$$I_m = \sum_{k=1}^{m} C_{kk} \leq 2 \; . \tag{5.11}$$

In [16] it was shown, that as many as two mutually unbiased bases already suffice in detecting pure state entanglement in bipartite qudit systems in $\mathbb{C}^d \otimes \mathbb{C}^d$. Additionally, an alternate proof for the existence of at most $d+1$ MUBs was given by hypothetically considering the existence of $m > d+1$ MUBs, which could result in falsely detecting separable states to be entangled. Using a complete set of $d+1$ MUBs, the quantity $2 - I_{d+1}$ may serve as a witness for bound entanglement detection. How to achieve the detection of bound entanglement using the defined quantity will be shown in chapter 6.2.

6 Geometry of Bipartite Systems

6.1 The Magic Simplex

A convex subset $\mathcal{S}$ in an affine space [25] is a collection of points where for any two points x_1, x_2 belonging to this set, it holds that a mixture x also belongs to it.

$$x = \lambda_1 x_1 + \lambda_2 x_2 \in \mathcal{S}, \quad \lambda_1 + \lambda_2 = 1, \quad \lambda_i \geq 0 \tag{6.1}$$

The convex hull is then defined as the smallest convex set containing subset $\mathcal{S}$. If a collection of $p+1$ points is not confined to a $p-1$-dimensional space, then its convex polytope[8] is referred to as a p-simplex. Analogously, for a p-simplex of $p+1$ points it holds

$$x = \sum_{i=0}^{p} \lambda_i x_i, \quad \sum_{i=0}^{p} \lambda_i = 1, \quad 0 \leq \lambda_i \leq 1 \ . \tag{6.2}$$

While this is not always the case for a convex set $\mathcal{S}$, take for example a circular disk where it might not be possible to obtain any x from finitely many pre-determined pure points, *every* point x within a simplex may be uniquely defined by a convex combination of at most $p+1$ of its pure points.

The magic simplex is a construction that relies upon the properties of a simplex defined by a collection of $d+1$ pure states on a Hilbert space $\mathcal{H}_d$. The special simplex $\mathcal{W}$ that will be investigated within the scope of this thesis is a simplex spanned by $d+1$ pure Bell states [40].

$$\mathcal{W} = \Big\{ \sum_{kl} c_{kl} P_{kl} |\, c_{kl} \geq 0, \sum_{kl} c_{kl} = 1 \Big\} \tag{6.3}$$

The $P_{kl} = |\Omega_{kl}\rangle\langle\Omega_{kl}|$ are projectors onto the maximally entangled bipartite Bell-type states $|\Omega_{kl}\rangle$, which constitute the only pure points of the simplex. Starting from the state

$$|\Omega_{00}\rangle = \frac{1}{\sqrt{d}} \sum_{s} |s\rangle \otimes |s\rangle \tag{6.4}$$

all d remaining Bell-type states can be governed via

$$|\Omega_{kl}\rangle = (W_{kl} \otimes \mathbb{I})|\Omega_{00}\rangle \tag{6.5}$$

$$P_{kl} = (W_{kl} \otimes \mathbb{I}) P_{00} (W_{kl}^{\dagger} \otimes \mathbb{I}) \tag{6.6}$$

[8] A convex polytope is the convex hull of a finite set of points x_i

where the $W_{kl} = \sum_{j=0}^{d-1} e^{\frac{2\pi jk}{d}} |j\rangle\langle j+l|$ denote the Weyl operators that were already introduced in chapter 2.2.5. The action of W_{kl} on $|s\rangle$ is given by

$$W_{kl}|s\rangle = \omega^{k(s-l)}|s-l\rangle \ . \tag{6.7}$$

The indexes (k,l) associated to the density matrices P_{kl} form a discrete and classical phase space $\mathbb{T} := \{(p,q)\}$ of finitely many elements.

Symmetry operations mapping $\Lambda : \mathcal{W} \mapsto \mathcal{W}$ space, while preserving mixtures via $\Lambda(a\rho + (1-a)\sigma) \mapsto a\Lambda(\rho) + (1-a)\Lambda(\sigma)$ and the intersection $\Lambda : \Omega_{sep} \cap \mathcal{W} \mapsto \Omega_{sep} \cap \mathcal{W}$ at the same time can be obtained by applying local unitary transformations in combination with point transformations M. While the constituents $\omega^m W_{kl}$ of the Heisenberg Weyl group preserving translational symmetry may represent the former, the point transformations can be introduced in the form of:

1. Horizontal and vertical shear $H : \begin{pmatrix} p \\ q \end{pmatrix} \mapsto \begin{pmatrix} p \\ q+p \end{pmatrix}$ and $V : \begin{pmatrix} p \\ q \end{pmatrix} \mapsto \begin{pmatrix} p+q \\ q \end{pmatrix}$
2. Quarter rotation $R : \begin{pmatrix} p \\ q \end{pmatrix} \mapsto \begin{pmatrix} q \\ -p \end{pmatrix}$
3. Squeezing $R : \begin{pmatrix} p \\ q \end{pmatrix} \mapsto \begin{pmatrix} r \cdot p \\ -s \cdot q \end{pmatrix}$, $r \cdot s \equiv d+1$ for r, d coprime
4. Reflections via inversion of momentum $\Lambda_{p_{inv}} : p \mapsto -p$ and space $\Lambda_{q_{inv}} : q \mapsto -q$ as well as diagonal reflections $\Lambda_{diag} : \{q \mapsto p, p \mapsto q, \forall q, p\}$

According to theorem 2 in [41] and by extension to the d-dimensional case, the group constituted by symmetry transformations in $\mathcal{W}$ is equivalent to the group formed by affine transformations in the discrete classical phase space obtained via

$$\begin{pmatrix} k \\ l \end{pmatrix} \mapsto \begin{pmatrix} k' \\ l' \end{pmatrix} = \begin{pmatrix} m & n \\ p & q \end{pmatrix} \begin{pmatrix} k \\ l \end{pmatrix} + \begin{pmatrix} j \\ r \end{pmatrix} \ . \tag{6.8}$$

The indices $m, n, p, q \in \mathbb{F}_d$ and $mq - np \neq 0$. The set of d^2 points of the classical phase space can be divided into subsets of d elements, referred to as lines [42].

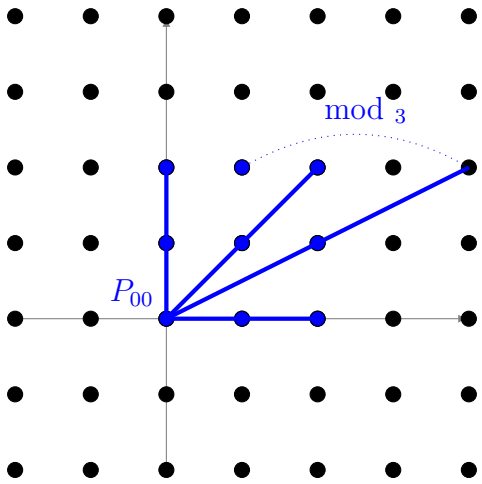

Figure 6.1.1: Non-parallel phase space lines in d=3 originating from (0,0)

A line corresponding to separable states can be governed by keeping m, n, p, q fixed for certain combinations (k, l) while variating (j, r). Parallel lines do not share any points in the classical phase space, while two non-parallel lines intersect at precisely one point (see figure 6.1.1).

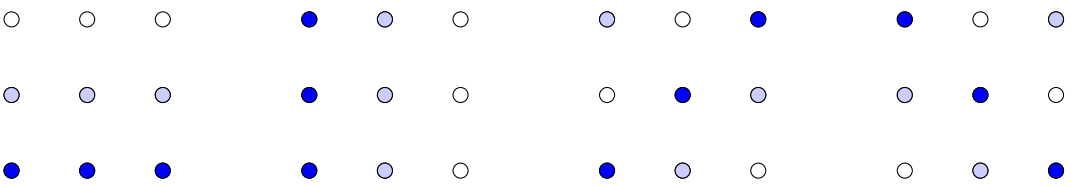

Figure 6.1.2: Sets of parallel phase space lines in d=3

Transformations of line states result in other line states. This stems from the previously defined premise that the introduced transformations do not change the properties of separability.

6.2 Bound Entanglement Detection via MUB Witnesses

Separability versus entanglement of a bipartite family of states that lies within the simplex, resembles an extention of the family of isotropic states and is of the form

$$\rho_M[d] = \Big(1 - \frac{q[1]}{(d^2-(d+1))} - \frac{q[2]}{(d+1)}\Big)\frac{1}{d^2}\mathbb{I}_{d^2}[d] + \frac{q[1]}{(d^2-(d+1))}P_{00}[d] + \\ + \frac{q[2]}{(d+1)(d-1)}\sum_{i=1}^{d-1}P_{i0}[d] + \sum_{j=3}^{d+1}\sum_{i=0}^{d-1}\Big(\frac{(-q[j])}{d^2}\mathbb{I}_{d^2}[d] + \frac{q[j]}{d}P_{i,j-2}[d]\Big) \tag{6.9}$$

shall be investigated within the context of the special simplex $\mathcal{W}$ defined in 6.3. The $d \times d$-dimensional class of states is based on that which has been investigated in [1], but with the distinction that it is defined by Bell projectors of all phase space lines. These states are mixtures of the maximally mixed (which is again related to the sum over all P_{kl}) and pure maximally entangled states, where parts involving the latter can graphically be thought of as a combination of P_{kl} involving a parameter split in the first line of phase space, while adding up the remaining ones.

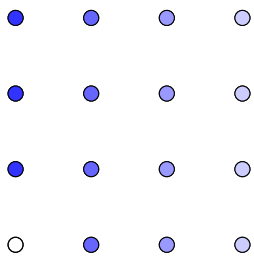

Figure 6.2.1: Graphical illustration of P_{kl} constituting the chosen family of states ρ_M for $d = 4$

While the parameters $q[i]$, $i \geq 3$ combine the P_{kl} of each line except for the first one into equally weighted, separable mixtures, the choice of opening up the first line using $q[1], q[2]$ accounts for the possibility of unequal mixtures of the maximally entangled states in the first line.

6.2.1 Starting with $3 \otimes 3$

Because there exists no bound entanglement for bipartite systems with subsystem dimensions of $d = 2$, the detection of bound entanglement via the MUB criterion is first considered for bipartite states ρ_M with $d = 3$ for each party. A complete set of mutually unbiased bases for $d = 3$ is obtained via

$$B_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{6.10}$$

$$B_1 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & \omega^2 & \omega \\ 1 & \omega & \omega^2 \\ 1 & 1 & 1 \end{pmatrix} \tag{6.11}$$

$$B_2 = \frac{1}{\sqrt{3}} \begin{pmatrix} \omega^2 & \omega & 1 \\ \omega^2 & 1 & \omega \\ 1 & 1 & 1 \end{pmatrix} \tag{6.12}$$

$$B_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} \omega & 1 & \omega^2 \\ \omega & \omega^2 & 1 \\ 1 & 1 & 1 \end{pmatrix} \ . \tag{6.13}$$

By utilizing complex conjugation in the second subsystem, the symmetry of bipartite $U \otimes U^*$ symmetric states such as ρ_M will be exploited during witness construction. For I_d^j denoting the j-th basis and dimension d, this assumption yields terms of the form

$$I_d^j = \mathrm{Tr}(\sum_i \langle b_i^j| \otimes (\langle b_i^j|W_{kl}^\dagger)^* \ \rho_M \ |b_i^j\rangle \otimes (W_{kl}|b_i^j\rangle)^*, \tag{6.14}$$

where the Weyl-operators cyclically shift the order of vectors in the bases B_j. The quantity

$$\langle \mathfrak{W} \rangle_{\rho_M} = 2 - \sum_j I_d^j \tag{6.15}$$

is first checked to ensure $\langle \mathfrak{W} \rangle_{\rho_M} \geq 0$ for all separable states, then minimized with respect to positivity and the PPT criterion in order to find the maximally possible amount of bound entanglement for a specific choice of parameters k, l (meaning certain cyclic shifts in the order of MUB vectors applied to the second subsystem) for each quantity I_d^j. Mathematically, the minimization can be formulated as

$$\min_{\substack{\forall k_j, l_j : 0 \leq k_j, l_j \leq d-1 \\ \forall q[i] : 1 \leq i \leq d+1}} \{ \langle \mathfrak{W}(k_j, l_j, q[i]) \rangle_{\rho_M} | \, \rho_M(q[i]) \geq 0, \, \rho_M^\Gamma(q[i]) \geq 0 \} \ . \tag{6.16}$$

For d=3, the two witnesses $\mathfrak{W}_1$ and $\mathfrak{W}_2$ yielding maximal values for bound entanglement can be governed by applying the shifts W_{01} and W_{02} in I_3^1 on the vectors contained in the first MUB. They correspond to the matrices:

$$\mathfrak{W}_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{6.17}$$

$$\mathfrak{W}_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{6.18}$$

The verification that these are in fact valid entanglement witnesses can be done by utilizing a separable state and observing the expectation values for all possible local unitary transformations. For both $\mathfrak{W}_1$ and $\mathfrak{W}_2$ as well as all other higher-dimensional witnesses to come, this check has been conducted using the package [43] that provides an implementation of a composite parameterization for the unitary group U(d). It exclusively yielded positive results, therefore indicating that $\langle \mathfrak{W} \rangle_{\rho_M} \geq 0$ is satisfied for all separable states.

Explicitly, the formulation of the expectation values for measurements on the state ρ_M employing the witnesses yields

$$\langle \mathfrak{W}_1 \rangle_{\rho_M} = \mathrm{Tr}(\rho_M \mathfrak{W}_1) : \frac{1}{3}(2 - q[1] + q[2] - 2q[3] + q[4]) \tag{6.19}$$

$$\langle \mathfrak{W}_2 \rangle_{\rho_M} = \mathrm{Tr}(\rho_M \mathfrak{W}_2) : \frac{1}{3}(2 - q[1] + q[2] + 3q[3] - 2q[4]) \; . \tag{6.20}$$

Analytical minimization including positivity (all eigenvalues of $\rho_M \geq 0$) and PPT (same for ρ_M^{PT}) lead to optimal values of bound entanglement for the choice of parameters $q[i]$ given in each of the following result tables that are labeled by R_i.

R_1	$\langle \mathfrak{W}_1 \rangle_{\rho_M}$	$\langle \mathfrak{W}_2 \rangle_{\rho_M}$
$q[1]$	$\frac{5}{3}(-1+\sqrt{3})$	$\frac{5}{3}(-1+\sqrt{3})$
$q[2]$	0	0
$q[3]$	$\frac{2}{3}$	$\frac{2}{3}-\frac{1}{\sqrt{3}}$
$q[4]$	$\frac{2}{3}-\frac{1}{\sqrt{3}}$	$\frac{2}{3}$
$2-I_d$	$1-\frac{2}{\sqrt{3}}$	$1-\frac{2}{\sqrt{3}}$

Figure 6.2.2: Table of optimized parameters $q[i]$ for the witnesses $\mathfrak{W}_1$ and $\mathfrak{W}_2$.

A cut through the simplex exploiting $q[2] = 0$ and $q[1] = \frac{5}{3}(-1+\sqrt{3})$ gained in optimization R_1, shows a 2-dimensional depiction of the areas of positivity, PPT and bound entanglement.

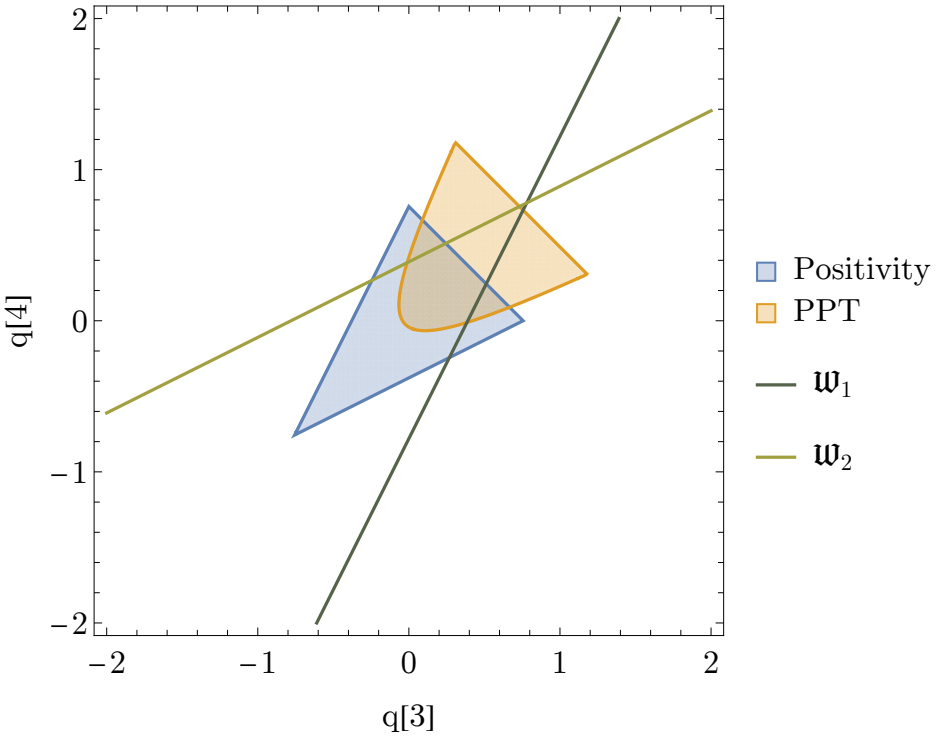

Figure 6.2.3: Cut 1: Illustration of bound entanglement witnesses for d=3 with $q[1] = \frac{5}{3}(-1+\sqrt{3})$, $q[2] = 0$.

Though it shall be noted that the graphical representations only serve as relational illustrations as in fact, the angles between the axes $q[3]$ and $q[4]$ are not necessarily orthogonal (but tend to orthogonality in higher dimensions) and therefore do not directly reflect the actual geometry of the simplex. Illustrations depicting accurate reflections of the simplex geometry can be seen in [41] for some bipartite qutrit systems.

Another property to investigate, is the isotropy of the state. Due to the isotropy, the amount of bound entanglement that can be detected utilizing a MUB witness is expected to remain unchanged if one of the line states is removed. Any combination of the first line with another should exhibit the same entanglement properties. Following the same minimization procedure as before but setting $q[3] = 0$ or $q[4] = 0$ respectively, yields the results listed in table 6.2.4.

$R_2(q[3]=0)$	$\langle \mathfrak{W}_1 \rangle_{\rho_M}$	$\langle \mathfrak{W}_2 \rangle_{\rho_M}$	$R_3(q[4]=0)$	$\langle \mathfrak{W}_1 \rangle_{\rho_M}$	$\langle \mathfrak{W}_2 \rangle_{\rho_M}$
$q[1]$	$\frac{5}{9}(-5+3\sqrt{3})$	$\frac{5}{3}(-5+4\sqrt{3})$	$q[1]$	$\frac{5}{9}(-5+4\sqrt{3})$	$\frac{5}{3}(-5+3\sqrt{3})$
$q[2]$	$-\frac{16}{9}$	$\frac{8}{9}(-2+\sqrt{3})$	$q[2]$	$\frac{8}{9}(-2+\sqrt{3})$	$-\frac{16}{9}$
$q[3]$	0	0	$q[3]$	$\frac{1}{\sqrt{3}}$	$-\frac{1}{\sqrt{3}}$
$q[4]$	$-\frac{1}{\sqrt{3}}$	$\frac{1}{\sqrt{3}}$	$q[4]$	0	0
$2-I_d$	$1-\frac{2}{\sqrt{3}}$	$1-\frac{2}{\sqrt{3}}$	$2-I_d$	$1-\frac{2}{\sqrt{3}}$	$1-\frac{2}{\sqrt{3}}$

Figure 6.2.4: Table of optimized parameters $q[i]$, removal of line 2 ($q[3]$=0) in optimization R_2 and 3 ($q[4]$=0) in R_3.

Evidently, the amount of entanglement detected by the MUB witnesses remains maximal and is equal in the cases R_2 and R_3. Cuts fixing $q[3](q[4]) = -\frac{1}{\sqrt{3}}$ or $q[3](q[4]) = \frac{1}{\sqrt{3}}$ have one MUB witness optimally detecting bound entanglement. This is illustrated in figure 6.2.5 for R_2.

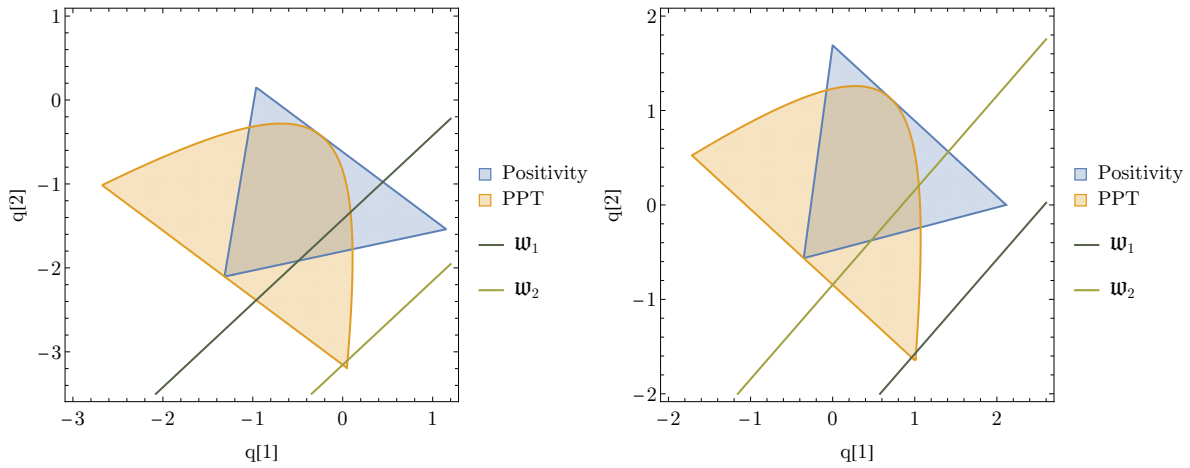

Figure 6.2.5: Cut 2 (left) and 3 (right): bound entanglement witnesses for d=3 for R_2 with $q[4] = -\frac{1}{\sqrt{3}}$ (left) and $q[4] = \frac{1}{\sqrt{3}}$ (right).

Both witnesses depicted in Cut 2 and 3 detect bound entanglement in families of states ρ_M defined via a mixture of the identity and maximally entangled Bell-states of phase space lines 1 and 3.

6.2.2 MUB-Witnesses for Bound Entanglement in $4 \otimes 4$

The procedure of finding a MUB witness detecting bound entanglement for bipartite systems ρ_M of dimension $4 \otimes 4$ is similar to the approach for those with subsystem dimension $d = 3$.

Starting with a complete set of MUBs, criterion 6.15 is applied. The maximum value for bound entanglement is achieved for Witnesses $\mathfrak{W}_1$ and $\mathfrak{W}_3$.

$$\mathfrak{W}_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{6.21}$$

$$\mathfrak{W}_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{6.22}$$

Witness $\mathfrak{W}_1$ has been governed by applying shifts W_{01}, while $\mathfrak{W}_3$ results from shifts W_{03} in the correlation function I_4^1, permuting the order of vectors within the first MUB.

It shall be noted, that instead of shifting the order of vectors within a basis with Weyl operators, Witnesses can generally be gained by looking at all possible permutations. This has been checked for $d = 4$ and although there exist other combinations of MUBs detecting bound entanglement, the optimum value is obtained for the cyclic shifts imposed on the vectors in B_0 constituting the second system via the Weyl operators W_{01} and W_{03}. Shifting the order of vectors with W_{02} does not yield optimal values. Furthermore, one finds that Weyl shifts in other bases (B_1-B_d) do not have an effect on the amount of bound entanglement that can be detected.

The expectation values for measurements on ρ_M using $\mathfrak{W}_1$ and $\mathfrak{W}_3$ yield

$$\langle \mathfrak{W}_1 \rangle_{\rho_M} : \frac{1}{4}(3 - q[1] + q[2] - 3q[3] + q[4] + q[5]) \tag{6.23}$$

$$\langle \mathfrak{W}_3 \rangle_{\rho_M} : \frac{1}{4}(3 - q[1] + q[2] + q[3] + q[4] - 3q[5]) \; . \tag{6.24}$$

Numerical optimization over the parameters $q[i]$, with $q[2] = 0$ and $q[4] = \frac{3}{16}$ leads to the set of solutions contained in table 6.2.6.

$\mathrm{R}_4(q[2]=0,\, q[4]=\frac{3}{16})$	$\langle \mathfrak{W}_1 \rangle_{\rho_M}$	$\langle \mathfrak{W}_3 \rangle_{\rho_M}$
$q[1]$	$2+\frac{1}{16}$	$2+\frac{1}{16}$
$q[2]$	0	0
$q[3]$	$\frac{9}{16}$	$\frac{1}{16}$
$q[4]$	$\frac{3}{16}$	$\frac{3}{16}$
$q[5]$	$\frac{1}{16}$	$\frac{9}{16}$
$2 - I_d$	$1-\frac{9}{8}$	$1-\frac{9}{8}$

Figure 6.2.6: Table of optimized parameters $q[i]$, solution R_4 for choice of $q[2]$=0 and $q[4] = \frac{3}{16}$.

Choosing fixed values from table 6.2.6 for $q[1]$, $q[2]$ and $q[4]$, one obtains the following 2-dimensional representation of a cut through the simplex.

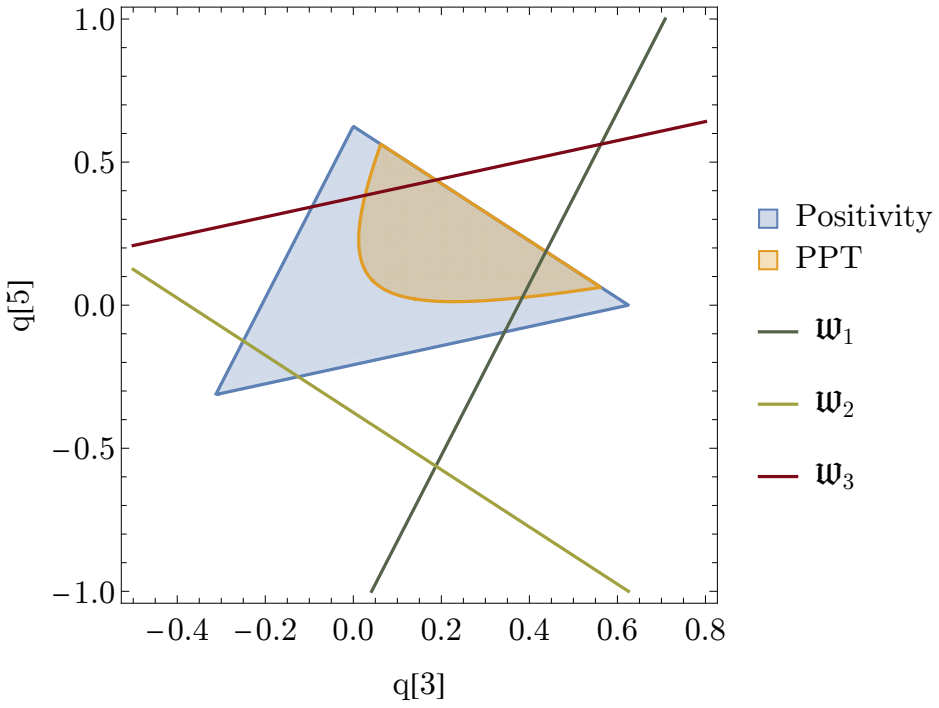

Figure 6.2.7: Cut 4: bound entanglement witnesses for d=4 with $q[1] = 2 + \frac{1}{16}$, $q[2] = 0$, $q[4] = \frac{3}{16}$.

As can be seen from the graph, the witness $\mathfrak{W}_2$ obtained via shifts W_{02} does not detect bound entanglement.

Removing line 2 consisting of all P_{k1} from the state ρ_M, a task that can be achieved by setting $q[3] = 0$, shows that $\mathfrak{W}_1$ and $\mathfrak{W}_3$ are optimal MUB witnesses for the choice of parameters $q[i]$ in table 6.2.8.

$\mathrm{R}_5(q[3] = 0)$	$\langle\mathfrak{W}_1\rangle_{\rho_{iso}}$	$\langle\mathfrak{W}_3\rangle_{\rho_{iso}}$
$q[1]$	$\frac{33}{64}$	$\frac{121}{64}$
$q[2]$	$-\frac{135}{64}$	$-\frac{15}{64}$
$q[3]$	0	0
$q[4]$	$-\frac{3}{8}$	$\frac{1}{8}$
$q[5]$	$-\frac{1}{2}$	$\frac{1}{2}$
$2 - I_d$	$-\frac{1}{8}$	$-\frac{1}{8}$

Figure 6.2.8: Table of optimized parameters $q[i]$, removal of line 2 ($q[3]$=0) in optimization R_5.

Doing the same for line 4 by fixing $q[5] = 0$, one obtains the values listed in table 6.2.9

$\mathrm{R}_6(q[5]=0)$	$\langle\mathfrak{W}_1\rangle_{\rho_{iso}}$	$\langle\mathfrak{W}_3\rangle_{\rho_{iso}}$
$q[1]$	$\frac{121}{64}$	$\frac{33}{64}$
$q[2]$	$-\frac{15}{64}$	$-\frac{135}{64}$
$q[3]$	$\frac{1}{2}$	$-\frac{1}{2}$
$q[4]$	$\frac{1}{8}$	$-\frac{3}{8}$
$q[5]$	0	0
$2-I_d$	$-\frac{1}{8}$	$-\frac{1}{8}$

Figure 6.2.9: Table of optimized parameters $q[i]$, removal of line 4 ($q[5]$=0) in optimization R_6.

And also upon removal of line 3 via $q[4]=0$, one observes that witnesses $\mathfrak{W}_1$ and $\mathfrak{W}_3$ detect the same amount of bound entanglement.

$\mathrm{R}_7(q[4]=0)$	$\langle\mathfrak{W}_1\rangle_{\rho_M}$	$\langle\mathfrak{W}_3\rangle_{\rho_M}$
$q[1]$	$\frac{99}{64}$	$\frac{99}{64}$
$q[2]$	$-\frac{45}{64}$	$-\frac{45}{64}$
$q[3]$	$\frac{3}{8}$	$-\frac{1}{8}$
$q[4]$	0	0
$q[5]$	$-\frac{1}{8}$	$\frac{3}{8}$
$2-I_d$	$-\frac{1}{8}$	$-\frac{1}{8}$

Figure 6.2.10: Table of optimized parameters $q[i]$, removal of line 3 ($q[4]$=0) in optimization R_7.

After investigation of the effect of the witnesses $\mathfrak{W}_1$ and $\mathfrak{W}_3$, it proves useful to take a closer look at their formulation in terms of Bell projectors. Although it is not generally possible for any arbitrary witnesses to be decomposed into Bell projectors, it is possible to do so in this case. The decompositions of $\mathfrak{W}_1$ and $\mathfrak{W}_3$ are

$$\mathfrak{W}_1 = -2P_{00} + 2\sum_{i=1}^{d-1} P_{i,0} + \sum_{j=2}^{d-1}\sum_{i=0}^{d-1} P_{ij} \ , \tag{6.25}$$

$$\mathfrak{W}_3 = -2P_{00} + 2\sum_{i=1}^{d-1} P_{i,0} + \sum_{j=1}^{d-2}\sum_{i=0}^{d-1} P_{ij} \ . \tag{6.26}$$

The witnesses are built from combinations of the P_{kl}, with the characteristic that $\mathfrak{W}_1$ lacks projectors $P_{k,1}$ constituting phase space line 2 and $\mathfrak{W}_3$ lacks $P_{k,3}$ constituting the fourth line.

6.2.3 MUB-Witnesses for Bound Entanglement in $5 \otimes 5$

Using the same schematic for bipartite systems of d=5, there exist 4 MUB Witnesses yielding maximal values for bound entanglement. They are again obtained via cyclic shifts in the order of vectors of the first MUB applied to the second subsystem. Formulating them again in terms of Bell projectors yields

$$\mathfrak{W}_1 = -3P_{00} + 2\sum_{i=1}^{d-1} P_{i,0} + \sum_{j=1}^{d-1}\sum_{i=0}^{d-1} P_{ij}(1-\delta_{j1}) \tag{6.27}$$

$$\mathfrak{W}_2 = -3P_{00} + 2\sum_{i=1}^{d-1} P_{i,0} + \sum_{j=1}^{d-1}\sum_{i=0}^{d-1} P_{ij}(1-\delta_{j2}) \tag{6.28}$$

$$\mathfrak{W}_3 = -3P_{00} + 2\sum_{i=1}^{d-1} P_{i,0} + \sum_{j=1}^{d-1}\sum_{i=0}^{d-1} P_{ij}(1-\delta_{j3}) \tag{6.29}$$

$$\mathfrak{W}_4 = -3P_{00} + 2\sum_{i=1}^{d-1} P_{i,0} + \sum_{j=1}^{d-1}\sum_{i=0}^{d-1} P_{ij}(1-\delta_{j4})\ . \tag{6.30}$$

Expectation values for measurements on ρ_M reduce to

$$\langle\mathfrak{W}_1\rangle_{\rho_M} = \frac{1}{5}(4 - q[1] + q[2] - 4q[3] + q[4] + q[5] + q[6]) \tag{6.31}$$

$$\langle\mathfrak{W}_2\rangle_{\rho_M} = \frac{1}{5}(4 - q[1] + q[2] + q[3] - 4q[4] + q[5] + q[6]) \tag{6.32}$$

$$\langle\mathfrak{W}_3\rangle_{\rho_M} = \frac{1}{5}(4 - q[1] + q[2] + q[3] + q[4] - 4q[5] + q[6]) \tag{6.33}$$

$$\langle\mathfrak{W}_4\rangle_{\rho_M} = \frac{1}{5}(4 - q[1] + q[2] + q[3] + q[4] + q[5] - 4q[6])\ . \tag{6.34}$$

One is again able to find analytical results for the parameters $q[i]$ that yield optimal values for bound entanglement. They are chosen such that it is possible to see two witnesses depicted in one graph. Interestingly, the witnesses $\mathfrak{W}_1$ and $\mathfrak{W}_4$ who are both lacking lines which are $+1/-1$ line apart from the first phase space line can be grouped together in a sense of parameter choices for $q[1]$ and $q[2]$. The same holds for witnesses $\mathfrak{W}_2$ and $\mathfrak{W}_3$.

R_8	$\langle \mathfrak{W}_1 \rangle_{\rho_M}$	$\langle \mathfrak{W}_4 \rangle_{\rho_M}$
$q[1]$	$\frac{228-95\sqrt{5}}{25}$	$\frac{228-95\sqrt{5}}{25}$
$q[2]$	$-\frac{72}{25}$	$-\frac{72}{25}$
$q[3]$	$-1+\frac{2}{\sqrt{5}}$	$-1+\frac{1}{\sqrt{5}}$
$q[4]$	$-\frac{1}{\sqrt{5}}$	$-\frac{1}{\sqrt{5}}$
$q[5]$	$-\frac{1}{\sqrt{5}}$	$-\frac{1}{\sqrt{5}}$
$q[6]$	$-\frac{1}{\sqrt{5}}$	$-\frac{2}{\sqrt{5}}$
$2-I_d$	$-1+\frac{2}{\sqrt{5}}$	$-1+\frac{2}{\sqrt{5}}$

Figure 6.2.11: Optimization R_8 for parameters $q[i]$.

Plotting an illustration of a 2-dimensional slice through the simplex for fixed values of $q[1]$, $q[2]$, $q[4]$ and $q[5]$ obtained in optimization R_8 shows again how two witnesses, this time $\mathfrak{W}_1$ and $\mathfrak{W}_4$ detect two regions of bound entanglement in figure 6.2.12.

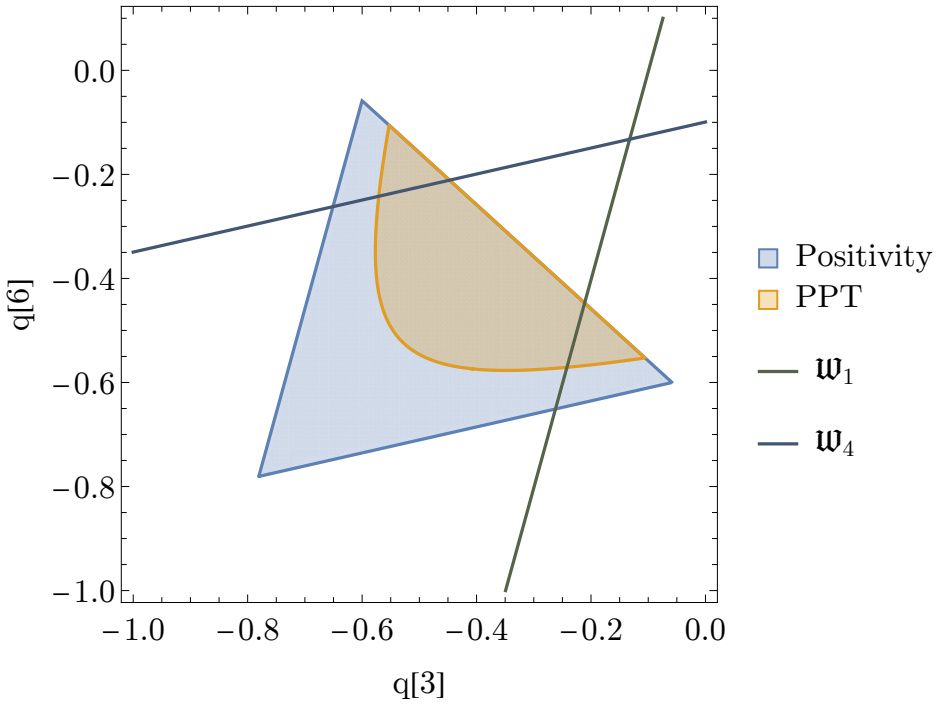

Figure 6.2.12: Cut 5: bound entanglement witnesses for d=5 with fixed parameters $q[1]$, $q[2]$, $q[4]$, $q[5]$.

Analogously, the same relational effect can be observed for witnesses $\mathfrak{W}_2$ and $\mathfrak{W}_3$ and a different cut through the simplex $\mathcal{W}$. Analytical results for the $q[i]$ leading to optimal values for the detection of bound entanglement can be taken from table 6.2.13.

R_9	$\langle \mathfrak{W}_2 \rangle_{\rho_M}$	$\langle \mathfrak{W}_3 \rangle_{\rho_M}$
$q[1]$	$\frac{19}{25}(13-5\sqrt{5})$	$\frac{19}{25}(13-5\sqrt{5})$
$q[2]$	$-\frac{48}{25}$	$-\frac{48}{25}$
$q[3]$	$\frac{1}{5}-\frac{1}{\sqrt{5}}$	$\frac{1}{5}-\frac{1}{\sqrt{5}}$
$q[4]$	$-\frac{4}{5}+\frac{2}{\sqrt{5}}$	$-\frac{4}{5}+\frac{1}{\sqrt{5}}$
$q[5]$	$-\frac{4}{5}+\frac{1}{\sqrt{5}}$	$-\frac{4}{5}+\frac{2}{\sqrt{5}}$
$q[6]$	$\frac{1}{5}-\frac{1}{\sqrt{5}}$	$\frac{1}{5}-\frac{1}{\sqrt{5}}$
$2-I_d$	$-1+\frac{2}{\sqrt{5}}$	$-1+\frac{2}{\sqrt{5}}$

Figure 6.2.13: Optimization R_8 for parameters $q[i]$.

Fixing $q[1]$, $q[2]$, $q[3]$ and $q[6]$, one observes that also $\mathfrak{W}_2$ and $\mathfrak{W}_3$ detect two regions of bound entanglement.

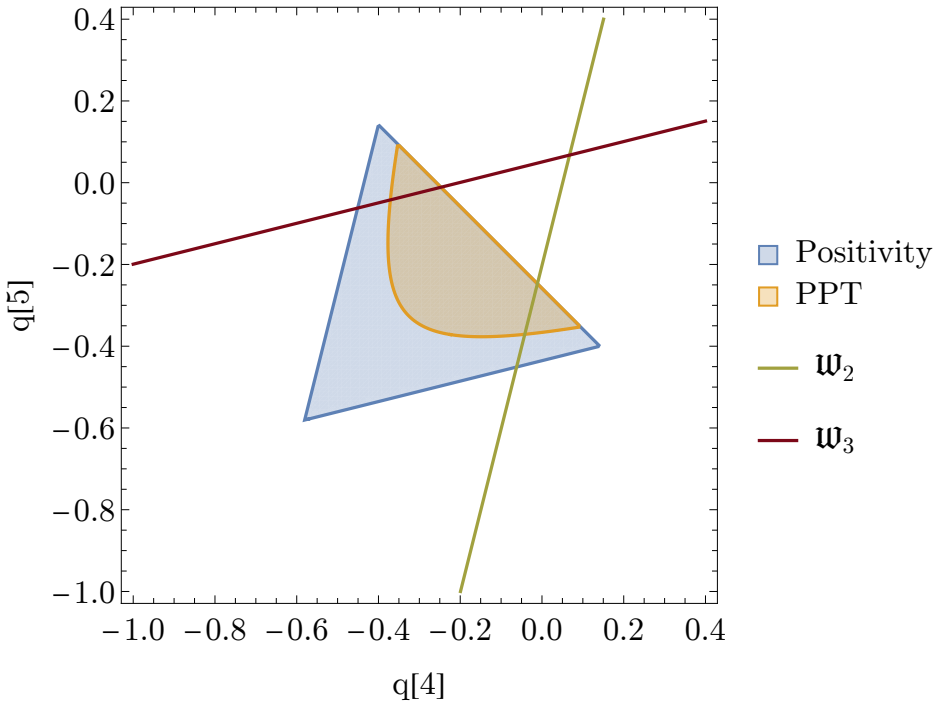

Figure 6.2.14: Cut 5: bound entanglement witnesses for d=5 with fixed parameters $q[1]$, $q[2]$, $q[3]$, $q[6]$.

6.3 D-Dimensional Witness Generalization

The observation that - at least for a certain class of bipartite systems ρ_M of prime dimension - optimal bound entanglement witnesses obtained via the MUB criterion can be generated using cyclic shifts W_{0i}, with $1 \leq i \leq d-1$ incites a closer look at the mathematical formulation of those witnesses.

A general d-dimensional Witness is denoted as

$$\begin{aligned}
\mathfrak{W}_i &= (2-d)\, P_{00} + 2\sum_{m=1}^{d-1} P_{m0} \\
&\quad + \sum_{m=0}^{d-1}\sum_{n=1}^{d-1} (1-\delta_{ni})\, P_{mn} \\
&= (2-d)\, P_{00} + 2\sum_{m=1}^{d-1} W_{m0}\otimes \mathbb{I}_d \times P_{00} \times W_{m0}^{\dagger}\otimes \mathbb{I}_d \\
&\quad + \sum_{m=0}^{d-1}\sum_{n=1}^{d-1} (1-\delta_{ni})\, W_{mn}\otimes \mathbb{I}_d \times P_{00} \times W_{mn}^{\dagger}\otimes \mathbb{I}_d \\
&= (2-d)\, P_{00} + \frac{2}{d}\sum_{m=1}^{d-1}\sum_{k,l=0}^{d-1} \omega^{m(k-l)} |k,k\rangle\langle l,l| \\
&\quad + \frac{1}{d}\sum_{m=0}^{d-1}\sum_{n=1}^{d-1}\sum_{k,l=0}^{d-1} (1-\delta_{ni})\, \omega^{m(k-l)} |(k-n),k\rangle\langle (l-n),l| \; .
\end{aligned}$$

For k=l, the sum (without part$(2-d)\, P_{00}$) simplifies to:

$$\begin{aligned}
\mathfrak{W}_i &\overset{\text{k=l}}{=} (d-1) \times \frac{2}{d}\sum_{k=0}^{d-1} |k,k\rangle\langle k,k| \\
&\quad + D \times \frac{1}{d}\sum_{n=1}^{d-1}\sum_{k=0}^{d-1} (1-\delta_{ni})\, |(k-n),k\rangle\langle (k-n),k| \\
&= \frac{1}{d}\sum_{k=0}^{d-1}\sum_{n=1}^{d-1} \left(2(d-1)|k\rangle\langle k| + d\times(1-\delta_{ni})\, |(k-n)\rangle\langle (k-n)|\right)\otimes |k\rangle\langle k|
\end{aligned}$$

For k≠l, the sum simplifies to

$$
\begin{aligned}
\mathfrak{W}_i \overset{\mathrm{k}\neq\mathrm{l}}{=} & \frac{2}{d}\sum_{k,l=0}^{d-1}|k,k\rangle\langle l,l|\overbrace{\sum_{m=1}^{d-1}\omega^{m(k-l)}}^{=-1} \\
& + \frac{1}{d}\sum_{n=1}^{d-1}\sum_{k,l=0}^{d-1}(1-\delta_{ni})\,|(k-n),k\rangle\langle(l-n),l|\overbrace{\sum_{m=0}^{d-1}\omega^{m(k-l)}}^{=0} \\
= & -\frac{2}{d}\sum_{k,l=0}^{d-1}|k,k\rangle\langle l,l|\,.
\end{aligned}
$$

Recombining both parts for the cases of k=l and k≠l again, the expression for the Witness yields

$$
\mathfrak{W}_i = (-d)P_{00} + \sum_{k=0,n=1}^{d-1} 2|k,k\rangle\langle k,k| + (1-\delta_{ni})\,|(k-n),k\rangle\langle(k-n),k|\,. \tag{6.35}
$$

It is observed for $d = 4$ that only witnesses $\mathfrak{W}_{i\neq 2}$ yield optimal values for bound entanglement. On the other hand, in the investigated prime dimensional bi-partite systems, all witnesses yield the optimal value of bound entanglement. A closer look at the phase space lines departing from P_{00} in dimension $d = 4$ which are defined via repeated application of W_{12}, W_{21} and W_{13} reveals the structure depicted in figure 6.3.1.

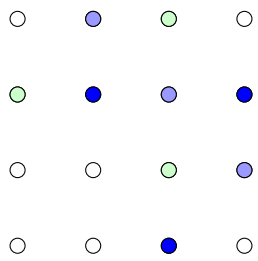

Figure 6.3.1: Points on lines defined by W_{12}, W_{21} and W_{13} originating from P_{00}

Witnesses $\mathfrak{W}_1$ and $\mathfrak{W}_3$ (missing P_{i1} and P_{i3}) each measure the same amount of points per phase space line. Furthermore, the n-dependent terms

$$
\sum_{\substack{k=0,n=1\\k\neq 2}}^{d-1}(W_{02}\otimes\mathbb{I}_d)\,(1-\delta_{n1})\,|(k-n),k\rangle\langle(k-n),k|(W_{02}\otimes\mathbb{I}_d)^\dagger = \tag{6.36}
$$

$$
\sum_{\substack{k=0,n=1\\k\neq 2}}^{d-1}(1-\delta_{n3})\,|(k-n),k\rangle\langle(k-n),k| \tag{6.37}
$$

in the sum 6.35 are transformed into each other by application of W_{02}. Considered as a whole, with terms $k = 2$ included, the terms for $\mathfrak{W}_1$ and $\mathfrak{W}_3$ are not symmetric under exchange of indices, while for $\mathfrak{W}_2$ they are.

$$\begin{aligned}\sum_{k=0,n=1}^{d-1} (1-\delta_{n2})\,|(k-n),k\rangle\langle(k-n),k| &= \sum_{k=0,n=1}^{d-1} (1-\delta_{n2})\,|k,(k-n)\rangle\langle k,(k-n)| \\ &= |3,0\rangle\langle 3,0| + |2,0\rangle\langle 2,0| \\ &+ |0,1\rangle\langle 0,1| + |2,1\rangle\langle 2,1| \\ &+ |1,2\rangle\langle 1,2| + |3,2\rangle\langle 3,2| \\ &+ |2,3\rangle\langle 2,3| + |0,3\rangle\langle 0,3| \end{aligned} \tag{6.38}$$

6.4 Bound Entanglement Detection via MUB Witnesses in Higher Dimensions

In the higher dimensions until $d < 9$, applying the found entanglement witnesses derived in earlier chapters to the state ρ_M yields similar results. For even prime power or composite dimensions $d = 6$ and $d = 8$, there are substructures in the phase space lines. Not all witnesses yield the same maximal values for bound entanglement. Numerical results for the maximum values attained are listed in table 6.4.1.

$\mathfrak{W}_i$	d=6	d=7	d=8
$\mathfrak{W}_1$	-0.091752	-0.08136	-0.07322
$\mathfrak{W}_2$	-0.091752	-0.08136	-0.07322
$\mathfrak{W}_3$	$-1.14826\cdot10^{-6}$	-0.08136	-0.07322
$\mathfrak{W}_4$	-0.091752	-0.08136	$-2.13422\cdot10^{-7}$
$\mathfrak{W}_5$	-0.091752	-0.08136	-0.07322
$\mathfrak{W}_6$	-	-0.08136	-0.07322
$\mathfrak{W}_7$	-	-	-0.07322

Figure 6.4.1: Table of optimial values for bound entanglement for 6≤ d≤ 8.

Again, it can be observed that for $d = 6$ and $d = 8$, permutations in the first MUB employing $W_{0\frac{d}{2}}$ do not yield the maximal values that can be obtained during optimization with other Weyl shifts.

6.5 Lower Bound on the MUB Criterion

Instead of using the upper bound of the MUB criterion, one could also consider the question of whether the lower bound that has recently been derived in [44] can also be used for the purpose of bound entanglement detection.

Generally, the lower bound on the MUB correlation function for our specific class of witnesses can be derived by making use of the Weyl permutations with respect to one basis again and minimizing the expression over the set of separable states. To give an example, for d=3 one can compute the values listed in table 6.5.1.

	W_{00}	W_{01}	W_{02}
B_1	1	$\frac{2}{3}$	$\frac{2}{3}$
B_2	1	1	1
B_3	1	$\frac{2}{3}$	$\frac{2}{3}$
B_4	1	$\frac{2}{3}$	$\frac{2}{3}$

Figure 6.5.1: Lower bound for shifts W_{0i} in the first MUB.

The dependency of the minimum on the choice of specific Weyl shifts applied shows that the lower bound has to be used with care. Furthermore, if we go to higher dimensions such as $d = 4$ and apply multiple different shifts in several mutually unbiased bases, the dependence of this lower bound on the type of permutations becomes even more complex. To illustrate this, note the following examples, where the Weyl operators W_{02} and W_{11} are applied to two bases at the same time.

$$
\begin{aligned}
L_{-,-,-,W_{02},W_{11}} &= 0.427939 \\
L_{-,W_{02},-,W_{11},-} &= 0.635714 \\
L_{W_{02},-,-,W_{11},-} &= 0.5
\end{aligned}
$$

This illustrates, that the lower bound on the set of separable states behaves very different to the upper bound that was used for the detection of bound entanglement in this thesis. An analysis of whether this lower bound could also be used as a witness for bound entanglement within the magic simplex did not yield very promising results in d=3 and d=4. Proving or disproving mathematically the suitability of the lower bound for bound entanglement detection would be an open task for future investigations.

7 Conclusion

Between two parties of a system with $d > 6$ there can exist a weak type of entanglement that cannot be distilled by any means of local operations and classical communication (LOCC). This means that no operation applied locally to either of two parties Alice and Bob or any form of classical communication between them can ever yield a maximally entangled state. As the tensor product Hilbert space permits a vast amount of states, it was the aim of this thesis to study a certain class of bipartite states ρ_M with respect to its separability. This family of states is embedded in the magic simplex, which is a highly symmetrical space constructed from d^2 generalized Bell projectors. For witnessing bound entanglement we have constructed an observable based on complete sets of MUBs and optimized the ordering. This MUB-witness bears also the advantage to be experimentally feasible.

In detail, for systems of dimensions of up to $8 \otimes 8$, regions of positivity, positive partial transpose as well as entanglement found via the upper bound of the MUB criterion have been studied. Besides confirming the results from [1], it has been found that there is a quite general method of constructing bound entanglement witnesses by employing the use of MUBs and Weyl operators. Applied to a certain basis, the Weyl shifts induce a different labeling of the vectors contained within the basis. For d of prime order, any Weyl shift that is applied to subsystem 2 with respect to the correlation function involving the first MUB yields maximal values of bound entanglement for certain parameter choices for ρ_M. In even dimensions $d \leq 8$, this behavior is only observed for some specific shifts, namely those that are not equal to $W_{0\frac{d}{2}}$.

Although it is generally not possible to construct mutually unbiased bases for $d = 6$, the expression of the optimal witness (optimal in the sense that they yield the highest values for bound entanglement) in terms of Bell projectors makes a generalization to dimensions $d \neq p^m$ possible.

When it comes to characterizing the set of bound entangled states, there are a variety of open issues up for further investigation. Utilizing the results of this thesis as a basis, one could aim for the construction of non-linear witnesses which could possibly lead to more insight on the structure of this set of bound entangled states. Also, one could investigate other classes of quantum states than ρ_M, for example by choosing different parameterizations and combinations of P_{kl}, which could possibly reveal more bound entanglement. One could also consider calculating the volume of bound entangled states detected via MUB witnesses, though this might prove to be a resource extensive (with respect to computation cost) endeavor.

Last but not least, a closer look at the MUB criterion's lower bound [44] on the set of separable states might prove to be worthwhile. Though it is not a tight bound, proving or even disproving the suitability of detecting bound entangled states using the lower bound might yield more insight on the structure of the set of separable states.

References

[1] Beatrix C. Hiesmayr and Wolfgang Löffler. "Mutually unbiased bases and bound entanglement". In: *Physica Scripta* 2014.T160 (2014), p. 014017.

[2] Asher Peres. "Separability Criterion for Density Matrices". In: *Physical Review Letters* 77.8 (Aug. 1996), pp. 1413–1415.

[3] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. "Separability of mixed states: necessary and sufficient conditions". In: *Physics Letters A* 223.1 (Nov. 1996), pp. 1–8.

[4] Paweł Horodecki, Michał Horodecki, and Ryszard Horodecki. "Bound Entanglement Can Be Activated". In: *Physical Review Letters* 82.5 (Feb. 1999), pp. 1056–1059.

[5] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. "Separability of n-particle mixed states: necessary and sufficient conditions in terms of linear maps". In: *Physics Letters A* 283.1 (2001), pp. 1–7.

[6] Ryszard Horodecki et al. "Quantum entanglement". In: *Reviews of Modern Physics* 81.2 (June 2009), pp. 865–942.

[7] Michal Horodecki, Pawel Horodecki, and Ryszard Horodecki. "Mixed-state entanglement and distillation: is there a "bound" entanglement in nature?" In: *Physical Review Letters* 80.24 (June 1998). arXiv: quant-ph/9801069, pp. 5239–5242.

[8] W. Dür. "Multipartite bound entangled states that violate Bell's inequality". In: *Physical Review Letters* 87.23 (Nov. 2001). arXiv: quant-ph/0107050.

[9] Remigiusz Augusiak. "Bound entanglement maximally violating Bell inequalities: Quantum entanglement is not fully equivalent to cryptographic security". In: *Phys. Rev. A* 74 (July 2006).

[10] Tamás Vértesi and Nicolas Brunner. "Disproving the Peres conjecture by showing Bell nonlocality from bound entanglement". en. In: *Nature Communications* 5 (Nov. 2014), p. 5297.

[11] W. Dür et al. "Distillability and partial transposition in bipartite systems". In: *Physical Review A* 61.6 (May 2000). arXiv: quant-ph/9910022.

[12] David P. DiVincenzo et al. "Evidence for bound entangled states with negative partial transpose". In: *Physical Review A* 61.6 (May 2000), p. 062312.

[13] Karol Horodecki et al. "Secure Key from Bound Entanglement". In: *Physical Review Letters* 94.16 (Apr. 2005), p. 160502.

[14] Tobias Moroder et al. "Steering Bound Entangled States: A Counterexample to the Stronger Peres Conjecture". In: *Phys. Rev. Lett.* 113.5 (Aug. 2014), p. 050404.

[15] Michael Epping and Časlav Brukner. "Bound entanglement helps to reduce communication complexity". In: *Physical Review A* 87.3 (Mar. 2013), p. 032305.

[16] Christoph Spengler et al. “Entanglement detection via mutually unbiased bases”. In: *Physical Review A* 86.2 (Aug. 2012), p. 022311.

[17] J.J. Rotman. *A First Course in Abstract Algebra: With Applications*. Pearson Prentice Hall, 2006.

[18] Gary L. Mullen and Daniel Panario. *Handbook of Finite Fields*. Boca Raton, FL: CRC Press, Taylor & Francis Group, 2013.

[19] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information*. 10th anniversary ed. Cambridge ; New York: Cambridge University Press, 2010.

[20] Christoph Spengler. “Geometrical aspects of qudits concerning Bell inequalities”. In: *arXiv:0907.1286 [quant-ph]* (July 2009). arXiv: 0907.1286.

[21] W.M. de Muynck. *Foundations of Quantum Mechanics, an Empiricist Approach*. Fundamental Theories of Physics. Springer Netherlands, 2002.

[22] Jirí Blank, Pavel Exner, and Miloslav Havlícek. *Hilbert Space Operators in Quantum Physics*. en. Google-Books-ID: 8AbBDAEACAAJ. Springer Netherlands, Sept. 2008.

[23] Florian Mintert et al. “Measures and dynamics of entangled states”. In: *Physics Reports* 415.4 (Aug. 2005). arXiv: quant-ph/0505162, pp. 207–259.

[24] Reinhold A. Bertlmann and Philipp Krammer. “Bloch vectors for qudits”. In: *Journal of Physics A: Mathematical and Theoretical* 41.23 (June 2008). arXiv: 0806.1174, p. 235303.

[25] I. Bengtsson and K. Zyczkowski. *Geometry of Quantum States: An Introduction to Quantum Entanglement*. Cambridge University Press, 2006.

[26] Florian Mintert et al. “Measures and dynamics of entangled states”. In: *Physics Reports* 415.4 (Aug. 2005). arXiv: quant-ph/0505162, pp. 207–259.

[27] Charles H. Bennett et al. “Quantum nonlocality without entanglement”. In: *Physical Review A* 59.2 (Feb. 1999), pp. 1070–1091.

[28] Heide Narnhofer. “Entanglement reflected in Wigner functions”. In: *Journal of Physics A: Mathematical and General* 39.22 (2006), p. 7051.

[29] Reinhold A. Bertlmann and Philipp Krammer. “Entanglement witnesses and geometry of entanglement of two-qutrit states”. In: *Annals of Physics* 324.7 (2009), pp. 1388 –1407.

[30] Walter Thirring et al. “Entanglement or separability: The choice of how to factorize the algebra of a density matrix”. In: *The European Physical Journal D* 64.2-3 (Oct. 2011). arXiv: 1106.3047, pp. 181–196.

[31] Andreas Gabriel, Beatrix C. Hiesmayr, and Marcus Huber. “Criterion for k-separability in mixed multipartite systems”. In: *arXiv:1002.2953 [quant-ph]* (Feb. 2010). arXiv: 1002.2953.

[32] Barbara M. Terhal. “Detecting quantum entanglement”. In: *Natural Computing* 287.1 (Sept. 2002), pp. 313–335.

[33] Julian Schwinger. “UNITARY OPERATOR BASES”. In: *Proceedings of the National Academy of Sciences* 46.4 (1960), pp. 570–579.

[34] Thomas Durt et al. “On mutually unbiased bases”. In: *International Journal of Quantum Information* 08.04 (June 2010), pp. 535–640.

[35] Andreas Klappenecker and Martin Roetteler. “Constructions of Mutually Unbiased Bases”. In: *arXiv:quant-ph/0309120* (Sept. 2003). arXiv: quant-ph/0309120.

[36] William K Wootters and Brian D Fields. “Optimal state-determination by mutually unbiased measurements”. In: *Annals of Physics* 191.2 (May 1989), pp. 363–381.

[37] Wan Zhe-Xian. *Quaternary Codes*. en. Google-Books-ID: 9RjtCgAAQBAJ. World Scientific, Nov. 1997.

[38] Maurice R. Kibler. “An angular momentum approach to quadratic Fourier transform, Hadamard matrices, Gauss sums, mutually unbiased bases, the unitary group and the Pauli group”. en. In: *Journal of Physics A: Mathematical and Theoretical* 42.35 (2009), p. 353001.

[39] M. Lewenstein et al. “Optimization of entanglement witnesses”. In: *Physical Review A* 62.5 (Oct. 2000), p. 052310.

[40] Bernhard Baumgartner, Beatrix Hiesmayr, and Heide Narnhofer. “A special simplex in the state space for entangled qudits”. In: *Journal of Physics A: Mathematical and Theoretical* 40.28 (2007), p. 7919.

[41] Bernhard Baumgartner, Beatrix C. Hiesmayr, and Heide Narnhofer. “State space for two qutrits has a phase space structure in its core”. In: *Physical Review A* 74.3 (Sept. 2006), p. 032327.

[42] Kathleen S. Gibbons, Matthew J. Hoffman, and William K. Wootters. “Discrete phase space based on finite fields”. In: *Physical Review A* 70.6 (Dec. 2004), p. 062101.

[43] Christoph Spenger. *Composite parameterization and Haar measure for unitary groups – from Wolfram Library Archive*. Aug. 2011.

[44] Joonwoo Bae, Beatrix C. Hiesmayr, and Daniel McNulty. “Linking Entanglement Detection and State Tomography via Quantum 2-Designs”. In: *arXiv:1803.02708 [quant-ph]* (Mar. 2018). arXiv: 1803.02708.