MASTERARBEIT

Titel der Masterarbeit

„Mutually Unbiased Quantum Bases: Existence, Entanglement, Information“

verfasst von

Bogdan Jin-Wha Pammer, BSc

angestrebter akademischer Grad

Master of Science (MSc)

Wien, 2015

Studienkennzahl lt. Studienblatt:	A 066 876
Studienrichtung lt. Studienblatt:	Masterstudium Physik
Betreut von:	o.Univ.-Prof. Dr. Anton Zeilinger

Contents

Chapter 1

Introduction

Two bases $\{|\Psi_i\rangle\}$ and $\{|\Phi_j\rangle\}$ for a Hilbert space of dimension d are called *mutually unbiased* if

$$|\langle\Psi_i|\Phi_j\rangle|^2 = \frac{1}{d} \quad \forall i, j. \tag{1.1}$$

This notion could be traced back to early discussions of complementarity by the pioneers of quantum mechanics, such as Werner Heisenberg, Wolfgang Pauli or Hermann Weyl. In the current literature however, Julian Schwinger's paper from 1960 [21] is the often cited locus classicus for theoreticians' engagement with mutually unbiased bases (MUBs).

MUBs are interesting because they exemplify and make it possible to utilize one key characteristic of quantum systems - complementarity. The results of a measurement in one basis do not tell us anything about the results in a complementary or mutually unbiased basis. Hence it does not surprise that early approaches to MUBs were motivated by the problem of (optimal) quantum state determination. [13,25,26] MUBs are also of interest in quantum cryptography, especially for quantum key distribution. [6] More recently the role MUBs can play in effectively detecting entanglement received much attention. [9,22]

In arbitrary dimension d there can be maximally $d+1$ mutually unbiased bases. [13,26] We therefore refer to a set of $d+1$ MUBs as *complete*. Proofs of this fact can be found in Section 3.1 and Section 3.2.

The puzzling thing about MUBs however is that complete sets seem to not exist in arbitrary dimension. So far, constructions for prime dimension ($d = p$) and prime power dimension ($d = p^n$) are known. We will analyse these constructive proofs from a specific angle in Section 5.3. No other general statement other than "We don't know" was established concerning existence in composite dimension ($d = d_A d_B$). For dimension $d = 6$ it is widely conjectured that no more than 3 MUBs do exist. [7] The existence problem of MUBs is related to a variety of unsolved mathematical problems. [3]

This thesis will proceed as following. After some remarks on notation, the fundamental connection between complex Hadamard matrices will be elucidated and the notion of *equivalent classes* of MUBs will be introduced in Chapter 2. In Chapter 3 we will review some basic, insightful and useful properties of complete sets of mutually unbiased bases, before we turn to applying them. Chapter 4 will explore the role of entanglement in MUBs. One genuine result concerning so-called *product* MUBs and an alternative proof for an already known result will be presented there. In Chapter 5 we will discuss the connection between MUBs and *unitary operator bases*. This connection goes back to Schwinger. [21] A much cited and more recent result [2] will be discussed there and a genuine result, which I think could open a new avenue to the existence problem of MUBs, will be presented. Chapter 6 will conclude the thesis.

1.1 Some Remarks on Notation

In this thesis we deal primarily with generalized quantum bits or *q-dits*, which are represented as vectors in $\mathbb{C}^d$. We will employ the standard *Dirac notation*. Furthermore $A^\dagger$ denotes the adjoint and $\bar{A}$ the complex conjugate of A. The associated Hilbert-Schmidt space is the space of all complex $d \times d$ Matrices, denoted with $\mathbb{M}(\mathbb{C}, d)$ and the “standard trace" scalar-product is

$$\langle A|B\rangle = Tr(A^\dagger B) \quad A, B \in \mathbb{M}(\mathbb{C}, d). \tag{1.2}$$

The following notation will also be employed during the whole thesis. $P_{ij} = |i, j\rangle\langle i, j|$ is the projector on the ith vector of the jth basis of a complete set of MUB, with $i = 0, ...d-1$ and $j = 0, ...d$. Non-complete sets of MUBs, with $i = 0, ...d-1$ and $j = 0, ...M-1$, will be denoted as $\{P_{ij}\}_M$.

Special unitary operator bases corresponding to $\{P_{ij}\}_M$ will be denoted as $\{U_{kj}\}_M$ or $\{Q_{kj}\}_M$. The latter notation will be used for unitary operator bases, that have a certain subset structure, forming cyclic groups under matrix multiplication. This notation is relevant for Section 3.2 and Chapter 5 and will be elucidated there further.

We define

$$\omega_N = e^{\frac{2\pi i}{N}}. \tag{1.3}$$

If $N = d$, the dimension of the discussed system, and if this is obvious from the context, the index is omitted. Then we write ω instead of ω_d. Π is used for permutation matrices, D for unitary diagonal matrices and F for the Fourier matrix of dimension d,

$$F_{ij} = \omega^{ij}. \tag{1.4}$$

The standard addition and multiplication when applied to indices is always modulo d. $\oplus$, $\ominus$, $\odot$ and $\oslash$ will denote addition, addition of the additive inverse, multiplication and multiplication with the multiplicative inverse on the respective Galois field. This is particularly relevant for Section 5.3.

Chapter 2

Equivalent Sets of MUBs and Hadamard Matrices

There is a natural connection between mutually unbiased bases and complex Hadamard matrices, since the columns and rows of a complex Hadamard matrix form orthonormal bases mutually unbiased to the standard basis. A set of M MUBs including the standard basis therefore can also be represented as $\{\mathbb{1}, H_1, ...H_{M-1}\}$ or $\{H_j\}_M$, with either the columns or rows of the complex Hadamard matrices H_j being vectors mutually unbiased to each other.

However, while two complex Hadamard matrices are called equivalent ($H \simeq H'$), if there exists a pair of diagonal unitary matrices (D_1, D_2) and permutation matrices (Π_1, Π_2) such that

$$H' = D_1 \Pi_1 H \Pi_2 D_2, \tag{2.1}$$

this definition of equivalence cannot be directly applied to sets of mutually unbiased bases. The reason for this is the following: If we treat the columns of H as the basis-vectors, while D_2 corresponds to the free choice of a global phase for quantum states and Π_2 to a relabelling of vectors within the bases, D_1 and Π_1 will effectively change the basis vectors and affect whether two columns are mutually unbiased or not. Note further, that in systems of composite dimensions $d = d_A d_B$, which can be interpreted as a composite system $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$, D_1 and Π_1 change the entanglement structure of the bases.

In order to identify *equivalence classes* of sets of MUBs we therefore need to go back to what we mean when we talk of *bases*. We use the term with (at least) a double meaning. On the one hand we mean *basis of* $\mathbb{C}^d$ as a mathematical term, well known from linear algebra. On the other hand *basis* or *the projectors onto basis-vectors* in quantum mechanics has a physical meaning: It is the labelling of a special set of measurements of a quantum system or an ensemble of such quantum systems. Furthermore these measurements (or projections) are endowed with statistical physical meaning concerning measurement outcomes via the *Born rule*.

Since the predictions of Quantum Mechanics are assumed to be invariant under relabelling of the measurement apparatus and global phases, different bases of $\mathbb{C}^d$ can be treated as physically equivalent. Furthermore we operate on an abstract level where we do not have spatial structures imposing a "natural distinction" between product vectors and entangled vectors. Hence it is per se also a question of labelling whether the basis vector $|\phi_i\rangle$ is a product vector and $|\phi_j\rangle$ is maximally entangled or vice versa or whether both of them are partially entangled. We will adopt the mathematical definition of *equivalent classes* of MUBs developed by Brierley et al. in [4].

Definition 1. (Brierley et al. [4], Appendix A) *Let $\{V_j\}_M \equiv \{V_0, ..., V_{M-1}\}$ be a set of M matrices in $U(d)$, whose columns are interpreted as vectors of M bases. The bases represented by $\{V_j\}_M$ and $\{V_j'\}_M$ are equivalent to each other*

$$\{V_1, ... V_{M-1}\} \simeq \{V_1', ... V_{M-1}'\} \tag{2.2}$$

if they can be transformed into each other by a succession of the following five transformations

- *a global unitary transformation U applied from the left*

$$\{V_j\}_M \rightarrow \{U V_j\}_M \tag{2.3}$$

- *M diagonal unitary transformations D_j from the right which attach phase factors to each column of the M matrices*

$$\{V_j\}_M \rightarrow \{V_j D_j\}_M \tag{2.4}$$

- *M permutations of the elements within each basis*

$$\{V_j\}_M \rightarrow \{V_j \Pi_j\}_M \tag{2.5}$$

- *pair-wise exchange of two bases*

$$\{..., V_j, ..., V_{j'}, ...\} \rightarrow \{..., V_{j'}, ..., V_j, ...\} \tag{2.6}$$

- *an overall complex conjugation*

$$\{V_j\}_M \rightarrow \{\overline{V}_j\}_M \tag{2.7}$$

which leaves the values of all scalar products invariant.

Definition 1 lists the transformations under which the system of equations imposing orthogonality and mutually unbiasedness on the MUB elements, spelt out in (3.5), are invariant. This means, if one set of MUBs in an equivalent class exists, all the others do as well.

This definition of equivalent sets of bases allows to define a *standard form* of sets of MUBs. All sets of MUBs are equivalent in the sense of Definition 1 to a set in standard form, which has the following characteristics:

- $V_0 = \mathbb{1}$ due to (2.3), which fixes U up to multiplication with a unitary diagonal matrix D', that can be compensated by $D_0 = D'^{\dagger}$ and a permutation Π', that can be compensated by $\Pi_0 = \Pi'^{\dagger}$.

- All other V_j are complex Hadamard matrices $V_j = H_j$, whose columns can be dephased due to (2.4). This means all entries in the first column can be set 1.

- Additionaly, H_1 can always be chosen as a dephased Hadamard matrix. This means the entries of the first row and the first column are 1. This can always be achieved since U is only fixed up to D'. Since D' is multiplied from the right side it can be chosen in a way that it maps the first column of H_1 onto a column whose entries are all 1. (Note that due to this convention, any set of MUBs can be chosen to have at least one product vector in H_1. This is the first row consisting of 1s entirely.)

- Furthermore, due to the freedom of choosing Π' (which is again multiplied globally from the left) the second column of H_1 can always be chosen in a way that the real valued phases α of the entries $e^{i\alpha}$ are non-decreasing. (Note that the freedom of choosing Π' puts sets of MUBs with potentially different entanglement structures in the same equivalence class.)

- Because of (2.5)-(2.7) the standard form is not unique. There are different sets of complex Hadamard matrices in standard form in the same equivalence class.

From this definition of the standard form, it follows that all pairs of mutually unbiased bases are equivalent to a pair $\{\mathbb{1}, H_1\}$. The problem of finding all pairs of mutually unbiased bases in dimension d is therefore equivalent to finding all distinct complex Hadamard matrices. In other words:

Theorem 1. *The set of all dephased Hadamard matrices corresponds one-to-one to all pairs of MUBs (up to equivalence).*

The "straight forward" approach to the existence problem of sets of MUBs, which means to look at all the orthogonality and mutually unbiasedness conditions on a set of MUBs and to solve the highly overdetermined system of equations, therefore requires the knowledge of all complex Hadamard matrices in the respective dimension. The classification of complex Hadamard matrices is a highly sophisticated endeavour, which is far from being complete.

Since the classification of Hadamard matrices is complete for $d = 2,...,5$ Brierley et al. were able to classify all equivalence classes of MUBs for these dimensions. [4] Even for $d = 6$ it has not been yet possible to find and classify all complex Hadamard matrices. A detailed study of MUBs and Hadamard matrices in dimension 6 can be found in [3]. Szöllősi found in his PhD thesis [23] the conjectured 4-parameter family of complex Hadamard matrices. In [3] it is conjectured that it might be possible with such a family to find more than 3 MUBs in dimension 6. However no explicit form of this family is known and it has not (yet) been possible to gain additional results for $d = 6$ from this. A useful database with all known complex Hadamard matrices is run by Życzkowski. [5]

The aim of the following discussions and approaches to the existence problem of MUBs is to learn about them by avoiding the existence problem of complex Hadamard matrices. This is done either by exploiting other mathematical resources than the "pedestrian" approach (as done in Chapter 5) or by restricting oneself to physically relevant sub-problems, such as product MUBs (see Chapter 4). First, however, we shall proceed by introducing some interesting and useful properties of MUBs.

Chapter 3

Some Properties of Complete Sets of Mutually Unbiased Bases

3.1 Complete Sets of Mutually Unbiased Bases as Informationally Complete Positive Operator-Valued Measures

Why are MUBs of great interest in quantum information theory and foundations of quantum mechanics? One reason is that a complete set of MUBs (cMUB), consisting of $d+1$ mutually unbiased bases, constitutes an informationally complete positive operator-valued measure (IC-POVM). A POVM is a set of measurements $\{P_i\}$ with

$$\sum_i P_i = \mathbb{1}. \tag{3.1}$$

A POVM is informationally complete if the measurement results $p_i = Tr(\rho P_i)$ uniquely determine the quantum state ρ and vice versa. In other words $\rho = \rho'$ if and only if $\forall i\ p_i = p'_i$.

Theorem 2. *A complete set of mutually unbiased bases $\{\frac{P_{ij}}{d+1}\}$ is an IC-POVM.*

Proof. It is obvious that

$$\sum_{ij} \frac{P_{ij}}{d+1} = \mathbb{1}. \tag{3.2}$$

Furthermore we need to show that $\Lambda = \rho - \rho' = 0$ if and only if $Tr(\Lambda P_{ij}) = 0\ \forall i, j$. This in turn is only the case if $\{P_{ij}\}$ spans the space of all hermitian $d \times d$ matrices. This is the case and can easily be checked by Gram-Schmidt orthogonalisation. One starts out with the first or standard basis $\{P_{i0}\}$, which is orthogonal by definition and orthogonalises the remaining projectors base by base, respective to each other and $\{P_{i0}\}$.

$$\begin{aligned} \tilde{P}_{\alpha 0} &= P_{\alpha 0} \\ \tilde{P}_{\alpha\beta} &= P_{\alpha\beta} - \sum_{\alpha>i} \frac{Tr(P_{\alpha\beta}\tilde{P}_{i\beta})}{Tr(\tilde{P}_{i\beta}\tilde{P}_{i\beta})}\tilde{P}_{i\beta} - \frac{\beta}{d}\mathbb{1} \end{aligned} \tag{3.3}$$

The "last" projector of each base is $P_{d-1,\beta} = \mathbb{1} - \sum_{i=0}^{d-2} P_{d-1,\beta}$. A straight forward calculation yields $\tilde{P}_{d-1,\beta} = 0$. This procedure gives d orthogonal vectors for the first (standard) basis and $d-1$ orthogonal vectors for the remaining d MU-bases. Since all projectors are hermitian, we have shown that $\{P_{ij}\}$ spans the space of all hermitian $d \times d$ matrices. □

It is a corollary that there cannot be more than $d+1$ MUBs, since otherwise the space of all hermitian $d \times d$ matrices would have more than d^2 dimensions. From Theorem 2 follows directly that all density matrices ρ can be written as

$$\rho = \sum_{ij} p_{ij} P_{ij} - \mathbb{1}. \tag{3.4}$$

Furthermore (1.1) can be re-written as

$$Tr(P_{ij}P_{mn}) = \delta_{in}\delta_{jm} + (1-\delta_{jm})\frac{1}{d}. \tag{3.5}$$

Straight forward calculation yields

$$Tr(P_{ij}\rho) = p_{ij} \tag{3.6}$$

and for all density matrices the following equations hold:

$$p_{ij} \geq 0 \quad \forall i,j \tag{3.7}$$

$$\begin{aligned} \sum_i p_{ij} &= 1 \quad \forall j \\ \sum_{ij} p_{ij}^2 &\leq 2 \end{aligned} \tag{3.8}$$

with

$$\sum_{ij} p_{ij}^2 = 2 \tag{3.9}$$

for and only for pure states.

A complete set of MUBs therefore allows to map density matrices ρ on what we will call MUB probablility vectors or, in short, 'p-vectors' with the attributes outlined in (3.8). Not all p-vectors however represent density matrices. Additionally, the positivity criterion

$$\rho \geq 0 \tag{3.10}$$

is required. It should be remarked that (3.7) is a necessary but not sufficient condition for positivity.

Note that the p-vector p_{ij} has d^2-1 degrees of freedom, that is as many as the space of all traceless hermitian $d \times d$ matrices. Any density matrix ρ of dimension d can be mapped onto a traceless hermitian matrix simply by

$$\rho \to \tilde{\rho} = \rho - \mathbb{1}/d. \tag{3.11}$$

A complete set of MUBs of dimension d provides, therefore, a bijective map between the space of all traceless hermitian matrices and the above introduced p-vectors (if the restriction from (3.7) is omitted). A modification of (3.4) and (3.6) gives both directions explicitly:

$$\begin{aligned} \tilde{\rho} &= \sum_{ij} \tilde{p}_{ij} P_{ij}, \\ \tilde{p}_{ij} &= Tr(P_{ij}\tilde{\rho}), \end{aligned} \tag{3.12}$$

with

$$\begin{aligned} \tilde{p}_{ij} &= p_{ij} - \frac{1}{d}, \\ \sum_{i} \tilde{p}_{ij} &= 0. \end{aligned} \tag{3.13}$$

Since cMUBs are a IC-POVM, they allow for full quantum state tomography. Ivanovic shows in [13] that quantum state tomography is optimal, when done with a complete set of MUBs.

Next to cMUBs, symmentrical informationally complete POVMs (SIC-POVMs) are the second prominent group of IC-POVMs. The elements Π_i of a SIC-POVM $\{\frac{\Pi_i}{d}\}$ $(i = 1, ...d^2)$ fulfill the following defining relations:

$$\begin{aligned} \sum_{i} \frac{1}{d}\Pi_i &= \mathbb{1} \\ Tr(\Pi_i\Pi_j) &= \delta_{ij} + (1-\delta_{ij})\frac{1}{d+1}. \end{aligned} \tag{3.14}$$

cMUBs and SIC-POVMs share the interesting property that they are both *quantum 2-designs*. A property that we will elaborate on in Chapter 3.3.

3.2 MUBs and Unitary Operator Bases

A cMUB $\{P_{ij}\}$ allows for the following elegant construction:

$$\begin{aligned} &Q_{kj} = \sum_i \omega^{ik} P_{ij}, \\ &Q_0 = Q_{0j} = \mathbb{1}, \\ &k = 0,...d-1; i = 0,...d-1; j = 0,...d. \end{aligned} \tag{3.15}$$

Straight forward calculations show that $\{\frac{1}{\sqrt{d}} Q_{kj}\}$ constitutes a unitary operator ONB for $\mathbb{M}(\mathbb{C}, d)$, with the following group structure:

$$\begin{aligned} Q_{kj} &= Q_j^k \\ Q_{kj}^\dagger &= Q_j^{-k} \\ Q_{k,j} Q_{l,j} &= Q_{k+l,j} \end{aligned} \tag{3.16}$$

with the addition of indices being $\mod d$ and $Q_j := Q_{1j}$. Note that the eigenvectors of Q_{kj} are $|i, j\rangle$ $(j = 0,...d-1)$ with ω^{ki} as eigenvalues. Since the Fourier transformation is bijective, Theorem 3 follows immediately:

Theorem 3. *For every set of M mutually unbiased bases $\{P_{ij}\}_M$ there exist $M(d-1)+1$ mutually orthogonal unitary matrices $\{Q_{kj}\}$, consisting of M cyclic groups generated by M mutually orthogonal unitary matrices $\{Q_j\}$ and conversely, for each such set $\{Q_{kj}\}$ there is a set of M mutually unbiased bases $\{P_{ij}\}_M$.*

Proof. (⇒) The construction in (3.15) proves the first direction of Theorem 3.
(⇐) If $\{\mathbb{1}, \frac{1}{\sqrt{d}} Q_{kj}\}$ $(k = 1,...d-1; j = 0,...M-1)$ is an ONB of the Hilbert-Schmidt space fulfilling (3.16) we can define

$$R_{ij} = \frac{1}{d} \sum_{k=0}^{d-1} \omega^{-ik} Q_{kj} \tag{3.17}$$

and obtain

$$\begin{aligned} Tr(R_{ij} R_{mn}) &= \frac{1}{d^2} \sum_{k,l} \omega^{-(ki+lm)} Tr(Q_{kj} Q_{ln}) \\ &= \frac{1}{d^2} \sum_{k,l} \omega^{-(ki+lm)} d(\delta_{k,d-l} \delta_{j,n} + \delta_{0,k} \delta_{0,l} (1-\delta_{j,n})) \\ &= \frac{1}{d} (\delta_{j,n} \sum_k \omega^{-k(i-m)} + (1-\delta_{j,n})) \\ &= \frac{1}{d} (d \delta_{j,n} \delta_{i,m} + (1-\delta_{j,n})) \\ &= \delta_{j,n} \delta_{i,m} + \frac{1}{d} (1-\delta_{j,n}), \end{aligned} \tag{3.18}$$

which is the defining equation for MUBs. This completes the proof. □

In a similar way, a complete set of MUBs allow the following construction of a basis $\{\Phi, \phi_{j,k}\}$ for $\mathbb{C}^d \otimes \mathbb{C}^d$:

$$\begin{aligned} |\Phi\rangle &= \frac{1}{\sqrt{d}} \sum_i |i\rangle \otimes |i\rangle = \frac{1}{\sqrt{d}} \sum_i |i,j\rangle \otimes \overline{|i,j\rangle} \\ |\phi_{kj}\rangle &= \frac{1}{\sqrt{d}} \sum_i \omega^{ki} |i,j\rangle \otimes \overline{|i,j\rangle}, \end{aligned} \tag{3.19}$$

whereby the range of indices is the same as in (3.15). Note that $|i\rangle$ denotes the standard basis and that the first line is independent of j. The complex conjugation of the basis vectors $\overline{|i,j\rangle}$ is to be understood as complex-conjugation of the vector's coefficients in the standard basis.

3.3 A Complete Set of MUBs is a Quantum 2-Design

The concept of *quantum designs* was introduced by Zauner in his PhD thesis [27] (see also [20], [10], [11], [12]) and is closely related to the notion of POVMs used in quantum theory.

Definition 2. *A quantum design is a set $D = \{P_1, ..., P_v\}$ $(v \geq 2)$ of complex (or real) $d \times d$ projection matrices.*

- *D is **regular** if $Tr(P_i) = r \quad \forall i$*
- *D is **coherent** if $\sum P_i = l\mathbb{1} \quad l \in \mathbb{R}$*
- *Let G be an arbitrary group of unitary $d \times d$ matrices. Then D is **k-coherent** with respect to the group G if the following relation holds for all matrices $U \in G$: $\sum_i P_i^{\otimes k} = \sum_i (U P_i U^{-1})^{\otimes k}$*
- *D is a quantum **t-design** w.r.t. G if it is k-coherent $\forall k \leq t$ w.r.t. G.*
- *D is of **degree n**, if the set $\Lambda = \{Tr(P_i P_j) : 1 \leq i < j \leq v\} = \{\lambda_1, ...\lambda_n\}$ is of cardinality n.*
- *A subset of D is an **orthogonal class** if the corresponding projections are mutually orthogonal. If the sum of all its projection matrices adds up to the identity matrix, then an orthogonal class is said to be complete. A quantum design is called **resolvable** if it can be written as the disjoint union of complete orthogonal classes.*

- *A degree 2 resolvable quantum design will be called an* ***affine quantum design****.*

A set of MUBs $\{P_{ij}\}_m$ is an affine quantum design. As we will show in this section cMUBs are quantum 2-designs. Furthermore SIC-POVMs are also quantum 2-designs of degree 1.

Theorem 4. (Zauner [27], Theorem 1.15) *Let $D = \{P_1, ..., P_v\}$ be a regular quantum design, let $G \subseteq U(b)$, then D is t-coherent w.r.t. G if and only if*

$$\frac{1}{v}\sum_i P_i^{\otimes t} = \int_G (UP_0U^\dagger)^{\otimes t} du. \tag{3.20}$$

Some authors refer to (3.20) rather than Definition 2 as the defining relation for quantum t-designs. For our considerations $\{P_i = |\phi_i\rangle\langle\phi_i|\}$ are projectors on normalized pure states in $\mathbb{C}^d$. We can therefore rewrite (3.20) as an integral over $\mathbb{C}S^{d-1}$, the complex unit-sphere in $\mathbb{C}^d$:

$$\frac{1}{v}\sum_i |\phi_i\rangle\langle\phi_i|^{\otimes t} = \int_{\mathbb{C}S^{d-1}} |\psi\rangle\langle\psi|^{\otimes t} d\psi \tag{3.21}$$

Since we take $G = SU(d)$, G is irreducible. Since the integration is over the invariant Haar measure, we obtain (due to Schur's Lemma) that

$$\int_{\mathbb{C}S^{d-1}} |\psi\rangle\langle\psi|^{\otimes t} d\psi = \frac{\mathbb{1}_{Sym}}{Tr(\mathbb{1}_{Sym})}, \tag{3.22}$$

with $\mathbb{1}_{Sym}$ being the identity on $\mathscr{H}_{Sym} \subseteq \mathscr{H}^{\otimes t}$, the totally symmetric subspace and $Tr(\mathbb{1}_{Sym}) = \binom{d+t-1}{t}$.

Theorem 5. *$\{P_i\}$ is a quantum t-design if and only if*

$$\frac{1}{v^2}\sum_{ij} Tr(P_iP_j)^k = \frac{1}{\binom{d+k-1}{k}} \quad \forall k = 1, ..., t. \tag{3.23}$$

Proof. ($\Leftrightarrow$) That (3.23) is necessary and sufficient can be proven by defining

$$R = \frac{1}{v}\sum_i P_i^{\otimes k} - \frac{\mathbb{1}_{Sym}}{Tr(\mathbb{1}_{Sym})}. \tag{3.24}$$

$Tr(R^\dagger R) = 0$ if and only if $R = 0$. Since $Tr(R^\dagger R) = 0$ if and only if (3.23) holds, we have shown that (3.23) is necessary and sufficient for $\{P_i\}$ to be a quantum t-design. □

Theorem 6. *Complete sets of MUBs and SIC-POVMs are quantum 2-designs and the complete set of MUBs in $d = 2$ is a quantum 3-design.*

Proof. The proof is straight forward by inserting (3.5) and for SIC-POVMs respectively, (3.14) into (3.23). □

Chapter 4

Entanglement in Mutually Unbiased Bases

4.1 Conservation of Entanglement in Complete Sets of MUBs

One interesting line of enquiry into the problem of existence of MUBs was opened by Wiesniak et al. [24] by analysing the "amount of entanglement" in complete sets of MUBs. They made use of the fact that complete sets of MUBs are complex projective 2-designs. As discussed in Section 3.3 this implies

$$\int_{\mathbb{C}S^{d-1}} (\langle\Psi| \otimes \langle\Psi|) M (|\Psi\rangle \otimes |\Psi\rangle) \mathrm{d}\Psi = \frac{1}{d(d+1)} \sum_{ij} Tr[(P_{ij} \otimes P_{ij}) M] \tag{4.1}$$

for an arbitrary Matrix $M \in \mathbb{M}(\mathbb{C}, d)^{\otimes 2}$ and $\{P_{ij} = |\phi_{ij}\rangle\langle\phi_{ij}|\}$ being a complete set of MUBs in $\mathbb{C}^d$. Furthermore, by taking the sum over several matrices M, this implies that polynomials $\mathbf{P}(\Psi)$ that are bi-quadratic in the coefficients of Ψ respective to a fixed basis fulfill

$$\int_{\mathbb{C}S^{d-1}} \mathbf{P}(\Psi) \mathrm{d}\Psi = \frac{1}{d(d+1)} \sum_{ij} \mathbf{P}(\phi_{ij}). \tag{4.2}$$

The purity of the reduced density matrix is not only a measure for entanglement between two systems (A and B), but also a bi-quadratic polynomial. Hence by setting $\mathbf{P}(\Psi) = Tr(Tr_B(|\Psi\rangle\langle\Psi|)^2)$ Wiesnak et al. showed in [24] that entanglement in complete sets of MUBs is conserved. By using

$$\int_{\mathbb{C}S^{d-1}} \mathbf{P}(\Psi) \mathrm{d}\Psi = \frac{d_A d_B}{(d+1)}, \tag{4.3}$$

a result obtained in [16], the "amount of entanglement" of any complete set of MUBs can be quantified with

$$\sum_{ij} Tr(Tr_B(P_{ij})^2) = d_A d_B(d_A + d_B), \tag{4.4}$$

with $\mathbb{C}^d = \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$ and $d = d_A d_B$. This insight implies the following:

Lemma 1. *If $d_A \leq d_B$ and the first $d_A + 1$ bases consist of product states only, the remaining $d_A(d_B - 1)$ bases consist entirely of maximally entangled states.*

Note that for maximally entangled ϕ_{ij} we get $Tr(Tr_B(P_{ij})^2) = 1/d_A$ and for ϕ_{ij} being a product state $Tr(Tr_B(P_{ij})^2) = 1$. It follows immediately that the maximal number of product MUBs is $d_A + 1$.

4.2 A New Proof for the Conservation of Entanglement in Complete Sets of MUBs

We can also present a new and alternative proof for (4.4). We start by identifying the matrix $M \in \mathbb{M}(\mathbb{C}, d)^{\otimes 2}$ that fulfills the following equation

$$\langle ij|\overline{\langle ij|}M_B|ij\rangle\overline{|ij\rangle} = Tr(Tr_B(P_{ij})^2). \tag{4.5}$$

Equivalently one can look at M_A returning the purity of the reduced density matrix, when tracing out system A. If we take M to be an operator on $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B} \otimes \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$, straight forward calculation yields that

$$\begin{aligned} M_B &= \sum_{m,n=0}^{d_A-1} (\sum_{k=0}^{d_B-1} |m\rangle_A |k\rangle_B |n\rangle_A |k\rangle_B)(\sum_{k'=0}^{d_B-1} \langle m|_A \langle k'|_B \langle n|_A \langle k'|_B) \\ &= \sum_{k,k'=0}^{d_B-1} \mathbb{1}_A \otimes |k\rangle\langle k'|_B \otimes \mathbb{1}_A \otimes |k\rangle\langle k'|_B. \end{aligned} \tag{4.6}$$

M_B has furthermore a d_A^2-times degenerate eigenvalue $\lambda_1 = d_B$ and a $(d^2 - d_A^2)$-times degenerate eigenvalue $\lambda_2 = 0$ and

$$M_B|\Phi\rangle = d_B|\Phi\rangle, \tag{4.7}$$

with

$$|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle \otimes |i\rangle. \tag{4.8}$$

If we employ the construction (3.19) we get

$$Tr(M) = \langle\Phi|M|\Phi\rangle + \sum_{kj}\langle\phi_{kj}|M|\phi_{kj}\rangle. \tag{4.9}$$

Due to the following relation

$$\begin{aligned}\langle\Phi|M|\Phi\rangle + \sum_{k=1}^{d-1}\langle\phi_{kj}|M|\phi_{kj}\rangle &= \sum_{i,i'=0}^{d-1}\langle ij|\overline{\langle ij|}M|i'j\rangle\overline{|i'j\rangle}\sum_{k=0}^{d-1}\omega^{k(i-i')} \\ &= \sum_{i=0}^{d-1}\langle ij|\overline{\langle ij|}M|ij\rangle\overline{|ij\rangle}\end{aligned} \tag{4.10}$$

we obtain, by inserting in (4.9), that

$$\begin{aligned}\sum_{ij}\langle ij|\overline{\langle ij|}M_B|ij\rangle\overline{|ij\rangle} &= Tr(M_B) + d\langle\Phi|M_B|\Phi\rangle \\ &= d_B d_A^2 + d d_B \\ &= d_A d_B(d_A + d_B),\end{aligned} \tag{4.11}$$

which proves the result from (4.4) obtained by Lubkin. [16] This proof for the conservation of entanglement in complete sets of MUBs is alternative to the one in [24], since it does not draw on the quantum-design property. Note that the same result is obtained when tracing out sub-system A by using M_A.

4.3 Direct and Indirect Product Bases

Wiesniak et al [24] introduce the distinction between *direct* and *indirect* product bases. Direct product bases in dimension d can be denoted as $\{|a_i, b_j\rangle\}$ ($i = 1,...d_A$; $j = 1,...d_B$) with $\{|a_i\rangle\}$ and $\{|b_j\rangle\}$ being bases on the respective subspaces. An indirect product base is a product base that cannot be written this way. We denote them with the more general notation $\{|\psi_i, \Psi_i\rangle\}$ with $i = 1,...d$. Concerning direct product bases, the following lemma can be proved (see also [24]):

Lemma 2. (Wiesniak et al. [24], Lemma 5) *Two direct product bases* $\{|a_i, b_j\rangle\}$ *and* $\{|a'_i, b'_i\rangle\}$ *are mutually unbiased if and only if* $\forall i, i', j, j'$ $|\langle a_i|a'_{i'}\rangle|^2 = 1/d_A \wedge |\langle b_j|b'_{j'}\rangle|^2 = 1/d_B$ *or in words:* $|a_i\rangle$ *is mutually unbiased to* $|a'_{i'}\rangle$ *and* $|b_j\rangle$ *to* $|b'_{j'}\rangle$.

Proof. Since $\{|a_i\rangle\}$ and $\{|b_j\rangle\}$ are bases for the subspaces, for the two direct product bases to be mutually unbiased

$$|\langle a_i|a'_{i'}\rangle|^2|\langle b_j|b'_{j'}\rangle|^2 = \frac{1}{d_A d_B} \quad \forall i, i', j, j', \tag{4.12}$$

it must hold that

$$\begin{aligned}\sum_i |\langle a_i|a'_{i'}\rangle|^2|\langle b_j|b'_{j'}\rangle|^2 = |\langle b_j|b'_{j'}\rangle|^2 = \frac{1}{d_B}\\ \sum_j |\langle a_i|a'_{i'}\rangle|^2|\langle b_j|b'_{j'}\rangle|^2 = |\langle a_i|a'_{i'}\rangle|^2 = \frac{1}{d_A}.\end{aligned} \tag{4.13}$$

□

McNulty et al. studied in [17] in great detail product bases for $d = 6$. For this purpose they also generalised Lemma 2 to

Lemma 3. (McNulty et al. [17], Lemma 3) *The product state* $\{|\phi,\Phi\rangle\}$ *in dimension* $d = d_A d_B$ *is mutually unbiased to the set of orthogonal product states* $\{|\psi_i,\Psi\rangle\}$ *(i = 1,...p) if and only if* $|\phi\rangle$ *is mutually unbiased to* $|\psi_i\rangle \in \mathbb{C}^{d_A}$ *and* $|\Phi\rangle$ *is MU to* $|\Psi\rangle \in \mathbb{C}^{d_B}$.

The proof is parallel to the proof of Lemma 2. McNulty's formulation of Lemma 3 is stronger since it is a statement about single product basis vectors rather than a whole basis. For $d \leq 6$ [17] proves a stronger statement, also covering the more general case of indirect product bases.

Theorem 7. (McNulty et al. [17], Theorem 1) *The product state* $\{|\phi,\Phi\rangle\}$ *in dimension* $d = d_A d_B \leq 6$ *is mutually unbiased to the set of orthogonal product states* $\{|\psi_i,\Psi_i\rangle\}(i = 1,...d_A d_B)$ *if and only if* $|\phi\rangle$ *is mutually unbiased to* $|\psi_i\rangle \in \mathbb{C}^{d_A}$ *and* $|\Phi\rangle$ *is mutually unbiased to* $|\Psi_i\rangle \in \mathbb{C}^{d_B}$.

The proof relies on the structure of all sets of MU product bases in dimension $d = 4, 6$ elaborated in [17]. McNulty conjectures that Theorem 7 also holds for $d > 6$, but that a similar proof would require knowledge of the structure of all sets of MU product bases in higher dimension. It is however possible to generalize McNulty's result to arbitrary dimension, without relying on the explicit structure of MU product bases in higher dimensions. If a product vector $|\phi,\Phi\rangle$ is MU to a general product base $\{|\psi_i,\Psi_i\rangle\}$ for $\mathbb{C}^{d_A d_B}$ we have

$$|\langle\phi|\psi_i\rangle|^2|\langle\Phi|\Psi_i\rangle|^2 = \frac{1}{d_A d_B} \quad \forall i. \tag{4.14}$$

Furthermore we can write

$$\begin{aligned}Tr(\mathbb{1}\otimes|\Phi\rangle\langle\Phi|) &= \sum_i \langle\psi_i,\Psi_i|(\mathbb{1}\otimes|\Phi\rangle\langle\Phi|)|\psi_i,\Psi_i\rangle\\ &= \sum_i |\langle\Psi_i|\Phi\rangle|^2 = d_A\\ Tr(|\phi\rangle\langle\phi|\otimes\mathbb{1}) &= \sum_i |\langle\psi_i|\phi\rangle|^2 = d_B.\end{aligned} \tag{4.15}$$

If we define

$$\begin{aligned} q_i &:= \frac{1}{d_B} + \mu_i = |\langle \Psi_i | \Phi \rangle|^2 \quad 0 < q_i \leq 1 \\ p_i &:= \frac{1}{d_A} + \epsilon_i = |\langle \psi_i | \phi \rangle|^2 \quad 0 < p_i \leq 1, \end{aligned} \tag{4.16}$$

we obtain by inserting into (4.14) and (4.15)

$$\begin{aligned} \sum_i q_i = d_A, \quad \sum_i p_i = d_B, \\ \sum_i \epsilon_i = 0, \quad \sum_i \mu_i = 0, \\ \frac{\mu_i}{d_A} + \frac{\epsilon_i}{d_B} + \mu_i \epsilon_i = 0, \\ \sum_i \mu_i \epsilon_i = 0. \end{aligned} \tag{4.17}$$

From (4.17) we obtain the following condition:

$$\frac{1}{d_A} \sum_i \frac{-\mu_i^2}{q_i} = 0. \tag{4.18}$$

Since $\frac{-\mu_i^2}{q_i} \leq 0 \quad \forall i$ we obtain that $\mu_i = 0$. From this follows $\epsilon_i = 0$ and

$$|\langle \psi_i | \phi \rangle|^2 = \frac{1}{d_A} \quad |\langle \Psi_i | \Phi \rangle|^2 = \frac{1}{d_B}, \tag{4.19}$$

which completes the proof of the generalisation of Theorem 7.

Theorem 8. *The product state $\{|\phi, \Phi\rangle\}$ in dimension $d = d_A d_B$ is mutually unbiased to the set of orthogonal product states $\{|\psi_i, \Psi_i\rangle\}(i = 1, ...d_A d_B)$ if and only if $|\phi\rangle$ is MU to $|\psi_i\rangle \in \mathbb{C}^{d_A}$ and $|\Phi\rangle$ is mutually unbiased to $|\Psi_i\rangle \in \mathbb{C}^{d_B}$.*

4.4 Product Bases in Dimension 6 and Other Related Results

Constructions of complete sets of MUBs in prime power dimension $d = p^n$ always allow for $p+1$ (direct) product bases and the remaining bases being maximally entangled (compare the construction in Section 5.3.2). For $d = p^2$ this structure is even required. [14]

In dimension 6, the straight forward approach mentioned above furthermore bears the nice analytic result that a triplet of product bases in dimension 6 cannot be extended by even one mutually unbiased vector. [19] [17] By combining the completely worked out structure of product bases in dimension 6 with computational results, one can furthermore obtain that in a complete set of MUBs in dimension 6 there cannot be any other product base than the standard basis. [18] These results were achieved on the foundation of having characterised all possible sets of MUBs in [4], which again relied on the knowledge of all complex Hadamard matrices in dimensions 2 to 5. With the generalized Theorem 8 it should therefore be possible (with a good amount of patience and hard work) to proceed parallel to [17] and obtain results for product MUBs for composite dimensions 10, 12 and 15, whereby 12 is looked at as a product space of dimension 3 × 4.

The results obtained for product MUBs can be extended to a larger category of bases in a natural way, namely those in the same equivalence class. As discussed in Chapter 2 the defining equations (3.5) are invariant under the transformations listed in Definition 1. Hence the results from [19] also cover results for those non-product bases in the same equivalence class. An example for this is e.g. the result that for $d = 6$ the MUB duple $\{\mathbb{1}, F\}$, with F being the Fourier matrix, cannot be part of a complete set of MUBs; a result that was independently obtained in [8].

Chapter 5

Mutually Unbiased Bases and Unitary Operator Bases

5.1 Schwinger's 1960 Paper

Schwinger's 1960 paper [21] is often referred to as introducing the concept of MUBs. Schwinger starts out by defining a unitary operator U with the eigenbasis $\{|u_i\rangle\}$. He further defines a second unitary V in the following way:

$$V|u_i\rangle = |u_{i+1}\rangle. \tag{5.1}$$

In words: V simply relabels or permutes the basis elements of U. From this definition and the cyclic property of V,

$$V^d = \mathbb{1}, \tag{5.2}$$

Schwinger then derives the following properties of the operator pair U and V and their eigenbases:

$$U^d = \mathbb{1}, \tag{5.3}$$

$$\begin{aligned} \langle u_k|v_j\rangle &= \frac{1}{\sqrt{d}}\omega^{kj}, \\ |\langle u_k|v_j\rangle|^2 &= \frac{1}{d}, \end{aligned} \tag{5.4}$$

$$|u_k\rangle = \frac{1}{\sqrt{d}}\sum_l \omega^{-kl}|v_l\rangle, \tag{5.5}$$

$$\begin{aligned} U|u_k\rangle &= \omega^k|u_k\rangle, \\ V|v_k\rangle &= \omega^k|v_k\rangle \end{aligned} \tag{5.6}$$

and

$$VU = \omega UV. \tag{5.7}$$

Schwinger writes " *(t)hus the properties of U and V exhibit the maximum degree of incompatability.*" [21] This is the locus classicus for what we today call MUBs. Schwinger continues by elaborating a property that will be crucial in our approach to the existence problem. The unitary matrices generated by U and V,

$$X_{mn} = \frac{1}{\sqrt{d}} U^m V^n \quad m, n = 0, ...d-1, \tag{5.8}$$

form a unitary operator ONB for $\mathbb{M}(\mathbb{C}, d)$. Schwinger does not talk about complete sets of operators exhibiting a maximum degree of incompatability, but he elaborates on another interesting connection between the integer factorization of d and unitary operator bases. He points out that in non-prime dimensions $d = d_A d_B$, one can always reorganise the indices k in the following way:

$$k = d_B k_A + k_B \quad k_A = 0, ..., d_A - 1; k_B = 0, ..., d_B - 1. \tag{5.9}$$

Then he defines

$$\begin{aligned} |u_k\rangle &= |u_{k_A}, u_{k_B}\rangle, \\ |v_k\rangle &= |v_{k_A}, v_{k_B}\rangle, \end{aligned} \tag{5.10}$$

with the following operators and relations

$$\begin{aligned} U_A|u_{k_A}, u_{k_B}\rangle &= \omega_{d_A}^{k_A}|u_{k_A}, u_{k_B}\rangle, \quad U_B|u_{k_A}, u_{k_B}\rangle = \omega_{d_B}^{k_B}|u_{k_A}, u_{k_B}\rangle, \\ V_A|v_{k_A}, v_{k_B}\rangle &= \omega_{d_A}^{k_A}|v_{k_A}, v_{k_B}\rangle, \quad V_B|v_{k_A}, v_{k_B}\rangle = \omega_{d_B}^{k_B}|v_{k_A}, v_{k_B}\rangle \end{aligned} \tag{5.11}$$

and

$$\begin{aligned} V_A|u_{k_A}, u_{k_B}\rangle &= |u_{k_A+1}, u_{k_B}\rangle, \quad V_B|u_{k_A}, u_{k_B}\rangle = |u_{k_A}, u_{k_B+1}\rangle, \\ U_A|v_{k_A}, v_{k_B}\rangle &= |v_{k_A+1}, v_{k_B}\rangle, \quad U_B|v_{k_A}, v_{k_B}\rangle = |v_{k_A}, v_{k_B+1}\rangle. \end{aligned} \tag{5.12}$$

These definitions reproduce the properties

$$U_j^{d_j} = V_j^{d_j} = \mathbb{1}, \quad V_j U_j = \omega_{d_j} U_j V_j \quad j = A, B \tag{5.13}$$

together with the commutativity of two operators with different subscripts j. Subsequent factorization concludes with a factorization in f prime factors and allows to describe a basis for $\mathbb{M}(\mathbb{C}, d)$ generated by f commuting bases for Hilbert-Schmidt spaces of prime dimension, $\mathbb{M}(\mathbb{C}, p_j)$. The basis for $\mathbb{M}(\mathbb{C}, d)$ can then be written as

$$\begin{aligned} X_{mn} &= \prod_{j=1}^{f} X_{m_j n_j} \\ X_{m_j n_j} &= \frac{1}{\sqrt{p_j}} U_j^{m_j} V_j^{n_j} \quad m_j, n_j = 0, ..., p_j - 1. \end{aligned} \tag{5.14}$$

In Schwinger's approach, the basis of the Hilbert-Schmidt space in composite dimension can be "naturally" seen as commuting subspaces of prime dimension. This leads Schwinger to refer to prime dimension as *fundamental quantum degrees of freedom.* As we already saw in Theorem 3 and as we will explore in the next sections, unitary operator bases and MUBs are connected in a profound way. Furthermore it would not be surprising if the integer decomposition (i.e. whether it is a system of prime power or composite dimension) comes to bear in the existence problem of MUBs, as widely conjectured.

Before we move on, we shall however explicate one relationship in Schwinger's approach. (5.5) shows that the eigenvectors of V are the Fourier transformation of the eigenvectors of U. We have furthermore seen that the eigenvectors of U and V are mutually unbiased. In the language of complex Hadamard matrices, the pair $\{U,V\}$ therefore corresponds to the pair $\{\mathbb{1},F\}$, with F being the Fourier matrix. Furthermore, assuming that U and V can be written in the following way

$$\begin{aligned} U &= \sum_k \omega^k |u_k\rangle\langle u_k|, \\ V &= \sum_k \omega^k |v_k\rangle\langle v_k|, \end{aligned} \tag{5.15}$$

the conditions (5.5) and (5.7) are equivalent. Since (5.15) is not only the case in Schwinger's approach, but also relevant for the new approach developed in the next section, we will formulate the following Lemma.

Lemma 4. *Given (5.15), the condition (5.5) for the eigenvectors and the condition for the commutator of the corresponding unitary matrices (5.7) are equivalent.*

Proof. (⇒) Assuming (5.5) and (5.15) we obtain

$$\begin{aligned} U|v_k\rangle &= |v_{k+1}\rangle, \\ \langle v_k|U &= \langle v_{k-1}| \end{aligned} \tag{5.16}$$

and hence

$$\begin{aligned} VU &= \frac{1}{\sqrt{d}}\sum_k \omega^k |v_k\rangle\langle v_k|U = \frac{1}{\sqrt{d}}\sum_k \omega^k |v_k\rangle\langle v_{k-1}| = \\ &= \frac{1}{\sqrt{d}}\sum_k \omega^{k+1} |v_{k+1}\rangle\langle v_k| = \omega U V. \end{aligned} \tag{5.17}$$

(⇐) Starting with (5.7) and (5.15) we can write

$$\begin{aligned} VU|v_l\rangle =& \omega UV|v_l\rangle \quad \Leftrightarrow \\ VU|v_l\rangle =& \omega^{l+1} U|v_l\rangle \end{aligned} \tag{5.18}$$

and since the eigenvalues of U and V are not degenerate we obtain

$$U|v_l\rangle = |v_{l+1}\rangle. \tag{5.19}$$

Since both matrices V and U generate a set of d commuting matrices and since those two sets $\{U^n\}$ and $\{V^n\}$ are orthogonal, their eigenvectors are mutually unbiased. Hence we can use the following ansatz

$$|v_l\rangle = \sum_k H_{kl}|u_l\rangle, \tag{5.20}$$

with H_{kl} again being a complex Hadamard matrix. By inserting into (5.19) we obtain

$$H_{k,l+1} = \omega^k H_{k,l}, \tag{5.21}$$

which is, up to equivalences as discussed in Definition 1, the Fourier matrix F_{kl}. This completes the proof of the Lemma. □

This indicates that the commutator relations of the two generating matrices in a unitary operator basis maps onto the choice of the second complex Hadamard matrix H_1 in $\{\mathbb{1}, H_1, ...\}$.

5.2 A New Approach to the Existence Problem

Bandyopadhyay et al. [2] develop a similar approach to the one that was shortly introduced in Section 3.2. The following two theorems are proven there:

Theorem 9. (Bandyopadhyay et al. [2], Theorem 3.2) *If there is a maximally commuting basis of orthogonal unitary matrices in $\mathbb{M}(\mathbb{C}, d)$, then there is a set of $d+1$ mutually unbiased bases.*

Theorem 10. (Bandyopadhyay et al. [2], Theorem 3.4) *Let $\mathscr{B}_1, ..., \mathscr{B}_M$ be a set of M MUBs in $\mathbb{C}^d$, then there are M classes $\mathscr{C}_1, ..., \mathscr{C}_M$ of d commuting unitary matrices, such that matrices in $\mathscr{C}_1 \cup ... \cup \mathscr{C}_M$ are pairwise orthogonal.*

Theorem 3 is obviously closely related to Theorem 9 and Theorem 10. The proof for Theorem 10 presented in [2] is equivalent to the first direction of the proof for Theorem 3 above. It is however possible to generalize Theorem 9 by drawing on the fact that the proof in [2] is stronger than the actual formulation of Theorem 9 and as we shall show can be reformulated.

Theorem 11. *For every set of M mutually unbiased bases $\{P_{ij}\}$ exist $M(d-1)+1$ mutually orthogonal unitary matrices $\{U_{kj}\}$, consisting of M subsets of d pairwise commuting elements (each subset containing the identity) and conversely, for each such set of mutually orthogonal unitary matrices $\{U_{kj}\}$ there is a set of M mutually unbiased bases $\{P_{ij}\}$.*

Proof. (⇐) Assume we have a set of $M(d-1)+1$ mutually orthogonal unitary matrices $\{U_{kj}\}$ fulfilling the following relation:

$$[U_{kj}, U_{lj}] = 0 \quad \forall k, l. \tag{5.22}$$

Each commuting subset can be simultaneously diagonalized. We can therefore write

$$U_{kj} = \sum_i \lambda_{ik}^{(j)} |\psi_i^{(j)}\rangle\langle\psi_i^{(j)}| = \sum_i \lambda_{ik}^{(j)} P_{ij}. \tag{5.23}$$

Since the matrices in $\{U_{kj}\}$ are assumed to also be mutually orthogonal and unitary, the eigenvalues constitute the entries of Hadamard matrices:

$$\begin{aligned} \lambda_{ik}^{(j)} &= H_{ik}^{(j)} \\ \sum_i H_{ik}^{(j)} \overline{H}_{il}^{(j)} &= d\delta_{kl}. \end{aligned} \tag{5.24}$$

Since each set contains the identity and since there is phase freedom,

$$[U_{kj}, U_{lj}] = 0 \Leftrightarrow [e^{i\alpha} U_{kj}, e^{i\beta} U_{lj}] = 0, \tag{5.25}$$

the Hadamard matrices can be brought into their dephased form. We can furthermore assume without loss of generality that $U_{0j} = \mathbb{1}$. The orthogonality relations for $j \neq j'$ can therefore be written as

$$Tr(U_{kj} U_{lj'}^\dagger) = \delta_{k0}\delta_{l0}. \tag{5.26}$$

By inserting (5.23) into (5.26) and applying (5.24) we obtain

$$Tr(P_{ij} P_{i'j'}) = \delta_{ii'}\delta_{jj'} + (1-\delta_{jj'})\frac{1}{d}. \tag{5.27}$$

This means that all sets of pairwise orthogonal and pairwise commuting unitary matrices $\{\{U_{i,0}\}, ...\{U_{i,m}\}\}$ have mutually unbiased eigenvectors. The "inner structure" of these pairwise orthogonal and pairwise commuting unitary matrices is furthermore completely captured in dephased Hadamard matrices.

(⇒) For the other direction of the proof, see Theorem 3 or Theorem 9. □

It is however important to note that the construction presented in the proof for Theorem 3 is not the only way to construct commuting subsets. It makes use of the Fourier matrix F, which is a special instant of the more general set of dephased Hadamard matrices. Any arbitrary set of M complex Hadamard matrices $\{H^{(1)}, ..., H^{(M)}\}$ provides a valid construction. Knowledge of all complex Hadamard matrices and all sets of MUBs therefore allows to construct all possible sets of orthogonal unitary matrices with maximally commuting subsets.

The connection between MUBs and sets of orthogonal unitary matrices with maximally commuting subsets is obviously not 1-to-1. It is however possible to strengthen Theorem 3 and establish a stronger correspondence, if one demands that the commuting subsets are in fact cyclic groups under matrix multiplication. In order to show this we shall first prove the following Lemma.

Lemma 5. *Each set of mutually orthogonal unitary matrices* $\{Q_j^k\}_M$ *with cyclic subset structure as defined in (3.16) can be written as* $\{Q_j^k = V_j T^k V_j^\dagger\}$*, with* V_j *being unitary matrices and* T *being the "twisting-operator" defined as*

$$T = \begin{pmatrix} 1 & & & \\ & \omega_d & & \\ & & \omega_d^2 & \\ & & & \ddots \end{pmatrix}. \tag{5.28}$$

Proof. Any cyclic group of unitary matrices $\{Q_j^k\}$ can be simultaneously diagonalized and therefore written as $\{V_j D^k V_j^\dagger\}$. D being a diagonal matrix with entries $|e_i| = 1$ and without loss of generality, $e_1 = 1$. Furthermore we have

$$D^d = \begin{pmatrix} 1 & & & \\ & e_2^d & & \\ & & e_3^d & \\ & & & \ddots \end{pmatrix} = \mathbb{1}. \tag{5.29}$$

We therefore obtain that e_j is a d-th root of 1,

$$e_j = \omega_d^k \quad k \in \{0,1,2,...d-1\}. \tag{5.30}$$

D furthermore needs to generate a group of d distinct (orthogonal) elements (including $\mathbb{1}$). This is the maximally possible number, since the sub-space of mutually commuting operators has dimension d. If however there would exist a pair of diagonal elements, e_i and e_j, so that

$$e_i = e_j, \tag{5.31}$$

there would also exist an n-dimensional subspace $\{\Lambda : \Lambda = \lambda(|i\rangle\langle i| - |j\rangle\langle j|), \lambda \in \mathbb{C}\}$ that is orthogonal to D and all elements generated by D. Furthermore, there would be no element in this subspace that could be generated by D. Hence, D could not generate a group of d mutually orthogonal unitary operators. We can therefore conclude that in the case of mutually orthogonal unitary matrices with cyclic group structure, D must be equal to T or a permutation thereof. □

Theorem 12. *For each equivalence class of a set of M mutually unbiased bases $\{P_{ij}\}_M$ exists "exactly one" set of $M(d-1)+1$ mutually orthogonal unitary matrices $\{Q_{kj}\}_M$, consisting of M cyclic groups generated by m mutually orthogonal unitary matrices $\{Q_1, ...Q_M\}$ and conversely, for each such set $\{Q_{kj}\}_M$ there is an equivalence class of a set of M mutually unbiased bases $\{P_{ij}\}_M$.*

Proof. We need to show that the construction presented in the proof for Theorem 3 is the only one possible. We shall first prove that each $\{Q_j^k\}_M$ or $\{V_j T^k V_j^\dagger\}_M$ uniquely determines one set of MUBs $\{P_{ij}\}_M$.

($\Leftarrow$)The eigenvectors of Q_j^k are $V_j|i\rangle$ with ω^{ik} as eigenvalues. The matrices Q_j have no degenerate eigenvalues; their eigenbases are therefore uniquely determined. Since we have proven above that the eigenvalues of the subsets are mutually unbiased, the first direction of the proof is completed. It remains to be shown that the construction presented in (3.15) is the only possible construction of a set $\{Q_j^k\}$ satisfying the cyclic group properties formulated in (3.16).

($\Rightarrow$) We have shown above that such a construction consists neccessarily of a set of complex Hadamard matrices,

$$Q_{kj} = \sum_i H_{ik}^{(j)} P_{ij}. \tag{5.32}$$

As Lemma 5 shows, the additional condition of cyclicity is only fulfilled if

$$H_{ik} = \omega_d^{ik}. \tag{5.33}$$

This completes the proof. □

"Exactly one" here refers to the fact that the equivalence is stronger than the equivalence classes introduced in Definition 1. The cyclic group structure fixes the free parameters defined in (2.3), the global unitary and (2.4), the basis vector's free phases. The freedoms defined, however, in (2.5), (2.6) and (2.7), namely the permutation of basis vectors and bases as well as complex conjugation, are and ought to be preserved. It follows as a corollary that

$$P_{ij} = V_j|i\rangle\langle i|V_j^\dagger. \tag{5.34}$$

Theorem 12 is interesting because it is not just a constructive result, but it establishes a necessary 1-to-1 relationship between sets of MUBs $\{P_{ij}\}_M$ and orthogonal unitary matrices, with cyclical subsets $\{Q_{kj}\}_m$. If a k-parametric set of the one exists, so does it for the other etc. To reformulate: We have shown that the problem of the existence of sets of MUBs is equivalent to showing that a set of $\{T^k, V_1 T^k V_1^\dagger, ... V_{M-1} T^k V_{M-1}^\dagger\}$ mutually orthogonal matrices exists. As we have seen in Section 5.1 however $\{T^k, V_1 T^k V_1^\dagger, T^l V_1 T^k V_1^\dagger\}$ is also an orthonormal basis for the Hilbert-Schmidt space. All other elements in $\{T^k, V_1 T^k V_1^\dagger, \dots V_{M-1} T^k V_{M-1}^\dagger\}$ can therefore be written as a linear combination of those elements. In the next chapter we shall elaborate the connections between existing constructions for complete sets of MUBs and Theorem 12.

5.3 The Standard Constructions for MUBs

The Weyl-Heisenberg matrices can be regarded as "the" unitary operator ONB. They play a central role in all known constructions for complete sets of MUBs. In their monograph-like review paper [7] Durt et al. discuss in detail the constructions for complete sets of MUBs in prime and prime-power dimensions and they manage to develop a unified view of the constructions by Ivanovic [13], Wootters and Field [26], Bandyopadhyay et al. [2] and Lawrence et al. [15] based on the Weyl-Heisenberg matrices. The Weyl-Heisenberg matrices are defined as

$$S_{jk} = \sum_{i=0}^{d-1} \omega^{ij} |i\rangle\langle i+k|, \tag{5.35}$$

whereby all additions and multiplications of the indices are modulo d. Straight forward calculations yield that $\{S_{jk}\}$ is an orthogonal basis for the Hilbert-Schmidt space consisting of unitary matrices including the identity. Hence all matrices except for the identity are traceless. Furthermore the Weyl-Heisenberg matrices have two generators

$$S_{jk} = S_{10}^j S_{01}^k \tag{5.36}$$

and the following multiplication property

$$S_{jk} S_{rs} = \omega^{kr} S_{j+r,k+s}. \tag{5.37}$$

From (5.37) follows that

$$[S_{jk}, S_{rs}] = 0 \Leftrightarrow kr - sj = 0. \tag{5.38}$$

5.3.1 Prime Dimensions

For prime dimensions $d = p$ (since addition and multiplication modulo p constitute a finite field) the condition in (5.37) can be read as symplectic product μ on the vector space $\mathbb{F}_p^2$. We can therefore re-write (5.37) as

$$[S_{jk}, S_{rs}] = 0 \Leftrightarrow \mu\left(\begin{pmatrix} j \\ k \end{pmatrix}, \begin{pmatrix} r \\ s \end{pmatrix}\right) = kr - sj = 0. \tag{5.39}$$

Since

$$\mu\left(\begin{pmatrix} j \\ k \end{pmatrix}, \begin{pmatrix} j \\ k \end{pmatrix}\right) = 0 \tag{5.40}$$

we obtain

$$\mu\left(n\begin{pmatrix} j \\ k \end{pmatrix}, \begin{pmatrix} j \\ k \end{pmatrix}\right) = 0 \quad \forall n \in \mathbb{F}_p. \tag{5.41}$$

The ratio $\frac{j}{k}$ can take $p+1$ different values, namely $\{0,..,p-1\}$ and ∞ for $(k=0, j=1)$. It follows immediately that there are $p+1$ subsets with p commuting matrices lying on different lines in the vector space $\mathbb{F}_p^2$. Furthermore in prime dimension

$$S_{jk}^p = \omega_p^{p(p-1)/2}\mathbb{1} \tag{5.42}$$

holds. Hence, in the case of odd prime numbers, matrices with different index ratios $\frac{j}{k}$, e.g. $\{S_{01}, S_{11}, S_{21}, ...S_{10}\}$, generate mutually orthogonal cyclic subsets and therefore correspond to the generators from Theorem 12 $\{Q_1, ...Q_m\}$. The case $d = 2$ (and prime powers in general) is special. The simple square root of 1 ($\omega_2 = -1$) does not suffice to generate the desired group structure. The Pauli matrices are the well known solution securing the group structure in the 2-dimensional case. It is however necessary for this construction that p is a prime number since otherwise $\binom{j}{k}$ would not be elements in a vector space and there would exist a pair (n, n') fulfilling

$$\mu\left(n\begin{pmatrix} j \\ k \end{pmatrix}, n'\begin{pmatrix} j' \\ k' \end{pmatrix}\right) = 0, \tag{5.43}$$

with $\frac{j}{k} \neq \frac{j'}{k'}$. Hence the commuting subsets would "overlap."

5.3.2 Prime Power Dimensions

In the case of prime power dimensions ($d = p^n$), it is however possible to label elements of a Galois field $\mathbb{F}_{p^n}$ with the numbers $\{0, ..., p^n - 1\}$ and use the Galois field $\mathbb{F}_{p^n}$ and the respective vector-space $\mathbb{F}_{p^n}^2$ for a similar construction. We follow here the conventions employed in [7]. It is important to note that in the construction below, while indices are connected by the Galois field operations ($\oplus, \odot$), the field-elements are associated to natural numbers. The S_{jk} matrices however are (and must be) elements of the Hilbert-Schmidt space $\mathbb{M}(\mathbb{C}, p^N)$ and not $\mathbb{M}(\mathbb{F}_{p^n}, p^n)$. We re-define the Weyl-Heisenberg matrices as:

$$S_{jk} = \sum_{i=0}^{d-1} \omega_p^{i \odot j} |i\rangle\langle i \oplus k|. \tag{5.44}$$

For the following reason it is crucial to use ω_p and not ω_{p^n} in (5.44): While $\omega \in \mathbb{C}$, the index i is an element of $\mathbb{F}_{p^N}$. For the expression $\omega_p^{i\odot j}$ to be defined properly we need to assign natural numbers modulo d to all elements in $\mathbb{F}_{p^N}$. Therefore, for the construction to work we require the following identity

$$\omega^{i\oplus j} = \omega^{i+j}, \tag{5.45}$$

with $\omega^i, \omega^j \in \mathbb{C}$ and $\omega^i \omega^j = \omega^{i+j}$. The construction in [7] ensures this property by defining $\oplus$ the following way. The elements of the Galois field $\mathbb{F}_{p^N}$ can be written as polynomials of order $\leq N-1$

$$i = \sum_{m=0}^{N-1} i_m p^m. \tag{5.46}$$

The sum of two field elements

$$i = j \oplus k \tag{5.47}$$

can then be defined as component-wise addition modulo p

$$i_m = j_m + k_m \mod p, \tag{5.48}$$

which draws the connection to the construction in [2]. It is always possible to find such a field representation. It is interesting to note that if one labels the standard basis the following way

$$|i\rangle_{p^n} = \bigotimes_{m=0}^{N-1} |i_m\rangle, \tag{5.49}$$

the following simple and intuitive relation follows

$$|i \oplus j\rangle_{p^N} = \bigotimes_{m=0}^{N-1} |i_m + j_m\rangle. \tag{5.50}$$

From the definition in (5.48) follows for ω_p the relation required in (5.45), since

$$\omega_p^i \omega_p^j = \omega_p^{i_0} \omega_p^{j_0} = \omega_p^{i_0+j_0} = \omega_p^{i\oplus j}. \tag{5.51}$$

It can be easily shown that this would not hold for ω_{p^n}. It follows that

$$S_{j,k} S_{r,s} = \omega_p^{k\odot r} S_{j\oplus r, k\oplus s} \tag{5.52}$$

and

$$[S_{jk}, S_{rs}] = 0 \Leftrightarrow (k \odot r)_0 = (j \odot s)_0 \Leftarrow k \odot r = j \odot s. \tag{5.53}$$

As one can easily check, these S_{jk} matrices, constructed with the help of Galois fields, constitute an ONB of unitary matrices for $\mathbb{M}(\mathbb{C}, p^n)$. Note that we encounter in (5.53) for the prime power case, a symplectic structure corresponding to (5.38). We can therefore define

$$\begin{aligned} U_{k,j} &= S_{j\odot k,k} \\ U_{k,d} &= S_{k,0} \end{aligned} \tag{5.54}$$

fulfilling $[U_{kj}, U_{k'j}] = 0$. The eigenvectors shared by commuting subsets constitute a complete set of MUBs for prime-power dimensions. For the construction in (5.54) it does not matter whether d is an odd or even prime power. In an attempt to fix free phases by introducing additional structure, Durt [7] shows that it is possible to define abelian groups $\{U_{kj}\}$ fulfilling

$$\tilde{U}_{k,j}\tilde{U}_{k',j} = \tilde{U}_{k\oplus k',j} \tag{5.55}$$

by emplyoing this ansatz,

$$\tilde{U}_{k,j} = \alpha_{j,k} S_{j\odot k,k}. \tag{5.56}$$

(5.55) and $[\tilde{U}_{k,j}, \tilde{U}_{k',j}] = 0$ follow immediately. This ansatz also shows that there are $d+1$ distinct sets of d mutually commuting matrices. It is now only necessary to show that a choice for $\alpha_{j,k}$ exists which fulfills the relations induced by (5.52):

$$\alpha_{j,k}\alpha_{j,k'} = \alpha_{j,k\ominus k'}\omega_p^{j\odot k\odot k'}. \tag{5.57}$$

The possible choices for $\alpha_{j,k}$ differ, whether we are dealing with odd or even prime powers:

$$\alpha_{j,k} = \begin{cases} \omega_p^{\ominus j\odot k\odot k\oslash 2} \\ \prod_{m,n=0}^{N-1} i^{j\odot(k_m 2^m)(k_n 2^n)} & d = 2^N, \end{cases} \tag{5.58}$$

which completes the constructive proof for the existence of mutually unbiased bases in prime-power dimensions, as developed in [7]. We shall not elaborate at this point the connections and equivalences to other constructions in detail.

Note however that the ansatz (5.56) does not result in cyclic sub-groups. Furthermore the choice of α_{jk} is not necessarily unique to construct a basis $\{\tilde{U}_{kj}\}$ fulfilling (5.55) and (5.56). This illustrates the fact that cyclicity of the subsets is the condition that imposes the stronger correspondence, elaborated above, between unitary orthonormal bases and MUBs and not merely the abelian subgroup property. Although (5.58) as suggested in [7] is very elegant, it is still arbitrary. For an alternative phase convention for the construction in prime power dimension, see [1]. As we could see, in order to obtain a complete set of MUBs it is not necessary to engage in the rather long-winded discussion of defining and finding the factors α_{jk}, since the shared eigenvectors of the commuting subsets of $\{S_{kj}\}$ give the very same complete set of MUBs independent of the leading phases.

While the Q_{kj} matrices have no degenerate eigenvalues, the eigenvalues of U_{kj} are $p^N - 1$ degenerate. Only the overlap of the eigenbases in the commuting sets fixes the MUB vectors. In the next sections we shall now juxtapose the H-, U- and Q-matrices of the complete set of MUBs for $d = 4$.

5.4 H-, U- and Q-Matrices in d=4

$$\begin{aligned}\{H_j\} = \Bigg\{ &\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}, \frac{1}{2}\begin{pmatrix}1&1&1&1\\1&-1&1&-1\\1&1&-1&-1\\1&-1&-1&1\end{pmatrix}, \frac{1}{2}\begin{pmatrix}1&1&1&1\\i&-i&i&-i\\i&i&-i&-i\\-1&1&1&-1\end{pmatrix},\\ &\frac{1}{2}\begin{pmatrix}1&1&1&1\\i&-i&i&-i\\1&1&-1&-1\\-i&i&i&-i\end{pmatrix}, \frac{1}{2}\begin{pmatrix}1&1&1&1\\1&-1&1&-1\\i&i&-i&-i\\-i&i&i&-i\end{pmatrix}\Bigg\}\end{aligned} \tag{5.59}$$

are one standard form expression in complex Hadamard matrices for $d = 4$, as introduced in Chapter 2. The equivalent U-matrices as defined in (5.54) take the following form,

$$\begin{aligned}\{U_{jk}\} = \Bigg\{ &\Bigg\{\mathbb{1}, \begin{pmatrix}1&0&0&0\\0&-1&0&0\\0&0&1&0\\0&0&0&-1\end{pmatrix}, \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&-1&0\\0&0&0&-1\end{pmatrix}, \begin{pmatrix}1&0&0&0\\0&-1&0&0\\0&0&-1&0\\0&0&0&1\end{pmatrix}\Bigg\},\\ &\Bigg\{\mathbb{1}, \begin{pmatrix}0&1&0&0\\-1&0&0&0\\0&0&0&1\\0&0&-1&0\end{pmatrix}, \begin{pmatrix}0&0&1&0\\0&0&0&1\\-1&0&0&0\\0&-1&0&0\end{pmatrix}, \begin{pmatrix}0&0&0&1\\0&0&-1&0\\0&-1&0&0\\1&0&0&0\end{pmatrix}\Bigg\},\\ &\Bigg\{\mathbb{1}, \begin{pmatrix}0&0&1&0\\0&0&0&-1\\1&0&0&0\\0&-1&0&0\end{pmatrix}, \begin{pmatrix}0&0&0&1\\0&0&1&0\\0&-1&0&0\\-1&0&0&0\end{pmatrix}, \begin{pmatrix}0&1&0&0\\-1&0&0&0\\0&0&0&-1\\0&0&1&0\end{pmatrix}\Bigg\},\\ &\Bigg\{\mathbb{1}, \begin{pmatrix}0&0&0&1\\0&0&-1&0\\0&1&0&0\\-1&0&0&0\end{pmatrix}, \begin{pmatrix}0&1&0&0\\1&0&0&0\\0&0&0&-1\\0&0&-1&0\end{pmatrix}, \begin{pmatrix}0&0&1&0\\0&0&0&-1\\-1&0&0&0\\0&1&0&0\end{pmatrix}\Bigg\},\\ &\Bigg\{\mathbb{1}, \begin{pmatrix}0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}, \begin{pmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{pmatrix}, \begin{pmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{pmatrix}\Bigg\}\Bigg\},\end{aligned} \tag{5.60}$$

while the Q-matrices from Theorem 12 take the following form in dimension 4,

$$
\begin{aligned}
\{Q_{jk}\} = \Bigg\{ &\Bigg\{ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -i \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -i & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & i \end{pmatrix}, \mathbb{1} \Bigg\}, \\
&\Bigg\{ \frac{1}{2} \begin{pmatrix} 0 & 0 & 1-i & -1+i \\ 0 & 0 & 1-i & 1-i \\ -1+i & 1-i & 0 & 0 \\ -1+i & -1+i & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \end{pmatrix}, \frac{1}{2} \begin{pmatrix} 0 & 0 & -1-i & -1-i \\ 0 & 0 & 1+i & -1-i \\ 1+i & 1+i & 0 & 0 \\ -1-i & 1+i & 0 & 0 \end{pmatrix}, \mathbb{1} \Bigg\}, \\
&\Bigg\{ \frac{1}{2} \begin{pmatrix} 0 & 0 & 1+i & 1+i \\ 0 & 0 & 1+i & -1-i \\ 1+i & -1-i & 0 & 0 \\ -1-i & -1-i & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \\ 0 & 0 & 0 & i \\ 0 & 0 & -i & 0 \end{pmatrix}, \frac{1}{2} \begin{pmatrix} 0 & 0 & 1-i & -1+i \\ 0 & 0 & -1+i & -1+i \\ 1-i & 1-i & 0 & 0 \\ 1-i & -1+i & 0 & 0 \end{pmatrix}, \mathbb{1} \Bigg\}, \\
&\Bigg\{ \frac{1}{2} \begin{pmatrix} 0 & 0 & 1-i & 1+i \\ 0 & 0 & -1-i & -1+i \\ -1+i & 1+i & 0 & 0 \\ -1-i & 1-i & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{pmatrix}, \frac{1}{2} \begin{pmatrix} 0 & 0 & -1-i & -1+i \\ 0 & 0 & 1-i & 1+i \\ 1+i & -1+i & 0 & 0 \\ 1-i & -1-i & 0 & 0 \end{pmatrix}, \mathbb{1} \Bigg\}, \\
&\Bigg\{ \frac{1}{2} \begin{pmatrix} 0 & 0 & 1+i & 1-i \\ 0 & 0 & 1-i & 1+i \\ 1+i & 1-i & 0 & 0 \\ 1-i & 1+i & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \frac{1}{2} \begin{pmatrix} 0 & 0 & 1-i & 1+i \\ 0 & 0 & 1+i & 1-i \\ 1-i & 1+i & 0 & 0 \\ 1+i & 1-i & 0 & 0 \end{pmatrix}, \mathbb{1} \Bigg\} \Bigg\}.
\end{aligned}
\tag{5.61}
$$

The subsets of the U- and Q-matrices are ordered so that the respective subsets correspond to each other, i.e. to the same bases. Note that the Fourier matrix is not part of (5.59). By Lemma 4 the commutator relations for the Q-matrices in (5.61) therefore do not correspond to the Fourier matrix.

Chapter 6

Conclusion

Theorem 8 and Theorem 12 are the main results of this thesis. Theorem 8 allows to investigate all product MUBs for $d = 10, 15$ in a similar fashion as in [17], since all complex Hadamard matrices are known for $d \leq 5$.

Theorem 12, following the footsteps of [2] translated the existence problem into a problem about unitary operator basis, avoiding the existence problem of complex Hadamard matrices. Lemma 4 shows that the commuting relation of two generators in a unitary operator basis maps onto the “connecting" Hadamard matrix H_{ij}. By disclosing restrictions on the commuting relations, imposed by the structure of $\{Q_{kj}\}$, the author hopes that more can be learned about the existence problem of MUBs, without restricting oneself to specific constructions.

Furthermore, we presented an alternative proof for the conversation of entanglement in complete sets of MUBs. A result first presented in [24].

Bibliography

[1] D. M. Appleby. SIC-POVMS and MUBS: Geometrical Relationships in Prime Dimension. In L. Accardi, G. Adenier, C. Fuchs, G. Jaeger, A. Y. Khrennikov, J.-Å. Larsson, and S. Stenholm, editors, *American Institute of Physics Conference Series*, volume 1101 of *American Institute of Physics Conference Series*, pages 223–232, March 2009.

[2] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and F. Vatan. A new proof for the existence of mutually unbiased bases. *Algorithmica*, 34(4):512–528, December 2002.

[3] I. Bengtsson, W. Bruzda, Å. Ericsson, J.-Å. Larsson, W. Tadej, and K. Życzkowski. Mutually unbiased bases and hadamard matrices of order six. *Journal of Mathematical Physics*, 48(5):–, 2007.

[4] S. Brierley, S. Weigert, and I. Bengtsson. All Mutually Unbiased Bases in Dimensions Two to Five. *ArXiv e-prints*, July 2009.

[5] W. Bruzda, W. Tadej, and K. Życzkowski. A catalogue of complex hadamard matrices. `http://chaos.if.uj.edu.pl/~karol/hadamard`.

[6] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin. Security of Quantum Key Distribution Using d-Level Systems. *Physical Review Letters*, 88(12):127902, March 2002.

[7] T. Durt, B.-G. Englert, I. Bengtsson, and K. Bengtsson. On mutually unbiased bases. *International Journal of Quantum Information*, 08(04):535–640, 2010.

[8] M. Grassl. On SIC-POVMs and MUBs in Dimension 6. *eprint arXiv:quant-ph/0406175*, June 2004.

[9] B. Hiesmayr and W. Löffler. Mutually unbiased bases and bound entanglement. *Physica Scripta*, 2014(T160):014017, 2014.

[10] S. G. Hoggar. t-Designs in Projective Spaces. *European J. Combin.*, 3:233–254, 1982.

[11] S. G. Hoggar. Parameters of t-Designs in $\mathbb{F}P^{d-1}$. *European J. Combin.*, 4:29–36, 1984.

[12] S. G. Hoggar. t-designs with general angle set. *European J. Combin.*, 13:257–271, 1992.

[13] I. D. Ivanovic. Geometrical description of quantal state determination. *Journal of Physics A: Mathematical and General*, 14(12):3241, 1981.

[14] J. Lawrence. Entanglement patterns in mutually unbiased basis sets. *Phys. Rev. A*, 84:022338, Aug 2011.

[15] J. Lawrence, Č. Brukner, and A. Zeilinger. Mutually unbiased binary observable sets on n qubits. 65:32320, 2002.

[16] E. Lubkin. Entropy of an n-system from its correlation with a k-reservoir. *Journal of Mathematical Physics*, 19:1028–1031, May 1978.

[17] D. McNulty and S. Weigert. All mutually unbiased product bases in dimension 6. *Journal of Physics A: Mathematical and Theoretical*, 45(13):135307, 2012.

[18] D. McNulty and S. Weigert. The limited role of mutually unbiased product bases in dimension 6. *Journal of Physics A: Mathematical and Theoretical*, 45(10):102001, 2012.

[19] D. McNulty and S. Weigert. On the Impossibility to Extend Triples of Mutually Unbiased Product Bases in Dimension Six. *ArXiv e-prints*, March 2012.

[20] A. Neumaier. Combinatorial configurations in terms of distances. *Memorandum 81-01*, 1981.

[21] J. Schwinger. Unitary operator bases. *Proceedings of the National Academy of Sciences*, 46(4):570–579, 1960.

[22] C. Spengler, M. Huber, S. Brierley, T. Adaktylos, and B. Hiesmayr. Entanglement detection via mutually unbiased bases. *Phys. Rev. A*, 86:022311, Aug 2012.

[23] F. Szöllősi. *Construction, classification and parametrization of complex Hadamard matrices*. PhD thesis, Central European University, Budapest, 2011.

[24] M. Wiesniak, T. Paterek, and A. Zeilinger. Entanglement in mutually unbiased bases. *New Journal of Physics*, 13(5):053047, 2011.

[25] W. K. Wootters. A Wigner-function formulation of finite-state quantum mechanics. *Annals of Physics*, 176:1–21, May 1987.

[26] W. K. Wootters and B. D. Fields. Optimal state-determination by mutually unbiased measurements. *Annals of Physics*, 191(2):363 – 381, 1989.

[27] G. Zauner. *Quantum Designs.* PhD thesis, University of Vienna, 1999.

Acknowledgements

I would like to thank the Vienna Institute for Quantum Optics and Quantum Information (IQOQI) of the Austrian Academy of Sciences (OAW) for partially funding the research for this thesis, as well as Anton Zeilinger and Časlav Brukner for their supervision. Furthermore, I would like to thank Marcus Appleby for very helpful discussions and comments.
I would also like to thank the Wonmo Pyongae Foundation for supporting me with a scholarship in this period and its founder Mrs. Hak Ja Han for being a source of encouragement and inspiration.

Abstract

Mutually unbiased bases (MUBs) play an important role in quantum information theory and the foundations of quantum physics. So far, however, constructions for complete sets of such bases are only known in prime or prime-power dimension, despite extensive research being dedicated to the topic. This problem is known as the MUB existence problem. Not much is known about the existence of MUBs in composite dimensions.

This thesis explores the difficulties of those approaches to the existence problem which employ Hadamard matrices and derives new general results for the connection between MUBs and Unitary Operator Bases. Furthermore, the thesis explores the role of entanglement for complete sets of MUBs and generalizes a result concerning product MUBs to arbitrary dimension. The connection to Schwinger's notion of fundamental quantum degrees of freedom will be explored. Possible avenues towards analysing the existence problem and the role of entanglement in sets of MUBs are suggested.

Zusammenfassung

Mutually Unbiased Bases (MUBs) spielen sowohl in der Quanteninformationstheorie, als auch für die Grundlagen der Quantenphysik eine zentrale Rolle. Trotz weitreichender Forschung sind bis dato nur Konstruktionen vollständiger Sätze von MUBs bekannt, wenn es sich um ein Quantensystem handelt, dessen Dimension eine Primzahl oder eine Primzahlpotenz ist. Über die übrigen Fälle ist wenig bekannt.

Diese Arbeit setzt sich mit den Schwierigkeiten des Zugangs über Hadamard Matrizen zu diesem Existenzproblem von MUBs auseinander. Ein allgemeines Resultat bezüglich des Zusammenhangs von MUBs und unitären Operatorbasen wird bewiesen. Des weiteren wird die Rolle von Verschränkung in vollständigen Sätzen von MUBs analysiert und ein bereits bekanntes Resultat betreffend Produkt-MUBs für beliebige Dimensionen verallgemeinert. Darüber hinaus werden der Zusammenhang zu Schwingers "fundamentalen Quantenfreiheitsgraden" behandelt und weitere Zugänge zum Existenzproblem von MUBs und zur Analyse von Verschränkung in Sätzen von MUBs skizziert.

Curriculum Vitae

Name Bogdan Jin-Wha Pammer

Present Address
University of Vienna
Boltzmanngasse 5,
A-1090 Vienna, Austria

Education

- Studying **MA** in History and Philosophy of Science, University of Vienna *since Oct 2013*
- **BSc** in Physics (Distinction), University of Vienna *Feb 2012*
  Univ.-Prof. Dr. Reinhold A. Bertlmann (Supervisor)
  Thesis: "Geometry of Entanglement"
- **Matura** (Distinction), Bundesrealgymnasium Steyr Michaelerplatz *June 2007*

Work

- **Researcher** *May 2014 - Feb 2015*
  Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences (OAW)
- **Teaching Assistant** *Oct 2013 - Feb 2014*
  University of Vienna
- **Teaching Assistant** *Oct 2010 - June 2011*
  University of Vienna
- **Tutor** University of Vienna *Oct 2009 - June 2011*