Mathematik

Dissertationsthema

Nice Complete Sets of Pairwise Quasi-Orthogonal Masas

—From the Basics to a Unique Encoding—

Inaugural-Dissertation
zur Erlangung des Doktorgrades
der Naturwissenschaften
im Fachbereich Mathematik und Informatik
der Mathematisch-Naturwissenschaftlichen Fakultät
der Westfälischen Wilhelms-Universität Münster

vorgelegt von
Sebastian Krusekamp
aus Paderborn
– 2014 –

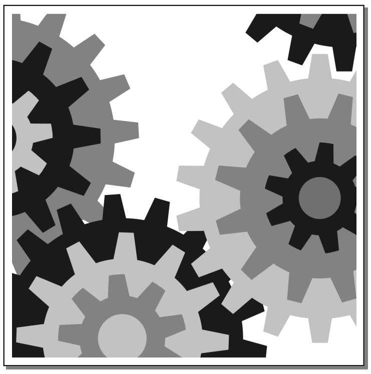
Dekan	:	Prof. Dr. Martin Stein
Erster Gutachter	:	Prof. Dr. Dr. h.c. Joachim Cuntz
Zweiter Gutachter	:	Prof. Dr. Andreas Winter
Tag der mündlichen Prüfung	:	14.8.2014
Tag der Promotion	:	14.8.2014

Westfälische Wilhelms-Universität Münster
SFB 878 Groups, Geometry & Actions
erc European Research Council

PhD Thesis

Nice Complete Sets of Pairwise Quasi-Orthogonal Masas

—From the Basics to a Unique Encoding—



Sebastian Krusekamp

Münster 2014

Supervised by Prof. Dr. Dr. h.c. Joachim Cuntz

Abstract

Mutually unbiased bases (MUBs) have gained considerable importance in the field of quantum physics over the past twenty-five years. Various applications have been found (see e.g. the survey article [35]), and connections to different mathematical domains of interest, such as unitary Hadamard matrices ([13]), Galois fields ([114]), Latin squares and design theory ([79, 112]), and finite geometry ([89]), are numerous.

The counterpart of mutually unbiased bases on the level of matrix algebras are pairwise quasi-orthogonal maximal abelian *-subalgebras, briefly called *masas.* Whereas physicists' accounts on the subject mainly focus on the picture of MUBs (e.g. [27, 35]), the present mathematical thesis centres on the algebraic framework of quasi-orthogonal masas.

Starting from the very basics, we first thoroughly discuss the connections between the equivalent pictures of (mutually) unbiased bases, unbiased unitary Hadamard matrices, and quasi-orthogonal masas, and illustrate two of the most famous constructions of so-called *complete* sets of pairwise quasi-orthogonal masas in prime power dimensions. Though this is a mathematical thesis, we also turn our attention to basic physical aspects of MUBs.

We attach special importance on *standard* pairs of masas ([44]), and generalise this notion to pairs which we call *normal.* While standard pairs in dimension d model actions of the cyclic group of order d on the complex functions on d different points, normal masa pairs model actions of direct sums $\mathbb{Z}/d_0 \times \cdots \times \mathbb{Z}/d_m$ on the same function space, where $d = d_0 \cdots d_m$ is any factorisation of the dimension. We shortly address a further generalisation of normal masa pairs, and demonstrate that this generalised class comprises all quasi-orthogonal pairs in dimension four.

Our concept of normal masa pairs is compatible with the existing definition of nice masa families by Aschbacher, Childs, and Wocjan ([3]), in the sense that each normal masa pair is a nice family of length two. Moreover, each masa pair in a *complete* nice family is automatically normal. According to Godsil and Roy ([40]), all known constructions of complete quasi-orthogonal masa sets produce nice families.

We show that the generalised Clifford algebra, as defined by Yamazaki and Morris in the sixties ([74,75,115]), is an appropriate framework for the construction of nice complete masa families. As the main result of this thesis, we prove that, although various constructions of nice complete families have been proposed so far (e.g. [1, 9, 49, 60, 114]), one *unique* method permits to encode *all* nice complete families.

Calderbank, Cameron, Kantor, and Seidel ([23]) had established an equivalent result earlier, in terms of so-called *symplectic spreads,* as has later been observed by Godsil and Roy ([40]). By contrast to this approach, the one presented here is based on more or less elementary means of matrix algebra.

The unique encoding of nice complete masa families opens the theoretical door to classify the latter. While the complete nice masa families in the smallest dimensions turn out to be essentially unique, it is known that there are many prime power dimensions admitting inequivalent complete families. However, the classification of these families appears to be an extraordinarily complicated matter of its own, and is not dealt with in the present work.

Danksagung (Acknowledgements)

Herzlich möchte ich mich an erster Stelle bei meinem Betreuer Prof. Dr. Dr. h.c. Joachim Cuntz bedanken. Er erlaubte mir frei und eigenständig zu arbeiten, nahm sich zugleich aber stets Zeit für ausführliche Besprechungen, die für mich nicht nur mathematisch sehr anregend und lehrreich, sondern oft genug auch persönlich ermutigend waren, gerade wenn sich Erfolge mitunter nur schleppend einstellten.

Meinen Freunden und Kollegen am Fachbereich Mathematik der Wilhelms-Universität Münster, vor allem in der Arbeitsgruppe *Funktionalanalysis, Operatoralgebren und nichtkommutative Geometrie,* danke ich für das menschlich wie mathematisch hervorragende Arbeitsumfeld. Zum Glück gehören Elke und Gabi dazu, die immer einen klaren Kopf und ein gutes Wort haben, vom richtigen Formular ganz zu schweigen.

Meine Freunde Klaus und Walther waren mir zugleich wunderbare Büro-Kollegen. Beiden bin ich darüber hinaus, wie auch Thomas und Moritz, zu Dank verpflichtet für konkrete fachliche Hilfe und fruchtbare Diskussionen.

Prof. Dr. Andreas Winter gab mir wertvolle Impulse bei meiner Suche nach einem interesssanten Thema. Zudem erklärte er sich bereit, Zweitgutachter dieser Arbeit zu sein. Für beides danke ich ihm herzlich. Prof. Dr. Urs Hartl nahm sich die Zeit, Fragestellungen meiner Arbeit mit mir zu diskutieren. Ihm bin ich ebenso dankbar wie Prof. Dr. William M. Kantor, der mir mit großer Klarheit und Freundlichkeit eine Forschungsfrage beantwortete, die mich so lange verfolgte.

Großen Dank schulde ich Franziska für die Korrektur meiner sprachlichen Mängel in wichtigen Textpassagen.

Meiner Familie danke ich; meinen Freundinnen und Freunden, neben den bereits genannten vor allem Thomas, Doris und Stefan mit Alida, Marika und Frank, Barbara und Thomas, Jule und Didi, Robert, Carl und schließlich Bruno, für ihre vielfältige Unterstützung in den vergangenen Jahren. Zu guter Letzt danke ich meiner Freundin Johanna, für alles.

Contents

Introduction

In the present thesis, we study families of pairwise quasi-orthogonal maximal abelian *-subalgebras—called masas in short—of the complex $d \times d$-matrices, with a special emphasis on so-called *nice* masa families. Though doubtlessly of an intrinsic, purely mathematical interest, a very strong motivation for this topic stems from the field of quantum physics, since pairwise quasi-orthogonal masas in $M_d(\mathbb{C})$ can be considered as the algebraic counterpart of *mutually unbiased bases* (MUBs) in the Hilbert space $\mathbb{C}^d$.

Motivation and subject classification

A pair of orthonormal bases $(x_0, \dots, x_{d-1})$, $(y_0, \dots, y_{d-1})$ of $\mathbb{C}^d$ is said to be unbiased if the identity $|(x_i|y_j)|^2 = {}^1/_d$ holds for all $0 \leq i, j < d$. Pairs of unbiased bases correspond to so-called *complementary* pairs of quantum physical measurements (observables). Performing such measurements one after the other in any order, the second outcome is perfectly independent of the first. As one of the basic principles of quantum mechanics, this is *not* true in general.

A set of MUBs for the Hilbert space $\mathbb{C}^d$ containing $d+1$ members is called *complete*, for it is known that no larger sets can exist. Families of MUBs, complete families in particular, have met a number of important applications in quantum information theory in the recent decades, such as optimal state determination, quantum teleportation, or quantum cryptography (see [35] for a good survey), motivating various constructions proposed in physics literature ([1,9,24,34,38,42,49,55,60,81,88,95,112,114]). At the same time, all constructions of *complete* families exclusively work in dimensions being powers of primes, and it is by now widely believed that all other dimensions do not admit complete sets of MUBs. Nevertheless, this cannot even be shown for dimension six until today, in spite of remarkable efforts ([12,13,19,43,71–73,86]).

Over the past twenty years, the study of MUBs has also gained increasing interest among mathematicians from different areas, for it appears that the subject is deeply related to questions arising in the study of Hadamard matrices, finite fields, finite geometry, design theory and Latin squares, decompositions of Lie algebras, symplectic spreads, and many others ([16,23,24,40,58,79,80,88,114,117]).

While the literature on MUBs abounds with approaches to either prove the non-existence of complete MUB sets in dimensions other than prime powers (most notably in dimension six) on one side, and on various proposals of prime power constructions on the other, the task to *classify* the known constructions of complete MUB families seems, as far as we can see, a bit neglected.

It can e.g. be shown ([23,40]) that many of the published constructions, albeit they appear rather different at first sight, do in fact lead to MUB families which essentially (that is, up to a specific equivalence relation) coincide. How many inequivalent complete families of MUBs do exist for a given prime power dimension? At present, a general answer to this question seems far beyond reach.

All the same, a very important result concerning the classification of MUB families has been published by Aschbacher, Childs and Wocjan in 2007 ([3]). The authors declare a subclass of MUB families which they call *nice.* Among other results, they prove that if p^n is the smallest prime power dividing the dimension $d \in \mathbb{N}$ of the considered Hilbert space, nice families cannot exceed a length of $p^n + 1$. This upper bound does however not apply to all MUB sets, as is ensured by a certain method to gain masa families in square dimensions, presented earlier by Wocjan and Beth ([112]).

As has been conjectured by Boykin et al. ([16]), and later been verified by Godsil and Roy ([40]), all complete sets of MUBs constructed to this day are nice. It can therefore be conjectured that in fact *all* complete sets of MUBs are nice, which would imply in particular that complete sets exist only in prime power dimensions. However, let us point out that there is no actual mathematical fact supporting this conjecture.

Content and organisation of the present thesis

While physicists' accounts on the subject of mutually unbiased bases mainly focus on the Hilbert space picture (see e.g. [35,114]), we put quasi-orthogonal masas at the centre of our considerations in the present work.

Motivational sections commence each of the first three chapters, outlining the basic connections between (finite-dimensional) masas and quantum mechanical measurements in general (Section 1.1), in the case of quasi-orthogonal masas in particular (Section 2.1), and finally in the case of complete quasi-orthogonal families (Section 3.1).

The **first chapter** is concerned with the correspondences between maximal abelian *-subalgebras of the complex matrix algebra $M_d(\mathbb{C})$, unitary matrices, and mutually unbiased bases for the Hilbert space $\mathbb{C}^d$. After a basic discussion in Section 1.2, we study unitary Hilbert-Schmidt orthonormal bases for masas, whose possible structure depends on the divisibility of the dimension (Section 1.4). Since unitary Hadamard matrices, which will occur at many points in the present work, are a useful tool in this context, they are introduced beforehand in Section 1.3.

The concept of quasi-orthogonality is introduced in **Chapter 2**. After clarifying the links between quasi-orthogonal masas, unbiased bases, and unbiased unitaries within Section 2.2, we demonstrate in Section 2.3 how the set of masas in a fixed dimension can be considered as a metric space.

We then turn our attention to so-called standard pairs of masas (Section 2.4), which are the most regular and best-understood examples of quasi-orthogonal pairs. We also give explicit examples of non-standard masa pairs. Standard pairs model finite cyclic group actions and therefore serve as a key to understand the matrix algebra $M_d(\mathbb{C})$ as a crossed product (Section 2.5).

In **Chapter 3**, we come from pairs to larger families of quasi-orthogonal masas. We discuss maximality and completeness of such families in Section 3.2. We present the standard construction of complete families in prime dimensions, and give examples for non-completable quasi-orthogonal masa families. In general prime power dimensions, more sophisticated techniques must be employed to obtain complete quasi-orthogonal families. Two of these methods ([9, 114]) are demonstrated in Section 3.3.

While most "prime power constructions" bear a certain resemblance to each other, the aforementioned technique by Wocjan and Beth ([112]) to gain MUB families in square dimensions is, to all appearances, of an essentially different nature, for it exceeds the upper bound for the length of MUBs which can be achieved by prime power techniques. We present this method in Section 3.4.

A survey of connections of MUBs to the mathematical area of *design theory,* including a few remarks on applications to entanglement and entropy of MUBs, concludes this chapter (Section 3.5).

Chapter 4 contains most of the main results of the present thesis. We first study nice error bases in Section 4.1. Such bases are at the heart of the so-called nice families of MUBs (i.e. masas respectively), as introduced by Aschbacher et al. in [3]. Before we turn to general nice masa families in Section 4.3, we present a subclass of nice masa pairs which we call *normal* in Section 4.2.

Loosely speaking, a normal masa pair in the complex $d \times d$-matrices models, for a factorisation $d = d_0 \cdots d_m$ of the dimension, an action of the group $\mathbb{Z}/d_0 \times \cdots \times \mathbb{Z}/d_m$ on the function algebra $\mathbb{C}[\mathbb{Z}/d]$. Normal masa pairs generalise standard masa pairs, which are related to actions of the cyclic group $\mathbb{Z}/d$ on the algebra $\mathbb{C}[\mathbb{Z}/d]$, and are at the same time nice masa families (of length two) in the sense of [3].

Rephrasing a result by Boykin et al. ([16]), we then demonstrate that each nice complete family of masas essentially stems from a partition of one specific nice error basis (Section 4.4). As an alternative framework for this result, we propose the *generalised Clifford algebra,* defined in the sense of Yamazaki and Morris ([74, 75, 115]).

In Section 4.5, we define another subclass of quasi-orthogonal masa pairs, generalising the class of normal pairs, and prove that this subclass comprises all masa pairs in the complex 4×4-matrices.

At the beginning of **Chapter 5** (Section 5.1), we show that all nice complete masa families are encoded by certain families of symmetric matrices over a prime field. The rest of this chapter is dedicated to the study of the mentioned matrix families, for which we propose the acronymic expression *smid families,* since they consist of symmetric matrices with pairwise invertible differences.

We first study a natural equivalence relation for smid families, which proves to be compatible with the equivalence of the associated complete masa families. As a main result of the present work, there is thus a one-to-one correspondence between equivalence classes of nice complete masa families and complete smid families.

The investigation of general smid families turns out to be a rather complicated task, so we limit ourselves to consider the smallest non-trivial case of smid families in the symmetric 2×2-matrices over a prime field $\mathbb{F}_p$ in the following sections. We first study smid families being linear subspaces in Section 5.2, then derive connections between smid families in $M_2(\mathbb{F}_p)$, permutation polynomials, and Latin squares in Section 5.3.

In Section 5.4, we finally provide some computer algebraic results on the number of inequivalent smid families of arbitrary length in some small matrix algebras $M_n(\mathbb{F}_p)$.

Some of the sections are, sometimes only in parts, marked as **excursions**. These concern aspects of quasi-orthogonal masas which are hopefully interesting, but nevertheless not essential for the present work, so that the reader may easily leave them out.

Diverse mathematical areas are touched upon in this thesis. As a courtesy to the reader, we therefore provide **reminders** at various points, where we collect the needed results of the topic in question. Feel free to skip these parts if you are familiar with the respective subjects.

Let us finally mention that, though we have tried to shed light on a number of aspects and thematic links of quasi-orthogonal masas, we are fully aware that the present work does not cover by far all that there is to say on the subject. Whereas some topics are treated rather shortly, for instance topological aspects, connections to finite geometry (see e.g. [82,89,90]), and entanglement (e.g. [63]), others are completely omitted for the sake of simplicity.

For this reason, we intentionally considered neither relations to Lie algebras (see e.g. [16,42]) nor existing generalisations of mutually unbiased bases (e.g. [58,68]) on the mathematical side. What is more, we hardly involved projective spaces, although they doubtlessly provide a natural alternative to the usual Hilbert spaces in this context. We have further confined ourselves strictly to the study of masas in the complex matrix algebras $M_d(\mathbb{C})$, leaving aside the real matrices on the one hand, and more general C^*-algebras or von Neumann algebras on the other.

Concerning physics, we do neither consider advanced information theoretical applications such as the Mean King's problem, dense coding, quantum teleportation, quantum key distribution etc. (see e.g. [35]), nor the generalised quantum mechanical measurement concept described by *SIC-POVMs* (see e.g. [2]). Also, connections to the important topic of *entropy* ([5,25,85]) are left aside.

Requirements, notations and conventions

The prerequisites for the present work mainly comprise elementary linear algebra and analysis. In particular, basic facts concerning complex *-algebras are presumed to be known.

Apart from this, the author made the attempt to keep this thesis as self-contained as possible, by providing short introductions (*reminders*) to some more advanced topics that might not be familiar to some readers, namely basic aspects of Galois fields, Latin squares, finite projective geometry, design theory, and abstract C*-algebras. Nevertheless, some previous knowledge and practise in the respective areas, especially in the study of Galois fields, is certainly helpful.

Most of the notations used in the present work are standard in mathematical literature. Within the *-algebra $M_d(\mathbb{C})$ of complex $d \times d$-matrices ($d \in \mathbb{N}$), we denote the *-subalgebra of diagonal matrices by $\mathcal{D}_d$, and the group of unitary matrices by $\mathcal{U}_d$. We always assume projections to be orthogonal, i.e. in our terminology, a projection is an element $p \in M_d(\mathbb{C})$ fulfilling $p^2 = p = p^*$.

The automorphism group of some algebraic structure $\mathcal{A}$ (e.g. an algebra) is denoted Aut $\mathcal{A}$. By a **-automorphismϕ* of $M_d(\mathbb{C})$, we mean an algebra automorphism fulfilling the identity $\phi(a^*) = \phi(a^*)$ for all $a \in M_d(\mathbb{C})$. We shall make extensive use of the fact that all *-automorphisms of $M_d(\mathbb{C})$ are *inner,* i.e. given by a unitary conjugation.

As a convention, we always count from zero. Accordingly, we consider the **symmetric group** S_d as the group of permutations of the set $\{0, \ldots, d-1\}$. Whenever it is clear from the context that some variables i, a, b are integers, we often write $a \leq i \leq b$ instead of $i \in \{a, \ldots, b\}$ etc.

Throughout the whole thesis, we endow the complex Hilbert space $\mathbb{C}^d$ with the standard scalar product, linear in the first and conjugate linear in the second argument, and denoted $(\cdot \mid \cdot)$, for any dimension $d \in \mathbb{N}$. We represent $\mathbb{C}^d$ by columns, denoting the **standard basis elements** by

$$z_i = (0, \ldots, 0, \underset{\substack{| \\ i\text{th pos.}}}{1}, 0, \ldots, 0)^T$$

for all $0 \leq i < d$, where a^T designates the transpose of a matrix a in any dimensions. In the first two chapters, all bases are given a definitive order and hence written as *tuples.* From Chapter 3 on, we are sometimes concerned with (operator) bases, which we consider as *sets* for convenience. However, we take care that no contradictions spring from this slightly incongruent notation.

As is well-known, the *-algebra $M_d(\mathbb{C})$ of complex $d{\times}d$-matrices, endowed with the usual involution and norm, is (*-)isomorphic to the linear operators $\mathcal{L}(\mathbb{C}^d)$ on the d-dimensional Hilbert space. This gives rise to the following

Convention 0.0.1. We represent any linear operator $a \in \mathcal{L}(\mathbb{C}^d)$ w.r.t. the standard basis, that is we set $a_{i,j} = \big(a\, z_i \,\big|\, z_j\big)$ and declare a *-isomorphism

$$\mathcal{L}(\mathbb{C}^d) \xrightarrow{\cong} M_d(\mathbb{C}), \quad a \longmapsto \big(a_{i,j}\big)_{0 \le i,j < d}.$$

Having in mind this fixed representation, we shall always identify the linear operators $\mathcal{L}(\mathbb{C}^d)$ and the complex $d{\times}d$-matrices.

We denote the unit matrix of $M_d(\mathbb{C})$ by I_d, further we define *matrix units* $\mathrm{E}_{i,j}$ in $M_d(\mathbb{C})$ for all $0 \le i,j < d$, having only one non-zero entry at position (i,j), which equals one.

$$\mathrm{E}_{i,j} = \begin{array}{c} j\text{th column} \\ | \\ \left(\begin{array}{ccc} & 1 & \\ & & \\ & & \end{array}\right) \end{array} \begin{array}{l} \\ \\ — i\text{th row} \\ \\ \end{array}$$

By the **trace** of a matrix in $M_d(\mathbb{C})$, we shall usually mean the *normalised* trace

$$\tau : M_d(\mathbb{C}) \longrightarrow \mathbb{C}, \quad \big(a_{i,j}\big) \longmapsto \frac{1}{d}\sum_{i=0}^{d-1} a_{i,i}.$$

Consequently, we also define the **Hilbert-Schmidt scalar product**and norm via the normalised trace, that is we set

$$(a \,|\, b)_{\mathrm{HS}} = \tau(ab^*) \quad \text{and} \quad \|a\|_{\mathrm{HS}} = \sqrt{(a \,|\, a)_{\mathrm{HS}}}$$

for all $a, b \in M_d(\mathbb{C})$. For the sake of readability, none of the last previous notations reflect the dimension d, but the latter will always be clear from the context. The non-normalised trace, though admittedly preferred by many physicists, only occurs a few times, and is then denoted by Tr. We say a matrix $a \in M_d(\mathbb{C})$ is *trace-free* if $\tau(a) = 0$.

Tensor products will play a crucial role in this work. If a given dimension $d \in \mathbb{N}$ admits a factorisation $d = d_0 \cdots d_m$ ($m, d_0, \ldots, d_m \in \mathbb{N}$), it is well-known that the matrix algebra $M_d(\mathbb{C})$ is isomorphic to the tensor product $M_{d_0}(\mathbb{C}) \otimes \cdots \otimes M_{d_m}(\mathbb{C})$. At the same time, the respective *-isomorphism is of course not unique. We fix one which "respects" the standard basis defined above.

Convention 0.0.2. Let $d = d_0 \cdots d_m$ ($m, d, d_0, \ldots, d_m \in \mathbb{N}$) be a factorisation of a given dimension d. Further set $\tilde{d}_0 = 1, \tilde{d}_1 = d_0, \ldots, \tilde{d}_m = d_0 \cdots d_{m-1}$. It is easily checked that a bijection is defined by

$$\begin{aligned} \{0, \ldots, d_0 - 1\} \times \cdots \times \{0, \ldots, d_m - 1\} &\xrightarrow{\alpha} \{0, \ldots, d-1\}, \\ (i_0, \ldots, i_m) &\longmapsto \sum_{k=0}^{m} i_k \tilde{d}_k. \end{aligned}$$

Unless otherwise specified, we shall always make the following identifications.

$$\begin{array}{ccccccc} \mathbb{C}^{d_0} \otimes \cdots \otimes \mathbb{C}^{d_m} & \xrightarrow[\cong]{\phi_0} & \mathbb{C}^d & \qquad & M_{d_0}(\mathbb{C}) \otimes \cdots \otimes M_{d_m}(\mathbb{C}) & \xrightarrow[\cong]{\tilde{\phi}_0} & M_d(\mathbb{C}) \\ z_{i_0} \otimes \cdots \otimes z_{i_m} & \longmapsto & z_{\alpha(i_0, \ldots, i_m)} & & \mathrm{E}_{i_0, j_0} \otimes \cdots \otimes \mathrm{E}_{i_m, j_m} & \longmapsto & \mathrm{E}_{\alpha(i_0, \ldots, i_m), \alpha(j_0, \ldots, j_m)} \end{array}$$

The isomorphism ϕ_0 induces $\tilde{\phi}_0$ in the sense that for all elements $a \in \bigotimes_{k=0}^{m} M_{d_k}(\mathbb{C})$, $x \in \bigotimes_{k=0}^{m} \mathbb{C}^{d_k}$, we have $\tilde{\phi}_0(a)\phi_0(x) = \phi_0(ax)$.

We fix the isomorphism $\tilde{\phi}_0$ above because it preserves a matrix property called **monomiality,** which will be of some importance for this work. A matrix is called monomial if each row and each column contains exactly one non-zero entry. (This is obviously an exclusive property of *matrices,* i.e. it makes no sense to call an operator monomial unless one specifies a matrix representation.) We will at some points make use of the fact that for monomial matrices $a_0 \in M_{d_0}(\mathbb{C}), \ldots, a_m \in M_{d_m}(\mathbb{C})$, the matrix $\tilde{\phi}_0(a_0 \otimes \cdots \otimes a_m)$ is again monomial. As a matter of course, the same does not apply for all isomorphisms $\bigotimes_{k=0}^{m} M_{d_k}(\mathbb{C}) \cong M_d(\mathbb{C})$.

Chapter 1

Maximal abelian *-subalgebras (masas) in the complex d×d-matrices

The main issue of the present thesis is the investigation of maximal abelian *-subalgebras (called *masas*in short) of the complex $d\times d$-matrices. To be precise, we will mostly investigate *families* of masas, fulfilling a geometric condition named *quasi-orthogonality.* In this first chapter, we confine ourselves to discussing aspects of one single masa.

There are a various connections between masas and theoretical quantum mechanics. As a motivation, we present one such connection at the beginning of each of the first three chapters, starting with the concept of *compatible observables* in Section 1.1.

The second section is concerned with a very basic discussion of the correspondences between masas, unitary matrices, and orthonormal bases. In Section 1.3, we introduce (complex) Hadamard matrices, which will play a central role in this thesis. One of their many applications follows in Section 1.4, where we construct Hilbert-Schmidt orthonormal bases for masas in the complex $d\times d$-matrices.

1.1 *Motivation:* Finite dimensional quantum systems and maximal abelian *-subalgebras

One of the basic axioms of quantum mechanics is that one cannot perform any measurement on a physical system without simultaneously exerting influence on it. This is strongly reflected by the fact that an *operator* is associated with a quantum mechanical measurement process.

First of all, a state of a d-dimensional quantum system is described by a unit vector of the Hilbert space $\mathbb{C}^d$. A measurement performed on such a system can have at most

d different outcomes and is formalised by a self-adjoint linear operator $a \in M_d(\mathbb{C})$, or better to say by its (real) eigenvalues and eigenspaces: the outcome, i.e. the physical quantity one is interested in, of the measurement associated with the operator a will be one of its eigenvalues. After the measurement process, the state of the considered system will belong to the eigenspace of the detected eigenvalue.

The operator a—or any normalised basis of eigenvectors and set of eigenvalues corresponding to it—as well as the actual physical measurement are usually identified and both referred to as an *observable*.

Another basic axiom of quantum physics is that the outcome of any measurement is, in general, not determined, but *probabilistic,* even in case the system's state is known. Suppose a d-dimensional quantum system is prepared in an initial state $z \in \mathbb{C}^d_1$, and the observable a has eigenstates $x_0, \dots, x_{d-1} \in \mathbb{C}^d_1$ with corresponding eigenvalues $\lambda_0, \dots, \lambda_{d-1} \in \mathbb{R}$ (since a is self-adjoint, we can assume that the eigenstates are pairwise orthogonal). For simplicity, we suppose the spectrum of a is non-degenerated. Then the probability of detecting an eigenvalue λ_i (that is to find the system in a final state x_i) is given by $|(z|x_i)|^2$, where $(\cdot|\cdot)$ designates the standard scalar product of the Hilbert space $\mathbb{C}^d$. Note that these probabilities automatically sum up to one by Parseval's identity.

Figure 1.1 illustrates the measurement process associated with the observable a. The arrows are labeled with the probabilities of the outcomes. Now suppose a second

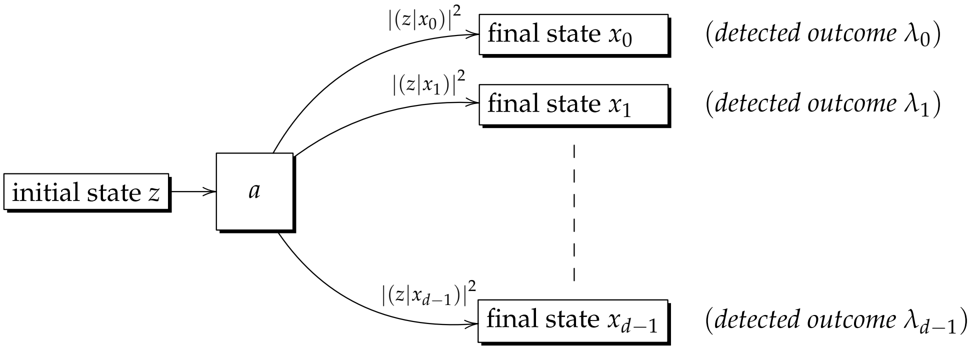


Figure 1.1: *Basic quantum mechanical measurement*

observable b shares the eigenstates of a and is measured directly *after* the measurement associated with a is performed. Then the system is already in an eigenstate x_{i_0} of b, hence the probability distribution of the new outcome is a Dirac distribution, that is

$$|(x_{i_0}|x_i)|^2 = \begin{cases} 1 & \text{if } i = i_0 \\ 0 & \text{else.} \end{cases}$$

As a consequence, the probability to find the system in a final state x_{i_0} after first measuring a and then b is the same as after solely measuring a, namely still $|(z|x_{i_0})|^2$. This is visualised in Figure 1.2. You immediately see that on the one hand, the outcome of measurement b is *predicted* by the outcome of a. On the other hand, you can as well flip the order of the measurements without changing the probability distribution for the final state. Such observables are called *compatible*.

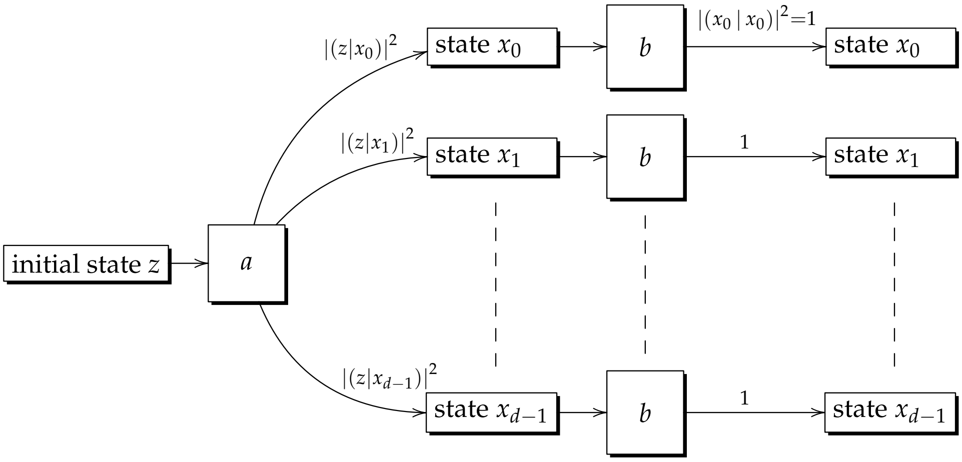


Figure 1.2: *Compatible observables*

On the level of operators, compatibility translates in to *commutativity*, since operators $a, b \in M_d(\mathbb{C})$ sharing a common basis of eigenvectors commute. Consider a set of compatible observables, i.e. commuting self-adjoint operators $a_0, \ldots, a_{m-1} \in M_d(\mathbb{C})$, where $m \in \mathbb{N}$. Then obviously all real linear combinations and products of these operators are self-adjoint and commute as well, hence the matrices a_i generate a real algebra of self-adjoint commuting matrices $\mathcal{M} = \mathcal{A}_{\mathbb{R}}(a_0, \ldots, a_{m-1})$.

Since all matrices in $\mathcal{M}$ share the same basis of eigenvectors, they can all be diagonalised *simultaneously*. There is thus a unitary matrix $u \in \mathcal{U}_d$ such that $u\mathcal{D}_d^{\mathbb{R}}u^*$ includes $\mathcal{M}$, where we denote by $\mathcal{D}_d^{\mathbb{R}}$ the diagonal matrices with real entries.

As an immediate consequence, the dimension of the real matrix algebra $\mathcal{M}$ is less or equal than d, and a maximal algebra of commuting observables is precisely the self-adjoint part of the complex subalgebra $u\mathcal{D}_d u^* \subset M_d(\mathbb{C})$. The latter is obviously a complex algebra closed under involution and maximal abelian, i.e. there is no larger abelian subalgebra $\mathcal{M}' \subset M_d(\mathbb{C})$ such that $u\mathcal{D}_d u^* \subsetneq \mathcal{M}'$. Such *maximal abelian *-subalgebras*of the $d \times d$-matrices are at the centre of interest in the present thesis.

As a concluding remark, let us note that there is also link between *evolutions* of quantum systems and *maximal abelian *-subalgebras.* Evolutions of a (closed) d-dimensional quantum system can be described by unitaries in $\mathcal{U}_d$, and the eigenstates of a unitary matrix $v \in \mathcal{U}_d$ correspond precisely to quantum states which are *stable* under the respective evolution process. In other words, if the system is initially in an eigenstate of v, then it will remain in this state under the corresponding evolution. A maximal (complex) *-algebra generated by evolutions $v_0, \ldots, v_{m-1} \in \mathcal{U}_d$, sharing a common basis of eigenstates, is of course abelian and thus a *maximal abelian *-subalgebra*of $M_d(\mathbb{C})$.

1.2 Masas in the complex d×d-matrices, and associated orthonormal bases and unitaries

Throughout this section, let $d \in \mathbb{N}$ be an arbitrary but fixed dimension of the considered matrix algebra $M_d(\mathbb{C})$. Recall that τ denotes the *normalised* trace on $M_d(\mathbb{C})$.

Masas in complex matrix algebras

First of all, let us give a proper definition of the mathematical object which is at the centre of the present work.

Definition 1.2.1. *Let $\mathcal{A}$ be a *-algebra. A* masa$\mathcal{M} \subset \mathcal{A}$ *is a $\underline{m}$aximal $\underline{a}$belian $\underline{^*}$-sub$\underline{a}$lgebra of $\mathcal{A}$, that is a commutative subalgebra which is invariant under involution and maximal in the sense that if $\mathcal{M}' \subset \mathcal{A}$ is another abelian *-subalgebra of $\mathcal{A}$ containing $\mathcal{M}$, then $\mathcal{M}$ and $\mathcal{M}'$ coincide.*

Clearly any masa contains the unit element if there is one. As a remark, a masa in a *C^*-algebra*is automatically closed (w.r.t. the C*-norm; we define C*-algebras in Section 4.4, see page 145); the same holds true in general von Neumann algebras. Masas in the matrix algebras $M_d(\mathbb{C})$ are particularly easy to describe.

Proposition 1.2.2. *A subset $\mathcal{M} \subset M_d(\mathbb{C})$ is a masa if and only if the following equivalent conditions hold.*

(i) The set $\mathcal{M}$ is a d-dimensional, *-invariant subspace of $M_d(\mathbb{C})$ of pairwise commuting matrices.

(ii) There is a unitary matrix $u \in \mathcal{U}_d$ such that $\mathcal{M} = u\mathcal{D}_d u^*$.

(iii) There is an orthonormal basis $\mathfrak{a}$ of the Hilbert space $\mathbb{C}^d$ such that $\mathcal{M}$ is exactly the set of all matrices in $M_d(\mathbb{C})$ having $\mathfrak{a}$ as a basis of eigenvectors.

(iv) There is a set of d pairwise orthogonal minimal projections $p_0, \ldots, p_{d-1}$ in $M_d(\mathbb{C})$ which (both algebraically and linearly) generate $\mathcal{M}$:

$$\mathcal{M} = \mathcal{A}^*(p_0, \ldots, p_{d-1}) = span_{\mathbb{C}}(p_0, \ldots, p_{d-1})$$

The set of minimal projections in assertion (iv) is unique, *and no other minimal projections are contained in $\mathcal{M}$.*

Proof. Recall that a non-zero projection is called *minimal* if it admits no proper subprojections, and that a projection in $M_d(\mathbb{C})$ is minimal precisely if its range space is one-dimensional.

If statement (iv) holds, then $\mathcal{M}$ is d-dimensional by assumption. Its elements being all linear combinations of the minimal projections $p_0, \ldots, p_{d-1}$, moreover $\mathcal{M}$ is clearly *-invariant and commutative. Hence item (iv) implies (i).

Next, we prove the chain of implications $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (iv)$. First note that if (i) applies, every element $a \in \mathcal{M}$ is normal:

$$a \in \mathcal{M} \quad \underset{\mathcal{M}\ ^*\text{-closed}}{\Leftrightarrow} \quad a^* \in \mathcal{M} \quad \underset{\mathcal{M}\text{ abelian}}{\Rightarrow} \quad aa^* = a^*a$$

Consequently, a basis $(a_0, \ldots, a_{d-1})$ of the subspace $\mathcal{M}$ is at the same time a family of pairwise commuting normal matrices. It is a well-known fact from linear algebra (cf. for example [48, theorem 2.5.5 on p. 135]) that such a family is *simultaneously unitarily diagonalisable:* there is a unitary matrix $u \in \mathcal{U}_d$ such that all the matrices $u^*a_0u, \ldots, u^*a_{d-1}u$ are *diagonal,* leading to $u^*\mathcal{M}u \subset \mathcal{D}_d$. By dimension, it then follows $\mathcal{M} = u\mathcal{D}_du^*$.

Now denote by $\mathfrak{a} = (x_0, \ldots, x_{d-1})$ the orthonormal basis of the Hilbert space $\mathbb{C}^d$ given by the columns of the unitary matrix u, so that the actions of u and u^* are given by

$$u : z_i \mapsto x_i, \ \ u^* : x_i \mapsto z_i \ \text{ for } 0 \leq i < d.$$

(Recall that $\mathfrak{e} = (z_0, \ldots, z_{d-1})$ is the standard orthonormal basis.) Then clearly $\mathfrak{a}$ is a basis of eigenvectors for all elements in $\mathcal{M}$, and on the other hand any matrix having $\mathfrak{a}$ as an orthonormal basis of eigenvectors is diagonalisable by u and hence belongs to $\mathcal{M}$; that is, statement (iii) applies.

In order to deduce assertion (iv) from (iii), we first label the minimal diagonal projections

$$q_i = \text{diag}(0, \ldots, 0, \underset{\substack{| \\ (i\text{th pos.})}}{1}, 0, \ldots, 0) \in M_d(\mathbb{C}),$$

where i ranges from 0 to $d-1$. Of course, these projections generate—in fact linearly span—the subalgebra $\mathcal{D}_d$ of diagonal matrices in $M_d(\mathbb{C})$. Thus $\mathcal{M}$ is generated by the projections $p_0 = uq_0u^*, \ldots, p_{d-1} = uq_{d-1}u^*$.

For the observation subsequent to item (iv), consider a minimal projection $q \in \mathcal{M}$ onto the subspace spanned by a non-zero vector $y = \sum_{i=0}^{d-1} \lambda_i x_i \in \mathbb{C}^d$. Then at least one of the coefficients $\lambda_0, \ldots, \lambda_{d-1} \in \mathbb{C}$, say λ_{i_0}, is non-zero. Now q and p_{i_0} are both elements of $\mathcal{M}$ and therefore commute, hence one calculates:

$$q p_{i_0} y = p_{i_0} q y \quad \Rightarrow \quad q \lambda_{i_0} x_{i_0} = p_{i_0} y \quad \Rightarrow \quad q \lambda_{i_0} x_{i_0} = \lambda_{i_0} x_{i_0} \quad \Rightarrow \quad q x_{i_0} = x_{i_0}$$

Since q is minimal by assumption, this shows that the projections q and p_{i_0} coincide. There are thus no minimal projections in $\mathcal{M}$ besides $p_0, \ldots, p_{d-1}$.

Let us finally demonstrate that the equivalent statements (i) to (iv) hold if and only if $\mathcal{M}$ is a masa. If the latter is the case, then by the argumentation above, there is a unitary u diagonalising $\mathcal{M}$, hence $\mathcal{M} \subset u\mathcal{D}_d u^*$. By maximality of $\mathcal{M}$, this implies $\mathcal{M} = u\mathcal{D}_d u^*$, that is item (ii). Conversely, assume statement (iv) applies, and consider any matrix $a \in M_d(\mathbb{C})$ commuting with all elements in $\mathcal{M}$, hence specially with the projections $p_0, \ldots, p_{d-1}$. If $0 \neq x_i \in \mathbb{C}^d$ spans the range of p_i for all $0 \leq i < d$ as before, we get

$$a\, x_i = a p_i\, x_i = p_i a\, x_i = \lambda_i x_i$$

for some coefficients $\lambda_i \in \mathbb{C}$. This leads to the identity $a = \sum_{i=0}^{d-1} \lambda_i p_i$, hence a belongs to $\mathcal{M}$. Thereby $\mathcal{M}$, as defined in item (iv), is maximal, and since it further is a commutative *-subalgebra, our proof is complete. □

Equivalence classes of orthonormal bases and unitaries associated with masas

Consider an orthonormal basis $\mathfrak{a}$ [a unitary matrix $u \in \mathcal{U}_d$] corresponding to a masa $\mathcal{M}$ as in Proposition 1.2.2. Then changing the order of the vectors in $\mathfrak{a}$ [the columns of u] or multiplying the basis vectors [the columns of u] by different *phase factors*—i.e. elements of the unit circle $\mathbb{T}$—clearly leaves the associated masa unchanged. It is not hard to see that this defines *classes* of unitaries and orthonormal bases respectively, such that each class corresponds to one specific masa in $M_d(\mathbb{C})$.

To make this precise, we first need the following definition, which occurs, for instance, in the article [59] by Andreas Klappenecker and Martin Rötteler.

Definition 1.2.3. *A matrix in $M_d(\mathbb{C})$ is called* monomial *if it contains precisely one non-zero entry in each column and each row.*

Note that a monomial matrix is always invertible; it is furthermore unitary if and only if all of its non-zero entries have modulus one.

Proposition 1.2.4. *The set of all monomial matrices in $M_d(\mathbb{C})$ is a* subgroup *of the general linear group GL_d. Likewise, the set of all unitary monomial matrices in $M_d(\mathbb{C})$ is a subgroup of the unitary group $\mathcal{U}_d$, which we denote by $\mathcal{W}_d$. For all $d \geq 2$, the subgroup $\mathcal{W}_d$ of the unitary group $\mathcal{U}_d$ is* not normal*.*

The proof can be found in the Appendix on page 211. ▷

An important subgroup of the monomial matrices is given by the set of all so-called *permutation matrices.* With each permutation $\sigma \in S_d$, one associates a matrix $w_\sigma \in \mathcal{U}_d$ acting on the standard orthonormal basis by

$$w_\sigma z_i = z_{\sigma(i)} \text{ for } 0 \leq i < d.$$

The monomial matrices hence being a generalisation of the permutation matrices, monomial matrices are sometimes also named *weighted permutation matrices;* its non-zero entries are called *weights.*

Identifying the masa $\mathcal{D}_d$ of diagonal matrices with the abelian *-algebra of complex-valued functions on d different points $\mathcal{C}(\{0,\dots,d-1\})$, conjugations by monomial matrices $\mathcal{W}_d$ represent *-automorphisms on the latter *-algebra. This result, made precise in the following lemma, is probably familiar to most of the readers, and can easily be deduced from more general results concerning *-homomorphisms of finite-dimensional C*-algebras (see for example [30, lemma III.2.1]). Nevertheless, we provide an elementary proof in the Appendix, which the reader may skip without any problems.

Lemma 1.2.5. *Every *-automorphism ϕ of the masa $\mathcal{D}_d \subset M_d(\mathbb{C})$ is given by conjugation with a unitary monomial matrix $w \in \mathcal{W}_d$, i.e. ϕ is defined by the formula $\phi(a) = waw^*$ for all $a \in \mathcal{D}_d$. Moreover, the following equivalence holds.*

$$u\mathcal{D}_d u^* = \mathcal{D}_d \textit{ for } u \in \mathcal{U}_d \quad \Leftrightarrow \quad u \in \mathcal{W}_d$$

The proof can be found in the Appendix on pages 212-213. ▷

Remark 1.2.6. The choice of the unitary monomial matrix $w_\sigma \in \mathcal{W}_d$ associated with a *-automorphism ϕ of $\mathcal{D}_d$ via $\phi(\cdot) = w_\sigma \cdot w_\sigma^*$ is of course not unique. For any tuple $(\lambda_0,\dots,\lambda_{d-1}) \in \mathbb{T}^d$, the unitary monomial $w = w_\sigma \text{diag}(\lambda_0,\dots,\lambda_{d-1})$ obviously corresponds to ϕ as well. This results in the group isomorphisms

$$\text{Aut}\,\mathcal{D}_d \cong \mathcal{W}_d/\mathbb{T}^d \cong S_d,$$

where the set of tuples $\mathbb{T}^d$ is identified with the intersection $\mathcal{U}_d \cap \mathcal{D}_d$.

The monomial unitaries are the appropriate tool to define classes of unitaries and bases respectively which are associated with masas.

Definition/Proposition 1.2.7. *Consider two unitary matrices $u, v \in \mathcal{U}_d$ and denote the orthonormal bases of the Hilbert space $\mathbb{C}^d$ given by their* columns *by $\mathfrak{a} = (x_0, \dots, x_{d-1})$ and $\mathfrak{b} = (y_0, \dots, y_{d-1})$ respectively.*

(i) We call the unitary matrices u and v column-equivalent *and write $u \sim v$ if there is a unitary monomial matrix $w \in \mathcal{W}_d$ such that $u = vw$.*

(ii) We say the bases $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent, *in signs $\mathfrak{a} \sim \mathfrak{b}$, if and only if the associated unitaries u and v are column-equivalent.*

(ii') The orthonormal bases $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent if and only if there is a permutation $\sigma \in S_d$ and elements $\lambda_0, \dots, \lambda_{d-1} \in \mathbb{T}$ such that $y_i = \lambda_i x_{\sigma(i)}$ for all $0 \leq i < d$.

Column-equivalence of unitaries and equivalence of orthonormal bases are indeed well-defined equivalence relations. We label the corresponding equivalence classes as $[u]$ and $[\mathfrak{a}]$ respectively.

It is straightforward to check the assertions made in the proposition above, so we omit the short proof. Clearly the classes of column-equivalent unitaries are the elements of the quotient $\mathcal{U}_d/\mathcal{W}_d$. Note that this quotient is *not* a group for $d \geq 2$, because $\mathcal{W}_d$ is not normal (see Proposition 1.2.4). We will investigate the structure of the quotient $\mathcal{U}_d/\mathcal{W}_d$ a little closer in Section 2.3.

As mentioned before, we have introduced the equivalence relations above because any two column-equivalent unitary matrices (equivalent orthonormal bases respectively) correspond to one and the same masa in the sense of Proposition 1.2.2.

Proposition 1.2.8. *Let $\mathfrak{m}_d$ be the set of all masas in the matrix algebra $M_d(\mathbb{C})$. For unitaries $u, v \in \mathcal{U}_d$, let $\mathfrak{c}_u$ and $\mathfrak{c}_v$ denote the orthonormal bases of $\mathbb{C}^d$ given by the columns of u and v respectively. Then the following equivalences hold.*

$$u \sim v \quad \Leftrightarrow \quad \mathfrak{c}_u \sim \mathfrak{c}_v \quad \Leftrightarrow \quad u\mathcal{D}_d u^* = v\mathcal{D}_d v^* \tag{1.1}$$

This justifies the notation $\mathcal{M}_{[\mathfrak{a}]} = \mathcal{M}_{[u]} = u\mathcal{D}_d u^*$ for the masa corresponding to the unitary u and the basis $\mathfrak{c}_u$ respectively. Furthermore, all maps in the commutative diagram below are bijections.

$$\begin{tikzcd}
\mathcal{U}_d/\mathcal{W}_d \arrow[rr, "{[u]\mapsto[\mathfrak{c}_u]}"] \arrow[dr, "{[u]\mapsto\mathcal{M}_{[u]}}"'] & & \{\text{ONBs of } \mathbb{C}^d\}/\sim \arrow[dl, "{\mathcal{M}_{[\mathfrak{a}]}\mapsfrom[\mathfrak{a}]}"] \\
& \mathfrak{m}_d &
\end{tikzcd}$$

Figure 1.3: *The set of masas $\mathfrak{m}_d \cong \mathcal{U}_d/\mathcal{W}_d \cong \{$ONBs of $\mathbb{C}^d\}/\sim$*

Proof. Let us start with the equivalences (1.1). By definition, the orthonormal bases $\mathfrak{c}_u$ and $\mathfrak{c}_v$, given by the columns of the unitaries $u, v \in \mathcal{U}_d$, are equivalent if and only if u and v are column-equivalent. Beyond that, Lemma 1.2.5 allows to conclude as follows.

$$\begin{aligned} & u\mathcal{D}_d u^* = \quad v\mathcal{D}_d v^* \\ \Leftrightarrow \quad & \mathcal{D}_d \quad = u^* v \mathcal{D}_d v^* u \quad \underset{1.2.5}{\Leftrightarrow} \quad \underset{w \in \mathcal{W}_d}{\exists} u^* v = w \quad \Leftrightarrow \quad u \sim v \end{aligned}$$

It is clear by these equivalences that the notations $\mathcal{M}_{[\mathfrak{a}]}$ and $\mathcal{M}_{[u]}$ are well-defined.

As for the diagram, it is evident that the horizontal mapping is well-defined and injective by definition of the respective equivalence classes. Moreover, it is surjective due to the one-to-one correspondence between the orthonormal bases of the Hilbert space $\mathbb{C}^d$ (considered as *tuples* of vectors) and the unitaries in $\mathcal{U}_d$. Both of the other mappings are well-defined and injective by the equivalences (1.1), furthermore surjective by Proposition 1.2.2 (i). The commutativity of the diagram is obvious. □

1.3 Complex Hadamard matrices

Complex Hadamard matrices play an extraordinarily important role in the study and construction of families of *quasi-orthogonal*masas, which will be introduced in Chapters 2 and 3. At the same time, they can also be used to construct certain Hilbert-Schmidt orthonormal bases for *one single* masa. Since this is the goal of the following section, we introduce Hadamard matrices already at this point.

Definition 1.3.1. *A matrix $h \in M_d(\mathbb{C})$ is called* complex Hadamard matrix of modulus $c \in \mathbb{R}^+$ *if all of its entries have modulus c and if it fulfils the equalities*

$$hh^* = h^*h = c^2 d \cdot \mathrm{I}_d.$$

By convention, one assumes $c = 1$ whenever the modulus is not mentioned explicitly. Obviously, a complex Hadamard matrix is unitary if and only if its modulus is $\sqrt{1/d}$, in which case we call it unitary Hadamard matrix*for short.*

Note that the condition $hh^* = h^*h = c^2 d \cdot \mathrm{I}_d$ is equivalent to the following: if $h_0, \ldots, h_{d-1} \in \mathbb{C}^d$ are the columns of the matrix h, then the scalar product of two of them is

$$(h_i \mid h_j) = \begin{cases} c^2 d & \text{if } i = j, \\ 0 & \text{else} \end{cases}$$

for all $0 \leq i, j < d$. The columns of a (complex) Hadamard matrix are thus always pairwise orthogonal. Of course the same holds for its rows.

We have already come across a very prominent complex Hadamard matrix in the proof of Proposition 1.2.4.

Definition 1.3.2. *For any $d \in \mathbb{N}$ and any primitive dth root of unity $\zeta_d \in \mathbb{T}$, the matrix $(\zeta_d^{ij})_{0\leq i,j<d}$ is a complex Hadamard matrix. If we set $\zeta_d = \exp(2\pi i/d)$, then*

$$\mathrm{F}_d = \frac{1}{\sqrt{d}}\left(\zeta_d^{ij}\right)_{0\leq i,j<d}$$

is known as the (unitary) Quantum Fourier (Transform) matrix *or* Discrete Fourier (Transform) matrix *of order d.*

In fact, the unitary F_d describes a quantum gate (i.e. a unitary operator) performing a discrete Fourier transform on a d-dimensional quantum system (the Hilbert space $\mathbb{C}^d$). In the language of *harmonic analysis,* this reads as follows.

Remark. Recall that the characters of a (locally compact) abelian group G are the continuous group homomorphisms from G to the unit circle. There are *d characters* $\chi_0, \dots, \chi_{d-1}$ of the finite abelian group $\mathbb{Z}_d := \mathbb{Z}/d$, given by

$$\chi_i : \mathbb{Z}_d \longrightarrow \mathbb{T}, \quad j \longmapsto \zeta_d^{ij}.$$

They form a group w.r.t. pointwise multiplication, the *Pontryagin dual* $\widehat{\mathbb{Z}_d}$ of $\mathbb{Z}_d$, and the *Fourier Transformation F_d* maps from the convolution algebra of L^1-functions $L^1(\mathbb{Z}_d)$ to the function algebra $\mathcal{C}(\widehat{\mathbb{Z}_d})$. (Being finite-dimensional, both of these function algebras are of course just $\mathbb{C}[\mathbb{Z}_d]$ as sets; however, they are endowed with different operations, cf. Section 2.5.) The map F_d is defined by

$$\begin{aligned} F_d : L^1(\mathbb{Z}_d) &\longrightarrow \mathcal{C}(\widehat{\mathbb{Z}_d}), \\ f &\longmapsto \hat{f}, \\ &\qquad \hat{f}(\chi_i) = \sum_{j\in\mathbb{Z}_d} f(j)\chi_i(j) = \sum_{j\in\mathbb{Z}_d} f(j)\zeta_d^{ij} \;\text{ for all } i \in \mathbb{Z}_d. \end{aligned}$$

Now represent elements in both involved function algebras as columns with respect to the bases given by the characteristic functions on the d base points. Then you immediately see that the Quantum Fourier Transform matrix F_d implements the Fourier Transformation F_d.

The Quantum Fourier matrix is a member of an important subclass of the complex Hadamard matrices.

Definition 1.3.3. *Let $n \in \mathbb{N}$ denote a natural number. A complex Hadamard matrix h in $M_d(\mathbb{C})$ (of modulus one) is said to be a Hadamard matrix* of Butson-type (n, d) *if all of its entries are nth roots of unity. If h is of Butson-type (n, d), then $\sqrt{1/d}\,h$ is said to be a* unitary Butson-type Hadamard matrix.

Observe that if $h \in M_d(\mathbb{C})$ is a complex Hadamard matrix and $w \in \mathcal{W}_d$ is a unitary monomial matrix, then both of the products wh and hw are again complex Hadamard matrices. It seems reasonable that in the theory of classification of complex Hadamard matrices, one does not want to distinguish between the Hadamard matrices h, wh and hw. This gives rise to the following equivalence relation.

Definition 1.3.4. *Two complex Hadamard matrices $h, h' \in M_d(\mathbb{C})$ are said to be equivalent if there are monomial unitaries $w_0, w_1 \in \mathcal{W}_d$ relating them via the identity $h' = w_0 h w_1$.*

Each complex Hadamard matrix is equivalent to one of a particularly simple form. Given a Hadamard matrix $h = (\eta_{i,j})_{0 \leq i,j < d}$, define diagonal matrices

$$w_0 = \mathrm{diag}(\bar{\eta}_{0,0}, \ldots, \bar{\eta}_{d-1,0}) \quad \text{and} \quad w_1 = \eta_{0,0}\mathrm{diag}(\bar{\eta}_{0,0}, \ldots, \bar{\eta}_{0,d-1}).$$

Then one calculates that $w_0 h w_1$ is of the form

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ 1 & * & \ldots & * \\ \vdots & \vdots & \ddots & \vdots \\ 1 & * & \ldots & * \end{pmatrix},$$

where the $*$-entries are complex numbers of modulus one. A complex Hadamard matrix given in this form is said to be *dephased.*

Remark 1.3.5. The notion of equivalence of unitary Hadamard matrices does *not* coincide with the column-equivalence of unitaries defined in the first section.

There are various methods to construct complex Hadamard matrices in the literature (e.g. [13, 54, 102] only for dimension six); also, there is a complete list of all complex Hadamard matrices in dimensions two to five ([103]). A very advisable web page ([22]) on the subject is maintained by Wojciech Bruzda, Wojciech Tadej and Karol Życzkowski, including a list of known constructions and open problems as well as a catalogue of complex Hadamard matrices up to dimension 16. However, the full classification of all complex Hadamard matrices in higher dimensions—even in dimension six—is generally considered as a very hard problem, see for example the articles [10, 13, 54, 102], all published between 2007 and 2012. A solution still seems far from reach at present.

Excursion: Different notions of Hadamard matrices

Originally, the term *Hadamard matrix*refers to orthogonal matrices with entries from the set $\{1, -1\}$. In spite of their name, these matrices were not introduced by Jacques Hadamard, but by James J. Sylvester in his paper [99] published in 1867. In 1893, they reappeared in the article *"Résolution d'une question relative aux déterminants"* ([45]) by Hadamard.

In his paper, Hadamard investigated the square matrices which we call *complex* Hadamard matrices today, and, among other results, showed that Hadamard matrices as defined by Sylvester can at most exist in dimensions 1, 2 or 4^n ($n \in \mathbb{N}$). Whether they *do* actually exist in all of these dimensions is an open question until today, known as the famous *Hadamard problem.* Hadamard matrices have gained importance in different fields of mathematics and physics, for instance in quantum information theory ([116]) and in design theory ([18]). Figure 1.4 gives an overview over the mentioned types of Hadamard matrices.

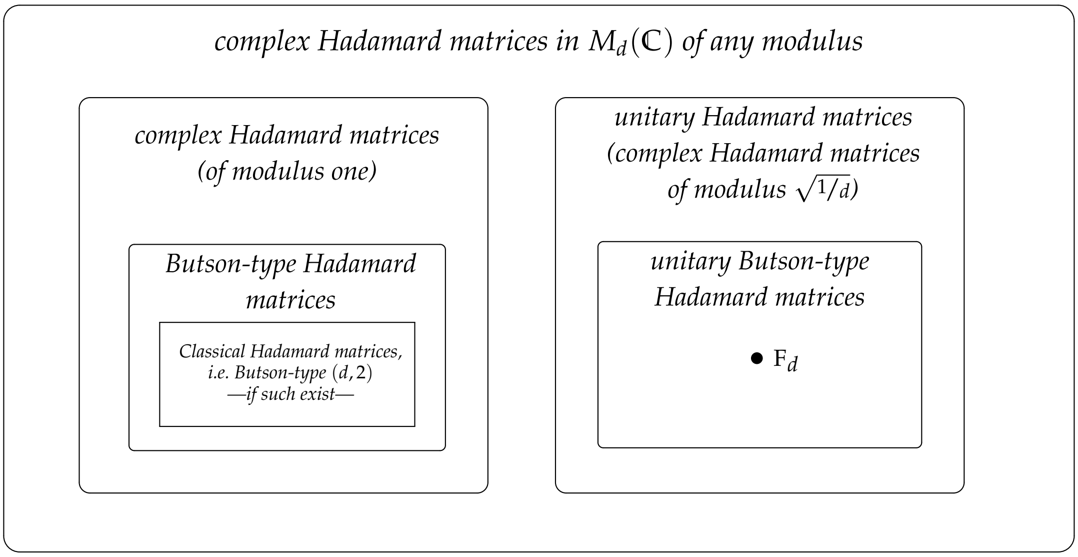

complex Hadamard matrices in $M_d(\mathbb{C})$ of any modulus
complex Hadamard matrices (of modulus one)
Butson-type Hadamard matrices
Classical Hadamard matrices, i.e. Butson-type $(d,2)$ —if such exist—
unitary Hadamard matrices (complex Hadamard matrices of modulus $\sqrt{1/d}$)
unitary Butson-type Hadamard matrices
• F_d

Figure 1.4: *Hadamard matrices*

We shall mention that there are generalisations of the original definition of Hadamard matrices which are fairly different from the ones presented above. This might explain why there is some confusion about the precise definition of the different types. First and foremost, we must underline that most, though not all, authors do *not* think of a complex Hadamard matrix when they use the term *generalised* Hadamard matrix, but refer to a quite different generalisation (see for instance [47]; for the present work, however, these other generalisations are of no interest).

At the same time, the name "Hadamard matrix" always refers to a *complex* Hadamard matrix for some authors. Others speak of "rescaled Hadamard matrices" whenever the entries are of modulus other than one. Yet other authors consider unitarity as one of the defining features of Hadamard matrices. We have chosen Definition 1.3.1 above (in accordance with many other authors, see for instance [28, 57, 69]) because it is the most consistent one in our opinion.

1.4 Unitary Hilbert-Schmidt orthonormal bases of masas

Unitary operator bases of the complex $d \times d$-matrices that are orthonormal w.r.t. the Hilbert-Schmidt scalar product are of special importance in this work (namely in Chapters 4 and 5). In this section, we concentrate on unitary Hilbert-Schmidt ONBs for a single masa.

Proposition 1.4.1. *Let $u \in \mathcal{U}_d$ be a unitary matrix, $\mathcal{M} = \mathcal{M}_{[u]}$ the associated masa and*

$$h = (\eta_{i,j})_{0 \leq i,j < d} \in M_d(\mathbb{C})$$

a $d \times d$-matrix. Furthermore, define diagonal matrices $h_0, \ldots, h_{d-1} \in \mathcal{D}_d$ containing the columns of h via the formula

$$h_j = diag(\eta_{0,j}, \ldots, \eta_{d-1,j})$$

for $0 \leq j < d$. Then the following statements are equivalent.

(i) The matrices $uh_0u^*, \ldots, uh_{d-1}u^* \in \mathcal{M}$ form a unitary Hilbert-Schmidt orthonormal basis of the masa $\mathcal{M}$.

(ii) The matrix h is a complex Hadamard matrix (of modulus one).

Proof. The elements $uh_0u^*, \ldots, uh_{d-1}u^*$ form a Hilbert-Schmidt orthonormal basis if and only if $h_0, \ldots, h_{d-1}$ do so: for $j_0, j_1 \in \{0, \ldots, d-1\}$, one calculates

$$\left(uh_{j_0}u^* \,\middle|\, uh_{j_1}u^*\right)_{\mathrm{HS}} = \tau(uh_{j_0}u^*uh_{j_1}^*u^*) = \tau(h_{j_0}h_{j_1}^*) = \left(h_{j_0} \,\middle|\, h_{j_1}\right)_{\mathrm{HS}}.$$

Recall that two diagonal matrices are orthogonal w.r.t. the Hilbert-Schmidt scalar product if and only if the the corresponding column vectors are orthogonal as elements of the Hilbert space $\mathbb{C}^d$. So we have shown that the columns of the matrix h are pairwise orthogonal precisely if the matrices $uh_0u^*, \ldots, uh_{d-1}u^*$ form an orthogonal family w.r.t. the Hilbert-Schmidt scalar product.

What is more, each matrix uh_ju^* is unitary if and only if h_j is unitary, and the last condition is met if and only if all entries of h_j have modulus one ($0 \leq j < d$). □

By Lemma 1.2.5, we can always assume that the matrix h in Proposition 1.4.1 above is dephased, so that the associated orthonormal basis of unitaries contains the identity matrix I_d. Accordingly, all other members of the basis are *trace-free*.

If $\mathfrak{v} = (1, v_1, \ldots, v_{d-1})$ is a Hilbert-Schmidt orthonormal basis of a masa $\mathcal{M}$ in $M_d(\mathbb{C})$, then of course $\mathcal{M}$ contains all products of the basis elements. If you consider the elements of $\mathfrak{v}$ as *algebraic* generators of $\mathcal{M}$, you may therefore find that your choice is redundant, in the sense that a proper subset of $\mathfrak{v}$ suffices to generate $\mathcal{M}$ as a *-algebra. On the other hand, once you start with such a generating subset of a basis, this does not in general allow to reconstruct the original orthonormal basis.

In the following example, we present an extraordinarily nice Hilbert-Schmidt orthonormal basis of the masa $\mathcal{D}_d \subset M_d(\mathbb{C})$ that contains all products of its elements.

Example 1.4.2. Fix the primitive dth root of unity $\zeta_d = \exp(2\pi\mathrm{i}/d) \in \mathbb{T}$ for each $d \in \mathbb{N}$ and set

$$\mathrm{z}_d = \operatorname{diag}\left(\zeta_d^0, \dots, \zeta_d^{d-1}\right).$$

The diagonal unitary z_d is sometimes called *clock matrix*. It generalises the Pauli matrix $\sigma_z = \operatorname{diag}(1, -1) \in M_2(\mathbb{C})$. It is one of the so-called *Weyl matrices* or *generalised Pauli matrices*. We give a short comment on the different names of these matrices at the end of Section 2.2 (Remark 2.2.3).

Fix a dimension d and a factorisation $d = d_0 \cdots d_m$ ($d_0, \dots, d_m \in \mathbb{N}$), and consider the following unitary diagonal matrices in $M_d(\mathbb{C})$:

$$\begin{aligned}
w_0 &= \mathrm{z}_{d_0} \otimes \mathrm{I}_{d_1} \otimes \mathrm{I}_{d_2} \otimes \cdots \otimes \mathrm{I}_{d_m}, \\
w_1 &= \mathrm{I}_{d_0} \otimes \mathrm{z}_{d_1} \otimes \mathrm{I}_{d_2} \otimes \cdots \otimes \mathrm{I}_{d_m}, \\
&\vdots \\
w_m &= \mathrm{I}_{d_0} \otimes \mathrm{I}_{d_1} \otimes \cdots \otimes \mathrm{I}_{d_{m-1}} \otimes \mathrm{z}_{d_m}
\end{aligned}$$

(Recall that we always employ the tensor product isomorphism defined in Convention 0.0.2, identifying $\mathcal{D}_{d_0} \otimes \cdots \otimes \mathcal{D}_{d_m}$ and $\mathcal{D}_d$.) Then the set of all products of these matrices,

$$\mathfrak{w}_{d_0,\dots,d_m} = \{w_0^{i_0} \cdots w_m^{i_m} \mid 0 \le i_k < d_k \text{ for all } 0 \le k \le m\},$$

is a Hilbert-Schmidt orthonormal basis of the diagonal masa $\mathcal{D}_d \subset M_d(\mathbb{C})$.

In fact, given two elements $w_0^{i_0} \cdots w_m^{i_m}$ and $w_0^{j_0} \cdots w_m^{j_m}$ in $\mathfrak{w}_{d_0,\dots,d_m}$, one computes:

$$\begin{aligned}
\left(w_0^{i_0} \cdots w_m^{i_m} \,\middle|\, w_0^{j_0} \cdots w_m^{j_m}\right)_{\mathrm{HS}} &= \tau\left(w_0^{i_0-j_0} \cdots w_m^{i_m-j_m}\right) \\
&= \tau\left(\mathrm{z}_{d_0}^{i_0-j_0} \otimes \cdots \otimes \mathrm{z}_{d_m}^{i_m-j_m}\right) = \prod_{k=0}^{m} \tau\left(\mathrm{z}_{d_k}^{i_k-j_k}\right) \\
&= \prod_{k=0}^{m} \underbrace{\frac{1}{d_k} \sum_{l=0}^{d_k-1} \zeta_{d_k}^{l(i_k-j_k)}}_{=\begin{cases} 1 & \text{if } i_k = j_k \\ 0 & \text{else} \end{cases}} = \begin{cases} 1 & \text{if } i_0 = j_0, \dots, i_m = j_m \\ 0 & \text{else} \end{cases}
\end{aligned}$$

In the first step, we have made use of the fact that all elements w_k commute and fulfil the equality $(w_k^*)^i = w_k^{d_k - i}$. We have also used the conventional notation $w_k^{-i} := (w_k^*)^i$, as we shall often do in the sequel.

Bases whose elements can be written as tensor products with respect to a fixed tensor representation $M_d(\mathbb{C}) \cong M_{d_0}(\mathbb{C}) \otimes \cdots \otimes M_{d_m}(\mathbb{C})$ are often referred to as *product bases* in the literature (see e.g. [71]). Product bases for the whole matrix algebra $M_d(\mathbb{C})$ will be of great importance from Chapter 3 on.

Let $\mathcal{M} = \mathcal{M}_{[u]}$ be a masa in $M_d(\mathbb{C})$, associated with a unitary $u \in \mathcal{U}_d$. Then a product basis for $\mathcal{M}$ is given by $u\, \mathfrak{w}_{d_0,\dots,d_m}\, u^*$. For future reference, we record this fact in the next proposition. Moreover, we show that for a fixed factorisation of the dimension d, these product bases of masas are in a sense unique.

Proposition 1.4.3. *Let $\mathcal{M} = u\mathcal{D}_d u^* \subset M_d(\mathbb{C})$ denote the masa associated with a unitary matrix $u \in \mathcal{U}_d$, and $d = d_0 \cdots d_m$ a factorisation of the dimension d.*

(i) Let $w_0, \dots, w_m$ be the unitary diagonal elements of the product basis $\mathfrak{w}_{d_0,\dots,d_m}$ defined in Example 1.4.2. Then the elements $v_0 = uw_0u^*, \dots, v_m = uw_mu^* \in \mathcal{M}$ form a product basis

$$u\, \mathfrak{w}_{d_0,\dots,d_m}\, u^* = \{v_0^{i_0} \cdots v_m^{i_m} \mid 0 \le i_k < d_k \text{ for all } 0 \le k \le m\}$$

for the masa $\mathcal{M}$.

(ii) Consider matrices $\tilde{v}_0, \dots, \tilde{v}_m \in \mathcal{M}$ satisfying the following conditions.

(iia) The elements $\tilde{v}_k$ are subject to the equation $\tilde{v}_k^{d_k} = 1$ for all $0 \le k \le m$.

(iib) The set of products $\{\tilde{v}_0^{i_0} \cdots \tilde{v}_m^{i_m} \mid 0 \le i_k < d_k \text{ for all } 0 \le k \le m\}$ is an orthonormal basis for the masa $\mathcal{M}$.

Then the matrices $\tilde{v}_0, \dots, \tilde{v}_m$ are unitaries, and there is a unitary matrix $\tilde{u} \sim u \in \mathcal{U}_d$ fulfilling the identities

$$\tilde{v}_0 = \tilde{u}w_0\tilde{u}^*, \dots, \tilde{v}_{d-1} = \tilde{u}w_{d-1}\tilde{u}^*.$$

Proof. Since the first part of the proposition is a direct consequence of Example 1.4.2, we only need to prove statement (ii). The elements $\tilde{v}_0, \dots, \tilde{v}_{m-1}$ belong to the masa $\mathcal{M}$, so there are diagonal matrices $\tilde{w}_0, \dots, \tilde{w}_{m-1} \in \mathcal{D}_d$ which satisfy the identity $\tilde{v}_k = u\tilde{w}_k u^*$ for all $0 \le k < d$. Condition (iia) implicates that all (diagonal) entries of the elements $\tilde{w}_0, \dots, \tilde{w}_{m-1}$ are dth roots of unity, so that the matrices $\tilde{v}_0, \dots, \tilde{v}_{m-1}$ are unitaries. Moreover, we get

$$(\tilde{v}_k^*)^i = \tilde{v}_k^{d_k - i}$$

for all $0 \le k < m$ and $0 \le i < d_k$.

Obviously, the diagonal matrices $\tilde{w}_0, \dots, \tilde{w}_{m-1}$ also obey conditions (iia) and (iib), where the masa $\mathcal{M}$ must be replaced by $\mathcal{D}_d$ in the second item. Condition (iib) permits to declare a *linear bijection* $\phi : \mathcal{D}_d \to \mathcal{D}_d$ mapping one orthonormal basis to another, by setting

$$\phi\left(w_0^{i_0} \cdots w_m^{i_m}\right) = \tilde{w}_0^{i_0} \cdots \tilde{w}_m^{i_m}$$

for all tuples $(i_0, \dots, i_{d-1}) \in \{0, \dots, d_0 - 1\} \times \cdots \times \{0, \dots, d_m - 1\}$.

We need to prove that ϕ is in fact a *-homomorphism (and thus, by the last paragraph, automatically a *-*auto*morphism). For a single basis element, we compute

$$\begin{aligned}\left(\phi\left(w_0^{i_0} \cdots w_m^{i_m}\right)\right)^* &= \left(\tilde{w}_0^{i_0} \cdots \tilde{w}_m^{i_m}\right)^* = \tilde{w}_0^{d_0 - i_0} \cdots \tilde{w}_m^{d_m - i_m} \\ &= \phi\left(w_0^{d_0 - i_0} \cdots w_m^{d_m - i_m}\right) = \phi\left(\left(w_0^{i_0} \cdots w_m^{i_m}\right)^*\right).\end{aligned}$$

As all elements in $\mathcal{D}_d$ are linear combinations of such basis elements and the involution is linear, this generalises to $\phi(a)^* = \phi(a^*)$ for all $a \in \mathcal{D}_d$. In the same way, one checks that $\phi(ab) = \phi(a)\phi(b)$ holds for all elements $a, b \in \mathcal{D}_d$. (In terms of abstract algebra, we could just have argued that ϕ sends the generators $w_0, \dots, w_{m-1}$ of the *-algebra $\mathcal{D}_d$ to generators $\tilde{w}_0, \dots, \tilde{w}_{m-1}$, subject to the same *-algebraic relations.)

According to Lemma 1.2.5, there is a unitary monomial matrix $w \in \mathcal{W}_d$ such that the identity $\phi(a) = waw^*$ applies for all $a \in \mathcal{D}_d$. Defining a unitary matrix $\tilde{u} = uw$, which is equivalent to u in the sense of Definition 1.2.7, we compute

$$\tilde{v}_k = u\, \tilde{w}_k\, u^* = u\, \phi(w_k)\, u^* = \tilde{u}\, w_k\, \tilde{u}^*$$

for all indices $0 \leq k \leq m$, which completes our proof. □

Writing the elements of $\mathfrak{w}_{d_0,\dots,d_m}$ as columns of a $d \times d$-matrix defines, for any order of columns, a complex Hadamard matrix (cf. Proposition 1.4.1). Fix an order of the columns and label the corresponding complex Hadamard matrix as h. Our aim is to show that the complex Hadamard matrix h is equivalent, in the sense of Definition 1.3.4, to the tensor product of Fourier matrices (see Definition 1.3.2)

$$\sqrt{d}\, \mathrm{F} = \sqrt{d}\, \mathrm{F}_{d_0} \otimes \cdots \otimes \mathrm{F}_{d_m}.$$

To this aim, we compare the columns of the latter matrix to the columns of h.

First observe that for any dimension $n \in \mathbb{N}$, the entries of the ith column of the rescaled Quantum Fourier matrix $\sqrt{n}\mathrm{F}_n$ correspond to the entries of the diagonal matrix $\mathrm{Z}_n^i = \operatorname{diag}(\zeta_n^{0 \cdot i}, \dots, \zeta_n^{(n-1) \cdot i})$. Therefore, identifying column vectors in $\mathbb{C}^d$ with diagonal matrices in $M_d(\mathbb{C})$ once more, the columns of the complex Hadamard matrix $\sqrt{d}\, \mathrm{F}$ are given by the tensor products $\mathrm{Z}_{d_0}^{i_0} \otimes \cdots \otimes \mathrm{Z}_{d_m}^{i_m}$, where the powers i_k range from 0 to $d_k - 1$ for $0 \leq k \leq m$. A comparison yields that these are precisely the basis elements

$w_0^{i_0} \cdots w_m^{i_m}$ of the Hilbert-Schmidt orthonormal basis $\mathfrak{w}_{d_0,\ldots,d_m}$. Hence, the columns of h and $\sqrt{d}\,\mathrm{F}$ coincide up to their order, i.e. h and $\sqrt{d}\,\mathrm{F}$ are equivalent complex Hadamard matrices.

It is indeed not hard to determine the "right order" of the columns of h (so that it would actually *coincide* with $\sqrt{d}\,\mathrm{F}$). However, it is quite technical to write this down, whence we pass on a detailed discussion thereof. Instead, we give a couple of examples in order to clarify the correspondences above.

Examples 1.4.4. (a) A Hilbert-Schmidt orthonormal basis of the diagonal matrices inside $M_4(\mathbb{C})$ is given by $\mathfrak{w}_4 = \{\mathrm{Z}_4^i \mid 0 \leq i \leq 3\}$.

The vectors in $\mathbb{C}^4$ corresponding to this basis are

$$\begin{pmatrix}1\\1\\1\\1\end{pmatrix}, \begin{pmatrix}1\\\mathrm{i}\\-1\\-\mathrm{i}\end{pmatrix}, \begin{pmatrix}1\\-1\\1\\-1\end{pmatrix}, \begin{pmatrix}1\\-\mathrm{i}\\-1\\\mathrm{i}\end{pmatrix},$$

and the matrix given by these columns (in the order above) is the rescaled Quantum Fourier matrix $2\mathrm{F}_4$.

(b) The orthonormal basis $\mathfrak{w}_{2,2}$ of $\mathcal{D}_4 \subset M_4(\mathbb{C})$ is given by

$$\begin{aligned}\mathfrak{w}_{2,2} &= \{\mathrm{Z}_2^{i_0} \otimes \mathrm{Z}_2^{i_1} \mid 0 \leq i_0, i_1 \leq d_j - 1\}\\ &= \{\mathrm{I}_2 \otimes \mathrm{I}_2,\ \mathrm{I}_2 \otimes \mathrm{Z}_2,\ \mathrm{Z}_2 \otimes \mathrm{I}_2,\ \mathrm{Z}_2 \otimes \mathrm{Z}_2\}.\end{aligned}$$

The vectors associated with this basis are

$$\begin{pmatrix}1\\1\\1\\1\end{pmatrix}, \begin{pmatrix}1\\-1\\1\\-1\end{pmatrix}, \begin{pmatrix}1\\1\\-1\\-1\end{pmatrix}, \begin{pmatrix}1\\-1\\-1\\1\end{pmatrix},$$

and they are the columns of the product matrix $2 \cdot \mathrm{F}_2 \otimes \mathrm{F}_2$:

$$\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix} \otimes \begin{pmatrix}1 & 1\\1 & -1\end{pmatrix} = \begin{pmatrix}1 & 1 & 1 & 1\\1 & -1 & 1 & -1\\1 & 1 & -1 & -1\\1 & -1 & -1 & 1\end{pmatrix}$$

The Discrete Fourier matrices F_d are not only of unitary Butson-type (d,d), but belong to another class of complex Hadamard matrices, the so-called *circulant Hadamard matrices*. Likewise, the Hadamard matrices $\mathrm{F}_{d_0} \otimes \cdots \otimes \mathrm{F}_{d_m}$ belong to a generalisation of the former class, the *block-circulant Hadamard matrices with circulant blocks*. The following definition of these special classes is adopted from M. Combescure, see [28].

Definition 1.4.5. *Let $h = (\eta_{i,j})_{0\leq i,j<d}$ denote a complex Hadamard matrix in $M_d(\mathbb{C})$.*

(i) We say h is circulant Hadamard matrix*if there is a tuple $(\alpha_0, \dots, \alpha_{d-1})$ in $\mathbb{T}^d$ such that $\eta_{i,j} = \alpha_{(d-1)i+j}$, where the right-hand side index is understood modulo d. The matrix h is thus of the form*

$$\begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \dots & \alpha_{d-1} \\ \alpha_{d-1} & \alpha_0 & \alpha_1 & \dots & \alpha_{d-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_0 \end{pmatrix}.$$

(ii) Let $d = kl$ be a factorisation of d ($k, l \in \mathbb{N}$). The matrix h is called block-circulant *if there are Hadamard matrices $a_0, \dots, a_l \in M_k(\mathbb{C})$ such that h is of the form*

$$\begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_{l-1} \\ a_{l-1} & a_0 & a_1 & \dots & a_{l-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \dots & a_0 \end{pmatrix}.$$

(iii) If h is block-circulant as in item (ii) and the matrices $a_0, \dots, a_l \in M_k(\mathbb{C})$ are again circulant, we say h is block-circulant with circulant blocks.

Obviously, the matrices $\mathrm{F}_{d_0} \otimes \cdots \otimes \mathrm{F}_{d_m}$ are, in case m is greater than 1, not only block-circulant with circulant blocks, but these blocks are again block-circulant and so on. We propose the name *block-circulant Hadamard matrix of depth m* for such matrices.

We end this section by a proposition concerning the uniqueness of (unitary conjugates of) the bases $\mathfrak{w}_{d_0,\dots,d_m}$. All members of these bases are unitary operators $v \in \mathcal{U}_d$ with Hilbert-Schmidt orthogonal powers $v, v^2, \dots, v^k$, where v^k equals the unit matrix I_d and the "degree" $k \in \mathbb{N}$ divides the dimension d. One may ask if the last condition is necessary; a negative answer might permit constructions of Hilbert-Schmidt orthonormal bases very different from the ones above. But the answer is positive.

Proposition 1.4.6. *Consider a unitary matrix $v \in \mathcal{U}_d$ such that v^n is the unit matrix I_d and all powers $v, v^2, \dots, v^n$ are pairwise Hilbert-Schmidt orthogonal, that is $\tau(v^k) = 0$ for all exponents $1 \leq k < n$. Then n divides the dimension d.*

The proof can be found in the Appendix on pages 213-214. ▷

Remark. The condition that the powers of v are pairwise Hilbert-Schmidt orthogonal is crucial in the proposition above. Otherwise it is straightforward to find, for any $k \in \mathbb{N}$, a unitary matrix $v \in \mathcal{U}_d$ such that $v^k = \mathrm{I}_d$. As an example, just take a primitive kth root of unity $\zeta_k \in \mathbb{T}$ and set $v = \mathrm{diag}(\zeta_k, \dots, \zeta_k)$.

Chapter 2

Quasi-orthogonality of masas

In this chapter we commence our study of quasi-orthogonal masas. Pairs of quasi-orthogonal masas on the level of matrix algebras correspond to *unbiased bases* on the level of Hilbert spaces. The importance of unbiasedness in quantum mechanics is an important motivation for the investigation of quasi-orthogonal masas. Therefore we start the chapter by sketching the physical meaning of unbiasedness in Section 2.1.

A thorough introduction of the mathematical notion of quasi-orthogonality and unbiasedness follows in Section 2.2. The set of all masas in a fixed dimension is a compact metric space and a smooth manifold, and quasi-orthogonal masa pairs are maximally distant points on this manifold, as we shall see in Section 2.3.

We then discuss the important distinction between *standard* and *non-standard* pairs of quasi-orthogonal masas in Section 2.4. Standard pairs play a central role in the present work. Among other things, they can be generalised to *normal* and *nice* pairs of masas, which are—under certain conditions, as far as normal pairs are concerned—the basic building blocks for the nice masa families presented in Chapters 4 and 5.

We take one more look at standard pairs of masas in the excursional Section 2.5, discussing their connection to certain finite dimensional crossed products.

2.1 *Motivation:* Pairs of mutually unbiased bases in quantum physics

Let a and b denote two observables in a d-dimensional quantum system, i.e. two self-adjoint operators in the matrix algebra $M_d(\mathbb{C})$. In Section 1.1, we have considered the case that a and b are *compatible*, i.e. they have a common basis of eigenstates and hence the result of measurement b is completely determined once the system is prepared by a measurement of a (provided the spectrum of a is non-degenerated; see Figure 1.2 on page 11). To put it differently, preparing the system by measuring a degenerates the probability distribution for the possible outcomes of b to a Dirac distribution.

In general, this is of course not true, but still the outcome of the second measurement b is influenced by the outcome of a. To see this, denote the eigenstates of a by $x_0, \dots, x_{d-1} \in \mathbb{C}_1^d$, those of b by $y_0, \dots, y_{d-1} \in \mathbb{C}_1^d$. Then for each $0 \leq i < d$, a probability measure on d points is defined by

$$P_i(j) = \big|(x_i \,|\, y_j)\big|^2 \qquad (0 \leq j < d).$$

If the system is in an eigenstate x_{i_0} after performing measurement a, then the probability to detect any eigenstate y_j of b is given by $P_{i_0}(j) = |(x_{\mathbf{i_0}} \,|\, y_j)|^2$. This fact is illustrated in Figure 2.1.

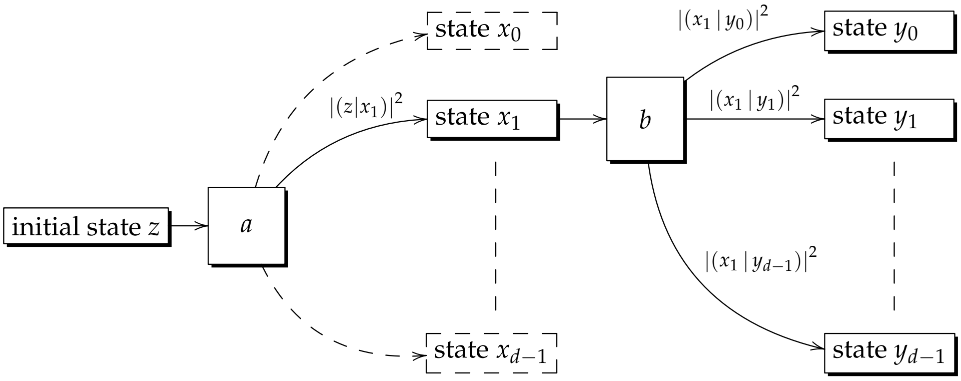


Figure 2.1: *Incompatible observables*

In case the observables a and b are not compatible, the probability measures P_i may be more or less "close to a Dirac distribution". One may immediately agree (leaving aside details on distances between probability measures) that the *uniform distribution* on d points, given by $P(j) = {}^1\!/_d$ for $0 \leq j < d$, can be considered as the opposite to a Dirac distribution. In this sense, the very reverse of "all measures $P_0, \dots, P_{d-1}$ are Dirac distributions" is "all measures $P_0, \dots, P_{d-1}$ are uniform".

Let us consider the case that all of the distributions $P_0, \dots, P_{d-1}$ are uniform. Then preparing a system by a measurement of a leaves the experimenter—independently of the outcome—in *maximal ignorance* about the outcome of measurement b, which is again the exact opposite of the case of compatible observables. Julian Schwinger, who apparently was the first to discuss such pairs of observables in 1960 ([91]), called the measurements a and b *maximal non-commutative* and coined the term *complementary* for the associated operators.

On the level of the eigenbases of a and b, this situation is reflected by the identities

$$\big|(x_i \,|\, y_j)\big|^2 = \frac{1}{d} \qquad (0 \leq i, j < d). \tag{2.1}$$

Pairs of bases fulfilling equations (2.1) are called *unbiased*. To our best knowledge, this expression was introduced in 1989 by William K. Wootters and Brian D. Fields ([114]).

Why "unbiased"?

Although one could as well call pairs of bases with the property (2.1) *complementary* by analogy with the associated observables, the term unbiased prevailed. We conclude this section by giving an ad hoc motivation for this expression.

In the area of statistics, one calls statistical data *biased* if they are systematically distorted (be it due to a false choice of the sample, inappropriate calculations or whatever). We recommend the Wikipedia page for a basic but quick introduction on this subject ([110]).

Now suppose your goal as a physicist or an engineer is to construct a *perfect random generator* picking one out of a finite set of d numbers. Having two complementary observables a and b at hand, you can first prepare a d-dimensional quantum system by a measurement of a, then measure b (where you assign a natural number to each outcome of measurement b).

Only if the chosen observables are precisely complementary—which is, as far as we know, not quite easy to achieve in experimental quantum physics—your random generator will pass a statistical test of many reruns, i.e. the outcomes will show the behaviour of a uniform distribution. If not, the result is *systematically distorted*, and a statistician would thus state that your random generator (and hence the chosen pair of bases) is *biased*.

2.2 Quasi-orthogonal masas, unbiased bases and unbiased unitaries

As before, we equip the complex matrix algebra $M_d(\mathbb{C})$ with the Hilbert-Schmidt scalar product. Two masas in $M_d(\mathbb{C})$ can clearly not be orthogonal subspaces, because they intersect in the line $\mathbb{C} \cdot \mathrm{I}_d$. However, the masas minus this line can well be orthogonal. In this case, the masas are said to be *orthogonal in the sense of S. Popa*, who invented this notion in 1983 (see [83]), or *quasi-orthogonal.*

Definition 2.2.1. *Two masas $\mathcal{M}, \mathcal{N} \subset M_d(\mathbb{C})$ are called* quasi-orthogonal*if the subspaces $\mathcal{M} \ominus \mathbb{C} \cdot \mathrm{I}_d$ and $\mathcal{N} \ominus \mathbb{C} \cdot \mathrm{I}_d$ of $M_d(\mathbb{C})$ are Hilbert-Schmidt orthogonal. We use the following notation.*

$$\mathcal{M} \perp_q \mathcal{N} \quad :\Leftrightarrow \quad \mathcal{M} \ominus \mathbb{C} \cdot \mathrm{I}_d \perp \mathcal{N} \ominus \mathbb{C} \cdot \mathrm{I}_d$$

We start by giving two very important examples, the first of which involves the standard cyclic permutation matrix

$$\mathrm{X}_d = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & & \vdots & \vdots \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix} \in \mathcal{W}_d.$$

Like the diagonal matrix $\mathrm{Z}_d \in \mathcal{W}_d$ introduced in Example 1.4.2, the unitary monomial X_d, also known as *shift matrix*, is one of the Weyl matrices. For $d = 2$, it obviously coincides with the Pauli matrix

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

We comment on the various names of the matrices X_d and Z_d at the end of this section.

Examples 2.2.2. (a) The permutation matrix $\mathrm{X}_d \in \mathcal{W}_d$ generates a masa $\mathcal{M} = \mathcal{A}^*(\mathrm{X}_d)$ in $M_d(\mathbb{C})$ which is quasi-orthogonal to the diagonal masa $\mathcal{D}_d$. The so-called *standard pair* $\{\mathcal{D}_d, \mathcal{M}\}$ is considered in detail in Section 2.4.

(b) The masas $\mathcal{D}_d$ and $\mathcal{M}_{[u]} = u\mathcal{D}_d u^*$ are quasi-orthogonal if and only if $u \in \mathcal{U}_d$ is a unitary Hadamard matrix.

Proof. For the first example, you convince yourself without difficulty that the tuple

$$\left(\mathrm{I}_d, \mathrm{X}_d, \ldots, \mathrm{X}_d^{d-1}\right)$$

is a Hilbert-Schmidt orthonormal system, so that $\mathcal{M}$ is of dimension d and thus a masa. Likewise, we know from Example 1.4.2 that the powers of the diagonal matrix Z_d form an orthonormal basis of the masa $\mathcal{D}_d$. We have to demonstrate that the spaces

$$\mathcal{M} \ominus \mathbb{C} \cdot \mathrm{I}_d = \operatorname{span}\left(\mathrm{X}_d, \ldots, \mathrm{X}_d^{d-1}\right) \text{ and}$$
$$\mathcal{D}_d \ominus \mathbb{C} \cdot \mathrm{I}_d = \operatorname{span}\left(\mathrm{Z}_d, \ldots, \mathrm{Z}_d^{d-1}\right)$$

are orthogonal, that is we must check the equations

$$\left(\mathrm{X}_d^i \,\middle|\, \mathrm{Z}_d^j\right)_{\mathrm{HS}} = \tau\left(\mathrm{X}_d^i \mathrm{Z}_d^{d-j}\right) = 0 \text{ for all } 1 \le i, j < d.$$

This is straightforward, because actually all diagonal elements of the products $\mathrm{X}_d^i \mathrm{Z}_d^{d-j}$ are zero as long as i is non-zero, and otherwise we already know that $\tau(\mathrm{Z}_d^j)$ equals zero for all $1 \le j < d$.

For instance (b), let q_i be the minimal diagonal projections

$$q_i = \operatorname{diag}(0,\dots,0,\underset{(i\text{th pos.})}{\underset{|}{1}},0,\dots,0)$$

for all $0 \leq i < d$ as before. Furthermore, let $p_0 = uq_0u^*, \dots, p_{d-1} = uq_{d-1}u^*$ denote the minimal projections generating $\mathcal{M}_{[u]}$. By definition, $\mathcal{D}_d$ and $\mathcal{M}_{[u]}$ are quasi-orthogonal if and only if

$$\mathcal{D}_d \ominus \mathbb{C} \cdot \mathrm{I}_d \perp u\mathcal{D}_d u^* \ominus \mathbb{C} \cdot \mathrm{I}_d.$$

This relation holds precisely if the equation

$$\left(q_i - (q_i \,|\, \mathrm{I}_d)_{\mathrm{HS}} \mathrm{I}_d \,\middle|\, p_j - (p_j \,|\, \mathrm{I}_d)_{\mathrm{HS}} \mathrm{I}_d \right)_{\mathrm{HS}} = 0$$

holds true for all $0 \leq i, j < d$, which simplifies to

$$\begin{aligned} 0 &= \left(q_i - \frac{1}{d}\mathrm{I}_d \,\middle|\, p_j - \frac{1}{d}\mathrm{I}_d \right)_{\mathrm{HS}} \\ &= (q_i \,|\, p_j)_{\mathrm{HS}} - \frac{1}{d}\,(\mathrm{I}_d \,|\, p_j)_{\mathrm{HS}} - \frac{1}{d}\,(q_i \,|\, \mathrm{I}_d)_{\mathrm{HS}} + \frac{1}{d^2} \\ &= (q_i \,|\, p_j)_{\mathrm{HS}} - \frac{1}{d^2}. \end{aligned}$$

We label the columns of $u = \left(\mu_{i,j}\right)_{0 \leq i,j < d}$ as $x_0, \dots, x_{d-1}$ to compute the scalar product

$$\begin{aligned} (q_i \,|\, p_j)_{\mathrm{HS}} &= \tau\left(q_i p_j\right) = \tau\left(q_i u q_j u^*\right) = \frac{1}{d}\sum_{k=0}^{d-1} \left(q_i u q_j u^* \, x_k \,|\, x_k\right) \\ &= \frac{1}{d}\sum_{k=0}^{d-1} \left(q_i u q_j \, z_k \,|\, x_k\right) = \frac{1}{d}\left(q_i \, x_j \,|\, x_j\right) = \frac{1}{d}\left|\mu_{i,j}\right|^2. \end{aligned}$$

Combining the equations above yields the following equivalence.

$$\mathcal{D}_d \perp_q u\mathcal{D}_d u^* \quad \Leftrightarrow \quad \left|\mu_{i,j}\right|^2 = \frac{1}{d} \text{ for all } 0 \leq i,j < d$$

Hence the masas $\mathcal{D}_d$ and $\mathcal{M}_{[u]}$ are quasi-orthogonal if and only if u is a unitary Hadamard matrix. □

Remark 2.2.3. Given two masas $\mathcal{M}_{[u]}$ and $\mathcal{M}_{[v]}$ in $M_d(\mathbb{C})$, we can switch to the masas $\mathcal{D}_d$ and $\mathcal{M}_{[u^*v]}$ by the unitary conjugation $u^* \cdot u$. Of course unitary conjugations preserve the Hilbert-Schmidt scalar product and hence quasi-orthogonality. We can therefore always presume that one of two given masas is diagonal. In this sense, instance (b) above is the universal example of two quasi-orthogonal masas.

Unbiased bases and unitaries

As we will see in the sequel, quasi-orthogonal masas are closely linked to the so-called *unbiased bases* which are, as explained in the previous section, of some importance in physics.

Definition 2.2.4. *A pair* $\mathfrak{a} = (x_0, \ldots, x_{d-1})$ *and* $\mathfrak{b} = (y_0, \ldots, y_{d-1})$ *of orthonormal bases of the Hilbert space* $\mathbb{C}^d$ *is called* unbiased *if the equation*

$$|(x_i \,|\, y_j)| = \frac{1}{\sqrt{d}}$$

holds for all $0 \leq i, j < d$. *We say a pair of unitary matrices* $u, v \in \mathcal{U}_d$ *is unbiased if the pair of bases given by their columns is unbiased.*

The unbiasedness condition for bases first occured in a paper published by Julian Schwinger in 1960, concerning *unitary operator bases* ([91]). However, the term "unbiased" was not coined by Schwinger. As we have already mentioned in Section 2.1, this expression was introduced (to our best knowledge) in an article on *optimal state determination*, published in 1989 by Wootters and Fields ([114]).

Remark. A priori, one could of course define unbiasedness of unitaries with respect to their *rows* as well. The reason why we have chosen a definition based on the columns is that we aim at linking the unbiasedness of unitaries to the quasi-orthogonality of the associated masas. By our choice to notate any masa in $M_d(\mathbb{C})$ in the form $u\mathcal{D}_d u^*$ (and not $u^*\mathcal{D}_d u$), the associated basis of eigenvectors corresponds to the *columns* of the unitary matrix u.

It is common to say "the orthonormal bases $\mathfrak{a}$ and $\mathfrak{b}$ are unbiased" or "$\mathfrak{a}$ is unbiased w.r.t. $\mathfrak{b}$" instead of using the strictly correct formulation "the *pair* of bases $\{\mathfrak{a}, \mathfrak{b}\}$ is unbiased"; the same applies for unitary matrices. Moreover, speaking about unbiased bases, we always presume that the considered bases are *orthonormal*.

Examples 2.2.5. (a) The orthonormal basis $\mathfrak{f} = (f_0, \ldots, f_{d-1})$ given by the columns of the unitary Discrete Fourier matrix F_d (see Definition 1.3.2),

$$f_0 = \frac{1}{\sqrt{d}} \begin{pmatrix} 1 \\ 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}, f_1 = \frac{1}{\sqrt{d}} \begin{pmatrix} 1 \\ \zeta_d \\ \zeta_d^2 \\ \vdots \\ \zeta_d^{(d-1)} \end{pmatrix}, \ldots, f_{d-1} = \frac{1}{\sqrt{d}} \begin{pmatrix} 1 \\ \zeta_d^{d-1} \\ \zeta_d^{2(d-1)} \\ \vdots \\ \zeta_d^{(d-1)^2} \end{pmatrix},$$

is called the *Fourier basis* of the Hilbert space $\mathbb{C}^d$ (cp. [113, p. 3]). The Fourier basis is obviously unbiased w.r.t. the standard basis $\mathfrak{e}$. In other words, the unitary matrices I_d and $\mathtt{F}_d$ are unbiased.

(b) More generally, let $h \in \mathcal{U}_d$ denote any unitary Hadamard matrix. Then obviously h and I_d, i.e. the standard orthonormal basis $\mathfrak{e}$ and the columns of h, are unbiased.

Analogously to Example 2.2.2 (b), instance (b) directly above is universal in the sense that, given two unbiased bases, one of them can always be considered as the standard orthonormal basis $\mathfrak{e}$ by the next proposition, whose proof is straightforward.

Proposition 2.2.6. *(a) Let $u, v, w \in \mathcal{U}_d$ be unitary matrices. Then u and v are unbiased if and only if the same holds for the products wu and wv. Put differently, the orthonormal bases $\mathfrak{a} = (x_0, \ldots, x_{d-1})$ and $\mathfrak{b} = (y_0, \ldots, y_{d-1})$, given by the columns of u and v, are unbiased if and only if $w\mathfrak{a} = (w\,x_0, \ldots, w\,x_{d-1})$ and $w\mathfrak{b} = (w\,y_0, \ldots, w\,y_{d-1})$ are unbiased as well.*

(b) A pair of unitary matrices $u, v \in \mathcal{U}_d$ is unbiased if and only if the unit matrix I_d and u^*v are unbiased. The latter holds precisely if u^*v is a unitary Hadamard matrix.

Remark. The order of the products in part (a) of Proposition 2.2.6 is important. In general, unbiasedness of unitary matrices $u, v \in \mathcal{U}_d$ does *not* imply that uw and vw are unbiased for any unitary $w \in \mathcal{U}_d$. To see this, let $a \in \mathcal{D}_d$ be the diagonalisation of u^*v and w the diagonalising unitary, that is $u^*v = waw^*$. This implies the equalities

$$w^* \left(u^*v\right) w = (uw)^* \left(vw\right) = a \in \mathcal{D}_d.$$

A diagonal matrix being more or less the contrary of a Hadamard matrix, part (b) of the previous proposition asserts that uw and vw are not unbiased.

However, if the matrix w in the remark above is a *monomial* unitary matrix, that is $w \in \mathcal{W}_d$, unbiasedness of u and v does well imply the same for uw and vw. This reflects the obvious fact that changing the order of basis elements or multiplying vectors by elements of the unit circle does not influence whether two bases $\mathfrak{a}$ and $\mathfrak{b}$ are unbiased. We thus make the following

Observation 2.2.7. Let $\mathfrak{a}, \mathfrak{a}', \mathfrak{b}, \mathfrak{b}'$ denote orthonormal bases of the Hilbert space $\mathbb{C}^d$ and suppose $\mathfrak{a} \sim \mathfrak{a}'$, $\mathfrak{b} \sim \mathfrak{b}'$ in the sense of Definition 1.2.7. Then $\mathfrak{a}$ and $\mathfrak{b}$ are unbiased if and only if $\mathfrak{a}'$ and $\mathfrak{b}'$ are unbiased. Likewise, having two pairs of equivalent unitary matrices $u \sim u'$ and $v \sim v'$ $(u, u', v, v' \in \mathcal{U}_d)$, the pair $\{u, v\}$ is unbiased exactly if $\{u', v'\}$ is unbiased. It therefore makes sense to say that the *equivalence classes* (according to Definition 1.2.7) $[\mathfrak{a}]$ and $[\mathfrak{b}]$, or $[u]$ and $[v]$ respectively, are unbiased.

Let us recapitulate the precise connection between unbiased bases, unbiased unitaries, and quasi-orthogonal masas, which is essential for the present work.

Proposition 2.2.8. *Given two unitary matrices $u, v \in \mathcal{U}_d$, let $\mathfrak{a}$ and $\mathfrak{b}$ be the orthonormal bases given by their columns. The following statements are equivalent.*

(i) The masas $\mathcal{M}_{[u]}$ and $\mathcal{M}_{[v]}$ are quasi-orthogonal.

(ii) The (classes of the) unitaries u and v are unbiased.

(iii) The (classes of the) bases $\mathfrak{a}$ and $\mathfrak{b}$ are unbiased.

Proof. Assertions (ii) and (iii) are equivalent by definition of unbiasedness. Equivalence $(i) \Leftrightarrow (ii)$ immediately follows from observations we have made before. First of all, $\mathcal{M}_{[u]}$ and $\mathcal{M}_{[v]}$ are quasi-orthogonal if and only if $\mathcal{M}_{[u^*v]}$ is quasi-orthogonal to $\mathcal{D}_d$, cf. Remark 2.2.3. Next, Example 2.2.2 (b) tells us that $\mathcal{M}_{[u^*v]}$ and $\mathcal{D}_d$ are quasi-orthogonal precisely if u^*v is a unitary Hadamard matrix, and this again holds true if and only if u and v are unbiased according to Proposition 2.2.6 (b). □

Example 2.2.9. The adjoint of the Discrete Fourier matrix F_d diagonalises the cyclic permutation matrix X_d. For each $0 \leq i_0 < d$, one computes

$$\mathrm{F}_d^*\mathrm{X}_d\mathrm{F}_d\, z_{i_0} = \frac{1}{\sqrt{d}}\mathrm{F}_d^*\mathrm{X}_d \begin{pmatrix} 1 \\ \zeta_d^{i_0} \\ \zeta_d^{2i_0} \\ \vdots \\ \zeta_d^{(d-1)i_0} \end{pmatrix} = \frac{1}{\sqrt{d}}\mathrm{F}_d^* \begin{pmatrix} \zeta_d^{(d-1)i_0} \\ 1 \\ \zeta_d^{i_0} \\ \vdots \\ \zeta_d^{(d-2)i_0} \end{pmatrix}$$

$$= \frac{1}{\sqrt{d}}\bar{\zeta}_d^{i_0}\mathrm{F}_d^* \begin{pmatrix} 1 \\ \zeta_d^{i_0} \\ \zeta_d^{2i_0} \\ \vdots \\ \zeta_d^{(d-1)i_0} \end{pmatrix} = \bar{\zeta}_d^{i_0}\, z_{i_0}.$$

This is equivalent to the matrix identity $\mathrm{F}_d^*\mathrm{X}_d\mathrm{F}_d = \mathrm{Z}_d^*$, that is $\mathrm{X}_d = \mathrm{F}_d\mathrm{Z}_d^*\mathrm{F}_d^*$. It follows that the masa $\mathcal{M} = \mathcal{A}^*(\mathrm{X}_d)$, defined in Example 2.2.2 (a), is associated with the (unitary) Discrete Fourier matrix, for we have the equalities

$$\mathcal{M} = \mathcal{A}^*\left(\mathrm{F}_d\mathrm{Z}_d\mathrm{F}_d^*\right) = \mathrm{F}_d\mathcal{A}^*\left(\mathrm{Z}_d\right)\mathrm{F}_d^* = \mathrm{F}_d\mathcal{D}_d\mathrm{F}_d^*,$$

i.e. $\mathcal{M} = \mathcal{M}_{[\mathrm{F}_d]} = \mathcal{M}_{[\mathfrak{f}]}$. (Recall that according to Example 1.4.2, Z_d generates the diagonal masa $\mathcal{D}_d$.) The unitary matrices I_d and F_d being unbiased (cf. Examples 2.2.5), Proposition 2.2.8 proves, once more, the quasi-orthogonality of the masas $\mathcal{D}_d$ and $\mathcal{M}$.

Criteria for quasi-orthogonality

We begin with a criterion on the level of bases, providing a sufficient condition of unbiasedness which is slightly weaker than the one given in Definition 2.2.4.

Lemma 2.2.10. *The statements below are equivalent for orthonormal bases $\mathfrak{a} = (x_0, \dots, x_{d-1})$ and $\mathfrak{b} = (y_0, \dots, y_{d-1})$ of the Hilbert space $\mathbb{C}^d$.*

(i) The bases $\mathfrak{a}$ and $\mathfrak{b}$ are unbiased.

(ii) The inequality $\sum_{i=0}^{d-1} |(x_i \,|\, y_{\sigma(i)})| \leq \sqrt{d}$ holds for all permutations $\sigma \in S_d$.

Proof. The implication $(i) \Rightarrow (ii)$ is trivial. We give an indirect argument for the converse implication.

Consider bases $\mathfrak{a}$ and $\mathfrak{b}$ like above which are *not* unbiased. Then there are indices $0 \leq i_0, j_0 < d$ such that the modulus of the scalar product $(x_{i_0} \,|\, y_{j_0})$ does not equal $\sqrt{1/d}$. By the Parseval identity (applied to the element x_{i_0} above), it is straightforward that there are in particular scalar products $(x_i \,|\, y_j)$ whose modulus is *greater* than $\sqrt{1/d}$.

For clarity, we write the moduli of the scalar products $(x_i \,|\, y_j)$ in a matrix

$$M = \big(|(x_i \,|\, y_j)|\big)_{0 \leq i,j < d} \,.$$

As a first step, we rearrange the elements of the basis $\mathfrak{a}$ in such a way that only the rows $0, \dots, k-1$ of M contain elements of modulus greater than $\sqrt{1/d}$. By assumption, there is at least one such row, so we have $0 \leq k < d$. The possibly remaining rows of M contain—again due to Parseval's identity—only elements equal to $\sqrt{1/d}$.

Secondly, we rearrange the columns of M so that only the first l of them contain elements of modulus greater than $\sqrt{1/d}$. As for the rows, we know that there is at least one such column, and that the remaining columns contain only elements equal to $\sqrt{1/d}$.

Now the submatrix $M' = (|(x_i \,|\, y_j)|)_{0 \leq i < k, 0 \leq j < l}$ of M contains at least one element greater than $\sqrt{1/d}$ in each row and each column. For the sequel, suppose $k \leq l$ (the case $k > l$ is shown completely analogously, exchanging the roles of columns and rows). Then by construction of M', there are pairwise different indices $0 \leq j_0, \dots, j_{k-1} < l$ such that we have

$$\big|(x_i \,|\, y_{j_i})\big| > \sqrt{1/d}$$

for all $0 \leq i < k$.

For the remaining $d-k$ rows, we can choose indices $j_k, \dots, j_{d-1}$ so that the mapping $\sigma : i \mapsto j_i$ is a permutation of the set $\{0, \dots, d-1\}$. We then end up with the inequality

$$\sum_{i=0}^{d-1} |(x_i \,|\, y_{\sigma(i)})| = \sum_{i=0}^{k-1} \underbrace{|(x_i \,|\, y_{\sigma(i)})|}_{> \sqrt{1/d}} + (d-k)\sqrt{\frac{1}{d}} > \sqrt{d},$$

which contradicts condition (ii). □

The previous lemma will prove useful in Section 2.3. We now switch to the masa picture again. Let $\mathcal{M}, \mathcal{N} \subset M_d(\mathbb{C})$ be two quasi-orthogonal masas and $p \in \mathcal{M}$, $q \in \mathcal{N}$ projections. In the proof of Proposition 2.2.8, we have calculated

$$(q \,|\, p)_{\mathrm{HS}} = \frac{1}{d^2}.$$

As the normalised trace of any projection equals $1/d$, this identity can equivalently be expressed in the form $\tau(qp) = \tau(q)\tau(p)$. This trace-formula can be generalised to another important criterion for the quasi-orthogonality of masas.

Proposition 2.2.11. *Two masas $\mathcal{M}, \mathcal{N} \subset M_d(\mathbb{C})$ are quasi-orthogonal if and only if all pairs $a \in \mathcal{M}$, $b \in \mathcal{N}$ fulfil the equation*

$$\tau(ab) = \tau(a)\tau(b).$$

Proof. The masas $\mathcal{M}$ and $\mathcal{N}$ are quasi-orthogonal if and only if the equation

$$(a - (a \,|\, \mathrm{I}_d)\, \mathrm{I}_d \,|\, b^* - (b^* \,|\, \mathrm{I}_d)\, \mathrm{I}_d) = 0$$

holds for all elements $a \in \mathcal{M}$, $b \in \mathcal{N}$ (we omit the subscript $_{HS}$ for convenience here). This identity can be rewritten as follows.

$$\begin{aligned} 0 &= (a \,|\, b^*) - (a \,|\, \mathrm{I}_d)\, (\mathrm{I}_d \,|\, b^*) - \overline{(b^* \,|\, \mathrm{I}_d)}\, (a \,|\, \mathrm{I}_d) + (a \,|\, \mathrm{I}_d)\, \overline{(b^* \,|\, \mathrm{I}_d)}\, (\mathrm{I}_d \,|\, \mathrm{I}_d) \\ &= \tau(ab) - \tau(a)\tau(b) - \overline{\tau(b^*)}\tau(a) + \tau(a)\overline{\tau(b^*)} \\ &= \tau(ab) - \tau(a)\tau(b) \end{aligned}$$

□

For any subspace $\mathcal{K}$ of $M_d(\mathbb{C})$, let $\mathcal{P}_{\mathcal{K}} : M_d(\mathbb{C}) \to M_d(\mathbb{C})$ be the ortho-projection onto that space. If $(b_0, \ldots, b_n)$ is a Hilbert-Schmidt orthonormal basis of $\mathcal{K}$, the projection $\mathcal{P}_{\mathcal{K}}$ can be expressed as

$$\mathcal{P}_{\mathcal{K}}(a) = \sum_{i=0}^{n} (a \,|\, b_i)_{\mathrm{HS}}\, b_i$$

for all $a \in M_d(\mathbb{C})$. In terms of such projections, we can formulate another criterion for the quasi-orthogonality of two masas $\mathcal{M}, \mathcal{N} \subset M_d(\mathbb{C})$:

$$\mathcal{M} \perp_q \mathcal{N} \quad \Leftrightarrow \quad \mathcal{P}_{\mathcal{M}} \circ \mathcal{P}_{\mathcal{N}} = \mathcal{P}_{\mathcal{N}} \circ \mathcal{P}_{\mathcal{M}} = \mathcal{P}_{\mathbb{C} \cdot \mathrm{I}_d}$$

In the form above, this criterion is nothing but a reformulation of what we have already seen. Projections onto masas can, however, be expressed in quite a different form.

Definition/Proposition 2.2.12. *Let $\mathcal{M} \subset M_d(\mathbb{C})$ be a masa. For any Hilbert-Schmidt orthonormal basis $(b_0, \dots, b_{d-1})$ of $\mathcal{M}$, the projection $\mathcal{P}_{\mathcal{M}} : M_d(\mathbb{C}) \to M_d(\mathbb{C})$ onto $\mathcal{M}$ is given by*

$$\mathcal{P}_{\mathcal{M}}(a) = \mathcal{E}_{\mathcal{M}}(a) = \frac{1}{d} \sum_{i=0}^{d-1} b_i a b_i^*$$

for all $a \in M_d(\mathbb{C})$. The so-called trace-preserving conditional expectation *$\mathcal{E}_{\mathcal{M}}$ is hence independent of the chosen orthonormal basis $(b_0, \dots, b_{d-1})$ of $\mathcal{M}$. Moreover, $\mathcal{E}_{\mathcal{M}}$ does in fact preserve the trace, that is we have $\tau(\mathcal{E}_{\mathcal{M}}(a)) = \tau(a)$ for all $a \in M_d(\mathbb{C})$. If $\mathcal{N} \subset M_d(\mathbb{C})$ is another masa, then $\mathcal{M}$ and $\mathcal{N}$ are quasi-orthogonal if and only if*

$$\mathcal{E}_{\mathcal{M}} \circ \mathcal{E}_{\mathcal{N}} = \mathcal{E}_{\mathcal{N}} \circ \mathcal{E}_{\mathcal{M}} = \mathcal{E}_{\mathbb{C}\cdot 1_d},$$

in which case we call the conditional expectations $\mathcal{E}_{\mathcal{M}}$ and $\mathcal{E}_{\mathcal{N}}$ quasi-orthogonal as well.

Proof. Let $p_0, \dots, p_{d-1}$ be the minimal projections generating $\mathcal{M}$. The rescaled elements $p'_i = \sqrt{d}\, p_i$ $(0 \leq i < d)$ form a Hilbert-Schmidt orthonormal basis of $\mathcal{M}$, and consequently the projection $\mathcal{P}_{\mathcal{M}}$ is given by

$$\mathcal{P}_{\mathcal{M}}(a) = \sum_{i=0}^{d-1} \left(a \mid p'_i\right)_{\mathrm{HS}} p'_i$$

for all matrices $a \in M_d(\mathbb{C})$.

Our first goal is to prove the identity

$$\mathcal{P}_{\mathcal{M}}(a) = \sum_{i=0}^{d-1} p'_i a p'_i. \tag{2.2}$$

The sum on the right-hand side certainly belongs to $\mathcal{M}$, because it obviously commutes with all generators $p_0, \dots, p_{d-1}$ and $\mathcal{M}$ is a masa. Since the elements $p'_0, \dots, p'_{d-1}$ are pairwise orthogonal (i.e. $p'_i p'_{i_0} = 0$ for all $i \neq i_0, 0 \leq i, i_0 < d$), one computes

$$\left(\sum_{i=0}^{d-1} p'_i a p'_i \,\middle|\, p'_{i_0} \right)_{\mathrm{HS}} = \left(p'_{i_0} a p'_{i_0} \mid p'_{i_0}\right)_{\mathrm{HS}} = \tau(a p'_{i_0})$$

and

$$\left(\mathcal{P}_{\mathcal{M}}(a) \mid p'_{i_0}\right)_{\mathrm{HS}} = \left(a \mid p'_{i_0}\right)_{\mathrm{HS}} = \tau(a p'_{i_0}).$$

Equation (2.2) above now follows from a comparison of coefficients with respect to the basis $p'_0, \dots, p'_{d-1}$.

If $(b_0, \dots, b_{d-1})$ is another Hilbert-Schmidt orthonormal basis of $\mathcal{M}$, there are coefficients $\lambda_{i,k} \in \mathbb{C}$ for all $0 \leq i, k < d$ satisfying the identities

$$b_i = \sum_{k=0}^{d-1} \lambda_{i,k} p'_k.$$

We use the fact that $(\lambda_{i,k})_{0 \leq i,k < d}$ is a unitary matrix (it performs a change of orthonormal bases) to compute

$$\left(\sum_{i=0}^{d-1} b_i a b_i^* \,\middle|\, p'_{i_0} \right)_{\text{HS}} = \sum_{i=0}^{d-1} \sum_{k,l=0}^{d-1} \lambda_{i,k} \bar{\lambda}_{i,l} \left(p'_k a p'_l \mid p'_{i_0} \right)_{\text{HS}} = \underbrace{\sum_{i=0}^{d-1} \lambda_{i,i_0} \bar{\lambda}_{i,i_0}}_{=1} \tau(a p'_{i_0}) = \tau(a p'_{i_0}).$$

For the second step, notice that $(p'_k a p'_l | p'_{i_0})_{\text{HS}} = \tau(p'_k a p'_l p'_{i_0}) = \tau(a p'_l p'_{i_0} p'_k)$ is zero unless $k = l = i_0$. As before, a comparison of coefficients asserts

$$\sum_{i=0}^{d-1} b_i a b_i^* = \sum_{i=0}^{d-1} p'_i a p'_i.$$

It is evident that $\mathcal{E}_{\mathcal{M}}$ preserves the trace, and obviously the criterion for quasi-orthogonality stated in our proposition is just a reformulation of the condition presented directly before. □

Recall that there is a conditional expectation $\mathcal{E}_{\mathbb{C} \cdot \mathrm{I}_d}$ of the one-dimensional subspace $\mathbb{C} \cdot \mathrm{I}_d$. For future reference, we record this as a

Fact 2.2.13. For any Hilbert-Schmidt orthonormal basis $(b_0, \dots, b_{d^2-1})$ of the matrix algebra $M_d(\mathbb{C})$, the trace-preserving conditional expectation of the line $\mathbb{C} \cdot \mathrm{I}_d$ is given by

$$\mathcal{E}_{\mathbb{C} \cdot \mathrm{I}_d}(a) = \tau(a) \mathrm{I}_d = \frac{1}{d^2} \sum_{i=0}^{d^2-1} b_i a b_i^*.$$

The verification of this statement is similar to that of Proposition 2.2.12, if one replaces the projections there (generating the masa $\mathcal{M}$) by the standard basis of matrix units of $M_d(\mathbb{C})$ (see page 6). It can be found in many introductory textbooks on matrix algebra or C*-algebras, see for example [15]. Be aware, however, that many authors state the formula above in terms of the *non*-normalised trace. As a remark, a version of it also occurs in the aforementioned paper [91] by Schwinger.

In the next theorem, we collect the equivalent conditions for quasi-orthogonality of two masas established in this section, and add a few more.

Theorem 2.2.14 (Criteria for quasi-orthogonality)**.** *Consider masas $\mathcal{M}, \mathcal{N}$ in the matrix algebra $M_d(\mathbb{C})$, with associated unitaries $u_0, u_1 \in \mathcal{U}_d$ and orthonormal bases $\mathfrak{a} = (x_0, \dots, x_{d-1})$ and $\mathfrak{b} = (y_0, \dots, y_{d-1})$ of the Hilbert space $\mathbb{C}^d$ respectively, so that we have*

$$\mathcal{M} = \mathcal{M}_{[u_0]} = \mathcal{M}_{[\mathfrak{a}]}, \quad \mathcal{N} = \mathcal{M}_{[u_1]} = \mathcal{M}_{[\mathfrak{b}]}.$$

The following statements are equivalent.

(i) The masas $\mathcal{M}$ and $\mathcal{N}$ are quasi-orthogonal.

(ii) The classes of orthonormal bases $[\mathfrak{a}]$ and $[\mathfrak{b}]$ are unbiased.

(iii) The inequality $\sum_{i=0}^{d-1} |(x_i \mid y_{\sigma(i)})| \leq \sqrt{d}$ holds for all permutations $\sigma \in S_d$.

(iv) The classes of unitary matrices $[u_0]$ and $[u_1]$ are unbiased.

(v) The product $u_0^* u_1$ is a unitary Hadamard matrix.

(vi) All pairs $a \in \mathcal{M}$, $b \in \mathcal{N}$ obey the equation $\tau(ab) = \tau(a)\tau(b)$.

(vii) If $p \in \mathcal{M}$ and $q \in \mathcal{N}$ are minimal projections, then their Hilbert-Schmidt scalar product is given by $(p \mid q)_{HS} = 1/d^2$.

(viii) If at least one out of two elements $a \in \mathcal{M}$, $b \in \mathcal{N}$ is trace-free, then the Hilbert-Schmidt scalar product $(a \mid b)_{HS}$ equals zero. Especially, any two trace-free unitaries $v \in \mathcal{M}$ and $w \in \mathcal{N}$ are Hilbert-Schmidt orthogonal.

(ix) Let $(v_0, \dots, v_{d-1})$ and $(w_0, \dots, w_{d-1})$ be Hilbert-Schmidt orthonormal bases of $\mathcal{M}$ and $\mathcal{N}$ respectively, where $v_0 = w_0 = \mathrm{I}_d$. Then the set of products

$$\{v_i w_j \mid 0 \leq i, j < d\}$$

is a Hilbert-Schmidt orthonormal basis of $M_d(\mathbb{C})$.

(x) The conditional expectations $\mathcal{E}_{\mathcal{M}}$ and $\mathcal{E}_{\mathcal{N}}$ are quasi-orthogonal, that is they fulfil the identities

$$\mathcal{E}_{\mathcal{M}} \circ \mathcal{E}_{\mathcal{N}} = \mathcal{E}_{\mathcal{N}} \circ \mathcal{E}_{\mathcal{M}} = \mathcal{E}_{\mathbb{C} \cdot \mathrm{I}_d}.$$

Proof. The following scheme displays the equivalences we have already proved.

$$\begin{tikzcd}
(vi) \arrow[r, Leftrightarrow, "2.2.11"] & (i) \arrow[r, Leftrightarrow, "2.2.12"] \arrow[d, Leftrightarrow, "2.2.8"] & (x) & \\
(iii) \arrow[r, Leftrightarrow, "2.2.10"] & (ii) \arrow[r, Leftrightarrow, "2.2.8"] & (iv) \arrow[r, Leftrightarrow, "{2.2.6,(2)}"] & (v)
\end{tikzcd}$$

Assertions (vii) and $(viii)$ are special cases of (vi), and assertion (ix) follows immediately from $(viii)$ and by dimension ($\dim M_d(\mathbb{C}) = d^2$). The only implication we need to show is

$(\boldsymbol{ix}) \Rightarrow (\boldsymbol{i})$. It is clear that the family of unitary matrices $(w_0^*, w_1^*, \ldots, w_{d-1}^*)$ is also a Hilbert-Schmidt orthonormal basis for the masa $\mathcal{N}$. We have the identities

$$\left(v_i \,\middle|\, w_j^*\right) = \tau(v_i w_j) = \left(v_i w_j \,\middle|\, \mathrm{I}_d\right) = 0$$

for all $1 \leq i, j < d$, because the orthonormal basis $\{v_i w_j \mid 0 \leq i, j < d\}$ contains the unit matrix I_d. Accordingly, the masas $\mathcal{M}$ and $\mathcal{N}$ are quasi-orthogonal. □

Condition (vi) in the previous theorem yields the following corollary, which will prove very useful in the following section.

Corollary 2.2.15. *Let $\mathcal{M} \subset M_d(\mathbb{C})$ be a masa which is quasi-orthogonal to the diagonal masa $\mathcal{D}_d$, and consider an element $a \in \mathcal{M}$. Then all diagonal entries of the matrix a are* identical.

Proof. For all $0 \leq i < d$, let $\lambda_i \in \mathbb{C}$ be the diagonal element of the matrix a at position (i, i), and q_i the minimal diagonal projection as defined before (e.g. in the proof of Proposition 2.2.8). From condition (vi) of the theorem above, we then deduce for all $0 \leq i < d$:

$$\tau(aq_i) = \tau(a)\tau(q_i) \quad \Rightarrow \quad \frac{1}{d}\lambda_i = \frac{1}{d}\tau(a) \quad \Rightarrow \quad \lambda_i = \tau(a)$$

□

As a consequence of item (ix) in Theorem 2.2.14, every quasi-orthogonal pair of masas $\mathcal{M}, \mathcal{N} \subset M_d(\mathbb{C})$ algebraically generates the whole matrix algebra.

$$\mathcal{M} \perp_q \mathcal{N} \quad \Rightarrow \quad \mathcal{A}\left(\mathcal{M} \cup \mathcal{N}\right) = M_d(\mathbb{C}) \tag{2.3}$$

In the case of the standard pair of quasi-orthogonal masas, introduced in Example 2.2.2 (a), the induced basis according to item (ix) is particularly nice.

Example 2.2.16. Once more, consider the quasi-orthogonal masas $\mathcal{M}_{[\mathrm{F}_d]} = \mathcal{A}^*\left(\mathrm{X}_d\right)$ and $\mathcal{D}_d = \mathcal{A}^*\left(\mathrm{Z}_d\right)$ (see Example 2.2.2 (a) and 2.2.9). According to item (ix) of Theorem 2.2.14, the family of products

$$\left\{\mathrm{X}_d^i \mathrm{Z}_d^j \,\middle|\, 0 \leq i, j < d\right\}$$

is a Hilbert-Schmidt orthonormal basis for the matrix algebra $M_d(\mathbb{C})$. This is a prominent example of a so-called *nice unitary error basis*. We will thoroughly introduce such bases in Section 4.1.

Excursion: The many names of the shift and clock matrices

The literature in mathematics and physics abounds in various names for the shift matrix X_d and the clock matrix Z_d (in dimensions $d > 2$). To all appearances, they first turned up in several letters by J. J. Sylvester ([100, 101]) in the 1880s, for the purpose of a generalisation of the quaternions—which he described by the Pauli matrices—to higher-dimensional analogues such as "nonions" etc.

More than forty years later, in 1928, Hermann C. H. Weyl published a famous work connecting group theory and quantum mechanical dynamics ([107, 108]), where the shift and clock matrices play an important part, explaining the name *Weyl matrices* (cp. [43]) which we shall constantly use in the present work.

Since X_d and Z_d can be used as generators for the finite Heisenberg(-Weyl) group (see Example 4.1.3 (b)), the name *Heisenberg-Weyl matrices* seems even a little more common.

Last but not least, J. Schwinger made extensive use of the clock and shift matrices in an exposition on unitary operator bases ([91]) in 1960. That is probably why some people name them *(Weyl-)Schwinger matrices* (cp. [27,79]).

As explained before, the matrices X_d and Z_d are just the Pauli matrices if d equals two. For this reason, many physicists refer to them as *generalised Pauli matrices* (cp. [3,35,38]). Yet this name should be used with care, for there are different generalisations of the Pauli matrices in the literature. For instance, the generalised Gell-Mann matrices also generalise the Pauli matrices, and are of some interest in physics (see e.g. [14]).

It goes without saying that one might replace the term *matrix* by *operator* in all of the names mentioned.

2.3 Measures of quasi-orthogonality

In this section, we introduce three natural metrics on the set of masas in a fixed dimension. We shall see that two masas are maximally distant w.r.t. each of these metrics if they are quasi-orthogonal. For two of the metrics, maximal distance of two masas conversely implicates quasi-orthogonality. For this reason, these metrics can be understood as "measures of quasi-orthogonality" (the term "measure" is thus not used in its strict mathematical sense in this context).

Recall that for all $d \in \mathbb{N}$, $\mathfrak{M}_d$ denotes the set of masas in $M_d(\mathbb{C})$, and $\mathcal{W}_d$ the subgroup of monomial unitary matrices in the unitary group $\mathcal{U}_d$. As we have noticed in Proposition 1.2.8, the map $\mathcal{U}_d/\mathcal{W}_d \to \mathfrak{M}_d$, $[u] \mapsto \mathcal{M}_{[u]} = u\mathcal{D}_d u^*$, is a bijection between the quotient $\mathcal{U}_d/\mathcal{W}_d$ and the set of masas $\mathfrak{M}_d$.

The quotient $\mathcal{U}_d/\mathcal{W}_d$ does not inherit a group structure from $\mathcal{U}_d$ for all $d \geq 2$, because the subgroup $\mathcal{W}_d$ is not normal for all $d \neq 1$ according to Proposition 1.2.4. While the algebraic structure of the masa set $\mathfrak{M}_d$ is therefore rather poor, several observations can be made concerning its geometrical structure.

First of all, $\mathfrak{M}_d$ is a metric space. Since the unitary group $\mathcal{U}_d$ is a metric group, the quotient $\mathcal{U}_d/\mathcal{W}_d$ is equipped with the canonical quotient metric. Now $\mathcal{U}_d$ can be endowed with two different non-trivial metrics lying at hand, namely one induced by the operator norm and one by the Hilbert-Schmidt norm. This gives us two inherited metrics on $\mathfrak{M}_d$ that we call *maximum metric* and *mean metric,* labeled as d_{max} and d_{mean} respectively. We shall see in the sequel that these metrics do not coincide if the dimension d is greater than two.

Another metric is based on the conditional expectations defined for masas in Definition/Proposition 2.2.12. Recall that we have defined the conditional expectation $\mathcal{E}_{\mathcal{M}}$ for a masa $\mathcal{M}$ as the projection onto the linear subspace $\mathcal{M} \subset M_d(\mathbb{C})$. More precisely, $\mathcal{E}_{\mathcal{M}}$ is an element—an ortho-projection—of the *-algebra $\mathcal{L}(M_d(\mathbb{C}))$ of linear operators on the *Hilbert spaceM*$_d(\mathbb{C})$, where the latter is endowed with the Hilbert-Schmidt scalar product. We equip the operator algebra $\mathcal{L}(M_d(\mathbb{C})) \cong M_{d^2}(\mathbb{C})$ with the Hilbert-Schmidt scalar product as well. To avoid confusion, we label the latter as $(\!(\cdot\,|\,\cdot)\!)_{\mathrm{HS}}$, and the respective norm as $|\!|\!|\cdot|\!|\!|_{\mathrm{HS}}$. The restriction of this norm to the set of conditional expectations of masas in $M_d(\mathbb{C})$ induces a third metric on $\mathfrak{M}_d$, which we name *expectation metric,* labeled as d_{exp}. Here come the precise definitions.

Definition/Proposition 2.3.1. *Fix a dimension $d \in \mathbb{N}$, and let $u, v \in \mathcal{U}_d$ be unitary matrices. Further let $\mathfrak{a} = (x_0, \ldots, x_{d-1})$ and $\mathfrak{b} = (y_0, \ldots, y_{d-1})$ denote the orthonormal bases of the Hilbert space $\mathbb{C}^d$ given by the columns of u and v respectively. We assign the following real, positive quantities to the pair of masas $\{\mathcal{M}_{[u]}, \mathcal{M}_{[v]}\}$ in $\mathfrak{M}_d$.*

$$d_{exp}\left(\mathcal{M}_{[u]}, \mathcal{M}_{[v]}\right) = |\!|\!|\mathcal{E}_{\mathcal{M}_{[u]}} - \mathcal{E}_{\mathcal{M}_{[v]}}|\!|\!|_{HS} = \sqrt{\frac{2}{d^2}\sum_{i,j=0}^{d-1}\left(\frac{1}{d} - |(x_i\,|\,y_j)|^4\right)}$$

$$= \sqrt{\frac{2(d-1)}{d^2} - \frac{2}{d^2}\sum_{i,j=0}^{d-1}\left(\frac{1}{d} - |(x_i\,|\,y_j)|^2\right)^2}$$

$$d_{mean}\left(\mathcal{M}_{[u]}, \mathcal{M}_{[v]}\right) = \min_{w \in \mathcal{W}_d} \|u - vw\|_{HS} = \min_{\sigma \in S_d} \sqrt{\frac{2}{d}\sum_{i=0}^{d-1}\left(1 - |(x_i\,|\,y_{\sigma(i)})|\right)}$$

$$d_{max}\left(\mathcal{M}_{[u]}, \mathcal{M}_{[v]}\right) = \min_{w \in \mathcal{W}_d} \|u - vw\| = \min_{\sigma \in S_d} \sqrt{2\max_{0 \le i < d}\left(1 - |(x_i\,|\,y_{\sigma(i)})|\right)}$$

The formulas above define metrics $d_{exp}, d_{mean}, d_{max} : \mathfrak{M}_d \to \mathbb{R}_0^+$.

Proof. We first show that the maps $d_{max}, d_{mean} : \mathfrak{M}_d \times \mathfrak{M}_d \to \mathbb{R}_0^+$ do in fact correspond to quotient metrics, as explained directly before the present statement.

To this end, recall that if (G, d) is a (multiplicatively written) metric group containing a subgroup $H \subset G$, then the quotient G/H, that is the set of all left cosets of H in G, is endowed with the canonical quotient metric. Let $[g]$ denote the coset of g in the quotient G/H for all $g \in G$. The quotient metric on G/H is defined by

$$d'\left([g_0], [g_1]\right) = \inf_{h_0, h_1 \in H} d\left(g_0 h_0, g_1 h_1\right)$$

for all elements $g_0, g_1 \in G$.

Endow the unitary group $\mathcal{U}_d$ with the metric induced by the operator norm on $M_d(\mathbb{C})$. Then the quotient metric on $\mathcal{U}_d / \mathcal{W}_d$ is given by

$$d'([u], [v]) = \inf_{w_0, w_1 \in \mathcal{W}_d} \|u w_0 - v w_1\| = \inf_{w_0, w_1 \in \mathcal{W}_d} \|u w_0 w_0^* - v w_1 w_0^*\| = \inf_{w \in \mathcal{W}_d} \|u - v w\|$$

for all $u, v \in \mathcal{U}_d$, where we have used the property of the operator norm that the equality $\|a\| = \|au\|$ holds for all matrices $a \in M_d(\mathbb{C})$, $u \in \mathcal{U}_d$.

The group $\mathcal{W}_d$ of monomial unitaries is readily seen to be a closed (and of course bounded) subset of the finite-dimensional metric space $M_d(\mathbb{C})$, so the Heine-Borel Theorem tells us that $\mathcal{W}_d$ is compact. What is more, the map $\mathcal{W}_d \to \mathbb{R}_0^+$, $w \mapsto \|u - vw\|$, is obviously continuous for fixed unitaries $u, v \in \mathcal{U}_d$, and hence attains its minimum. On that account, we can write $d'([u], [v]) = \min_{w \in \mathcal{W}_d} \|u - vw\|$.

Our next goal is to express this metric in terms of the column vectors of the involved unitary matrices. We assign the orthonormal bases $\mathfrak{a}$ and $\mathfrak{b}$ to the unitaries u, v as in our assertion, and furthermore denote the standard orthonormal basis $\mathfrak{e} = (z_0, \ldots, z_{d-1})$ of the Hilbert space $\mathbb{C}^d$ as always. Recall that the operator norm of an element $a \in M_d(\mathbb{C})$ can be expressed as $\|a\| = \max_{0 \le i < d} \|a z_i\|$ (of course the same applies for all orthonormal bases of $\mathbb{C}^d$). The monotony of the real square function permits to switch from d' to the squared metric d'^2 for the following computations.

$$\begin{aligned} d'^2([u], [v]) &= \min_{w \in \mathcal{W}_d} \|u - vw\|^2 = \min_{\sigma \in S_d} \min_{(\lambda_0, \ldots, \lambda_{d-1}) \in \mathbb{T}^d} \max_{0 \le i < d} \|x_i - \lambda_i y_{\sigma(i)}\|^2 \\ &= \min_{\sigma \in S_d} \min_{(\lambda_0, \ldots, \lambda_{d-1}) \in \mathbb{T}^d} \max_{0 \le i < d} \left(2 - 2\mathrm{Re}\left(\lambda_i (x_i \,|\, y_{\sigma(i)})\right)\right). \end{aligned}$$

It is a matter of basic analysis that the mapping $\lambda_i \mapsto 2 - 2\mathrm{Re}\left(\lambda_i (x_i \,|\, y_{\sigma(i)})\right)$ attains its minimum if and only if the equation

$$\lambda_i = \frac{\overline{(x_i \,|\, y_{\sigma(i)})}}{|(x_i \,|\, y_{\sigma(i)})|}$$

holds for all $0 \leq i < d$. We thus end up with the expression

$$\begin{aligned} d'([u],[v]) &= \min_{\sigma \in S_d} \max_{0 \leq i < d} \sqrt{2 - 2|(x_i \,|\, y_{\sigma(i)})|} \\ &= \min_{\sigma \in S_d} \sqrt{2 \max_{0 \leq i < d} \Big(1 - |(x_i \,|\, y_{\sigma(i)})|\Big)}. \end{aligned}$$

The stated formula for the mean metric d_{mean} is verified similarly, replacing the operator norm by the Hilbert-Schmidt norm. The computations are left to the reader.

Just as d_{max} and d_{mean}, the mapping $d_{exp} : \mathfrak{M}_d \times \mathfrak{M}_d \to \mathbb{R}_0^+$ is a metric by definition, so we only need to verify the proposed expressions. We give a short sketch of the (quite lengthy) computations. Be aware that the Hilbert-Schmidt scalar product and norm defined for the operator algebra $\mathcal{L}(M_d(\mathbb{C})) \cong M_{d^2}(\mathbb{C})$ are defined w.r.t. the *normalised trace* according to our conventions.

Since a conditional expectation $\mathcal{E}_{\mathcal{M}}$ onto a masa $\mathcal{M}$ is an ortho-projection on a d-dimensional subspace of the d^2-dimensional Hilbert space $M_d(\mathbb{C})$, its Hilbert-Schmidt norm is given by $|\!|\!|\mathcal{E}_{\mathcal{M}}|\!|\!|_{\mathrm{HS}} = {}^{d}/_{d^2} = {}^{1}/_{d}$. Denoting the matrix units in $M_d(\mathbb{C})$ by $\mathrm{E}_{i,j}$ as before (see page 6), one calculates

$$\begin{aligned} |\!|\!|\mathcal{E}_{\mathcal{M}_{[u]}} - \mathcal{E}_{\mathcal{M}_{[v]}}|\!|\!|^2_{\mathrm{HS}} &= \frac{2}{d} - 2\mathrm{Re}\,(\!(\mathcal{E}_{\mathcal{M}_{[u]}} \,|\, \mathcal{E}_{\mathcal{M}_{[v]}})\!)_{\mathrm{HS}} \\ &= \frac{2}{d} - \frac{2}{d^2}\mathrm{Re} \sum_{i,j=0}^{d-1} \Big(\mathcal{E}_{\mathcal{M}_{[u]}}(\sqrt{d}\,\mathrm{E}_{i,j}) \,\Big|\, \mathcal{E}_{\mathcal{M}_{[v]}}(\sqrt{d}\,\mathrm{E}_{i,j})\Big)_{\mathrm{HS}} \end{aligned}$$

Now let $p_0, \dots, p_{d-1} \in M_d(\mathbb{C})$ be the minimal projections generating the masa $\mathcal{M}_{[u]}$, ordered such that the range of p_i is $\mathbb{C} \cdot x_i$ for all $0 \leq i < d$, and $q_0, \dots, q_{d-1}$ the respective projections generating $\mathcal{M}_{[v]}$. As a careful calculation reveals, the double sum in the last line above equals $d^2 \sum_{i,j=0}^{d-1} |(p_i \,|\, q_j)|^2$, so that we are left with

$$|\!|\!|\mathcal{E}_{\mathcal{M}_{[u]}} - \mathcal{E}_{\mathcal{M}_{[v]}}|\!|\!|^2_{\mathrm{HS}} = \frac{2}{d} - 2 \sum_{i,j=0}^{d-1} |(p_i \,|\, q_j)|^2.$$

Using the elementary identity $\big(p_i \,\big|\, q_j\big)_{\mathrm{HS}} = {}^{1}/_{d}|(x_i \,|\, y_j)|^2$, we finally come to

$$|\!|\!|\mathcal{E}_{\mathcal{M}_{[u]}} - \mathcal{E}_{\mathcal{M}_{[v]}}|\!|\!|^2_{\mathrm{HS}} = \frac{2}{d} - \frac{2}{d^2} \sum_{i,j=0}^{d-1} |(x_i \,|\, y_j)|^4 = \frac{2}{d^2} \sum_{i,j=0}^{d-1} \left(\frac{1}{d} - |(x_i \,|\, y_j)|^4\right),$$

and thus to the first of the proposed formulas for d_{exp}. The alternative expression is easily verified using the identity $\sum_{i,j=0}^{d-1} |(x_i \,|\, y_j)|^2 = d$. □

Observe that all metrics d_* introduced in Definition/Proposition 2.3.1 are invariant under global unitary conjugations, that is we have

$$d_*\left(\mathcal{M}_{[uv]}, \mathcal{M}_{[uw]}\right) = d_*\left(\mathcal{M}_{[v]}, \mathcal{M}_{[w]}\right) \quad \text{for all } u, v, w \in \mathcal{U}_d.$$

The metric d_{exp} occurs in a number of physicists' accounts on the subject of mutually unbiased bases (though not under this name), see for instance the articles [12, 13] by Ingemar Bengtsson. The author introduces the metric d_{exp} as *chordal Grassmannian distance* between planes of dimension $d-1$ in the euclidean space $\mathbb{R}^{d^2-1}$ (i.e. elements of the Grassmannian space $Gr(d-1, \mathbb{R}^{d^2-1})$), and he points out that this metric can be understood as chordal distance on a sphere in a real vector space (of greater dimension). Furthermore, he explains how to compute the average value of the metric d_{exp}, and sheds light on a connection to the so-called *Fubini-Study measure.* The expectation metric is also considered in the survey article [35] by Thomas Durt et al., with special emphasis on a link to density matrices. We are not aware of any publications treating the metrics d_{mean} and d_{max}.

Clearly all of the metrics defined above are constantly zero if d equals one, which coincides with the fact that the set of masas in $M_1(\mathbb{C}) \cong \mathbb{C}$ collapses to a single point. An elementary computation shows that for $d=2$, the distances d_{max} and d_{mean} coincide, but are different from d_{exp}. Already in dimension $d=3$, all of these metrics are pairwise different (and none is just a constant multiple of another). Nevertheless, we shall see that they are all *topologically equivalent,* that is they induce the same topology on $\mathfrak{M}_d$, for all $d \in \mathbb{N}$.

We will need the following analytical statement in the sequel.

Technical Lemma 2.3.2. *For $d \in \mathbb{N}$, let $S^{d-1} \subset \mathbb{R}^d$ denote the unit sphere in the real euclidean space $\mathbb{R}^n$. We define the following function on the sphere S^{d-1}.*

$$f : S^{d-1} \longrightarrow \mathbb{R}, \quad (t_j) \longmapsto \sum_{j=0}^{d-1} t_j^4$$

The range of the function f on S^{d-1} is the closed interval $[1/d, 1]$, and the function f attains its maxima exactly in set of unit vectors

$$\{(0,\ldots,0,\underset{(jth\ pos.)}{\underset{|}{1}},0,\ldots,0)^T \mid 0 \leq j < d\}.$$

(What is more, the minimum $1/d$ of f lies precisely at the point $(\sqrt{1/d}, \ldots, \sqrt{1/d})$.)

The proof, which is based on the method of Lagrange multipliers, can be found in the Appendix on pages 215-216. ▷

Recall that two metrics d, d' on a metric space X are said to be Lipschitz equivalent if there are constants $c, C \in \mathbb{R}^+$ such that the inequalities

$$cd'(x,y) \leq d(x,y) \leq Cd'(x,y)$$

hold for all $x, y \in X$. Lipschitz equivalence defines an equivalence relation. Besides that, it is not hard to see that Lipschitz equivalent metrics are also topologically equivalent (see e.g. [98, proposition 2.4.4]). The converse implication is not in general true—the metrics considered here give evidence of this fact, as the following assertion shows.

Lemma 2.3.3. *For all $d \in \mathbb{N}$, the metrics d_{max} and d_{mean} on the masa set $\mathfrak{M}_d$ (see Definition/Proposition 2.3.1) are Lippschitz equivalent and fulfil the inequalities*

$$d_{mean} \leq d_{max} \leq \sqrt{d} \cdot d_{mean}.$$

The metric d_{exp} is not Lipschitz equivalent to the others for $d \geq 2$, but still topologically equivalent.

Proof. As in Definition/Proposition 2.3.1, let $u, v \in \mathcal{U}_d$ be unitary matrices with associated ONBs $\mathfrak{a} = (x_0, \ldots, x_{d-1})$ and $\mathfrak{b} = (y_0, \ldots, y_{d-1})$ respectively, given by their columns.

Clearly the arithmetic mean of a finite set $S \subset \mathbb{R}$ is less than or equal to its maximal value, and if moreover S contains no negative elements, the sum over all values is greater than or equal to the maximal value of S. This suffices to prove the Lipschitz equivalence of the metrics d_{max} and d_{mean}.

$$\begin{aligned}
d^2_{mean}\left(\mathcal{M}_{[u]}, \mathcal{M}_{[v]}\right) &= \min_{\sigma \in S_d} \frac{2}{d} \sum_{i=0}^{d-1} \underbrace{(1 - |(x_i \,|\, y_{\sigma(i)})|)}_{\geq 0} \\
&\leq 2 \min_{\sigma \in S_d} \max_{0 \leq i < d} \left(1 - |(x_i \,|\, y_{\sigma(i)})|\right) = d^2_{max}\left(\mathcal{M}_{[u]}, \mathcal{M}_{[v]}\right) \\
&\leq 2 \min_{\sigma \in S_d} \sum_{i=0}^{d-1} \left(1 - |(x_i \,|\, y_{\sigma(i)})|\right) = d \cdot d^2_{mean}\left(\mathcal{M}_{[u]}, \mathcal{M}_{[v]}\right)
\end{aligned}$$

Next, we prove the topological equivalence of the metrics d_{max} and d_{exp}. To this aim, first suppose that

$$\begin{aligned}
d^2_{max}\left(\mathcal{M}_{[u]}, \mathcal{M}_{[v]}\right) &= 2 \min_{\sigma \in S_d} \max_{0 \leq i < d} \left(1 - |(x_i \,|\, y_{\sigma(i)})|\right) \\
&= 2 - 2 \max_{\sigma \in S_d} \min_{0 \leq i < d} |(x_i \,|\, y_{\sigma(i)})| < 2\delta
\end{aligned}$$

for some $\delta > 0$. This implies $\max_{\sigma \in S_d} \min_{0 \leq i < d} |(x_i \,|\, y_{\sigma(i)})| > 1 - \delta$, so there is a permutation $\sigma_0 \in S_d$ such that

$$|(x_i \,|\, y_{\sigma_0(i)})| > 1 - \delta \quad \text{for all } 0 \leq i < d.$$

Consequently, the remaining scalar products must be rather small. The Parseval identity tells us that

$$|(x_i \,|\, y_j)| < \sqrt{2\delta} \quad \text{for all } 0 \leq i, j < d,\ j \neq \sigma_0(i).$$

We can now compute an upper bound for the modulus of the expectation distance.

$$\begin{aligned}\frac{2}{d^2}\left|d^2_{exp}(\mathcal{M}_{[u]},\mathcal{M}_{[v]})\right| &= |d-\sum_{i,j=0}^{d-1}|(x_i\,|\,y_j)|^4| \\ &\leq |d-\sum_{i=0}^{d-1}|(x_i\,|\,y_{\sigma_0(i)})|^4|+|\sum_{\substack{i,j=0\\ i\neq j}}^{d-1}|(x_i\,|\,y_j)|^4| \\ &\leq |\sum_{i=0}^{d-1}(1-|(x_i\,|\,y_{\sigma_0(i)})|^4)|+4(d^2-d)\delta^2 \\ &\leq d(1-(1-\delta)^4)+4(d^2-d)\delta^2\end{aligned}$$

Since the last expression converges to zero for $\delta\to 0$, there is a positive real number $\delta>0$ for all $\varepsilon>0$ allowing the following implication.

$$d^2_{max}\left(\mathcal{M}_{[u]},\mathcal{M}_{[v]}\right)<\delta \quad\Rightarrow\quad d^2_{exp}\left(\mathcal{M}_{[u]},\mathcal{M}_{[v]}\right)<\varepsilon$$

As a consequence, each Cauchy sequence of masas $\mathcal{M}_n\in\mathfrak{M}_d$ ($n\in\mathbb{N}$) w.r.t. the metric d_{max} is at the same time a Cauchy sequence w.r.t. the expectation metric d_{exp}.

Conversely, assume that $(2/d^2)\,d^2_{exp}(\mathcal{M}_{[u]},\mathcal{M}_{[v]})<\delta$ for some $\delta>0$. Then we get

$$0\leq 1-\sum_{j=0}^{d-1}|(x_i\,|\,y_j)|^4\leq\sum_{i=0}^{d-1}\left(1-\sum_{j=0}^{d-1}|(x_i\,|\,y_j)|^4\right)=\sum_{i,j=0}^{d-1}\left(\frac{1}{d}-|(x_i\,|\,y_j)|^4\right)<\delta$$

and thus

$$\sum_{j=0}^{d-1}|(x_i\,|\,y_j)|^4>1-\delta \tag{2.4}$$

for each fixed index $0\leq i<d$. We can now apply the Technical Lemma 2.3.2 for the first time. Since the function $f:S^{d-1}\to\mathbb{R}$, $(t_j)\mapsto\sum_{j=0}^{n-1}t_j^4$, attains its maximum if and only if one component t_j equals one and all others are zero, and since moreover f is obviously continuous, we can conclude from equation (2.4) that there is some positive number $\varepsilon>0$ (depending on δ) and an index $0<j_i<d-1$ such that we have

$$1-|(x_i\,|\,y_{j_i})|<\varepsilon.$$

This inequality can of course be deduced for all $0\leq i<d$, for the same value $\varepsilon>0$. Beyond that, the Parseval identity imposes (if ε is small enough, which can be arranged) that j_{i_o} does not equal j_{i_1} for all $i_0\neq i_1$. The mapping $\sigma_0:i\mapsto j_i$ therefore is a permutation, and by definition of $\sigma_0\in S_d$, we have $|(x_i\,|\,y_{\sigma(i)})|>1-\varepsilon$ for all $0\leq i<d$. For the maximum metric, this means

$$d^2_{max}\left(\mathcal{M}_{[u]},\mathcal{M}_{[v]}\right)=2-2\max_{\sigma\in S_d}\min_{0\leq i<d}|(x_i\,|\,y_{\sigma(i)})|<2-2(1-\varepsilon)<2\varepsilon.$$

By the same argument as used in the converse case, this shows that each Cauchy sequence in $\mathfrak{M}_d$ w.r.t. the expectation metric is also a Cauchy sequence w.r.t. the maximum metric.

Finally, we construct a counterexample to demonstrate that the metrics d_{max} and d_{exp} are not Lipschitz equivalent (which implies the same for d_{mean} and d_{exp}, since Lipschitz equivalence is an equivalence relation). To this aim, we define orthonormal bases of the Hilbert space $\mathbb{C}^d$ which are "close" to the standard orthonormal basis $\mathfrak{e} = (z_0, \dots, z_{d-1})$ as follows. For all $1 \geq \varepsilon > 0$, an orthonormal basis $\mathfrak{e}_\varepsilon = (\tilde{z}_0, \dots, \tilde{z}_{d-1})$ is given by setting

$$\tilde{z}_0 = \begin{pmatrix} \varepsilon \\ \sqrt{1-\varepsilon^2} \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \tilde{z}_1 = \begin{pmatrix} \sqrt{1-\varepsilon^2} \\ -\varepsilon \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

and $\tilde{z}_i = z_i$ for all indices $2 \leq i < d$. (For convenience, we do not label the vectors $\tilde{z}_i$ with an ε.)

Suppose ε is less than $1/\sqrt{2}$, so that $\sqrt{1-\varepsilon^2} > \varepsilon$. Then you convince yourself that the squared d_{max}-distance between the masas $\mathcal{M}_{[\mathfrak{e}]}$ and $\mathcal{M}_{[\mathfrak{e}_\varepsilon]}$ is given by

$$\begin{aligned} d_{max}^2\left(\mathcal{M}_{[\mathfrak{e}]}, \mathcal{M}_{[\mathfrak{e}_\varepsilon]}\right) &= 2 - 2 \max_{\sigma \in S_d} \min_{0 \leq i < d} \left|(z_i \,|\, \tilde{z}_{\sigma(i)})\right| \\ &= 2 - 2\left|(z_1 \,|\, \tilde{z}_0)\right| = 2 - 2\sqrt{1-\varepsilon^2}. \end{aligned}$$

The squared distance of $\mathcal{M}_{[\mathfrak{e}]}$ and $\mathcal{M}_{[\mathfrak{e}_\varepsilon]}$ w.r.t. the expectation metric computes to

$$\begin{aligned} d_{exp}^2\left(\mathcal{M}_{[\mathfrak{e}]}, \mathcal{M}_{[\mathfrak{e}_\varepsilon]}\right) &= \frac{2}{d^2} \sum_{i,j=0}^{d-1} \left(\frac{1}{d} - |(x_i \,|\, y_j)|^4\right) \\ &= \frac{2}{d} - \frac{2}{d^2} \sum_{i,j=0}^{d-1} |(x_i \,|\, y_j)|^4 \\ &= \frac{2}{d} - \frac{2}{d^2}\left(d + 4\varepsilon^4 - 4\varepsilon^2\right) = \frac{8}{d^2}\left(\varepsilon^2 - \varepsilon^4\right) \end{aligned}$$

If ε tends to zero, then so does the ratio

$$\frac{d_{exp}^2}{d_{max}^2} \sim \frac{\varepsilon^2 - \varepsilon^4}{1 - \sqrt{1-\varepsilon^2}} \sim \frac{\varepsilon - \varepsilon^3}{\frac{1}{\varepsilon} - \sqrt{\frac{1}{\varepsilon^2} - 1}},$$

so that there is no constant $c > 0$ such that $c \cdot d_{max}(\mathcal{M}_{[\mathfrak{e}]}, \mathcal{M}_{[\mathfrak{e}_\varepsilon]}) \leq d_{exp}(\mathcal{M}_{[\mathfrak{e}]}, \mathcal{M}_{[\mathfrak{e}_\varepsilon]})$ holds for all $\varepsilon > 0$. The metrics d_{max} and d_{exp} are thus not Lipschitz equivalent. □

Since all norms on a finite-dimensional vector space are equivalent, the operator and the Hilbert-Schmidt norm on $M_d(\mathbb{C})$ induce the same topology on the unitary group $\mathcal{U}_d$. Therefore Lemma 2.3.3 states that all metrics we discuss here induce the natural quotient topology on the quotient $\mathcal{U}_d/\mathcal{W}_d$. From here on, we will always consider the set of masas as endowed with this topology.

It is a well-known fact that the unitary group $\mathcal{U}_d$ is a compact subset of the complex $d\times d$-matrices. The quotient map $q : \mathcal{U}_d \to \mathcal{U}_d/\mathcal{W}_d$, $u \mapsto [u]$, is clearly continuous, and thus a continuous surjection from a compact space onto $\mathfrak{M}_d$. As a consequence, $\mathfrak{M}_d$ is compact as well. More precisely, we can notate the following

Lemma 2.3.4. *For all $d \in \mathbb{N}$, the set of masas $\mathfrak{M}_d$ is a compact, and hence complete and bounded metric space (with respect to each of the metrics d_{exp}, d_{mean}, and d_{max}). The diameter of $\mathfrak{M}_d$ equals*

- $\sqrt{2(1-\sqrt{1/d})}$ *with respect to the quotient metrics d_{max} and d_{mean}, and*
- $\sqrt{2\frac{(d-1)}{d}}$ *with respect to the expectation metric d_{exp}.*

Proof. The compactness of $\mathfrak{M}_d$ has already been explained, and it is elementary that every compact metric space is complete and bounded.

Secondly, the stated upper bounds for the metrics are attained for masas which correspond to unbiased bases in $\mathbb{C}^d$, which do, as we have seen, exist for all $d \geq 2$.

Due to the inequality $d_{mean} \leq d_{max}$ (Lemma 2.3.3), the first upper bound has only to be checked for the metric d_{max}. To this end, let $\mathfrak{a} = (x_0, \dots, x_{d-1})$ and $\mathfrak{b} = (y_0, \dots, y_{d-1})$ be unbiased bases of the Hilbert space $\mathbb{C}^d$. In the proof of Lemma 2.2.10, we have already explained how to construct a permutation $\sigma_0 \in S_d$ in this case such that we have

$$|(x_i \,|\, y_{\sigma_0(i)})| \geq \frac{1}{\sqrt{d}}$$

for all $0 \leq i < d$. According to the Definition of the maximum metric, this leads to

$$d_{max}^2\left(\mathcal{M}_{[\mathfrak{a}]}, \mathcal{M}_{[\mathfrak{b}]}\right) = 2 - 2 \max_{\sigma\in S_d} \min_{0\leq i<d} |(x_i \,|\, y_{\sigma(i)})| \leq 2 - 2 \min_{0\leq i<d} |(x_i \,|\, y_{\sigma_0(i)})| \leq 2 - 2\frac{1}{\sqrt{d}}.$$

The upper bound for the expectation metric is immediately verified by the second expression stated for d_{exp} in Definition/Proposition 2.3.1. □

All of the metrics introduced in this section are, as we have seen, very natural distance measures on the set of masas. All the same, we would not have considered them in the present work if there was not the following important link to our main topic.

Theorem 2.3.5. *If the dimension d is at least two, the following assertions are equivalent for any two masas $\mathcal{M}, \mathcal{N}$ in $M_d(\mathbb{C})$.*

(i) The masas $\mathcal{M}$ and $\mathcal{N}$ are quasi-orthogonal.

(ii) The masas $\mathcal{M}$ and $\mathcal{N}$ are maximally distant w.r.t. to the mean metric d_{mean}.

(iii) The masas $\mathcal{M}$ and $\mathcal{N}$ are maximally distant w.r.t. the maximum metric d_{exp}.

Quasi-orthogonality of $\mathcal{M}$ and $\mathcal{N}$ moreover implies that $d_{max}(\mathcal{M},\mathcal{N})$ is maximal, but the converse is not generally true.

Proof. We have already seen in the proof of the last preceding lemma that assertion (i) implicates the others. For the converse implications, set $\mathcal{M} = \mathcal{M}_{[\mathfrak{a}]}$ and $\mathcal{N} = \mathcal{M}_{[\mathfrak{b}]}$ for orthonormal bases $\mathfrak{a} = (x_0, \dots, x_{d-1})$ and $\mathfrak{b} = (y_0, \dots, y_{d-1})$ respectively.

The implication $(ii) \Rightarrow (i)$ is proved indirectly, applying the criterion for unbiasedness presented in Lemma 2.2.10. According to this criterion, the assumption that the bases $\mathfrak{a}$ and $\mathfrak{b}$ are *not* unbiased implies that there is at least one permutation $\sigma_0 \in S_d$ such that we have

$$\sum_{i=0}^{d-1} |(x_i \,|\, y_{\sigma_0(i)})| > \sqrt{d}.$$

This leads to the inequality

$$d^2_{mean}\left(\mathcal{M}_{[\mathfrak{a}]}, \mathcal{M}_{[\mathfrak{b}]}\right) = 2 - \max_{\sigma \in S_d} \frac{2}{d} \sum_{i=0}^{d-1} |(x_i \,|\, y_{\sigma(i)})| < 2 - \frac{2}{\sqrt{d}}.$$

The mean metric is thus not maximal unless $\mathfrak{a}$ and $\mathfrak{b}$ are unbiased, that is to say, unless the masas $\mathcal{M}$ and $\mathcal{N}$ are quasi-orthogonal.

The second expression stated for the expectation metric in Definition/Proposition 2.3.1 makes it clear that $d_{exp}(\mathcal{M}_{[\mathfrak{a}]}, \mathcal{M}_{[\mathfrak{b}]})$ is not maximal unless the bases $\mathfrak{a}$ and $\mathfrak{b}$ are unbiased, showing that item (i) follows from item (iii).

The last statement of the theorem is proved by the following counterexample. Consider the standard orthonormal basis $\mathfrak{e} = (z_0, \dots, z_3)$, and the orthonormal basis

$$\mathfrak{a} = \left\{ \frac{1}{2}\begin{pmatrix}1\\1\\1\\1\end{pmatrix}, \frac{1}{2}\begin{pmatrix}1\\1\\-1\\-1\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\\0\\0\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix}0\\0\\1\\-1\end{pmatrix} \right\}$$

of the Hilbert space $\mathbb{C}^4$. Obviously, these bases are not unbiased, so that the associated masas in $M_4(\mathbb{C})$ are not quasi-orthogonal. Nevertheless, it is verified without effort that the maximum distance of the masas corresponding to these bases is maximal, that is

$$d_{max}\left(\mathcal{M}_{[\mathfrak{e}]}, \mathcal{M}_{[\mathfrak{a}]}\right) = \sqrt{2(1-\sqrt{1/4})} = 1.$$

□

Excursion: The set of masas in $\mathbf{M_d(\mathbb{C})}$ as a smooth manifold and homogeneous space

Put shortly, a *real manifold* of dimension d is a topological space M which locally looks like the euclidean space $\mathbb{R}^d$, that is there is an open cover $(U_\lambda)_\lambda$ of M, open subsets $U'_\lambda \subset \mathbb{R}^d$, and homeomorphisms $h_\lambda : U_\lambda \to U'_\lambda$. The manifold M is said to be *smooth* if for each pair of homeomorphisms h_λ, h_μ, partly defined on a common domain, the map $h_\mu \circ h_\lambda^{-1}$ is infinitely often differentiable on that domain.

The topological concept of a manifold is too complicated to permit a detailed introduction in only a few words. We refer the reader who is unfamiliar with this subject to introductory textbooks like [21].

Likewise, we will not define *Lie groups,* although they are involved in the following short discussion (see e.g. the textbook [20]). Loosely speaking, a Lie group is a group being a smooth manifold at the same time. The unitary group $\mathcal{U}_d \subset M_d(\mathbb{C})$ is a compact, connected, real Lie group of dimension d^2.

The next theorem is adopted from the textbook [20] (the original statement is much more explicit).

Theorem 2.3.6 (see theorem 4.3 in [20])**.** *Let G be a Lie group and H a closed subgroup of G. Then the quotient G/H is a smooth real manifold.*

The topology on the quotient manifold G/H is given by the quotient topology. Setting $G = \mathcal{U}_d$ and $H = \mathcal{W}_d$ in the statement above, we see that $\mathfrak{M}_d \cong \mathcal{U}_d/\mathcal{W}_d$ is a smooth manifold, endowed with the quotient topology. As we have seen, this topology coincides with the one given by the metrics above. It is not hard to check that the dimension of $\mathfrak{M}_d$ is given by

$$\dim \mathfrak{M}_d = \dim_{\mathbb{R}} \mathcal{U}_d - \dim_{\mathbb{R}} \mathcal{W}_d = d^2 - d.$$

Since homeomorphisms are the isomorphisms in the category of topological spaces, let Aut $(\mathcal{U}_d/\mathcal{W}_d)$ denote the set of all homeomorphisms from the space $\mathcal{U}_d/\mathcal{W}_d$ to itself. The unitary group $\mathcal{U}_d$ acts on the quotient $\mathcal{U}_d/\mathcal{W}_d$ as follows.

$$\rho : \mathcal{U}_d \longrightarrow \text{Aut}\,(\mathcal{U}_d/\mathcal{W}_d), \quad u \longmapsto \rho_u : [v] \mapsto [uv] \ \text{ for all } v \in \mathcal{U}_d \tag{2.5}$$

Going through the details, one finds that the mapping ρ is smooth, i.e. infinitely often differentiable. Beyond that, ρ is a *transitive* group action, since for all unitaries v, w in $\mathcal{U}_d$, one finds a third unitary $u \in \mathcal{U}_d$ such that $[uv] = [w]$ and hence $\rho_u([v]) = [w]$ (simply take $u = wv^*$). For this reason, the quotient $\mathcal{U}_d/\mathcal{W}_d$ meets the conditions of a so-called *homogeneous space,* see for example [20, definition 4.5 and p. 32].

The manifold $\mathcal{U}_d$ is *path-connected:* for any two unitaries $v, w \in \mathcal{U}_d$, there is a continuous mapping (a *path*) $\phi : [0,1] \to \mathcal{U}_d$, $\phi(\lambda) = u_\lambda$, such that $u_0 = v$ and $u_1 = w$. Since the canonical quotient map is continuous, this simultaneously defines a path $[u_\lambda]$ connecting the classes $[v]$ and $[w]$ in $\mathcal{U}_d/\mathcal{W}_d$. As a consequence, the latter is path-connected as well. Recall that any path-connected topological space is also connected. For manifolds, the converse implication is true as well, which follows from the fact that they are *locally path-connected.*

Summary 2.3.7. For all $d \in \mathbb{N}$, the set of masas $\mathfrak{m}_d \cong \mathcal{U}_d/\mathcal{W}_d$ is a compact, connected, metric, smooth real manifold of dimension $d^2 - d$, and a homogeneous space w.r.t. the action ρ of the unitary group $\mathcal{U}_d$, as defined in equation (2.5).

For $d \geq 2$, two points on the manifold $\mathfrak{m}_d$ are maximally distant w.r.t. the metrics d_{exp} and d_{mean} if and only if they represent quasi-orthogonal masas.

It may very well be as fruitful as interesting to investigate the manifold $\mathfrak{m}_d$ in more detail than we have done here. However, since the author is not a topologist, this is not a subject of the present thesis. Instead, we conclude this quick look on topological aspects of the masa set $\mathfrak{m}_d$ with an explicit computation of the smallest (non-trivial) example $\mathfrak{m}_2$.

For this purpose, consider the rectangular area $Q = [0,1] \times [-1,1] \subset \mathbb{R}^2$ in the 2-dimensional real plane, and consider the following relations on Q.

$$R: \quad (r,-1) \sim (r,+1) \ \text{ for all } r \in [0,1], \quad (0,\phi) \sim (0,\phi') \ \text{ for all } \phi,\phi' \in [-1,1]$$

It presents no difficulty to prove that the quotient Q/R is homeomorphic to the closed unit disc

$$D_2 = \left\{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 1\right\} \subset \mathbb{R}^2$$

(also see Figure 2.2 below).

Example 2.3.8. The manifold $\mathfrak{m}_2 \cong \mathcal{U}_2/\mathcal{W}_2$ of all masas in $M_2(\mathbb{C})$ is homeomorphic to the unit disc $D_2 \cong Q/R$. A homeomorphism is given by the following map.

$$D_2 \longrightarrow \mathfrak{m}_d, \quad [(r,\phi)] \longmapsto \left[\begin{pmatrix} \sin\left(\frac{\pi}{4}r\right) & \cos\left(\frac{\pi}{4}r\right) \\ \cos\left(\frac{\pi}{4}r\right) e^{\mathrm{i}\pi\phi} & -\sin\left(\frac{\pi}{4}r\right) e^{\mathrm{i}\pi\phi} \end{pmatrix}\right]$$

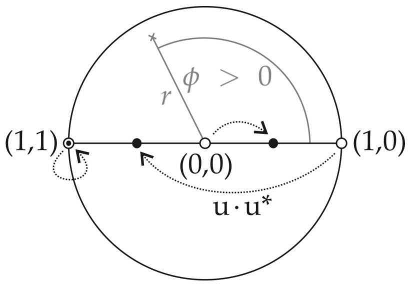


Figure 2.2: *The manifold* $\mathfrak{m}_2 \cong D_2$

The computations for the proof of this example are left to the reader. Let us finally give two instances of sets containing three mutually maximally distant points on $\mathfrak{m}_2$. To this end, we consider the unitary Hadamard matrices $h_0 = \mathrm{F}_2$ and

$$h_1 = \operatorname{diag}(1, \mathrm{i})\, \mathrm{F}_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ \mathrm{i} & -\mathrm{i} \end{pmatrix}$$

in $\mathcal{U}_2$, which are easily seen to be unbiased. The masas $\mathcal{D}_2$, $\mathcal{M}_{[h_0]}$, and $\mathcal{M}_{[h_1]}$ are therefore pairwise quasi-orthogonal, and thus correspond to maximally distant points on $\mathfrak{m}_2$ w.r.t. the metrics introduced in this section. One computes the following correspondences.

$$\mathcal{D}_2 \simeq (0,0) \qquad \mathcal{M}_{[h_0]} \simeq (1,0) \qquad \mathcal{M}_{[h_1]} \simeq (1,1)$$

These points are plotted as white dots in Figure 2.2. More generally, the boundary of the disc contains precisely all points which are maximally distant from the centre $(0,0)$ of the manifold $\mathfrak{m}_2$, as one would expect. Nonetheless, the situation is much less regular for general points on $\mathfrak{m}_2$. For example, conjugating the masas above by the unitary

$$u = \begin{pmatrix} \sin\left(\frac{\pi}{8}\right) & \cos\left(\frac{\pi}{8}\right) \\ \cos\left(\frac{\pi}{8}\right) & -\sin\left(\frac{\pi}{8}\right) \end{pmatrix},$$

one ends up with the points on $\mathfrak{m}_2$ marked as black dots in Figure 2.2, which hence are maximally distant as well.

2.4 Equivalent, standard, and non-standard pairs of quasi-orthogonal masas

In the present work, we do not want to distinguish between pairs of masas being identical up to their order. For this reason, we prefer the notation $\{\mathcal{M}, \mathcal{N}\}$ instead of $(\mathcal{M}, \mathcal{N})$ for pairs of masas $\mathcal{M}, \mathcal{N} \subset M_d(\mathbb{C})$. Moreover, we consider two pairs of masas as *practically the same* if a unitary conjugation allows to switch from one pair to the other (see also Remark 2.2.3). Both of these aspects are reflected in the next

Definition 2.4.1. *We say two pairs* $\{\mathcal{M}_0, \mathcal{M}_1\}$ *and* $\{\mathcal{N}_0, \mathcal{N}_1\}$ *of masas in* $M_d(\mathbb{C})$ *are equivalent or* isomorphic *if there is a* **-automorphism* $\phi : M_d(\mathbb{C}) \to M_d(\mathbb{C})$ *and a permutation* $\sigma \in S_2$ *such that*

$$\phi(\mathcal{M}_0) = \mathcal{N}_{\sigma(0)} \quad \text{and} \quad \phi(\mathcal{M}_1) = \mathcal{N}_{\sigma(1)}.$$

The equivalence relation for Hadamard matrices and that for pairs of quasi-orthogonal masas are related in the following way.

Lemma 2.4.2. *Let $h_0, h_1 \in \mathcal{U}_d$ be unitary Hadamard matrices. The pairs $\{\mathcal{D}_d, h_0\mathcal{D}_d h_0^*\}$ and $\{\mathcal{D}_d, h_1\mathcal{D}_d h_1^*\}$ of quasi-orthogonal masas in $M_d(\mathbb{C})$ are equivalent if and only if either h_1 or h_1^* is equivalent to h_0.*

Proof. By Definition 2.4.1, the pairs $\{\mathcal{D}_d, h_0\mathcal{D}_d h_0^*\}$ and $\{\mathcal{D}_d, h_1\mathcal{D}_d h_1^*\}$ are equivalent if and only if one of the statements below holds.

(a) There is a *-automorphism ϕ_0 of $M_d(\mathbb{C})$ such that

$$\phi_0(\mathcal{D}_d) = \mathcal{D}_d \quad \text{and} \quad \phi_0(h_0\mathcal{D}_d h_0^*) = h_1\mathcal{D}_d h_1^*.$$

(b) There is a *-automorphism ϕ_1 of $M_d(\mathbb{C})$ such that

$$\phi_1(\mathcal{D}_d) = h_1\mathcal{D}_d h_1^* \quad \text{and} \quad \phi_1(h_0\mathcal{D}_d h_0^*) = \mathcal{D}_d.$$

Since all *-automorphisms of $M_d(\mathbb{C})$ are inner, both ϕ_0 and ϕ_1 are unitary conjugations.

Suppose statement (a) applies. Then ϕ_0 is given by conjugation with a *monomial* unitary $w \in \mathcal{W}_d$ by Lemma 1.2.5. This leads to the following implications.

$$wh_0\mathcal{D}_d h_0^* w^* = h_1\mathcal{D}_d h_1^* \quad \Rightarrow \quad h_1^* w h_0 \mathcal{D}_d h_0^* w^* h_1 = \mathcal{D}_d \quad \underset{1.2.5}{\Rightarrow} \quad \underset{w' \in \mathcal{W}_d}{\exists} \; h_1^* w h_0 = w'$$

By the last assertion, the Hadamard matrix h_1 is equivalent to $h_0 = w^* h_1 w'$.

If we assume statement (b), then there is some unitary $u \in \mathcal{U}_d$ such that both uh_0 and $u^* h_1$ are monomial, say $uh_0 = w_0$ and $u^* h_1 = w_1$ for monomial unitaries w_0, w_1 in $\mathcal{W}_d$. This asserts the equality $u^* = h_0 w_0^* = w_1 h_1^*$, and thus the Hadamard matrices h_1^* and h_0 are equivalent by $h_1^* = w_1^* h_0 w_0^*$. □

We have introduced a particularly nice pair of quasi-orthogonal masas, namely $\{\mathcal{D}_d, \mathcal{A}^*(\mathrm{X}_d)\}$, in Example 2.2.2 (a). We have further computed the identity

$$\mathcal{A}^*(\mathrm{X}_d) = \mathrm{F}_d \mathcal{D}_d \mathrm{F}_d^*.$$

in Example 2.2.9, where F_d is the Quantum Fourier matrix introduced Definition 1.3.2. This quasi-orthogonal pair was first investigated by Sorin Popa in the aforementioned article [83]. It is often called the *standard pair of quasi-orthogonal masas,* see e.g. [44, 76]. More precisely, this notion is defined up to unitary equivalence.

Definition 2.4.3. *A(n ordered) pair $(\mathcal{M}, \mathcal{N})$ of masas in $M_d(\mathbb{C})$ is called* standard pair *if there is a *-automorphism ϕ of $M_d(\mathbb{C})$ such that*

$$\phi(\mathcal{D}_d) = \mathcal{M} \quad \textit{and} \quad \phi(\mathcal{A}^*(\mathrm{X}_d)) = \mathcal{N}.$$

Note that a standard pair is of course automatically quasi-orthogonal. On the face of it, the order of the pair $(\mathcal{M},\mathcal{N})$ seems to matter in the definition above, so that $(\mathcal{M},\mathcal{N})$ could be standard while $(\mathcal{N},\mathcal{M})$ is not at the same time. This is not true.

Lemma 2.4.4. *An ordered pair $(\mathcal{M},\mathcal{N})$ of masas in $M_d(\mathbb{C})$ is standard if and only if $(\mathcal{N},\mathcal{M})$ is standard as well.*

Proof. In Example 2.2.9, we have computed

$$\mathrm{X}_d = \mathrm{F}_d \mathrm{Z}_d^* \mathrm{F}_d^*. \tag{2.6}$$

The regularity of the involved matrices leads to a second equation, looking confusingly similar to the one above.

$$\mathrm{X}_d = \mathrm{F}_d^* \mathrm{Z}_d \mathrm{F}_d. \tag{2.7}$$

This is checked without difficulty on the standard basis $\mathfrak{e} = (z_0, \dots, z_{d-1})$: for each $0 \leq i_0 < d$, one calculates

$$\mathrm{F}_d^* \mathrm{Z}_d \mathrm{F}_d \, z_{i_0} = \frac{1}{\sqrt{d}} \mathrm{F}_d^* \mathrm{Z}_d \begin{pmatrix} 1 \\ \zeta_d^{i_0} \\ \zeta_d^{2i_0} \\ \vdots \\ \zeta_d^{(d-1)i_0} \end{pmatrix} = \frac{1}{\sqrt{d}} \mathrm{F}_d^* \begin{pmatrix} 1 \\ \zeta_d^{i_0+1} \\ \zeta_d^{2(i_0+1)} \\ \vdots \\ \zeta_d^{(d-1)(i_0+1)} \end{pmatrix} = z_{i_0+1} = \mathrm{X}_d \, z_{i_0}.$$

Now let $u \in \mathcal{U}_d$ denote the unitary matrix performing the *-automorphism ϕ via the conjugation $\phi(\cdot) = u \cdot u^*$. Using the equations above, we can prove the following equivalences, where we set $\tilde{u} = u\mathrm{F}_d$.

$$\begin{array}{cccccccc}
 & u\mathcal{D}_d u^* & = & \mathcal{M} & \text{and} & u\mathcal{A}^*(\mathrm{X}_d)\, u^* = & & \mathcal{N} \\
\underset{(2.6)}{\Leftrightarrow} & \mathcal{D}_d & = & u^*\mathcal{M}u & \text{and} & \mathrm{F}_d\mathcal{D}_d\mathrm{F}_d^* & = & u^*\mathcal{N}u \\
\Leftrightarrow & \mathrm{F}_d^*\mathcal{D}_d\mathrm{F}_d & = & \mathrm{F}_d^*u^*\mathcal{M}u\mathrm{F}_d & \text{and} & \mathcal{D}_d & = & \mathrm{F}_d^*u^*\mathcal{N}u\mathrm{F}_d \\
\underset{(2.7)}{\Leftrightarrow} & \mathcal{A}^*(\mathrm{X}_d) & = & \mathrm{F}_d^*u^*\mathcal{M}u\mathrm{F}_d & \text{and} & \mathcal{D}_d & = & \mathrm{F}_d^*u^*\mathcal{N}u\mathrm{F}_d \\
\Leftrightarrow & \tilde{u}\mathcal{A}^*(\mathrm{X}_d)\,\tilde{u} = & & \mathcal{M} & \text{and} & \tilde{u}\mathcal{D}_d\tilde{u}^* & = & \mathcal{N}
\end{array}$$

The first of these equivalent statements says the pair $(\mathcal{M},\mathcal{N})$ is standard, the last says $(\mathcal{N},\mathcal{M})$ is standard. □

Using the lemma above, we are able to formulate a notion of *unordered* standard pairs of masas that is compatible with the original Definition 2.4.3.

Definition 2.4.5. *A pair $\{\mathcal{M},\mathcal{N}\}$ of masas in $M_d(\mathbb{C})$ is said to be a* standard pair *if it is equivalent to the pair $\{\mathcal{D}_d, \mathrm{F}_d\mathcal{D}_d\mathrm{F}_d^*\}$.*

Standard pairs of quasi-orthogonal masas are, in a way, the most regular examples of quasi-orthogonal masa pairs. Our next goal is to collect some regularity properties of standard pairs. As a preparation of the respective Theorem 2.4.7, we need the following

Technical Lemma 2.4.6. *If $u \in \mathcal{U}_d$ is a unitary Hadamard matrix such that the equation $\mathrm{Z}_d u = uw$ holds for a monomial unitary $w \in \mathcal{W}_d$, then u is equivalent to the unitary Fourier matrix F_d.*

Proof. The monomial matrix w acts as a weighted permutation on the standard orthonormal basis $\mathfrak{e}$, so there is a permutation $\sigma \in S_d$ and weights $\lambda_0, \ldots, \lambda_{d-1} \in \mathbb{T}$ such that we have $w\, z_i = \lambda_i z_{\sigma(i)}$ for all $0 \le i < d$. We write $u = \sqrt{1/d}(\mu_{i,j})_{0\le i,j<d}$ with entries $\mu_{i,j} \in \mathbb{T}$. Then the equations $uw\, z_j = \mathrm{Z}_d u\, z_j$ assert

$$\begin{pmatrix} \mu_{0,\sigma(j)} \\ \mu_{1,\sigma(j)} \\ \mu_{2,\sigma(j)} \\ \vdots \\ \mu_{d-1,\sigma(j)} \end{pmatrix} = \bar{\lambda}_j \begin{pmatrix} \mu_{0,j} \\ \zeta_d \mu_{1,j} \\ \zeta_d^2 \mu_{2,j} \\ \vdots \\ \zeta_d^{d-1} \mu_{d-1,j} \end{pmatrix}$$

for all indices $0 \le j < d$. Iterating this last formula (w.r.t. the application of σ) yields the identity

$$\begin{pmatrix} \mu_{0,\sigma^i(j)} \\ \mu_{1,\sigma^i(j)} \\ \mu_{2,\sigma^i(j)} \\ \vdots \\ \mu_{d-1,\sigma^i(j)} \end{pmatrix} = \left(\prod_{k=0}^{i-1} \bar{\lambda}_{\sigma^k(j)}\right) \begin{pmatrix} \mu_{0,j} \\ \zeta_d^i \mu_{1,j} \\ \zeta_d^{2i} \mu_{2,j} \\ \vdots \\ \zeta_d^{(d-1)i} \mu_{d-1,j} \end{pmatrix}$$

for each fixed $0 < i < d$. It thereby immediately leads to a contradiction to assume $\sigma^i(j) = j$ for an index $0 < i < d$. For this reason, the permutation σ is *cyclic*, i.e. we have

$$\left\{\sigma^i(j) \;\middle|\; 0 \le i < d\right\} = \{0, \ldots, d-1\}$$

for all fixed $0 \le j < d$. We define a unitary diagonal matrix $w_0 = \mathrm{diag}(\mu_{0,0}, \ldots, \mu_{d-1,0})$, and a second monomial unitary $w_1 \in \mathcal{W}_d$ by its action

$$z_{\sigma^i(0)} \xmapsto{w_1} \left(\prod_{k=0}^{i-1} \bar{\lambda}_{\sigma^k(0)}\right) z_i \quad (0 \le i < d)$$

on the standard orthonormal basis. (Note that the assignment $\sigma^i(0) \mapsto i$ is in fact a permutation by the cyclicity of σ.) One verifies the equality $w_0 \mathrm{F}_d w_1\, z_{\sigma^i(0)} = u\, z_{\sigma^i(0)}$ for all $0 \le i < d$, thus the equivalence of the Hadamard matrices u and F_d. □

To state conditions (via) and (vib) of the next theorem, we need to define the following subgroup of the unitary matrices for masas $\mathcal{M}, \mathcal{N} \subset M_d(\mathbb{C})$.

$$\mathcal{W}(\mathcal{M}, \mathcal{N}) = \{v \in \mathcal{N} \cap \mathcal{U}_d \mid v\mathcal{M}v^* = \mathcal{M}\}$$

Note that we have the identity $\mathcal{W}(\mathcal{D}_d, \mathcal{N}) = \mathcal{N} \cap \mathcal{W}_d$. It is of course no loss of generality to assume that one of the involved masas is the diagonal masa $\mathcal{D}_d$ in the following

Theorem 2.4.7 (Criteria for standard pairs of masas). *For a unitary matrix $u \in \mathcal{U}_d$, let $\mathcal{M} = \mathcal{M}_{[u]} = u\mathcal{D}_d u^*$ be the associated masa in $M_d(\mathbb{C})$. The following statements are equivalent.*

(i) The pair $\{\mathcal{D}_d, \mathcal{M}\}$ is a standard pair of quasi-orthogonal masas.

(iia) There is a *-automorphism $\phi : M_d(\mathbb{C}) \to M_d(\mathbb{C})$ fulfilling the equations

$$\phi(\mathcal{D}_d) = \mathcal{D}_d \quad \text{and} \quad \phi(\mathcal{A}^*(\mathrm{X}_d)) = \mathcal{M}.$$

(iib) There is a *-automorphism $\psi : M_d(\mathbb{C}) \to M_d(\mathbb{C})$ fulfilling the equations

$$\psi(\mathcal{D}_d) = \mathcal{M} \quad \text{and} \quad \psi(\mathcal{A}^*(\mathrm{X}_d)) = \mathcal{D}_d.$$

(iiia) The unitary u is a Hadamard matrix equivalent to F_d.

(iiib) The unitary u^* is a Hadamard matrix equivalent to F_d.

(iv) There are unitary generators v_0 of $\mathcal{D}_d$ and v_1 of $\mathcal{M}$ having trace-free powers $v_0, \ldots, v_0^{d-1}$, $v_1, \ldots, v_1^{d-1}$, and commuting up to a primitive dth root of unity ω:

$$v_0 v_1 = \omega v_1 v_0 \tag{2.8}$$

(va) The masa $\mathcal{M}$ is quasi-orthogonal to $\mathcal{D}_d$ and generated by a unitary matrix $v_1 \in \mathcal{U}_d$ fulfilling $v_1\mathcal{D}_d v_1^* = \mathcal{D}_d$. (In other words, $\mathcal{M}$ is generated by a monomial unitary matrix corresponding to a weighted cyclic permutation.)

(vb) The masa $\mathcal{D}_d$ is quasi-orthogonal to $\mathcal{M}$ and generated by a unitary matrix $v_0 \in \mathcal{U}_d$ satisfying the equality $v_0\mathcal{M}v_0^* = \mathcal{M}$.

(via) There is an isomorphism of abelian groups $\mathcal{W}(\mathcal{D}_d, \mathcal{M}) / (\mathbb{T} \cdot \mathrm{I}_d) \cong \mathbb{Z}/d$.

(vib) There is an isomorphism of abelian groups $\mathcal{W}(\mathcal{M}, \mathcal{D}_d) / (\mathbb{T} \cdot \mathrm{I}_d) \cong \mathbb{Z}/d$.

Proof. The implications and equivalences in the following diagram suffice to prove our theorem.

$$\begin{tikzcd}
(iiia) \arrow[rr, Leftrightarrow] & & (iia) \arrow[r, Leftrightarrow] \arrow[dl, Rightarrow] & (i) \arrow[r, Leftrightarrow] & (iib) \arrow[rr, Leftrightarrow] \arrow[dd, Rightarrow] \arrow[dr, Rightarrow] & & (iiib) \\
 & (via) \arrow[dl, Rightarrow] & & & & (vib) \arrow[dr, Rightarrow] & \\
(va) \arrow[uu, Rightarrow] & & & & (iv) \arrow[rr, Rightarrow] & & (vb) \arrow[uu, Rightarrow]
\end{tikzcd}$$

According to Lemma 2.4.4, the pair $\{\mathcal{M},\mathcal{N}\}$ is standard if and only if both of the *ordered* pairs $(\mathcal{M},\mathcal{N})$ and $(\mathcal{N},\mathcal{M})$ are standard in the sense of the original Definition 2.4.3. A look at this definition is enough to see the equivalences $(iia) \Leftrightarrow (i) \Leftrightarrow (iib)$.

$\boldsymbol{(iia) \Leftrightarrow (iiia).}$ Condition (iia) states that there is a unitary $w \in \mathcal{U}_d$ such that

$$w\mathcal{D}_d w^* = \mathcal{D}_d \quad \text{and} \quad w\mathcal{A}^*(\mathrm{X}_d)\, w^* = \mathcal{M}.$$

The first of these equalities holds if and only if the unitary matrix w is monomial, that is $w \in \mathcal{W}_d$ (cf. Lemma 1.2.5). Thus statement (iia) is equivalent to the existence of a monomial unitary $w \in \mathcal{W}_d$ obeying the identity

$$w\mathrm{F}_d\mathcal{D}_d\mathrm{F}_d^* w^* = u\mathcal{D}_d u^*,$$

which is given precisely if $u^* w \mathrm{F}_d$ equals a monomial unitary $w' \in \mathcal{W}_d$. It is straightforward that this applies if and only if u and F_d are equivalent Hadamard matrices.

$\boldsymbol{(iia) \Rightarrow (iv).}$ As we have observed before, condition (iia) is equivalent to the existence of a monomial unitary matrix $w \in \mathcal{W}_d$ satisfying the identity

$$\mathcal{M} = w\mathcal{A}^*(\mathrm{X}_d)\, w^*.$$

We define unitaries $v_0 = w\mathrm{Z}_d w^* \in \mathcal{D}_d$ and $v_1 = w\mathrm{X}_d w^* \in \mathcal{M}$. Clearly these matrices generate $\mathcal{D}_d$ and $\mathcal{M}$ respectively, and their first $d-1$ powers are trace-free. One readily verifies the commutation relation $\mathrm{Z}_d\mathrm{X}_d = \zeta_d \mathrm{X}_d\mathrm{Z}_d$ and thus $v_0v_1 = \zeta_d v_1 v_0$.

$\boldsymbol{(iv) \Rightarrow (va).}$ The commutation relation (2.8) can be expressed in the form

$$v_0 = \omega v_1 v_0 v_1^*.$$

As v_0 generates $\mathcal{D}_d$, this shows $v_1\mathcal{D}_d v_1^* = \mathcal{D}_d$. Multiplying the equation above by v_1^* from the left yields the commutation relation $v_1^* v_0 = \omega v_0 v_1^*$. From this and the property $\tau(ab) = \tau(ba)$ of the trace, we deduce

$$\begin{aligned}
\left(v_0^i \,\middle|\, v_1^j\right)_{\mathrm{HS}} &= \tau\left(v_0^i\,(v_1^*)^j\right) = \bar{\omega}^i \tau\left(v_1^* v_0^i\,(v_1^*)^{j-1}\right) \\
&= \bar{\omega}^i \tau\left(v_0^i\,(v_1^*)^j\right)
\end{aligned}$$

for all $0 \leq i, j < d$. Since ω is primitive, the scalar product $(v_0^i | v_1^j)$ is thereby zero if $i \neq 0$. Otherwise it is zero for all $j \neq 0$ since the powers $v_1, \ldots, v_1^{d-1}$ are trace-free. This proves that $\mathcal{D}_d$ and $\mathcal{M}$ are quasi-orthogonal. (In just the same way—exchanging the roles of v_0 and v_1—one shows that (vi) implies (vb).)

$\boldsymbol{(va) \Rightarrow (iiia)}$**.** First note that due to the quasi-orthogonality of $\mathcal{D}_d$ and $\mathcal{M} = u\mathcal{D}_d u^*$, the unitary u is a Hadamard matrix, say $u = \sqrt{1/d}(\mu_{i,j})_{0 \leq i,j \leq d}$ for elements $\mu_{i,j} \in \mathbb{T}$. Since the unitary v_1 lies in $\mathcal{M}$, there is a diagonal unitary matrix $w \in \mathcal{W}_d$ such that $v_1 = uwu^*$ and hence

$$u = v_1 u w^*. \tag{2.9}$$

We further know from $v_1 \mathcal{D}_d v_1^* = \mathcal{D}_d$ that v_1 is monomial. Say v_1 and w act on the standard orthonormal basis $\mathfrak{e}$ by

$$v_1\, z_i = \lambda_i z_{\sigma(i)} \quad \text{and} \quad w\, z_i = \nu_i z_i$$

for a permutation $\sigma \in S_d$ and weights $\lambda_0, \ldots, \lambda_{d-1}, \nu_0, \ldots, \nu_{d-1} \in \mathbb{T}$.

Let $\mathfrak{x} = (x_0, \ldots, x_{d-1})$ denote the orthonormal basis of $\mathbb{C}^d$ given by the columns of the unitary Hadamard matrix u. Then equation (2.9) implies

$$x_j = u\, z_j = v_1 u w^*\, z_j = \bar{\nu}_j v_1 x_j \tag{2.10}$$

and thereby

$$\sum_{i=0}^{d-1} \mu_{i,j} z_i = \bar{\nu}_j \sum_{i=0}^{d-1} \mu_{i,j} \lambda_i z_{\sigma(i)}$$

for all $0 \leq j < d$. The last identity leads to $\mu_{\sigma(i),j} = \bar{\nu}_j \lambda_i \mu_{i,j}$ for each index pair (i, j). As we know that σ^d is the identity map, this results in

$$\mu_{i,j} = \mu_{\sigma^d(i),j} = \bar{\nu}_j \lambda_{\sigma^{d-1}(i)} \mu_{\sigma^{d-1}(i),j} = \ldots = (\bar{\nu}_j)^d \left(\prod_{k=0}^{d-1} \lambda_k \right) \mu_{i,j} \text{ and thus } \nu_j^d = \prod_{k=0}^{d-1} \lambda_k$$

for all $0 \leq j < d$. Combining this result with equation (2.10) above, we see that v_1^d equals the unit matrix up to a phase factor. Without loss of generality, we can assume $v_1^d = \mathrm{I}_d$. Then all spectral values of v_1 are dth roots of unity, and since v_1 generates the masa $\mathcal{M}$, the spectrum must contain d different points. We thus end up with the spectrum

$$\operatorname{sp}(v_1) = \{1, \zeta_d, \ldots, \zeta_d^{d-1}\}.$$

It is then straightforward that there is a monomial unitary $w' \in \mathcal{W}_d$ such that

$$v_1 = w' \mathrm{Z}_d w'^*.$$

We define $u' = w'^* u w'$ and apply equation (2.9) to obtain the following equivalences.

$$w' \mathrm{Z}_d w'^* u = v_1 u = uw \quad \Rightarrow \quad \mathrm{Z}_d w'^* u w' = w'^* u w w' \quad \Rightarrow \quad \mathrm{Z}_d u' = u' \underbrace{w'^* w w'}_{\in \mathcal{W}_d}$$

Now the Technical Lemma 2.4.6 tells us that the Hadamard matrix u' and hence u is equivalent to the unitary Fourier matrix F_d.
$(\boldsymbol{iia}) \Rightarrow (\boldsymbol{via})$. Applying the *-automorphism ϕ^{-1}, we can assume $\mathcal{M} = \mathcal{A}^*(\mathrm{X}_d)$. First recall the identity $\mathcal{W}(\mathcal{D}_d, \mathcal{A}^*(\mathrm{X}_d)) = \mathcal{A}^*(\mathrm{X}_d) \cap \mathcal{W}_d$ mentioned directly before this proposition. Consider some unitary element

$$v = \sum_{i=0}^{d-1} \lambda_i \mathrm{X}_d^i \in \mathcal{M}.$$

A look at the action of v on the standard orthonormal basis $\mathfrak{e}$ reveals that such an element is monomial if and only if *exactly one* of the coefficients $\lambda_0, \ldots, \lambda_{d-1} \in \mathbb{C}$ is non-zero (and thereby of modulus one). Consequently, the monomial unitaries in $\mathcal{M}$ are precisely the elements of the subgroup

$$\left\{ \mu \mathrm{X}_d^i \;\middle|\; \mu \in \mathbb{T}, 0 \leq i < d \right\}.$$

It is straightforward that the quotient of this subgroup by $\mathbb{T} \cdot \mathrm{I}_d$ is isomorphic to the cyclic group $\mathbb{Z}/d$.
$(\boldsymbol{via}) \Rightarrow (\boldsymbol{va})$. Let $v_1 \in \mathcal{M} \cap \mathcal{W}_d$ represent a generator of $\mathcal{W}(\mathcal{D}_d, \mathcal{M})/\mathbb{T} \cong \mathbb{Z}/d$. We can assume without loss of generality that v_1^d is the unit matrix. We have $v_1 \mathcal{D}_d v_1^* = \mathcal{D}_d$ by definition of v_1, so we only need to show that v_1 *generates* the masa $\mathcal{M}$. Since v_1 is a monomial unitary, it acts on the standard orthonormal basis $\mathfrak{e}$ by $v_1 z_i = \lambda_i z_{\sigma(i)}$ for a permutation $\sigma \in S_d$ and weights $\lambda_0, \ldots, \lambda_{d-1} \in \mathbb{T}$. In order to prove that v_1 generates $\mathcal{M}$, it suffices to show that the permutation σ is *cyclic.* It is then straightforward to check that the powers $\mathrm{I}_d, v_1, \ldots, v_1^{d-1}$ are pairwise Hilbert-Schmidt orthogonal and hence span the masa $\mathcal{M}$.

For a moment, suppose σ is *not* cyclic. Then it has a proper subcycle

$$i_0 \to \sigma(i_0) \to \sigma^2(i_0) \to \ldots \to \sigma^a(i_0) = i_0$$

of length $1 \leq a < d$, having no sub-subcycles, that is $\sigma^m(i_0) \neq i_0$ for all $0 < m < a$ ($i_0 \in \{0, \ldots, d-1\}$). Moreover, σ also performs a permutation on the $d - a$ points not lying on this subcycle, whose order $r \in \mathbb{N}$ thus divides $d - a$ and, since we have $\sigma^d = \mathrm{id}$, also d. Accordingly, there are factors $s, t \in \mathbb{N}$ such that $rs = d - a$ and $rt = d$. Subtracting the first from the second equation, we see that a is a multiple of r, leading to the identity $\sigma^a = \mathrm{id}$. For this reason, v_1^a is then a diagonal matrix. Now a conjugation by a diagonal matrix induces a trivial action on the masa $\mathcal{D}_d$, and so this immediately implies the isomorphism

$$\mathcal{W}(\mathcal{D}_d, \mathcal{M}) \,/\, (\mathbb{T} \cdot \mathrm{I}_d) \cong \mathbb{Z}/a,$$

contradicting condition (via).

By now we have verified all implications on the left-hand side of the scheme at the beginning of this proof. The missing implications on the right-hand side easily follow from what we have already shown, by applying the unitary conjugation $a \mapsto u^*au$, $a \in M_d(\mathbb{C})$. For the implication $(vib) \Rightarrow (vb)$ for instance, first apply the conjugation $u^* \cdot u$, then use implication $(via) \Rightarrow (va)$, replacing $\mathcal{M}$ by $\mathcal{M}' = u^*\mathcal{D}_d u$, finally re-conjugate by $u \cdot u^*$. The other missing implications are checked similarly. □

Condition (vi) of the previous theorem can be found in S. Popa's article [83], and items (via) and (vib) respectively have been formulated by A. Munemasa and Y. Watatani in [76], using a result from [31]. However, our techniques to prove the equivalences $(i) \Leftrightarrow (vi) \Leftrightarrow (via)$ are at some points different from the ones used in the mentioned papers. Our result concerning the implication $(via) \Rightarrow (i)$ is slightly stronger, for the authors of the paper [31] presume the quasi-orthogonality of the pair of masas considered for this implication.

As we will see in the next section, items (va) and (vb) respectively link standard pairs of masas to the subject of *C^*-dynamical systems* and thereby to *crossed products of C^*-algebras.* For now, we will focus on the question whether and in which dimensions there are non-standard pairs of quasi-orthogonal masas. You will not find examples in the smallest dimensions.

Observation 2.4.8. All pairs of quasi-orthogonal masas in $M_2(\mathbb{C})$ and $M_3(\mathbb{C})$ are standard pairs.

Proof. Let $\{\mathcal{D}_2, \mathcal{M}_{[u]}\}$ be a pair of quasi-orthogonal masas in $M_2(\mathbb{C})$ and define a unitary $v = u\sigma_z\, u^* \in \mathcal{M}$. (Then $\{v, \mathrm{I}_2\}$ is the basis $u\,\mathfrak{w}_2\,u^*$ of $\mathcal{M}_{[u]}$ as defined in Proposition 1.4.3.) The matrix v is obviously trace-free. Therefore Corollary 2.2.15 applies, so all diagonal elements of v are zero. In other words, the masa $\mathcal{M}$ is generated by a unitary monomial matrix, hence condition (va) of Theorem 2.4.7 is fulfilled and $\{\mathcal{D}_2, \mathcal{M}_{[u]}\}$ is a standard pair.

Now consider a quasi-orthogonal masa pair $\{\mathcal{D}_3, \mathcal{M}_{[u']}\}$ in $M_3(\mathbb{C})$, equipped with the product orthonormal basis $u'\,\mathfrak{w}_2\,u'^* = \{v', v'^2, \mathrm{I}_3\}$. As above, we know from Corollary 2.2.15 that all diagonal elements of v' are zero, so we can write

$$v' = \begin{pmatrix} 0 & \nu_{01} & \nu_{02} \\ \nu_{10} & 0 & \nu_{12} \\ \nu_{20} & \nu_{21} & 0 \end{pmatrix}$$

for certain complex entries $v_{ij} \in \mathbb{C}$. By the same argument, the diagonal elements of $(v')^2$ are zero. A calculation reveals that this asserts

$$\nu_{01}\nu_{10} = \nu_{02}\nu_{20} = \nu_{12}\nu_{21} = 0.$$

First suppose that ν_{01} equals zero. Then we get $\nu_{02} \neq 0$ and $\nu_{21} \neq 0$ since v' is unitary. The last equation then implies $\nu_{20} = \nu_{12} = 0$, hence v' is a monomial matrix in this case. A similar argumentation shows that v' is monomial as well if ν_{01} is not zero. As in the case of $M_2(\mathbb{C})$, condition (va) of Theorem 2.4.7 now ensures that the pair $\{\mathcal{D}_3, \mathcal{M}_{[u']}\}$ is standard. □

The smallest examples of non-standard quasi-orthogonal masa pairs occur in the complex 4×4-matrices.

Example 2.4.9. Let $\mathcal{M} \subset M_4(\mathbb{C})$ be the *-subalgebra generated by the unitary monomials

$$v_0 = \mathrm{I}_2 \otimes \sigma_x = \begin{pmatrix} 0 & \mathrm{I}_2 \\ \mathrm{I}_2 & 0 \end{pmatrix} \quad \text{and} \quad v_1 = \sigma_x \otimes \mathrm{I}_2 = \begin{pmatrix} \sigma_x & 0 \\ 0 & \sigma_x \end{pmatrix}$$

Then $\mathcal{M}$ is a masa and the pair $\{\mathcal{D}_4, \mathcal{M}\}$ forms a non-standard pair of quasi-orthogonal masas.

Proof. The generators v_0 and v_1 commute, and since both v_0 and v_1 are self-adjoint and their squares are the unit matrix, the *-algebra $\mathcal{A}^*(v_0, v_1)$ is linearly spanned by v_0, v_1, v_0v_1 and I_4. It presents no difficulty to verify that these elements are pairwise quasi-orthogonal, whence $\mathcal{M}$ is a masa. It is moreover straightforward that a linear combination

$$\lambda_0 v_0 + \lambda_1 v_1 + \lambda_2 v_0 v_1 + \lambda_3 \mathrm{I}_4$$

of the matrices above is monomial if and only if precisely one of the complex coefficients $\lambda_0, \ldots, \lambda_3 \in \mathbb{C}$ is non-zero. As each of the matrices v_0, v_1 and v_0v_1 generates only a two-dimensional subspace of $\mathcal{M}$, the latter cannot be generated by a *single* monomial matrix. This contradicts item (va) of Theorem 2.4.7, so $\mathcal{D}_d$ and $\mathcal{M}$ do not form a standard pair. □

Uffe Haagerup demonstrated in [44] that there are in fact uncountably many inequivalent non-standard pairs $\{\mathcal{D}_d, \mathcal{M}\}$ of quasi-orthogonal masas whenever the dimension d is not prime. We cite this result in the next proposition, and shortly sketch our own proof—which is slightly different from Haagerup's, but boils down to same idea—in the Appendix.

Proposition 2.4.10 (Haagerup 1996). *Let $d \in \mathbb{N}$ be the product of two non-trivial factors $a, b \in \mathbb{N}$. Then there are uncountably many pairwise inequivalent pairs of quasi-orthogonal masas in the matrix algebra $M_d(\mathbb{C})$. Accordingly, uncountably many of these pairs are* non-standard.

A sketch of the proof is provided in the Appendix on pages 216-217. $\triangleright$

At this point, one may be tempted to guess that all pairs of quasi-orthogonal masas are standard in prime dimensions. This had in fact been a long-standing conjecture, brought forward by Popa in [83]. However, it turned out to be false.

- In 1990, P. de la Harpe and V. Jones constructed non-standard pairs of quasi-orthogonal masas for all dimensions $d \geq 7$, $d \equiv 1 \mod 4$ ([31]), borrowing techniques from the area of the so-called *strongly regular graphs* to this aim.
- Using similar techniques, Munemasa and Watatani ([76]) showed in 1992 that there are non-standard pairs of quasi-orthogonal masas in all dimensions $d \geq 7$, $d \equiv 3 \mod 4$.

After these results had been established, the only dimension where the existence of non-standard pairs remained unclear was $d = 5$. This gap was filled by Haagerup in 1996, when he proved, using elementary but extraordinarily extensive computations, that all quasi-orthogonal pairs in $M_5(\mathbb{C})$ are standard (see [44]). We recapitulate the results above, including Observation 2.4.8 and Proposition 2.4.10, in the following

Fact 2.4.11. All pairs of quasi-orthogonal masas in $M_2(\mathbb{C})$, $M_3(\mathbb{C})$ and $M_5(\mathbb{C})$ are standard. In all other dimensions, there are non-standard pairs of quasi-orthogonal masas.

2.5 *Excursion:* Standard pairs of masas and crossed products

In short, a crossed product C*-algebra $\mathcal{A} \rtimes G$ is built out of a C*-algebra $\mathcal{A}$ and a locally compact group G acting on $\mathcal{A}$. One of the most elementary examples is the crossed product C*-algebra $C^*(\mathbb{Z}/d) \rtimes \mathbb{Z}/d$ of the group C*-algebra $C^*(\mathbb{Z}/d)$ by the cyclic group $\mathbb{Z}/d$, which is—provided the group action is *injective*—isomorphic to the matrix algebra $M_d(\mathbb{C})$.

We have seen in Theorem 2.4.7 that a standard pair of masas in $M_d(\mathbb{C})$ "models" an action of $\mathbb{Z}/d$ on the diagonal masa $\mathcal{D}_d$, and this fact links standard masa pairs to the topic of crossed products. In the present section, we outline the connection between a canonical matrix representation of the group C*-algebra $C^*(\mathbb{Z}/d)$ and the crossed product $C^*(\mathbb{Z}/d) \rtimes \mathbb{Z}/d$ on the one hand, and the standard masa pair $\{\mathcal{D}_d, \mathcal{A}^*(\chi_d)\}$, investigated in the previous section, on the other.

It is understood that our introduction of the basic ingredients, namely the group C*-algebra $C^*(\mathbb{Z}/d)$, its GNS-representation, C*-dynamical systems, and (C*-algebraic) crossed products, must be very rough. Many introductory textbooks on C*-algebras (see e.g. [15] or [77]) cover these topics. For a special introduction to crossed products, see for instance the book [111] by Dana P. Williams. Definition 2.5.1 and Propositions 2.5.2 and 2.5.3 are adoptions from this textbook.

A very short introduction to crossed products

A *C^*-algebra$\mathcal{A}$* is an involutive complex algebra endowed with a submultiplicative norm $\|\cdot\|$ and complete w.r.t. the latter (i.e. a *Banach algebra*), that moreover satisfies the *C^*-condition*, that is

$$\|a^*a\| = \|a\|^2 \quad \text{for all} \quad a \in \mathcal{A}.$$

Conversely, any norm on a *-algebra obeying this condition is called *C^*-norm.* For instance, the matrix algebra $M_d(\mathbb{C})$, endowed with the standard involution and matrix norm, is a C*-algebra. More general, the set of bounded linear operators on any Hilbert space is a C*-algebra.

A *group action* of a (locally compact) group G on a C*-algebra $\mathcal{A}$ is a continuous group homomorphism $\alpha : G \to \operatorname{Aut} \mathcal{A}$, $i \mapsto \alpha_i$. The triple $(\mathcal{A}, G, \alpha)$ is called a *C^*-dynamical system*. The basic idea behind the concept of *crossed product C^*-algebras* is to make the *-automorphisms $\alpha(G) \subset \operatorname{Aut} \mathcal{A}$ of a dynamical system *inner,* that is to construct a C*-algebra containing both a copy of $\mathcal{A}$ and unitaries $\{u_i \mid i \in G\}$ such that the action α is implemented by the identity $\alpha_i(a) = u_i a u_i^*$ for all $a \in \mathcal{A}$. (To be precise, this generally applies only for the *multiplier algebra* of the crossed product $\mathcal{A} \rtimes G$, but this shall not bother us here.)

For the rest of this section, we consider a dynamical system $(\mathcal{A}, G, \alpha)$ with a *finite abelian* group G to keep things easy. Furthermore, let H be a separable complex Hilbert space and $\mathcal{B}(H)$ the C*-algebra of bounded linear operators on H. We only need a few ingredients to construct the crossed product $\mathcal{A} \rtimes_\alpha G$. Let us start with a so-called covariant representation.

Definition 2.5.1. *A* covariant representation *of a dynamical system $(\mathcal{A}, G, \alpha)$ is a pair (π, u) consisting of a *-representation $\pi : \mathcal{A} \to \mathcal{B}(H)$ and a unitary group representation $u : G \to \mathcal{U}(H)$, $i \mapsto u_i$, such that the "covariance relation"*

$$\pi(\alpha_i(a)) = u_i \pi(a) u_i^*$$

holds for all $i \in G$ and $a \in \mathcal{A}$.

The crossed product also involves the *-algebra $\mathcal{C}(G, \mathcal{A})$ of continuous functions from G to $\mathcal{A}$. One defines a convolution product and an involution for $\mathcal{C}(G, \mathcal{A})$ similarly as for the convolution algebra $L^1(G)$, but "twisted" by the automorphism α, that is one sets

$$f * g(i) = \sum_{j \in G} f(j) \alpha_j (g(i-j)) \quad \text{and} \quad f^*(i) = \alpha_i (f(-i)) \tag{2.11}$$

for all elements $i \in G$ and functions $f, g \in \mathcal{C}(G, \mathcal{A})$. A norm on $\mathcal{C}(G, \mathcal{A})$ is given by $\|f\|_1 = \sum_{i \in G} \|f(i)\|$, where $\|\cdot\|$ is the C*-norm on $\mathcal{A}$. For every covariant representation (π, u) of G, there is an associated *-representation of $\mathcal{C}(G, \mathcal{A})$.

Proposition 2.5.2. *If (π, u) is a covariant representation of a C*-dynamical system $(\mathcal{A}, G, \alpha)$ on the Hilbert space H, then the mapping*

$$\begin{aligned} \pi \rtimes u : \mathcal{C}(G, \mathcal{A}) &\longrightarrow \mathcal{B}(H), \\ f \quad &\longmapsto \sum_{i \in G} \pi\left(f(i)\right) u_i \end{aligned}$$

defines a *-representation of $\mathcal{C}(G, \mathcal{A})$, which is norm decreasing with respect to the L^1-norm $\|\cdot\|_1$ on $\mathcal{C}(G, \mathcal{A})$ and the operator norm on $\mathcal{B}(H)$. We call $\pi \rtimes u$ the integrated form *of the representation (π, u).*

We have now collected all ingredients to define the crossed product $\mathcal{A} \rtimes_\alpha G$.

Proposition 2.5.3. *Let $(\mathcal{A}, G, \alpha)$ be a dynamical system and endow the function algebra $\mathcal{C}(G, \mathcal{A})$ with the twisted multiplication and involution introduced in equations* (2.11). *To each function $f \in \mathcal{C}(G, \mathcal{A})$, we assign a non-negative real number by setting*

$$\|f\| = \sup\left\{ \|\pi \rtimes u(f)\| \mid (\pi, u) \text{ covariant representation of } (\mathcal{A}, G, \alpha) \right\}.$$

This assignment defines a C*-norm on the *-algebra $\mathcal{C}(G, \mathcal{A})$, called the universal norm. *The completion of $\mathcal{C}(G, \mathcal{A})$ with respect to the universal norm is a C*-algebra, the so-called* crossed product of $\mathcal{A}$ by G, *denoted by $\mathcal{A} \rtimes_\alpha G$.*

Certainly, the propositions above contain a lot of explicit and implicit assertions in need of further remarks and proofs. However, this is not our business here. We refer to [111] for the details.

The GNS-representation of the group C*-algebra $C^*(\mathbb{Z}/d)$

For a general locally compact group G, the group C*-algebra $C^*(G)$ is defined as the completion of the convolution algebra $L^1(G)$ with respect to the so-called universal C*-norm (defined similarly as in Proposition 2.5.3). If G happens to be discrete and finite, this completion is trivial, and moreoever the algebra $L^1(G)$ coincides with the ordinary group algebra $\mathbb{C}[G]$. On the whole, we thus have the identities

$$C^*(G) = L^1(G) = \mathbb{C}[G].$$

The C*-algebra $C^*(G)$ is endowed with the convolution product

$$f * g(i) = \sum_{j \in G} f(j) g(i - j)$$

and the pointwise involution $f^*(i) = \overline{f(-i)}$ for all $i \in G$ and $f, g \in L^1(G)$.

Our next goal is to establish an isomorphic representation of $C^*(\mathbb{Z}/d)$ as an algebra of operators on a Hilbert space. The well-known GNS-construction offers a canonical way to find such (irreducible and isomorphic) *-representations of C*-algebras. We omit the details of this technique, which is based on *states* on C*-algebras (see for instance [77, section 3.4]), and simply present the resulting *-representation instead.

Following the lines of the GNS-construction for the C*-algebra $C^*(\mathbb{Z}/d)$, one first takes the set of L^2-functions on $\mathbb{Z}/d$ as Hilbert space H_0 for the desired representation. This is once more the set of mappings $\{f : \mathbb{Z}/d \to \mathbb{C}\}$, but this time equipped with a scalar product given by

$$(f \,|\, g) = (f * g^*)(0)$$

and an associated L^2-norm

$$\|f\|_2 = \sqrt{(f * f^*)(0)}$$

for all functions $f, g \in H_0 = L^2(\mathbb{Z}/d)$.

A faithful (i.e. injective) *-representation of $C^*(\mathbb{Z}/d)$ as *-subalgebra of linear operators on H_0 is then given by

$$\begin{aligned} \pi_0 : C^*(\mathbb{Z}/d) &\longrightarrow \mathcal{B}(H_0), \\ f \quad &\longmapsto \pi_0(f), \;\; \pi_0(f)\,g = f * g \;\text{ for all } g \in H_0. \end{aligned}$$

The Hilbert space H_0 being isomorphic to $\mathbb{C}^d$, the image of the representation π_0 can be considered as a *-subalgebra of the complex $d \times d$-matrices. Since the group C*-algebra $C^*(\mathbb{Z}/d)$ is abelian and of dimension d, the image $\pi_0(C^*(\mathbb{Z}/d))$ moreover is a d-dimensional abelian *-subalgebra, hence a masa in $M_d(\mathbb{C})$. You may agree that a representation of $C^*(\mathbb{Z}/d)$ as diagonal matrices would be a natural choice.

The characteristic functions $\delta_0, \dots, \delta_{d-1} \in L^2(\mathbb{Z}/d)$, given by

$$\delta_i(j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{else,} \end{cases}$$

form an orthonormal basis of H_0, and one might at first be tempted to identify this basis with the standard orthonormal basis $\mathfrak{e} = (z_0, \dots, z_{d-1})$ of $\mathbb{C}^d$. However, it turns out that the image of π_0 is *not* the diagonal masa under this choice. To achieve this goal, one has to choose as orthonormal basis of H_0 the *dual* basis to the one above, given by the elements

$$\tilde{z}_i = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \zeta_d^{-ij} \delta_j$$

for all indices $0 \le i < d$, and identify H_0 and $\mathbb{C}^d$ via the assignment $\tilde{z}_i \mapsto z_i$.

Clearly the basis elements $\tilde{z}_i$ serve as generators of the C*-algebra $C^*(\mathbb{Z}/d)$ as well, where we renormalise them w.r.t. the L^1-norm to $\tilde{q}_i = \sqrt{1/d}\,\tilde{z}_i$. An explicit computation reveals that the elements $\tilde{q}, \dots, \tilde{q}_{d-1}$ are pairwise orthogonal minimal *projections.* The action of an operator $\pi_0(\tilde{q}_i)$ on a basis vector $\tilde{z}_j$ computes to

$$\pi_0(\tilde{q}_i)\,\tilde{z}_j(m) = \frac{1}{\sqrt{d}}\tilde{z}_i * \tilde{z}_j\,(m) = \dots = \begin{cases} \frac{1}{\sqrt{d}}\zeta_d^{-jm} = \tilde{z}_j(m) & \text{if } i = j, \\ 0 & \text{else} \end{cases}$$

for all $i, j, m \in \mathbb{Z}/d$, so that we end up with

$$\pi_0(\tilde{q}_i)\,\tilde{z}_j = \begin{cases} \tilde{z}_j & \text{if } i = j, \\ 0 & \text{else.} \end{cases}$$

This shows that the C*-algebra $C^*(\mathbb{Z}/d)$ is mapped to the diagonal masa $\mathcal{D}_d$ in the chosen matrix representation. Moreover, we have identified the generating minimal projections q_i of the diagonal masa and $\tilde{q}_i$ of $C^*(\mathbb{Z}/d)$ for all $0 \le i < d$.

At last, let us compute the image of the canonical generator $\delta_1 \in C^*(\mathbb{Z}/d)$ under the *-representation π_0.

$$\pi_0(\delta_1)\,\tilde{z}_i(m) = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\zeta_d^{-ij}\,\underbrace{\delta_1 * \delta_j(m)}_{=\delta_{j+1}(m)} = \zeta_d^i \tilde{z}_i(m) \;\text{ for all } i, m \in \mathbb{Z}/d$$

$$\Rightarrow \quad \pi_0(\delta_1) = \mathrm{Z}_d$$

(Recall that $\mathrm{Z}_d \in \mathcal{D}_d$ denotes the clock matrix introduced in Example 1.4.2.)

The crossed product $C^*(\mathbb{Z}/d) \rtimes \mathbb{Z}/d$

Now let us consider a group action $\alpha : \mathbb{Z}/d \to \operatorname{Aut} C^*(\mathbb{Z}/d)$ which is *injective,* so that the subgroup $\alpha(\mathbb{Z}/d) \subset \operatorname{Aut} C^*(\mathbb{Z}/d)$ is isomorphic to $\mathbb{Z}/d$.

As we have observed in Section 1.2 (see Lemma 1.2.5 and Remark 1.2.6), the *-automorphisms of the masa $\mathcal{D}_d$ correspond to permutations of the minimal projections q_i, and this clearly carries over to $C^*(\mathbb{Z}/d)$. As a consequence, the action of the automorphism $\alpha_1 = \alpha(1)$ is defined by the formula $\alpha_1(\tilde{q}_i) = \tilde{q}_{\sigma(i)}$ for a permutation $\sigma \in S_d$.

By the injectivity of the action α, the group of automorphisms $\alpha(\mathbb{Z}/d)$ is of order d. Since this group is generated by α_1, the permutation σ must be *cyclic,* for otherwise the order of α_1 would be *less* than d. (A short argument for this last statement can be found in the proof of Theorem 2.4.7, implication $(via) \Rightarrow (va)$.) Possibly after a renumeration of the generators, we can assume $\sigma(i) = i + 1 \mod d$ for all $i \in \mathbb{Z}/d$.

For a general function $f \in C^*(\mathbb{Z}/d)$, the action of α_1 is then given by the formula

$$(\alpha_1 f)(i) = f(i-1) \;\text{ for all }\; i \in \mathbb{Z}/d. \tag{2.12}$$

According to Proposition 2.5.3, the crossed product $C^*(\mathbb{Z}/d) \rtimes_\alpha \mathbb{Z}/d$ equals the *-algebra $\mathcal{C}(\mathbb{Z}/d, C^*(\mathbb{Z}/d))$ (equipped with the universal C*-norm), because no completion is necessary in this finite-dimensional situation. We express the elements in $\mathcal{C}(\mathbb{Z}/d, C^*(\mathbb{Z}/d))$ as d-tuples of functions in $C^*(\mathbb{Z}/d)$, and embed the latter as follows.

$$\begin{aligned} C^*(\mathbb{Z}/d) &\overset{\iota}{\hookrightarrow} \mathcal{C}(\mathbb{Z}/d, C^*(\mathbb{Z}/d)) \\ f \quad &\longmapsto (f, 0, \dots, 0) \end{aligned}$$

The crossed product contains a unitary making the *-automorphism α inner, namely $u = (0, \delta_0, 0, \dots, 0)$. In fact, the conjugation $u \cdot u^*$ on the embedding $\iota(C^*(\mathbb{Z}/d))$ computes to

$$\begin{aligned} &(0, \delta_0, 0, \dots, 0) * (\tilde{q}_i, 0, \dots, 0) * (0, \delta_0, 0, \dots, 0)^* \\ &\quad = (0, \underbrace{\delta_0 * \alpha_1(\tilde{q}_i)}_{=\tilde{q}_{i+1}}, 0, \dots, 0) * (0, \dots, 0, \delta_0) = (\tilde{q}_{i+1}, 0, \dots, 0). \end{aligned}$$

We define an injective unitary representation $u : \mathbb{Z}/d \to \mathcal{U}_d$ by setting $u_i = \mathrm{X}_d^i$, where X_d denotes the shift matrix introduced on page 30. Then (π_0, u) is a covariant representation of the C*-dynamical system $(C^*(\mathbb{Z}/d), \mathbb{Z}/d, \alpha)$, since the covariance relation is satisfied (cf. Definition 2.5.1): for all $i, j \in \mathbb{Z}/d$, one computes

$$\pi_0\left(\alpha_j\left(\tilde{q}_i\right)\right) = \pi_0\left(\tilde{q}_{i+j}\right) = q_{i+j} = \mathrm{X}_d^j \, q_i \, \mathrm{X}_d^{-j} = u_j \, \pi_0(\tilde{q}_i) \, u_j^*.$$

The integrated form of (π_0, u) maps the crossed product $C^*(\mathbb{Z}/d) \rtimes_\alpha \mathbb{Z}/d$ to the matrix algebra $M_d(\mathbb{C})$ as follows.

$$\begin{aligned} \pi_0 \rtimes u : C^*(\mathbb{Z}/d) \rtimes_\alpha \mathbb{Z}/d &\longrightarrow M_d(\mathbb{C}) \\ (f_0, \dots, f_{d-1}) &\longmapsto \sum_{i \in \mathbb{Z}/d} \pi_0\left(f(i)\right) \mathrm{X}_d^i \end{aligned} \tag{2.13}$$

Obviously, the dimension of the crossed product $C^*(\mathbb{Z}/d) \rtimes_\alpha \mathbb{Z}/d$ equals d^2. In order to prove that the *-representation $\pi_0 \rtimes u$ is an isomorphism, it therefore suffices to check its surjectivity. To this aim, we combine the identity $\pi_0(\delta_1) = \mathrm{Z}_d$, computed at the end of the previous subsection, with the action of the integrated form $\pi_0 \rtimes u$. We thereby obtain the equalities

$$\pi_0 \rtimes u(0, \dots, 0, \underbrace{\delta_1 * \dots * \delta_1}_{j \text{ foldings, } i\text{th pos.}}, 0, \dots, 0) = \mathrm{Z}_d^j \mathrm{X}_d^i$$

for all $0 \leq i, j < d$, and we have convinced ourselves in Example 2.2.16 that the monomials on the right-hand side span the whole matrix algebra $M_d(\mathbb{C})$.

As a remark, recall that *-isomorphisms between C*-algebras are automatically *isometric,* that is we have $\|\pi_0 \rtimes u(a)\| = \|a\|$ for all elements $a \in C^*(\mathbb{Z}/d) \rtimes_\alpha \mathbb{Z}/d$.

Summary 2.5.4 (A canonical representation of the crossed product $C^*(\mathbb{Z}/d) \rtimes \mathbb{Z}/d$)**.** We use the notations introduced in this section. Consider the C*-dynamical system $(C^*(\mathbb{Z}/d), \mathbb{Z}/d, \alpha)$, where

$$\alpha : \mathbb{Z}/d \longrightarrow \mathrm{Aut}\left(C^*(\mathbb{Z}/d)\right)$$

is an injective group action, so that w.l.o.g., α_1 is the cyclic shift on the minimal projections $\tilde{q}_0, \dots, \tilde{q}_{d-1} \in C^*(\mathbb{Z}/d)$. As before, denote

- the standard GNS-representation $\pi_0 : C^*(\mathbb{Z}/d) \to M_d(\mathbb{C})$,
- the unitary $u = (0, \delta_0, 0, \dots, 0) \in C^*(\mathbb{Z}/d) \rtimes_\alpha \mathbb{Z}/d$, and
- the unitary *-representation $u : \mathbb{Z}/d \to \mathcal{U}_d$, defined by $u_i = \mathrm{X}_d^i$ for $i \in \mathbb{Z}/d$.

Then the *-automorphism α_1 is represented by conjugation with the unitary u inside the crossed product $C^*(\mathbb{Z}/d) \rtimes_\alpha \mathbb{Z}/d$. Moreover, the pair (π_0, u) is a covariant representation of the dynamical system $(C^*(\mathbb{Z}/d), \mathbb{Z}/d, \alpha)$, the associated integrated form $\pi_0 \rtimes u$ is an isomorphic *-representation, and the following diagram commutes.

$$\begin{tikzcd}
\alpha_1(f) \arrow[rrrrr, mapsto] \arrow[ddd, mapsto] & & & & & u * (f, 0, \dots, 0) * u^* \arrow[ddd, mapsto] \\
& \delta_1 \arrow[d, mapsto] & C^*\left(\mathbb{Z}/d\right) \arrow[r, hook, "\iota"] \arrow[d, "\pi_0"', "\cong"] & C^*\left(\mathbb{Z}/d\right) \rtimes_\alpha \mathbb{Z}/d \arrow[d, "\pi_0 \rtimes u"', "\cong"] & u \arrow[d, mapsto] & \\
& \mathrm{Z}_d & \mathcal{D}_d \arrow[r, hook, "\subset"] & M_d(\mathbb{C}) & \mathrm{X}_d & \\
\pi_0 \circ \alpha_1(f) \arrow[rrrrr, equal] & & & & & \mathrm{X}_d \pi_0(f) \mathrm{X}_d^*
\end{tikzcd}$$

Figure 2.3: *The crossed product $C^*(\mathbb{Z}/d) \rtimes \mathbb{Z}/d$*

Chapter 3

Families of pairwise quasi-orthogonal masas

This chapter is concerned with families of more than two pairwise quasi-orthogonal masas in the $d \times d$-matrices. As in the previous chapters, we start with a motivating section, outlining a central connection between so-called *complete* families of pairwise quasi-orthogonal masas and quantum physics.

In Section 3.2, we generalise the equivalence relation given for masa pairs in Section 2.4 to general families, and specify the mathematical notion of complete and maximal quasi-orthogonal masa families. We will present the basic facts known concerning this matter and a couple of open questions, among them the famous *MUB-problem*. Apart from that, we cite the standard construction of complete quasi-orthogonal masa families in prime dimensions and give examples of non-completable, inequivalent and non-standard quasi-orthogonal masa families.

Constructions of complete quasi-orthogonal masa families in general prime power dimensions are presented in Section 3.3. We conclude this chapter with an essentially different construction of quasi-orthogonal masa families which is known if the dimension is a square number (Section 3.4).

3.1 *Motivation:* Optimal state-determination of quantum systems

The density matrix

It is a deep philosophical question how to interpret the probabilistic nature of a single quantum mechanical measurement, as described in Section 1.1. This aspect is of course not addressed in this work, and there is no general consensus in the scientific community about it. Nevertheless, let us at least mention two interpretations of this (apparent) randomness which are commonly excluded. It does neither stem from statistical effects—i.e. the uncertainty of the outcome is inherent to *one single* physical system—, nor from an inability to perform exact measurements due to a lack of technical means or knowledge etc.

Anyway, what one observes in experimental contexts is almost never only one single quantum mechanical system. Normally physicists deal with so-called *statistical ensembles*, containing a large number of identical quantum systems (think e.g. of a flow of identical particles arriving at a detector in an accelerator). These systems are generally not in the same state, and this is what physicists call an ensemble in a *mixed state.* (By contrast, the state of one single system is said to be *pure.*) The overall state of the ensemble is described by a *density matrix*. In the sequel, we explain the concept of the density matrix by an easy example.

Suppose a large number of N identical d-dimensional quantum systems is prepared by a pre-measurement of an observable a, having a basis $\mathfrak{a} = (x_0, \dots, x_{d-1})$ of eigenstates in $\mathbb{C}_1^d$. For simplicity, let us think of N microscopic particles. Then for each $0 \leq i < d$, a number of n_i particles is prepared in an eigenstate x_i, where the numbers n_i clearly sum up to N. Afterwards, a detector measures a physical quantity corresponding to an observable b, with eigenstates $y_0, \dots, y_{d-1} \in \mathbb{C}_1^d$ and eigenvalues $\mu_0, \dots, \mu_{d-1} \in \mathbb{R}$. (As in Sections 1.1 and 2.1, we assume that the spectrum of the operator b is non-degenerated for simplicity.) Now the outcome of the second measurement is probabilistic in *two* ways. A particle arrives at measurement b in a state x_i with probability $\rho_i = {}^{n_i}/_N$ for $0 \leq i < d$, and then the probability of detecting a final state y_{j_0} (a value μ_{j_0} respectively) is given by $|(x_i|y_{j_0})|^2$ for all $0 \leq j_0 < d$. All in all, the probability to detect a final state y_{j_0} is given by

$$P(j_0) = \sum_{i=0}^{d-1} \rho_i \left| \left(x_i \,\middle|\, y_{j_0} \right) \right|^2 \tag{3.1}$$

for each $0 \leq j_0 < d$. It is straightforward that $P : \{0, \dots, d-1\} \to \mathbb{R}_0^+$ defines a probability measure. Figure 3.1 depicts the measurement of a mixed quantum state, prepared by a measurement of a. For clarity, we have added a virtual "filter" letting only pass particles in state y_0 after measurement b.

In this example, the density matrix (or density operator—recall that we always identify linear operators on $\mathbb{C}^d$ and the complex $d \times d$-matrices) of the ensemble after the pre-measurement a is given by

$$r = \sum_{i=0}^{d-1} \rho_i p_{x_i},$$

where $p_{x_i} \in M_d(\mathbb{C})$ is the ortho-projection onto the span of x_i for all $0 \leq i < d$. As you can easily check, the probability (3.1) of detecting a state y_{j_0} by measuring b is then

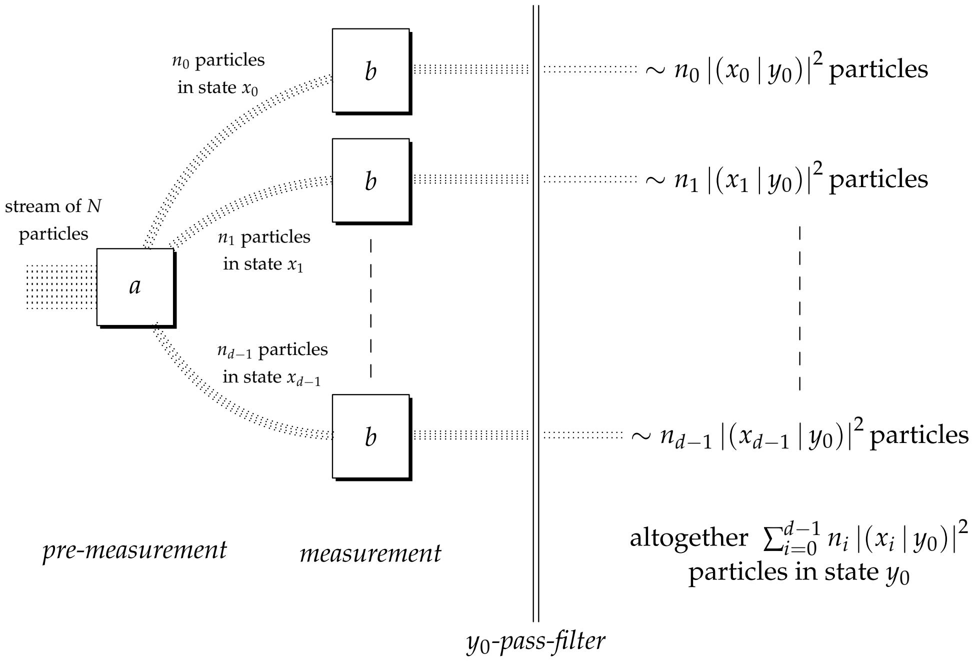

n_0 particles in state x_0
b
$\sim n_0 \, |(x_0 \,|\, y_0)|^2$ particles
b
$\sim n_1 \, |(x_1 \,|\, y_0)|^2$ particles
stream of N particles
a
n_1 particles in state x_1
n_{d-1} particles in state x_{d-1}
b
$\sim n_{d-1} \, |(x_{d-1} \,|\, y_0)|^2$ particles
pre-measurement
measurement
altogether $\sum_{i=0}^{d-1} n_i \, |(x_i \,|\, y_0)|^2$ particles in state y_0
y_0-pass-filter

Figure 3.1: *Measurements of mixed quantum states*

alternatively calculated by the formula

$$P(j_0) = \left(r\, y_{j_0} \,\middle|\, y_{j_0}\right). \tag{3.2}$$

The striking advantage of the concept of the density matrix is that the basis $\mathfrak{a}$ we have started with does no longer occur in equation (3.2). This gives rise to the following definition.

Definition 3.1.1. *A matrix $r \in M_d(\mathbb{C})$ is called* density matrix *if it is self-adjoint and positive semi-definite (that is, the spectrum is included in $\mathbb{R}_0^+$), and if moreover the (non-normalised) trace of r equals one.*

The trace condition $\mathrm{Tr}(r) = 1$ reflects that a density matrix describes a probability distribution. In actual experimental situations, the determination (or better to say *estimation,* see further below) of the density matrix is the best information one can hope for to describe the physical *behaviour* of the quantum mechanical ensemble. In general, its "inner reality" is inaccessible, as the following example illustrates.

Example 3.1.2. Let $\mathcal{A}$ and $\mathcal{B}$ denote two ensembles of a large number of N identical two-dimensional quantum systems. For a fixed orthonormal basis of states $z_0, z_1 \in \mathbb{C}^2$, suppose that one half of the particles of system $\mathcal{A}$ is in state z_0, the other half in state z_1. All particles of system $\mathcal{B}$, by contrast, are in the state $1/\sqrt{2}(z_0 + z_1)$. Then both ensembles have the same density operator, represented w.r.t. the orthonormal basis (z_0, z_1) by

$$r_{\mathcal{A}} = r_{\mathcal{B}} = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}.$$

Experimental determination of the density matrix

To determine the state of a quantum mechanical ensemble is to determine its density matrix. Surely this is a statistical task, so the actual goal is to *estimate* the density matrix (of the initial ensemble) which as much accuracy as possible.

The measurement of *one* observable on a large number of particles will surely not do the trick, for this will at least allow to determine d dimensions of the density matrix $r \in M_d(\mathbb{C})$. The measurement process must thus surely involve a number of different observables.

Let us start with the theoretical framework. In $M_d(\mathbb{C})$, consider m self-adjoint matrices $b_0, \ldots, b_{m-1} \in M_d(\mathbb{C})$ with non-degenerated spectra. For each $0 \leq k < m$, let

$$p_0^{(k)}, \ldots, p_{d-1}^{(k)} \in M_d(\mathbb{C})$$

be the minimal projections onto the eigenspaces of b_k, furthermore denote the masas

$$\mathcal{M}_k = \mathcal{A}^* \left(p_0^{(k)}, \ldots, p_{d-1}^{(k)} \right).$$

Since the real (that is to say self-adjoint) parts $\mathcal{M}_k^{(sa)} = \operatorname{span}_{\mathbb{R}}(p_0^{(k)}, \ldots, p_{d-1}^{(k)})$ of these masas overlap in $\mathbb{R} \cdot \mathrm{I}_d$, the dimension of the real space generated by them is at most $m(d-1)+1$. A necessary condition for this span to contain all self-adjoint matrices in $M_d(\mathbb{C})$ thereby is $m(d-1)+1 \geq d^2$ and thus $m \geq d+1$. From here on, we will assume $m = d+1$ as well as

$$\operatorname{span}_{\mathbb{R}} \left(\mathcal{M}_0^{(sa)}, \ldots, \mathcal{M}_d^{(sa)} \right) = M_d(\mathbb{C})^{(sa)}, \tag{3.3}$$

where $M_d(\mathbb{C})^{(sa)}$ is the real vector space of self-adjoint matrices inside $M_d(\mathbb{C})$.

Fix an orthonormal basis of matrices $\mathfrak{b}_k = (s_1^{(k)}, \ldots, s_{d-1}^{(k)})$ for each of the subspaces $\mathcal{M}_k^{(sa)} \ominus \mathbb{R}$. Then

$$\mathfrak{B} = \mathfrak{b}_0 \cup \ldots \cup \mathfrak{b}_d$$

is a basis for the (d^2-1)-dimensional real vector space $\mathcal{R} = M_d(\mathbb{C})^{(sa)} \ominus \mathbb{R} \cdot \mathrm{I}_d$, and a given density matrix r is completely determined by its coefficients w.r.t. $\mathfrak{B}$ (the trace condition for r telling us the "missing" coefficient $(r|\mathrm{I}_d) = 1/d$).

Suppose your aim as an experimental physicist is to determine the original density matrix r of a large ensemble of quantum systems (e.g. particles). As the considerations above show, your experimental setup will need $d+1$ different measurement devices, corresponding to observables $b_0, \dots, b_d \in M_d(\mathbb{C})$ (for practical reasons, you will surely avoid the need of *more* observables), further the "span condition" (3.3) must be fulfilled. For each $0 \leq k \leq d$, we set

$$r_k = P_{\mathcal{M}_k^{(sa)} \ominus \mathbb{R} \cdot \mathrm{I}_d}(r).$$

By the span condition, there are coefficients $\lambda_{i,k} \in \mathbb{R}$ such that

$$r = \sum_{k=0}^{d} \underbrace{\left(\sum_{i=1}^{d-1} \lambda_{i,k} s_i^{(k)} \right)}_{=r_k} + \frac{1}{d} \mathrm{I}_d \tag{3.4}$$

For each $0 \leq k \leq d$, you will perform a number of measurements of the observable b_k. The "raw data" you receive from these measurement sequences are relative frequencies of the outcomes of the b_k, that is *estimations* for the probabilities

$$\mu_{i,k} = \left(r y_i^{(k)} \,\middle|\, y_i^{(k)} \right) = d \cdot \left(r p_i^{(k)} \,\middle|\, p_i^{(k)} \right)_{\mathrm{HS}} \in [0,1],$$

where the unit vectors $y_i^{(k)} \in \mathbb{C}^d$ span the images of the respective projections $p_i^{(k)}$ (cf. equation (3.2)).

Since the coefficients $\mu_{0,k}, \dots, \mu_{d-1,k}$ determine the element r_k for each $0 \leq k \leq d$, the detected frequencies allow to compute statistical estimators $\tilde{\lambda}_{1,k}, \dots, \tilde{\lambda}_{d-1,k}$ for the actual coefficients $\lambda_{i,k}$ defined by equation (3.4). On the whole, the measurements of the observables $b_0, \dots, b_d$ produce an estimator (a statistical vector)

$$\tilde{r} = \sum_{k=0}^{d} \sum_{i=1}^{d-1} \tilde{\lambda}_{i,k} s_i^{(k)} + {}^1\!/_d$$

for the "original vector", that is the density matrix r. This is displayed in Figure 3.2, where an imaginary "splitting device" is added for clarity.

Optimal state determination

It goes without saying that every experimentalist will simultaneously aim to minimise the total number of measurements and to maximise the precision of the outcome. This is the idea of an *optimal state determination*. In 1989, the physicists W. K. Wootters and B. D. Fields described how *unbiased observables* permit to achieve a quantal state determination which is optimal in a precise mathematical sense ([114]). The measurement process from above is described in their article as well. For the rest of the section, we will briefly outline how to optimise this process. We keep all notations as above.

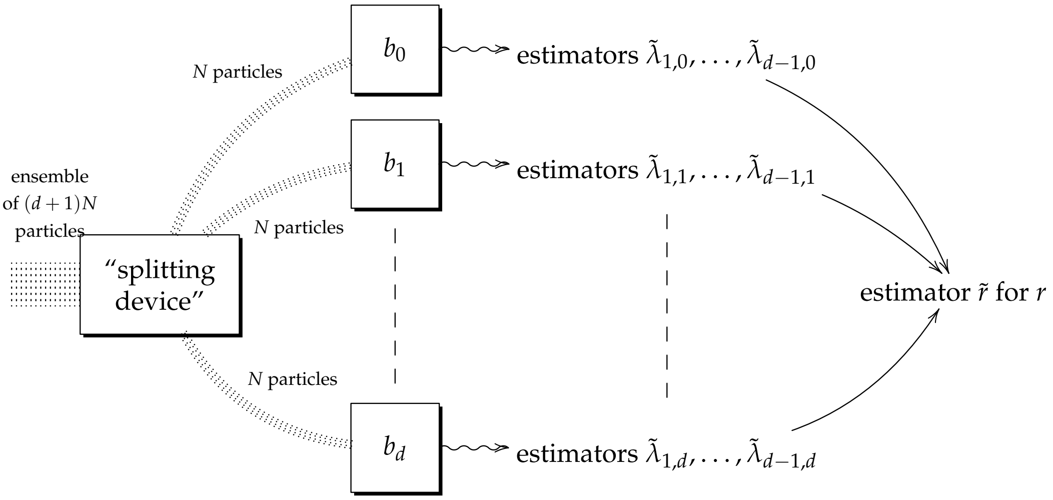

ensemble
of $(d+1)N$
particles
"splitting
device"
N particles
N particles
N particles
b_0
b_1
b_d
estimators $\tilde{\lambda}_{1,0}, \ldots, \tilde{\lambda}_{d-1,0}$
estimators $\tilde{\lambda}_{1,1}, \ldots, \tilde{\lambda}_{d-1,1}$
estimators $\tilde{\lambda}_{1,d}, \ldots, \tilde{\lambda}_{d-1,d}$
estimator $\tilde{r}$ for r

Figure 3.2: *Quantum state determination*

After sufficiently many measurements of the observables b_k, the outcomes of each estimator $\tilde{\lambda}_{i,k}$ can be approximated by a Gaussian normal distribution centred at the original value $\lambda_{i,k}$. Thereby the results for the statistical vector $\tilde{r}$ will be spread around the original vector r according to a *multi-dimensional Gaussian distribution*.

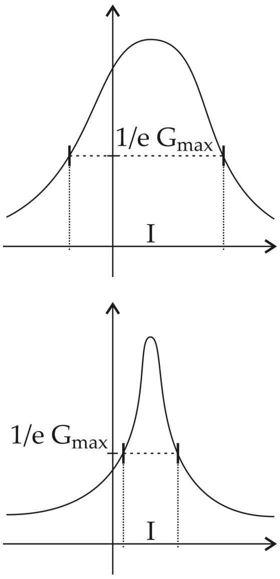


Figure 3.3: *Uncertainty intervals*

The crucial question is how to achieve the maximal certainty for the estimator $\tilde{r}$. Let us first recall how the degree of certainty is usually quantified in this context.

In the case of the statistical estimation for a single real parameter $\lambda \in \mathbb{R}$, approximately given by a Gaussian distribution $G : \mathbb{R} \to [0,1]$, the *uncertainty interval* is the smallest interval $I \subset \mathbb{R}$ such that the inequality $G(t) \geq {}^1\!/_e\, G_{\max}$ holds for all $t \in I$, where $G_{\max}$ is the absolute maximum of the distribution G (see Figure 3.3). It comes as no surprise that the narrower the uncertainty interval, the more precise the estimation can be considered to be.

For multi-dimensional Gaussians $G_d : \mathbb{R}^d \to [0,1]$, this is generalised to an *uncertainty volume* V, which is the volume of the smallest rectangular parallelepiped $V \subset \mathbb{R}^d$ containing the (ellipsoidal) region of all points $x \in \mathbb{R}^d$ satisfying the inequality $G(x) \geq {}^1\!/_e\, G_{\max}$. It would lead too far to define and to determine this parallelepiped in detail; we refer to textbooks on advanced probability theory to this end.

There is only one fact which is important to us here: the uncertainty volume is *minimal* for a d-dimensional normal distribution G if and only if the latter is the (rescaled) product of one-dimensional Gaussians on pairwise orthogonal real axes. If by contrast G is the amalgamation of the same one-dimensional Gaussians over *non-orthogonal* axes, then the growth of the uncertainty volume is proportional to the axes' proximity to being orthogonal. Figure 3.4 illustrates this fact (in a strongly simplified manner) for the case $d = 2$.

In the quantum state determination considered here, the individual measurements b_k produce $(d-1)$-dimensional Gaussians $\tilde{G}_k : \langle \mathfrak{b}_k \rangle \to [0,1]$ for all $0 \leq k \leq d$. These Gaussian distributions are symmetric (as in the upper graph of Figure 3.4). One can show that therefore their uncertainty volume $V_k \subset \langle \mathfrak{b}_k \rangle$ is independent of the choice of the orthonormal basis $\mathfrak{b}_k$. Now the measurement b_k yields no information about all other dimensions of the density matrix r. As a consequence, the probability density resulting from measurement b_k for the whole space $\mathcal{R}$ is given by the (rescaled) product of $\tilde{G}_k$ by a uniform distribution (on a reasonably large cuboid) on the complementary space $\mathcal{R} \ominus \langle \mathfrak{b}_k \rangle$. We denote the resulting Gaussian on $\mathcal{R}$ by G_k. The overall normal distribution G on $\mathbb{R}^{d^2-1}$ of the estimator $\tilde{r}$ is now the (rescaled) product of the individual distributions G_k, since these are *independent* due to the experimental situation.

Here comes the crucial point: the overall uncertainty volume V for the estimator $\tilde{r}$ is, as explained above, minimal if and only if G is the product of Gaussians on axes being pairwise orthogonal. In our situation, this is equivalent to the mutual orthogonality of the operator bases $\mathfrak{b}_0, \ldots, \mathfrak{b}_k$. In other words, *the uncertainty volume for the estimator $\tilde{r}$ is minimal if and only if the masas $\mathcal{M}_0, \ldots, \mathcal{M}_d$ are pairwise quasi-orthogonal.*

As a matter of course, there are formulas quantifying the amount of gained information corresponding to the uncertainty volume. To keep things short, we omit this aspect here and refer the reader to [114] for the particulars.

The volume V naturally also depends on the uncertainties V_k of the individual measurements b_k. However, these uncertainties depend on the measured ensemble, which is of course a priori *unknown,* and can thus not be taken into account. Hence, the optimal preparation of the overall measurement with respect to an unknown ensemble of quantum

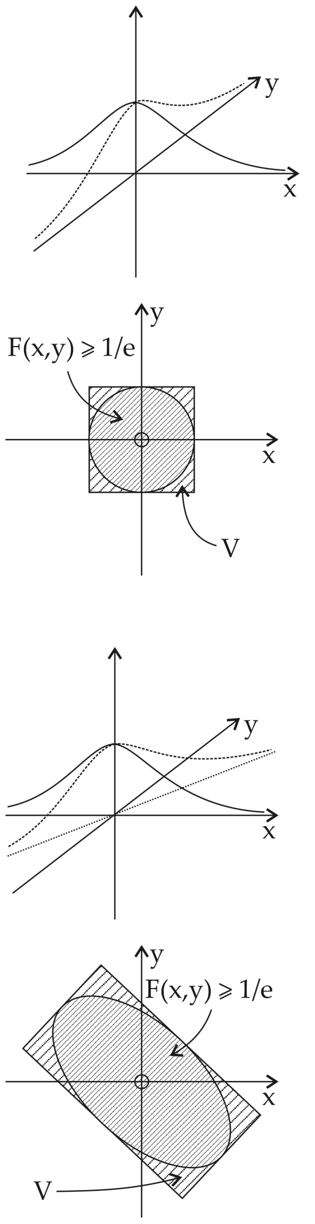


Figure 3.4: *Uncertainty volumes*

systems is to take pairwise quasi-orthogonal masas $\mathcal{M}_k$, i.e. pairwise unbiased bases for the respective observables.

Let us finally remark that for the experimental situation we consider here, detailed computations show that V is proportional to the fraction

$$\frac{\prod_{k=0}^{d} V_k}{vol(\mathfrak{b}_0, \dots, \mathfrak{b}_d)},$$

where the denominator designates the volume of the parallelepiped spanned by the unit vectors of the bases $\mathfrak{b}_k$. This leads to the same conclusions as above: the factors of the enumerator depend on the actual ensemble—which is unknown—, so the only way for the experimenter to minimise the overall uncertainty volume V is to maximise the denominator. It is well-known (or can be proved without difficulty by an induction argument) that the volume of the corresponding parallelepiped is maximal precisely if the unit vectors spanning it are pairwise perpendicular.

3.2 Maximal and complete families of pairwise quasi-orthogonal masas and the MUB-Problem

From pairs of quasi-orthogonal masas, considered in Chapter 2, we will come to general families $\{\mathcal{M}_0, \dots, \mathcal{M}_{n-1}\}$ of pairwise quasi-orthogonal masas ($n \in \mathbb{N}$) in this section. We will name such sets *quasi-orthogonal masa families* for short. The corresponding families of pairwise unbiased bases $\mathfrak{a}_0, \dots, \mathfrak{a}_{n-1}$ of the Hilbert space $\mathbb{C}^d$ are usually called *sets of mutually unbiased bases* or *MUBs.*

As for pairs, we do not want to distinguish between masa families coinciding up to their order and an overall unitary conjugation. This leads to the following generalisation of Definition 2.4.1.

Definition 3.2.1. *In $M_d(\mathbb{C})$, consider two families of masas $\mathscr{F} = \{\mathcal{M}_0, \dots, \mathcal{M}_{n-1}\}$ and $\mathscr{G} = \{\mathcal{N}_0, \dots, \mathcal{N}_{n-1}\}$ of the same length $n \in \mathbb{N}$. We say these families are equivalent or* isomorphic *if there is a permutation $\sigma \in S_n$ and a unitary matrix $u \in \mathcal{U}_d$ such that the identities $\mathcal{N}_i = u\mathcal{M}_{\sigma(i)}u^*$ apply for all indices $0 \leq i < n$.*

This definition is equivalent to the one brought forward by Calderbank et al. in [23], although the authors use a completely different terminology. Similarly as in the case of pairs of quasi-orthogonal masas, the equivalence relation defined above always allows us to assume that a given family of pairwise quasi-orthogonal masas contains the diagonal masa.

Complete quasi-orthogonal masa families and the MUB-Problem

What is the maximal length of a quasi-orthogonal family of masas inside the matrix algebra $M_d(\mathbb{C})$? To answer this question, observe that given a quasi-orthogonal family $\{\mathcal{M}_0, \ldots, \mathcal{M}_{n-1}\}$ in $M_d(\mathbb{C})$, the $(d-1)$-dimensional subspaces

$$\mathcal{M}_0 \ominus \mathbb{C} \cdot \mathrm{I}_d, \ldots, \mathcal{M}_{n-1} \ominus \mathbb{C} \cdot \mathrm{I}_d$$

are pairwise Hilbert-Schmidt orthogonal by definition of quasi-orthogonality. Beyond that, each of them is orthogonal to the line $\mathbb{C} \cdot \mathrm{I}_d$ by construction. The dimension of the complex matrix algebra $M_d(\mathbb{C})$ being d^2, this asserts

$$n(d-1)+1 \leq d^2 \text{ and hence } n \leq \frac{d^2-1}{d-1} = d+1,$$

where we assume $d \geq 2$ for convenience. This important fact was first mentioned by P. Delsarte, J. Goethals and J. Seidel in the year 1975 ([32]). We record it as an observation for future reference.

Observation/Definition 3.2.2. *For all $d \geq 2$, a family of pairwise quasi-orthogonal masas in $M_d(\mathbb{C})$ can have at most $d+1$ members, in which case it is called* complete.

The existence of complete quasi-orthogonal masa families in the matrix algebra $M_d(\mathbb{C})$ is not at all evident for a general dimension d. As a matter of fact, such sets can only be constructed in prime power dimensions at present—we will come to this in Section 3.3.

The next proposition is a direct consequence of the observation we have just made, the list of criteria for quasi-orthogonality stated in Theorem 2.2.14, and Theorem 2.3.5.

Proposition 3.2.3. *For all $d \geq 2$, there are at most $d+1$ mutually unbiased bases for the Hilbert space $\mathbb{C}^d$ and at most d mutually unbiased unitary Hadamard matrices in the unitary group $\mathcal{U}_d$. Moreover, the following assertions are equivalent for all $n \leq d+1$.*

(i) There is a family of n pairwise quasi-orthogonal masas inside the matrix algebra $M_d(\mathbb{C})$.

(ii) There are n mutually unbiased bases for the Hilbert space $\mathbb{C}^d$.

(iii) There is a family of $n-1$ mutually unbiased unitary Hadamard matrices in $M_d(\mathbb{C})$.

(iv) There are n pairwise quasi-orthogonal conditional expectations in the algebra of linear operators on the d^2-dimensional Hilbert space $M_d(\mathbb{C})$.

(v) There is a set of n pairwise maximally distant points in the quotient space (on the compact metric manifold) $\mathfrak{M}_d \cong \mathcal{U}_d / \mathcal{W}_d$, endowed with either of the metrics d_{exp} and d_{mean}.

By analogy with complete families of pairwise quasi-orthogonal masas, and in regard to the equivalences above, sets of $d+1$ MUBs in the Hilbert space $\mathbb{C}^d$, and of d mutually unbiased Hadamard matrices in $M_d(\mathbb{C})$ respectively, are called *complete* as well.

Let us remark that Proposition 3.2.3 is a very strong application of the masa picture. To all appearances, it does not lie at hand how to determine an upper bound for the length of sets of MUBs without using Observation 3.2.2 (nevertheless, there *are* ways, for instance an application of the so-called *Welch inequalities* for Hilbert spaces, see [11]).

As explained in Section 3.1, the question whether complete sets of MUBs exist in a given dimension arises very naturally in the context of quantum mechanics. We record this question, known as the *MUB-Problem*, together with some questions linked to it.

Questions 3.2.4. Let $d \geq 2$ be an arbitrary dimension.

(a) **The MUB-Problem.** Is there a complete set of mutually unbiased bases for the Hilbert space $\mathbb{C}^d$?

(b) If there are *no* complete sets of MUBs in $\mathbb{C}^d$—what is the maximal number of mutually unbiased bases?

(c) If there *are* complete set of MUBs in $\mathbb{C}^d$—how many different classes of unitarily inequivalent complete sets do exist?

As mentioned before, there are complete sets of MUBs in all prime power dimensions. However, it is not known whether these sets are unique in dimensions $d > 5$. What is more, there is so far no strict mathematical proof that there are dimensions *at all* which do *not* admit a complete set of MUBs. Even in dimension six, the question is still open. Apparently Gerhard Zauner was the first to conjecture, in his thesis published in 1999, that there is *no* complete set of MUBs in the Hilbert space $\mathbb{C}^6$, though he stated this conjecture in terms of so-called *quantum designs* ([117]). Since then, many efforts have been made; the achieved results indicate that the largest sets of MUBs in $\mathbb{C}^6$ most probably contain three members. These results stem both from computer algebraic methods (for example [19, 43, 86]) and theoretical approaches (such as [12, 13, 71–73]). At present, many researchers in the area conjecture that there are no complete sets of MUBs in dimensions other than prime powers.

The standard complete family of quasi-orthogonal masas in prime dimensions

The known constructions of complete quasi-orthogonal masa families in general prime power dimensions will be presented in Section 3.3. At this point, we will limit our considerations to the easiest case that the dimension $d = p$ is prime. There is a straightforward construction of a complete set of quasi-orthogonal masas in this case, which is often referred to as the *standard complete (quasi-orthogonal) family in prime dimensions.* Like the standard pair, it was brought forward by Popa in [83]. We will present this construction in the three pictures of quasi-orthogonal masas, unbiased bases and unbiased Hadamard matrices.

Construction 3.2.5 (Popa 1983)**.** Let $p \in \mathbb{P}$ be a prime number.

(a) For each $0 \leq k < p$, let $\mathcal{M}_k \subset M_p(\mathbb{C})$ be the masa generated by the unitary monomial matrix $g_k = \mathrm{X}_p \mathrm{Z}_p^k \in \mathcal{W}_d$. Then

$$\{\mathcal{D}_p, \mathcal{M}_0, \dots, \mathcal{M}_{p-1}\}$$

is a complete family of pairwise quasi-orthogonal masas in $M_p(\mathbb{C})$.

(b) If p is odd, define diagonal unitaries $w_k = \operatorname{diag}(1, 1, \zeta_p^{k \sum_{l=0}^{1} l}, \dots, \zeta_p^{k \sum_{l=0}^{p-2} l})$ and thereby unitary Hadamard matrices

$$h_k = w_k \mathrm{F}_p = \frac{1}{\sqrt{p}} \left(\zeta_p^{ij + k \sum_{l=0}^{i-1} l} \right)_{0 \leq i,j < p} \in M_p(\mathbb{C}),$$

where k ranges from 0 to $p-1$. Then the identities

$$g_k = w_k \mathrm{X}_p w_k^* = w_k \underbrace{\left(\mathrm{F}_p \mathrm{Z}_p^* \mathrm{F}_p^* \right)}_{= \mathrm{X}_p} w_k^* = h_k \mathrm{Z}_p^* h_k^*$$

hold for all $0 \leq k < p$, implying $\mathcal{M}_k = \mathcal{M}_{[h_k]} = w_k \mathrm{F}_p \mathcal{D}_p \mathrm{F}_p^* w_k^*$. Consequently, $\{h_0, \dots, h_{p-1}\}$ is a complete set of mutually unbiased Hadamard matrices.

If p equals two, set $w_0 = \mathrm{I}_2$, $w_1 = \operatorname{diag}(1, \mathrm{i})$, $h_0 = \mathrm{F}_2$ and

$$h_1 = w_1 \mathrm{F}_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ \mathrm{i} & -\mathrm{i} \end{pmatrix}.$$

Then one obtains $\mathcal{M}_0 = \mathcal{M}_{[h_0]}$ and $\mathcal{M}_1 = \mathcal{M}_{[h_1]}$, so h_0 and h_1 are unbiased Hadamard matrices in $M_2(\mathbb{C})$.

(c) Let $\mathfrak{a}_k$ denote the orthonormal basis given by the columns of the unitary h_k for each $0 \leq k < p$. According to item (b), each $\mathfrak{a}_k$ defines a basis of eigenvectors for the generator g_k, whence we have $\mathcal{M}_k = \mathcal{M}_{[\mathfrak{a}_k]}$. Thereby the bases $\mathfrak{e}, \mathfrak{a}_0, \dots, \mathfrak{a}_{p-1}$ form a complete set of MUBs.

The complete sets defined in items (a), (b), and (c) are called *standard complete families* (of quasi-orthogonal masas, MUBs and Hadamard matrices respectively) in dimension p. In a broader sense, we call a complete family (of masas/MUBs/Hadamard matrices) standard if it is equivalent to the family above in the corresponding sense.

Assertions (a) and (b) of this construction are checked by pure computation; assertion (c) is then immediate. Beyond that, you convince yourself that the masas $\mathcal{D}_d$, $\mathcal{M}_0$ and $\mathcal{M}_1$ from above are in fact *always* pairwise quasi-orthogonal, no matter if the dimension d is prime or not, so that each dimension (except $d = 1$) admits at least three pairwise quasi-orthogonal masas.

Representing the matrix algebra $M_d(\mathbb{C})$ as a tensor product with factors of prime dimension, one can deduce the following corollary from Construction 3.2.5.

Corollary 3.2.6. *For a natural number $d \geq 2$, let $p_0 \in \mathbb{P}$ be the smallest prime number dividing d. Then there are at least $p_0 + 1$ pairwise quasi-orthogonal masas in $M_d(\mathbb{C})$.*

The proof can be found in the Appendix on pages 217-218. ▷

Note that the generators $z_p, g_0, \ldots, g_{p-1}$ of the masas in the standard family pairwise commute up to a pth root of unity. This is ensured by the commutation relation $z_p x_p = \zeta_p x_p z_p$ that we have already used in the proof of Theorem 2.4.7. Criterion (iv) of Theorem 2.4.7 then results in the

Observation 3.2.7. Every two different masas from the standard family in $M_p(\mathbb{C})$ form a standard pair.

Now suppose there is a complete family $\mathscr{F}$ in $M_p(\mathbb{C})$ such that each pair of different masas in $\mathscr{F}$ is standard. Does this already imply that $\mathscr{F}$ is a standard family? For general prime dimensions, this is one among several open questions which lie quite at hand.

Questions 3.2.8. Let $p \in \mathbb{P}$ be a prime number.

(a) Is every complete family of quasi-orthogonal masas in $M_p(\mathbb{C})$ a standard family?

(b) If question (a) has positive answer: what is the maximal length of a quasi-orthogonal masa family in $M_p(\mathbb{C})$ which is *not* a subset of a standard family?

(c) If question (b) has negative answer: is it still true that every complete family of quasi-orthogonal masas in $M_p(\mathbb{C})$ is equivalent to a family where each masa is generated by a *monomial* unitary?

It seems quite hard to answer these questions for general prime dimensions. At least for the smallest dimensions ($p \in \{2, 3\}$), one consequence of the next proposition is a positive answer to question (a).

Proposition 3.2.9. *All quasi-orthogonal masa families in $M_2(\mathbb{C})$ and $M_3(\mathbb{C})$ are equivalent to a subfamily of the standard complete family from Construction 3.2.5. In particular, all complete quasi-orthogonal masa families in these dimensions are standard.*

Proof. We have already proved (Observation 2.4.8) that all pairs in $M_2(\mathbb{C})$ and $M_3(\mathbb{C})$ are standard. More precisely, we have computed in that very proof that

- all masas in $M_2(\mathbb{C})$ which are quasi-orthogonal to the diagonal masa are generated by a matrix of the form
$$\begin{pmatrix} 0 & \nu \\ 1 & 0 \end{pmatrix}$$
- all masas in $M_3(\mathbb{C})$ being quasi-orthogonal to $\mathcal{D}_3$ are generated by a matrix of the form
$$\begin{pmatrix} 0 & 0 & \nu_1 \\ 1 & 0 & 0 \\ 0 & \nu_0 & 0 \end{pmatrix}$$

for entries $\nu, \nu_0, \nu_1 \in \mathbb{T}$. (Recall that this *literally* holds true, i.e. not only up to equivalence.)

Given a family $\mathscr{F}$ of three quasi-orthogonal masas in $M_2(\mathbb{C})$, we may assume w.l.o.g. (possibly after a conjugation by an element of $\mathcal{W}_2$) that it contains $\mathcal{D}_2$ and $\mathcal{A}^*(\sigma_x)$. If $v \in \mathcal{U}_2$ is a generator of the third masa in $\mathscr{F}$, the equation $(\sigma_x \,|\, v)_{\text{HS}} = 0$ ensures, up to a phase factor, the identity

$$v = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \sigma_x \sigma_z.$$

If $\mathscr{G}$ is a quasi-orthogonal family of at least two masas inside $M_3(\mathbb{C})$, we may assume, by the same argument as just before, that it contains $\mathcal{D}_3$ and $\mathcal{A}^*(\mathrm{X}_3)$. Again using the orthogonality of the generators, one computes that every other masa in $\mathscr{G}$ is either generated by $\mathrm{X}_3\mathrm{Z}_3$ or by $\mathrm{X}_3\mathrm{Z}_3^*$. □

A complete list of all equivalence classes of quasi-orthogonal masa families in dimensions two to five was presented by S. Weigert, S. Brierley, and I. Bengtsson in 2010 ([103]). Since there is only one equivalence class of a complete quasi-orthogonal family in dimension $p = 5$ according to that list, question (a) still has positive answer for the matrix algebra $M_5(\mathbb{C})$.

A generalisation of Question 3.2.8 (a) is the following. Let $\mathscr{F}$ designate a (not necessarily complete) family of quasi-orthogonal masas, where every pair of two different masas is standard. Does this mean that $\mathscr{F}$ is a subfamily of a standard family? One may further ask whether all subfamilies of a standard family are equivalent if they are of the same length. The answers to both of these questions are negative for general prime dimensions ($p \geq 5$), as the following examples demonstrate.

Examples 3.2.10. (a) Consider a permutation $\rho \in S_5$ which is *not* affine linear as mapping $\rho : \mathbb{Z}_5 \to \mathbb{Z}_5$ and set $\tilde{w} = \operatorname{diag}(\zeta_5^{\rho(0)}, \dots, \zeta_5^{\rho(4)}) \in \mathcal{W}_5$. (For instance, take $\tilde{w} = \operatorname{diag}(\zeta_5^0, \zeta_5^1, \zeta_5^2, \zeta_5^4, \zeta_5^3)$.) Then the quasi-orthogonal masa family

$$\mathscr{F}_0 = \{\mathcal{D}_5, \mathcal{A}^*(\mathtt{X}_5), \mathcal{A}^*(\mathtt{X}_5\tilde{w})\}$$

is not a subfamily of a standard complete family, though every pair in $\mathscr{F}_0$ is standard as a quasi-orthogonal pair in $M_5(\mathbb{C})$.

(b) The subfamilies $\mathscr{F}_1 = \{\mathcal{D}_{13}, \mathcal{M}_0, \mathcal{M}_1\}$ and $\mathscr{F}_2 = \{\mathcal{D}_{13}, \mathcal{M}_2, \mathcal{M}_7\}$ of the standard family in $M_{13}(\mathbb{C})$ (see Construction 3.2.5) are inequivalent.

***Proof of example** (a).* For all primes $p \in \mathbb{P}$, let $\{\mathcal{D}_p, \mathcal{M}_0, \dots, \mathcal{M}_{p-1}\}$ denote the standard family of masas in $M_p(\mathbb{C})$ obtained by Construction 3.2.5. Recall that we have also defined diagonal matrices $w_0, \dots, w_{p-1} \in \mathcal{U}_p$ at that point, obeying the equalities

$$\mathcal{M}_k = w_k \mathtt{F}_p \mathcal{D}_p \mathtt{F}_p^* w_k^*$$

for $0 \le k < p$. For convenience, we set $\mathcal{M}_p = \mathcal{D}_p$ and $w_p = \mathtt{I}_p$ for the whole of this proof.

We will verify example (a) by contradiction, so let us assume the family $\mathscr{F}_0$ in example (a) is equivalent to a subset of a standard family. Then there are indices $k_0, k_1, k_2 \in \{0, \dots, 5\}$ and a *-automorphism ϕ of $M_5(\mathbb{C})$ according to the following diagram.

$$\begin{tikzcd}
\mathcal{D}_5 \arrow[d, "\phi"] & \mathcal{A}^*(\mathtt{X}_5) \arrow[d, "\phi"] & \mathcal{A}^*(\mathtt{X}_5\tilde{w}) \arrow[d, "\phi"] \\
\mathcal{M}_{k_0} & \mathcal{M}_{k_1} & \mathcal{M}_{k_2}
\end{tikzcd}$$

If k_0 is not 5, that is $\mathcal{M}_{k_0} \neq \mathcal{D}_5$, then conjugating the masas in the bottom row by the unitary $\mathtt{F}_5^* w_{k_0}^*$ maps $\mathcal{M}_{k_0}$ to the diagonal masa. It is a crucial observation that the same conjugation also transforms $\mathcal{M}_{k_1}$ and $\mathcal{M}_{k_2}$ to members of the standard family again.

To see this, one first checks the identities $w_k^* w_l = w_{l-k}$ for all $0 \le k, l \le p$, where p is a general prime number for the moment. As usual, the index $l - k$ is understood modulo p. Setting $m = l - k$, we then get $\mathtt{F}_p^* w_k^* w_l \mathtt{F}_p = \mathtt{F}_p^* w_m \mathtt{F}_p$ and thereby

$$\mathtt{F}_p^* w_k^* \, \mathcal{M}_l \, w_k \mathtt{F}_p = \mathtt{F}_p^* \left(w_m \mathtt{F}_p \mathcal{D}_p \mathtt{F}_p^* w_m^* \right) \mathtt{F}_p = \mathtt{F}_p^* \, \mathcal{A}^* \left(w_m \mathtt{X}_p w_m^* \right) \, \mathtt{F}_p.$$

Elementary computations yield the identities

$$w_m \mathtt{X}_p w_m^* = \mathtt{X}_p (\mathtt{Z}_p)^m \quad \text{and} \quad \mathtt{F}_p^* \, \mathtt{X}_p (\mathtt{Z}_p)^m \, \mathtt{F}_p = (\mathtt{X}_p)^{-m} \mathtt{Z}_p.$$

Combining these results, we finally get the equality

$$\mathtt{F}_p^* w_k^* \, \mathcal{M}_l \, w_k \mathtt{F}_p = \mathtt{F}_p^* \, \mathcal{A}^* \left(\mathtt{X}_p \mathtt{Z}_p^m \right) \, \mathtt{F}_p = \mathcal{A}^* \left(\mathtt{X}_p^{-m} \mathtt{Z}_p \right) = \mathcal{M}_m,$$

where the last step follows from $(\mathrm{X}_p^{-m}\mathrm{Z}_p)^m \sim \mathrm{X}_p\mathrm{Z}_p^m$ and the fact that p is prime. (Observe that we have proved the following: if $\mathscr{F}$ is a subfamily of the standard family in $M_p(\mathbb{C})$, then for *any* masa $\mathcal{M} \in \mathscr{F}$, there is a unitary conjugation mapping all masas in $\mathscr{F}$ to members of the standard family, especially $\mathcal{M}$ to $\mathcal{D}_p$. This generalises Lemma 2.4.4.)

With regard to these arguments, we can assume w.l.o.g. that there is *-automorphism ψ of $M_p(\mathbb{C})$ and indices $k, l \in \{0, \dots, 4\}$ such that we obtain the following diagram.

$$\begin{tikzcd}
\mathcal{D}_5 \arrow[d, "\psi"] & \mathcal{A}^*(\mathrm{X}_5) \arrow[d, "\psi"] & \mathcal{A}^*(\mathrm{X}_5\tilde{w}) \arrow[d, "\psi"] \\
\mathcal{D}_5 & \mathcal{M}_k & \mathcal{M}_l
\end{tikzcd}$$

Since the diagonal masa is invariant under ψ, the latter is a unitary conjugation by a monomial $w \in \mathcal{W}_d$. According to the diagram above, we furthermore know that the element $w\mathrm{X}_5w^*$ is contained in the masa $\mathcal{M}_k$. We have noticed earlier that all monomial matrices inside $\mathcal{M}_k = \mathcal{A}^*(\mathrm{X}_5\mathrm{Z}_5^k)$ are scalar multiples of powers of $\mathrm{X}_5\mathrm{Z}_5^k$. There is hence an integer $1 \leq s < 5$ and a scalar $\mu \in \mathbb{T}$ (actually a 5th root of unity) satisfying the equality

$$w\mathrm{X}_5w^* = \mu\mathrm{X}_5^s\mathrm{Z}_5^{ks}.$$

Suppose the monomial w acts on the standard orthonormal basis $\mathfrak{e}$ via $z_i \mapsto \lambda_i z_{\sigma(i)}$ for coefficients $\lambda_0, \dots, \lambda_4 \in \mathbb{T}$ (w.l.o.g. $\lambda_0 = 1$) and a permutation $\sigma \in S_5$. Then the equation above implies

$$w\mathrm{X}_5\, z_i \sim_{\mathbb{T}} \mathrm{X}_5^s w\, z_i$$

and thus $\sigma(i+1) = \sigma(i) + s \pmod 5$ for all $0 \leq i < 5$. Iterating this last formula yields $\sigma(i) = m + is$ for $0 \leq i < 5$, where we set $m = \sigma(0)$. This allows to specify the coefficients of w:

$$\begin{aligned}
w\mathrm{X}_5\, z_i = \mu\mathrm{X}_5^s\mathrm{Z}_5^{ks}w\, z_i \quad &\Rightarrow \quad \lambda_{i+1} = \lambda_i\mu\zeta_5^{ks\sigma(i)} \\
&\underset{(\lambda_0=1)}{\Rightarrow} \quad \lambda_i = \mu^i\zeta_5^{ks\sum_{t=0}^{i-1}\sigma(t)} \qquad (0 \leq i < 5)
\end{aligned}$$

At this point, we are able to determine the action of the monomial unitary $\psi(\mathrm{X}_5\tilde{w})$ on the standard basis. For $0 \leq i < 5$, one computes

$$\psi\left(\mathrm{X}_5\tilde{w}\right) z_{m+is} = w\left(\mathrm{X}_5\tilde{w}\right) w^*\, z_{m+is} = \mu\zeta_5^{ksm}\zeta_5^{\rho(i)+ks^2 i} z_{m+(i+1)s}.$$

According to our assumption, the monomial $\psi(\mathrm{X}_5\tilde{w})$ is an element of the masa $\mathcal{M}_l$, and the only monomial matrices in $\mathcal{M}_l$ which send each basis vector z_j to (a multiple of) z_{j+s} are scalar multiples of $\mathrm{X}_5^s\mathrm{Z}_5^{ls}$. There is thus a scalar $\tilde{\mu} \in \mathbb{T}$ so that the following implication applies for all $0 \leq i \leq 5$, where $\tilde{\tilde{\mu}} \in \mathbb{T}$ must be a 5th root of unity, say $\tilde{\tilde{\mu}} = \zeta_5^n$ for some exponent $0 \leq n < 5$.

$$\left.\begin{aligned} \psi\left(\mathrm{X}_5\tilde{w}\right) z_{m+is} &= \mu\zeta_5^{ksm}\zeta_5^{\rho(i)+ks^2i} z_{m+(i+1)s} \\ \tilde{\mu}\mathrm{X}_5^s\mathrm{Z}_5^{ls}\, z_{m+is} &= \tilde{\mu}\zeta_5^{lsm}\zeta_5^{ls^2i} \qquad z_{m+(i+1)s} \end{aligned}\right\} \quad \Rightarrow \quad \zeta_5^{\rho(i)+ks^2i} = \tilde{\tilde{\mu}}\zeta_5^{ls^2i} \tag{3.5}$$

Comparing the exponents in the right-hand equation leads to

$$\rho(i) \equiv (l-k)s^2i + n \bmod 5,$$

so that ρ is affine linear. Since this contradicts the choice of ρ, our assumption fails and thereby the family $\mathscr{F}_0$ is not a subfamily of a standard family. □

A similar proof for item (b) *is provided in the Appendix on page 218. However, having more powerful means at our disposal in Chapter 5, we will present a very short alternative proof in Example 5.1.14* (b). ▷

Since the family $\mathscr{F}_0$ in example (a) is not a subfamily of a standard family, one cannot find masas $\mathcal{N}_0, \mathcal{N}_1 \subset M_5(\mathbb{C})$ such that $\mathscr{F}_0 \cup \{\mathcal{N}_0, \mathcal{N}_1\}$ is complete (because all complete families in $M_5(\mathbb{C})$ are standard). Such families are the subject of the last part of this section.

Non-completable and maximal quasi-orthogonal masa families

Definition 3.2.11. *We call a family* $\mathscr{F}$ *of pairwise quasi-orthogonal masas in* $M_d(\mathbb{C})$ completable *if there is a masa family* $\mathscr{G}$ *such that* $\mathscr{F} \cup \mathscr{G}$ *is a complete quasi-orthogonal family. Otherwise, we say* $\mathscr{F}$ *is* non-completable.

The family $\mathscr{F}$ *is called* maximal *if it is not a proper subset of any larger quasi-orthogonal masa family. Otherwise* $\mathscr{F}$ *is said to be* extendible.

Trivially, any complete family is also maximal and "completable" at the same time. What is more, a maximal family $\mathscr{F}$ which is not complete is obviously *non-completable.* The converse is not always true, for a non-completable quasi-orthogonal family might still be *extendible.*

As Proposition 3.2.9 shows, there are no maximal incomplete sets in $M_2(\mathbb{C})$ and $M_3(\mathbb{C})$, whereas we have already come across a non-completable quasi-orthogonal family in Example 3.2.10 (a). The smallest dimension admitting *non-completable* quasi-orthogonal families is $d = 4$.

Example 3.2.12. The family containing the three pairwise quasi-orthogonal masas

$$\mathcal{D}_4,\ \mathcal{A}^*\left(\mathrm{X}_4\right) \text{ and } \mathcal{A}^*\left(\mathrm{X}_4\mathrm{Z}_4\right)$$

in the matrix algebra $M_4(\mathbb{C})$ is maximal.

Sketch of the proof. Even this smallest example of a non-completable masa family involves quite extensive computations, most of which we omit here.

According to Construction 3.2.5, the unitary Hadamard matrices corresponding to the masas $\mathcal{A}^*(\mathrm{X}_4)$ and $\mathcal{A}^*(\mathrm{X}_4\mathrm{Z}_4)$ are

$$H_0 = \mathrm{F}_4 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \mathrm{i} & -1 & -\mathrm{i} \\ 1 & -1 & 1 & -1 \\ 1 & -\mathrm{i} & -1 & \mathrm{i} \end{pmatrix} \quad \text{and} \quad H_1 = w_1 \mathrm{F}_4 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \mathrm{i} & -1 & -\mathrm{i} \\ \mathrm{i} & -\mathrm{i} & \mathrm{i} & -\mathrm{i} \\ -\mathrm{i} & -1 & \mathrm{i} & 1 \end{pmatrix},$$

where we have defined $w_1 = \mathrm{diag}(1, 1, \mathrm{i}, -\mathrm{i})$ as in the mentioned proposition. Any unit vector which is unbiased w.r.t. the standard orthonormal basis $\mathfrak{e}$ is—up to multiplication by a phase factor—of the form

$$\frac{1}{2}\begin{pmatrix} r_0 + \mathrm{i}s_0 \\ r_0 - \mathrm{i}s_0 \\ r_1 + \mathrm{i}s_1 \\ r_2 + \mathrm{i}s_2 \end{pmatrix} \tag{3.6}$$

for real numbers $r_j, s_j \in \mathbb{R}$ such that $r_j^2 + s_j^2 = 1$ for $0 \leq j \leq 2$. We may further assume $r_0 \geq 0$ without loss of generality.

Our goal is to show that there are no four pairwise orthogonal unit vectors in $\mathbb{C}^4$ of the form (3.6) which are unbiased to all columns of both matrices H_0 and H_1. In other words, no unitary Hadamard matrix in $M_4(\mathbb{C})$ is unbiased to H_0 and H_1 at the same time.

Assuming that a vector like in (3.6) is unbiased w.r.t. all columns of H_0 and H_1, one obtains eight (quadratic) equations for the variables $r_j, s_j \in \mathbb{R}$ (in addition to the three modulus equations above). Solving these equations leaves you with precisely *eight* vectors in $\mathbb{C}^4$ being unbiased to all columns of H_0 and H_1: setting $\nu = \frac{1+\mathrm{i}}{2\sqrt{2}}$, they are given by

$$x_0 = \begin{pmatrix} \nu \\ \bar{\nu} \\ \nu \\ -\bar{\nu} \end{pmatrix}, \; x_1 = \begin{pmatrix} \nu \\ \bar{\nu} \\ \bar{\nu} \\ -\nu \end{pmatrix}, \; x_2 = \begin{pmatrix} \nu \\ \bar{\nu} \\ -\bar{\nu} \\ \nu \end{pmatrix}, \; x_3 = \begin{pmatrix} \nu \\ \bar{\nu} \\ -\nu \\ \bar{\nu} \end{pmatrix},$$

and by their complex conjugates $\bar{x}_0, \ldots, \bar{x}_3$. (We define the complex conjugate of a vector by complex conjugation of each entry.) Now you convince yourself that the only non-trivial orthonormal systems in $\{x_0, \ldots, x_3, \bar{x}_0, \ldots, \bar{x}_3\}$ are of length *two*; this proves our assertion. □

One may be tempted to believe that it is not hard to generalise Example 3.2.10 (a) in order to produce non-completable families for all prime dimensions $p \geq 5$. However, this is not evident. We do not know if every complete family of quasi-orthogonal masas in $M_p(\mathbb{C})$ is standard for $p > 5$, but this is crucial for the proof of Example 3.2.10 (a).

We conclude this section with a result established by Mihály Weiner in 2010 ([104]). He proved, using the conditional expectations we have described in Section 2.2, that any family of d pairwise quasi-orthogonal masas in $M_d(\mathbb{C})$ is completable.

Proposition 3.2.13 (Weiner 2010). *Let $\mathscr{F} = \{\mathcal{M}_0, \ldots, \mathcal{M}_{d-1}\}$ denote a quasi-orthogonal masa family of length d inside the matrix algebra $M_d(\mathbb{C})$. Then there is a masa $\mathcal{N} \subset M_d(\mathbb{C})$ such that $\mathscr{F} \cup \{\mathcal{N}\}$ is a complete quasi-orthogonal family.*

The proof can be found in the Appendix on pages 219-221. ▷

3.3 Constructions of complete quasi-orthogonal families of masas in prime power dimensions

In the previous section, we have already presented the standard construction of pairwise quasi-orthogonal masas in prime dimensions (Construction 3.2.5). Apart from a number of constructions of quasi-orthogonal (standard or non-standard) masa *pairs* and some specific constructions in small dimensions (most notably $d = 6$), and in spite of uncountably many articles on that subject, effectively only a handful ways to gain quasi-orthogonal masa families, specially *complete* ones, are known.

We present two famous methods to produce complete families in prime power dimensions in this section. In a certain sense, one might even say that these are most probably the *only* known constructions (cf. Fact 4.3.7). Before all, let us briefly recall some basics concerning finite fields. (We always use the term field in its strictly algebraic sense here.)

Reminder: Some basic facts about finite fields

We confine ourselves to sketching the facts needed for our purposes. Both of the textbooks [64, 65] by Rudolf Lidl and Harald Niederreiter are very good references for proofs and details. A very advisable German introduction to the subject can be found in the textbook [66] by Falko Lorenz.

As is well-known, the residue class ring $\mathbb{Z}/d$, endowed with addition and multiplication modulo d, is a field if and only if d is a prime number, say $d = p \in \mathbb{P}$. This *prime* field $\mathbb{F}_p$, which is unique up to isomorphism, can be extended to a finite field $\mathbb{F}_{p^n}$ for all $n \in \mathbb{N}$, this being the unique field containing precisely p^n elements. The fields $\mathbb{F}_{p^n}$ ($n \in \mathbb{N}$, $p \in \mathbb{P}$) are the only existing finite fields and often called *Galois fields.* In the sequel, we briefly sketch a construction of these fields.

First one shows that there is a field $C \supset \mathbb{F}_p$ containing all roots of polynomials in the ring $\mathbb{F}_p[X]$, that is the ring of polynomials in one indeterminate X with coefficients from $\mathbb{F}_p$. The field C is the so-called *algebraic closure* of $\mathbb{F}_p$. For each polynomial $r \in \mathbb{F}_p[X]$, there exists a smallest subfield $K_r \subset C$ containing all roots of r, the *splitting field* of r. Consider the particular polynomial

$$q(X) = X^{p^n} - X$$

for fixed numbers $n \in \mathbb{N}$ and $p \in \mathbb{P}$. One can easily prove that the splitting field K_q consists precisely of all roots of q. What is more, the polynomial q is *separable*, i.e. its roots are pairwise different, whence the field $\mathbb{F}_{p^n} := K_q$ has precisely $\deg q = p^n$ elements.

The uniqueness of the field $\mathbb{F}_{p^n}$ follows, by a few arguments, from the fact that the splitting field of any polynomial is unique. To this aim, one first observes that a field F with p^n elements must be of characteristic p—that is to say, summing up p times the same element in F is zero for all elements in F, and p is minimal with this property. This simply holds because the characteristic of any finite field is a prime number.

Therefrom one deduces that F contains $\mathbb{F}_p$ as a subfield. Since the multiplicative group $F^\times$ of F contains $p^n - 1$ elements, we have the equality $x^{p^n-1} = 1$ and thereby

$$x^{p^n} - x = 0$$

for all $x \in F$ (this is actually the idea behind the choice of the polynomial q). This again implies that F is a splitting field of q as well, and thereby the isomorphism of fields $F \cong \mathbb{F}_{p^n}$ by the aforementioned result.

Once the existence of the field $\mathbb{F}_{p^n}$ is verified, one can prove that there is an irreducible polynomial $f \in \mathbb{F}_p[X]$ of degree n. If then η is a root of f, then $\mathbb{F}_{p^n}$ can be realised as algebraic extension $\mathbb{F}_p[\eta]$. By definition, the latter is the ring of all finite sums $\sum_{i=0}^m \alpha_i \eta^i$, where $m \in \mathbb{N}$. However, since η is algebraic over $\mathbb{F}_p$, i.e. a root of a polynomial in $\mathbb{F}_p[X]$, a basic theorem from algebra tells us that $\mathbb{F}_p[\eta]$ is actually a field.

What is more, writing $f(X) = \sum_{i=0}^n \beta_i X^i$, the identity $f(\eta) = 0$ leads to

$$\eta^n = -\beta_n^{-1} \sum_{i=0}^{n-1} \beta_i \eta^i.$$

Thereby the field $\mathbb{F}_p[\eta]$ is the $\mathbb{F}_p$-linear span of the powers $1, \eta, \dots, \eta^{n-1}$, hence in particular an *n-dimensional vector space over* $\mathbb{F}_p$. By its cardinality, it moreover coincides with the unique field containing p^n elements, that is $\mathbb{F}_{p^n}$.

Considering the field $\mathbb{F}_{p^n}$ as a vector space admits to define a field theoretic trace function, which will be of special importance for our issues.

Definition/Proposition 3.3.1. *Fix $p \in \mathbb{P}$, $n \in \mathbb{N}$, and consider the field $\mathbb{F}_{p^n}$ as the vector space $\langle 1, \eta, \ldots, \eta^{n-1} \rangle_{\mathbb{F}_p}$ like above. Then for every $\alpha \in \mathbb{F}_{p^n}$, the element*

$$Tr(\alpha) = \sum_{i=0}^{n-1} \alpha^{p^i},$$

called the absolute trace *of α, belongs to $\mathbb{F}_p$, that is to $\mathbb{F}_p \cdot 1 \subset \langle 1, \eta, \ldots, \eta^{n-1} \rangle_{\mathbb{F}_p}$. The so-defined* absolute trace function *$Tr : \mathbb{F}_{p^n} \to \mathbb{F}_p$, $\alpha \mapsto Tr(\alpha)$, is $\mathbb{F}_p$-linear. What is more, each linear transformation from $\mathbb{F}_{p^n}$ into its prime field $\mathbb{F}_p$ is given by $\alpha \mapsto Tr(\alpha\beta)$ for some element $\beta \in \mathbb{F}_{p^n}$.*

For a proof of the proposed properties of the field theoretic trace, see for example [65, theorem 2.23]. Whereas this is quite elementary, the verification of the next statement requires more work (see e.g. [64, theorem 5.37]).

Proposition 3.3.2. *Let $p \in \mathbb{P}$ be an odd prime number, $1 \neq \zeta_p \in \mathbb{T}$ a pth root of unity and $n \in \mathbb{N}$. Furthermore, let $Tr : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be the absolute trace function defined above. Identifying the prime field $\mathbb{F}_p$ and the integers $\{0, \ldots, p-1\}$ in the obvious way, the following equation holds for all $m \in \mathbb{Z} \setminus \{0\}$.*

$$\left| \sum_{\alpha \in \mathbb{F}_{p^n}} \zeta_p^{Tr(m\alpha^2 + n\alpha)} \right| = \sqrt{p^n} \tag{3.7}$$

The exponential sum on the left-hand side of this equation is an example of a Weyl sum.

A construction on the level of MUBs

The equation above is crucial for the following construction of complete sets of MUBs in (odd) prime power dimensions, which was presented by Wootters and Fields in the aforementioned article [114].

Construction 3.3.3 (Wootters and Fields 1989)**.** Consider an odd prime number $p \in \mathbb{P}$, a pth root of unity $1 \neq \zeta_p \in \mathbb{T}$, and a natural number $n \in \mathbb{N}$. Further set $d = p^n$ and fix an enumeration $\alpha_0, \ldots, \alpha_{d-1}$ of the field $\mathbb{F}_{p^n}$. Define column vectors

$$x_\gamma^{(\beta)} = \frac{1}{\sqrt{d}} \begin{pmatrix} \zeta_p^{\mathrm{Tr}(\beta\alpha_0^2 + \gamma\alpha_0)} \\ \zeta_p^{\mathrm{Tr}(\beta\alpha_1^2 + \gamma\alpha_1)} \\ \vdots \\ \zeta_p^{\mathrm{Tr}(\beta\alpha_{d-1}^2 + \gamma\alpha_{d-1})} \end{pmatrix} \in \mathbb{C}_1^d$$

for all $\beta, \gamma \in \mathbb{F}_{p^n}$. We may write $x_j^{(k)}$ instead of $x_{\alpha_j}^{(\alpha_k)}$, identifying the elements of $\mathbb{F}_{p^n}$ with their numbers w.r.t. the enumeration above. Then the standard basis $\mathfrak{e}$ and the bases

$$\mathfrak{a}_k = (x_0^{(k)}, \ldots, x_{d-1}^{(k)}),$$

where k ranges from 0 to $d-1$, form a complete set of MUBs in $\mathbb{C}^d$.

Proof. Both the orthonormality of the bases $\mathfrak{a}_0 \ldots, \mathfrak{a}_{d-1}$ and their respective unbiasedness can be verified by explicit computations. For the unbiasedness, equation (3.7) yields

$$\left|\left(x_\gamma^{(\beta)} \,\middle|\, x_{\gamma'}^{(\beta')}\right)\right| = \left|\frac{1}{d} \sum_{\alpha \in \mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}\left((\beta-\beta')\alpha^2 + (\gamma-\gamma')\alpha\right)}\right| \underset{(3.7)}{=} \frac{1}{d}\sqrt{d} = \frac{1}{\sqrt{d}}$$

for all $\beta, \beta', \gamma, \gamma' \in \mathbb{F}_{p^n}$ whenever $\beta \neq \beta'$. The unbiasedness of the bases $\mathfrak{a}_k$ w.r.t. the standard basis $\mathfrak{e}$ is obvious. □

Bearing in mind that the absolute trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ is just the identity if n happens to be one, one immediately sees that the construction above is a generalisation of the following, presented by I. D. Ivanovic eight years earlier ([49]).

Construction 3.3.4 (Ivanovic 1981)**.** Let $p \in \mathbb{P}$ be an odd prime number and $1 \neq \zeta_p \in \mathbb{T}$ a pth root of unity. In the Hilbert space $\mathbb{C}^p$, define vectors

$$x_j^{(k)} = \frac{1}{\sqrt{p}} \begin{pmatrix} 1 \\ \zeta_p^{k+j} \\ \zeta_p^{4k+2j} \\ \vdots \\ \zeta_p^{(p-1)^2 k + (p-1)j} \end{pmatrix} \in \mathbb{C}_1^p$$

for all $0 \leq j, k < p$. Then the standard basis $\mathfrak{e}$ and the bases $\mathfrak{a}_k = (x_0^{(k)}, \ldots, x_{p-1}^{(k)})$, where k ranges from 0 to $p-1$, form a complete set of MUBs in $\mathbb{C}^p$.

Remark 3.3.5. It might have caught the reader's eye that there is a striking similarity between the bases $\mathfrak{a}_k$ defined directly above and those introduced in Construction 3.2.5, where we have presented Popa's construction of the pairwise quasi-orthogonal masas $\mathcal{M}_k = \mathcal{A}^*(\mathrm{x}_p \mathrm{z}_p^k)$. In fact, one easily checks that for all $0 \leq k < p$, the basis $\mathfrak{a}_k$ consists of eigenvectors of the monomial $\mathrm{x}_p \mathrm{z}_p^{2k}$ for $p > 2$ (notice how this fails for $p = 2$). For this reason, the bases from Constructions 3.3.4 and 3.2.5 actually coincide up to the order of the involved bases and basis vectors.

Probably Popa was not aware of this coincidence. As a matter of fact, although his respective article [83] was published in 1983, he had already *submitted* it when Ivanovic published his paper [49], namely in 1981.

Unlike Popa's technique, both Ivanovic's construction and its generalisation fail to work in case p is even. The reason is that equation (3.7) does not apply if p equals two, as you can check without effort. However, this gap can be filled. Whereas Wootters and Fields come up with a completely elementary construction for the case $p = 2$ in the aforementioned paper [114], Andreas Klappenecker and Martin Rötteler present a somewhat more sophisticated approach in [60].

This last construction involves the Galois rings $GR(4, n)$ and the so-called *Teichmüller sets* $\mathcal{T}_n \subset GR(4, n)$. Using a trace map from the Galois ring $GR(4, n)$ to the residue class ring $\mathbb{Z}/4\mathbb{Z}$, one receives an equation similar to (3.7), where the exponential sum involves only fourth roots of unity. The bases constructed in this manner consist of columns where each entry is (up to an overall scaling factor $1/2^n$) a fourth root of unity as well. Since the next construction we present also covers this case, we omit this special construction and refer the interested reader to [60] for the details.

Two techniques which are more general than Construction 3.3.3 above shall not be left unmentioned.

Construction 3.3.6 (The planar function construction)**.** The construction of Wootters and Fields can be generalised, using so-called *planar functions* on the field $\mathbb{F}_{p^n}$ in the exponents of the vectors' entries, see for instance [88, theorem 4.1]. For the sake of simplicity, this generalisation is left aside in this thesis.

Construction 3.3.7 (The Alltop construction)**.** There is one construction of MUBs in prime power dimensions preceding *all* others mentioned in this work. In fact, W. O. Alltop published a technique which results in MUBs similar to the one by Wootters and Fields, but involving (non-planar) different mappings in the exponents of the vector entries, already in 1980 ([1]). However, Alltop's article is written in a framework which is fairly distant from ours; the term "mutually unbiased" does not even occur there. As for the planar function construction, we omit this approach to keep things simple.

A construction on the level of quasi-orthogonal masas

Somshubhro Bandyopadhyay et al. ([9]) presented an alternative construction of complete sets of MUBs in prime power dimensions in 2002, based on families of pairwise commuting unitaries. As the approach of Wootters and Fields generalises the technique of Ivanovic, so the one of Bandyopadhyay et al. generalises the one of Popa.

The technique of Bandyopadhyay et al. produces so-called *nice* families of quasi-orthogonal masas, which will be at the centre of our interest from Section 4.3 on. That is why its description will be rather detailed. In Section 5.1, we will rephrase this concept in the picture of the *generalised Clifford algebra* (see Construction 5.1.5).

In preparation of these purposes, we present the construction of Bandyopadhyay et al. not only in a slightly different terminology, but actually in an effectively different manner at some (minor) points, as the reader who is familiar with the respective article may notice.

The clock and shift matrices Z_d and X_d, already introduced in Chapters 1 and 2 (see Example 1.4.2 and the paragraph directly after Definition 2.2.1), enter the stage once more at this point. For the rest of this subsection, fix an (even or odd) prime $p \in \mathbb{P}$ and a natural number $n \in \mathbb{N}$, and set $d = p^n$. What is more, we shall always identify the matrix algebras $\bigotimes_n M_p(\mathbb{C})$ and $M_d(\mathbb{C})$ via our standard *-isomorphism (see Convention 0.0.2).

Definition/Proposition 3.3.8. *In the matrix algebra $\bigotimes_n M_p(\mathbb{C}) \cong M_d(\mathbb{C})$, we define unitary matrices*

$$\mathrm{B}_i = \quad \mathrm{I}_p \otimes \cdots \otimes \mathrm{I}_p \otimes \overset{\substack{(ith\ pos.)\\ |}}{\mathrm{Z}_p} \otimes \mathrm{I}_p \otimes \cdots \otimes \mathrm{I}_p$$

$$\textit{and} \quad \mathrm{C}_i = \begin{cases} i\,\mathrm{I}_p \otimes \cdots \otimes \mathrm{I}_p \otimes \sigma_x\sigma_z \otimes \mathrm{I}_p \otimes \cdots \otimes \mathrm{I}_p & \textit{if } p = 2, \\ \mathrm{I}_p \otimes \cdots \otimes \mathrm{I}_p \otimes \mathrm{X}_p\mathrm{Z}_p^* \otimes \mathrm{I}_p \otimes \cdots \otimes \mathrm{I}_p & \textit{else,} \end{cases}$$

for all indices $0 \leq i < n$. Obviously, the matrices $\mathrm{B}_0, \ldots, \mathrm{B}_{n-1}$ pairwise commute, and the same applies for the elements $\mathrm{C}_0, \ldots, \mathrm{C}_{n-1}$. For all $0 \leq i, j < n$, we further have the commutation relation

$$\mathrm{B}_i\mathrm{C}_j = \begin{cases} \zeta_p\mathrm{C}_j\mathrm{B}_i & \textit{if } i = j, \\ \mathrm{C}_j\mathrm{B}_i & \textit{else.} \end{cases} \tag{3.8}$$

The pth powers of all of the matrices B_i and C_i equal the unit matrix I_d, so that we can consider exponents of these matrices as elements of the prime field $\mathbb{F}_p$. The set of all ordered products

$$\mathfrak{L}^p_{2n} = \left\{ \mathrm{B}_0^{i_0} \cdots \mathrm{B}_{n-1}^{i_{n-1}}\mathrm{C}_0^{i_n} \cdots \mathrm{C}_{n-1}^{i_{2n-1}} \,\middle|\, i_0, \ldots, i_{2n-1} \in \mathbb{F}_p \right\}$$

is a Hilbert-Schmidt orthonormal basis for the matrix algebra $M_d(\mathbb{C})$.

The assertions in the definition/proposition above are effortlessly deduced from the basic commutation rule $\mathrm{Z}_p\mathrm{X}_p = \zeta_p\mathrm{X}_p\mathrm{Z}_p$ and the fact that the set

$$\left\{ \mathrm{X}_p^i\mathrm{Z}_p^j \,\middle|\, 0 \leq i, j < p \right\}$$

is a Hilbert-Schmidt orthonormal basis for $M_p(\mathbb{C})$ (cp. Example 2.2.16).

The key point in the construction of Bandyopadhyay et al. is to find a family of subsets $\mathfrak{E}_0 \cup \ldots \cup \mathfrak{E}_d$ covering the basis $\mathfrak{E}_{2n}^p$ such that

- each of the subsets $\mathfrak{E}_i$ is of length p^n,
- the basis elements in each subset $\mathfrak{E}_i$ commute,
- the spans $\mathcal{M}_i = \operatorname{span}_{\mathbb{C}}(\mathfrak{E}_i)$ are *-subalgebras at the same time.
- and for all $0 \leq i < j \leq d$, the intersection of the subsets $\mathfrak{E}_i$, $\mathfrak{E}_j$ contains precisely the unit matrix $\mathrm{I}_d \in \mathfrak{E}_{2n}^p$,

The commutative *-subalgebras $\mathcal{M}_i$ are then masas by dimension. What is more, they obviously form a complete quasi-orthogonal family by the last condition. (Given a Hilbert-Schmidt orthonormal basis for $M_d(\mathbb{C})$ containing the unit matrix, a cover that fulfils this last condition is also called *quasi-partition.* We defer to Section 4.3 for a more detailed introduction of this notion.)

A crucial step to find a cover of the basis $\mathfrak{E}_{2n}^p$ like above is the next

Definition 3.3.9. *Given a matrix $K = (k_{i,j})_{0 \leq i,j < n} \in M_n(\mathbb{F}_p)$, we define unitary matrices*

$$\mathrm{G}_i = \mathrm{G}_{K,i} = \mathrm{B}_0^{k_{i,0}} \cdots \mathrm{B}_{n-1}^{k_{i,n-1}} \mathrm{C}_i \in M_d(\mathbb{C})$$

for all $0 \leq i < n$. We denote by $\mathcal{M}_K$ the *-subalgebra of $M_d(\mathbb{C})$ generated by theses unitaries, that is we set

$$\begin{aligned}\mathcal{M}_K = \mathcal{A}^*(\mathrm{G}_0, \ldots, \mathrm{G}_{n-1}) = \mathcal{A}^*(\mathrm{B}_0^{k_{0,0}} & \cdots \mathrm{B}_{n-1}^{k_{0,n-1}} \mathrm{C}_0, \\ & \vdots \\ & \mathrm{B}_0^{k_{n-1,0}} \cdots \mathrm{B}_{n-1}^{k_{n-1,n-1}} \mathrm{C}_{n-1}).\end{aligned}$$

Although we have only defined quasi-orthogonality for *masas*according to our general purposes (see Definition 2.2.1), this notion can of course be applied for any two unital *-subalgebras of the complex $d \times d$-matrices. This generalisation is presupposed in the following statement.

Proposition 3.3.10. *With each matrix $K \in M_n(\mathbb{F}_p)$, we associate a *-subalgebra $\mathcal{M}_K$ of $M_d(\mathbb{C})$ according to Definition 3.3.9 above.*

(i) The *-subalgebra $\mathcal{M}_K$ is unital and of dimension $d = p^n$ for all $K \in M_n(\mathbb{F}_p)$.

(ii) The *-subalgebra $\mathcal{M}_K$ is commutative and hence a masa if and only if $K \in M_n(\mathbb{F}_p)$ is symmetric.

(iii) If $K, L \in M_n(\mathbb{F}_p)$ are two matrices, then the *-subalgebras $\mathcal{M}_K$ and $\mathcal{M}_L$ are quasi-orthogonal precisely if the difference $K - L$ is an invertible element of $M_n(\mathbb{F}_p)$.

(iv) Given any matrix $K \in M_n(\mathbb{F}_p)$, the *-subalgebra $\mathcal{M}_K \subset M_d(\mathbb{C})$ is quasi-orthogonal to the diagonal masa $\mathcal{A}^*(\mathrm{B}_0, \ldots, \mathrm{B}_{n-1}) = \mathcal{D}_d$.

Proof. Given a matrix $K = (k_{i,j})_{0 \le i,j < n} \in M_n(\mathbb{F}_p)$, the *-subalgebra $\mathcal{M}_K$ is, according to Definition 3.3.9, generated by the unitary matrices

$$\mathrm{G}_i = \mathrm{B}_0^{k_{i,0}} \cdots \mathrm{B}_{n-1}^{k_{i,n-1}} \mathrm{C}_i,$$

where i ranges from 0 to $n-1$. As a vector space, $\mathcal{M}_K$ is spanned by all (ordered) products of the unitaries $\mathrm{G}_0, \ldots, \mathrm{G}_{n-1}$, that is

$$\mathcal{M}_K = \operatorname{span}_{\mathbb{C}} \left\{ \mathrm{G}_0^{s_0} \cdots \mathrm{G}_{n-1}^{s_{n-1}} \mid s_0, \ldots, s_{n-1} \in \mathbb{F}_p \right\}. \tag{3.9}$$

Clearly the products spanning $\mathcal{M}_K$ correspond—up to scalar factors—to elements of the basis $\mathfrak{E}_{2n}^p$ (see Definition/Proposition 3.3.8). An explicit computation reveals that we have

$$\mathrm{G}_0^{s_0} \cdots \mathrm{G}_{n-1}^{s_{n-1}} \sim_{\mathbb{T}} \mathrm{B}_0^{S_0} \cdots \mathrm{B}_{n-1}^{S_{n-1}} \mathrm{C}_0^{s_0} \cdots \mathrm{C}_{n-1}^{s_{n-1}} \tag{3.10}$$

for each fixed vector $(s_0, \ldots, s_{n-1}) \in \mathbb{F}_p^n$, where the exponents S_j on the right-hand side are given by $S_j = \sum_{i=0}^{n-1} s_i k_{i,j}$ for all indices $0 \le j < n$.

(i). To begin with, the dimension of the *-subalgebra $\mathcal{M}_K$ is at most p^n, since $\mathcal{M}_K$ is spanned by at most p^n basis elements of the orthonormal basis $\mathfrak{E}_{2n}^p$ according to identity (3.9). By equation (3.10), two generators $\mathrm{G}_0^{s_0} \cdots \mathrm{G}_{n-1}^{s_{n-1}}$ and $\mathrm{G}_0^{t_0} \cdots \mathrm{G}_{n-1}^{t_{n-1}}$ of $\mathcal{M}_K$ can only correspond to the same basis element in $\mathfrak{E}_{2n}^p$ (up to a scalar factor) if the vectors $(s_0, \ldots, s_{n-1})$, $(t_0, \ldots, t_{n-1}) \in \mathbb{F}_p$ of the exponents coincide. The *-subalgebra $\mathcal{M}_K$ is thus spanned by exactly p^n pairwise different basis elements of $\mathfrak{E}_{2n}^p$. It is plain to see that $\mathcal{M}_K$ is unital, for it contains the product $\mathrm{G}_0^* \mathrm{G}_0 = \mathrm{I}_d$.

(ii). The *-subalgebra $\mathcal{M}_K$ is commutative (and hence a masa) if and only if all generators $\mathrm{G}_0, \ldots, \mathrm{G}_{n-1}$ commute. Relation (3.8) in Definition 3.3.8 makes it easy to establish the identity

$$\mathrm{G}_i \mathrm{G}_j = \zeta_p^{k_{i,j} - k_{j,i}} \mathrm{G}_j \mathrm{G}_i$$

for all $0 \le i, j < n$. Obviously, this asserts that all generators $\mathrm{G}_0, \ldots, \mathrm{G}_n$ commute if and only if the matrix K is symmetric.

(iii). Let $K = (k_{i,j})$ and $L = (l_{i,j})$ be two matrices in $M_n(\mathbb{F}_p)$, and $\mathcal{M}_K$, $\mathcal{M}_L$ the *-subalgebras of $M_d(\mathbb{C})$ associated to them. Further, let $\mathrm{G}_0, \ldots, \mathrm{G}_{n-1}$ denote the generators of $\mathcal{M}_K$ as before, and define generators $\mathrm{H}_0, \ldots, \mathrm{H}_{n-1}$ for $\mathcal{M}_L$ by analogy.

For vectors $(s_0, \ldots, s_{n-1}), (t_0, \ldots, t_{n-1}) \in \mathbb{F}_p^n$, we define the sums $S_j = \sum_{i=0}^{n-1} s_i k_{i,j}$ and $T_j = \sum_{i=0}^{n-1} t_i l_{i,j}$ for all $0 \le j < n$. Then by equation (3.10), the masas $\mathcal{M}_K$ and $\mathcal{M}_L$

are spanned by basis elements of the form

$$\mathrm{B}_0^{S_0} \cdots \mathrm{B}_{n-1}^{S_{n-1}} \mathrm{C}_0^{s_0} \cdots \mathrm{C}_{n-1}^{s_{n-1}} \quad \text{and} \quad \mathrm{B}_0^{T_0} \cdots \mathrm{B}_{n-1}^{T_{n-1}} \mathrm{C}_0^{t_0} \cdots \mathrm{C}_{n-1}^{t_{n-1}}$$

respectively. Two such unitaries correspond to the same element of the basis $\mathfrak{E}_{2n}^p$ (up to a phase factor) precisely if the the identities $s_i = t_i$ and $S_i = T_i$ are satisfied for all $0 \leq i < n$, which leads to the set of equations

$$\sum_{i=0}^{n-1} t_i l_{i,j} = \sum_{i=0}^{n-1} t_i k_{i,j} \quad (0 \leq j < n).$$

Combining these equalities, we obtain the identity of rows

$$\sum_{i=0}^{n-1} t_i \left(k_{i,0} - l_{i,0}, \ldots, k_{i,n-1} - l_{i,n-1}\right) = 0 \tag{3.11}$$

for the matrix $K - L$.

On the one hand, equation (3.11) is solved by a non-trivial vector of coefficients $0 \neq (t_0, \ldots, t_{n-1}) \in (\mathbb{F}_p)^n$ exactly if the masas $\mathcal{M}_K$ and $\mathcal{M}_L$ contain a common element, which is not the unit matrix, of the basis $\mathfrak{E}_{2n}^p$—namely a scalar multiple of $\mathrm{B}_0^{T_0} \cdots \mathrm{B}_{n-1}^{T_{n-1}} \mathrm{C}_0^{t_0} \cdots \mathrm{C}_{n-1}^{t_{n-1}}$. By definition of the masas $\mathcal{M}_K$ and $\mathcal{M}_L$, this holds precisely if they are *not* quasi-orthogonal. On the other hand, equation (3.11) clearly admits a non-trivial solution by coefficients $t_0, \ldots, t_{n-1} \in \mathbb{F}_p$ if and only if the matrix $K - L$ is not regular. Combining the previous equivalences, we obtain statement (iii) by contraposition.

(iv). The choice of generators $\mathrm{B}_0, \ldots, \mathrm{B}_{n-1}$ makes it obvious that the *-subalgebra $\mathcal{A}^*(\mathrm{B}_0, \ldots, \mathrm{B}_{n-1})$ is the diagonal masa $\mathcal{D}_d$. Moreover, each of the *-subalgebra $\mathcal{M}_K$, $K \in M_n(\mathbb{F}_p)$, contains, besides the unit matrix, only such elements of the basis $\mathfrak{E}_{2n}^p$ in which at least one non-trivial power of one of the matrices $\mathrm{C}_0, \ldots, \mathrm{C}_{n-1}$ occurs. For this reason, all *-subalgebras $\mathcal{M}_K$ are quasi-orthogonal to $\mathcal{A}^*(\mathrm{B}_0, \ldots, \mathrm{B}_{n-1})$. □

Consider a set of m symmetric matrices $K_0, \ldots, K_{m-1} \in M_n(\mathbb{F}_p)$ for $m \in \mathbb{N}$, with the property that all differences $K_i - K_j$ are either invertible or zero ($0 \leq i, j < m$). By the last preceding proposition, such a set gives rise to a family of $m + 1$ pairwise quasi-orthogonal masas $\mathcal{D}_d, \mathcal{M}_{K_0}, \ldots, \mathcal{M}_{K_{m-1}} \subset M_d(\mathbb{C})$.

In order to find a *complete* quasi-orthogonal masa family this way, we are in need of a family of length $m = d$ of symmetric matrices like above. Whereas Bandyopadhyay et al. cite an explicit construction of such matrix families in [9], we rely on the following, rather non-trivial result from field theory at this point, which goes back to G. Seroussi and A. Lempel ([93]).

Theorem 3.3.11 (Seroussi and Lempel 1983)**.** *For every natural number $n \in \mathbb{N}$ and every prime $p \in \mathbb{P}$, there exists a symmetric representation of the Galois field $\mathbb{F}_{p^n}$ inside $M_n(\mathbb{F}_p)$, that is a set of symmetric matrices $\mathcal{S} = \{K_0, \ldots, K_{d-1}\} \subset M_n(\mathbb{F}_p)$ and a bijective mapping $\phi : \mathbb{F}_{p^n} \to \mathcal{S}$ which is a* field isomorphism*.*

If a set of symmetric matrices $\mathcal{S} = \{K_0, \ldots, K_{d-1}\} \subset M_n(\mathbb{F}_p)$ represents the Galois field $\mathbb{F}_{p^n}$, then clearly every difference of two non-identical matrices in $\mathcal{S}$ is invertible by the properties of a field. This completes our collection of ingredients for the construction presented in [9].

Construction 3.3.12 (Bandyopadhyay et al. 2002)**.** Let $\mathcal{S} = \{K_0, \ldots, K_{d-1}\} \subset M_n(\mathbb{F}_p)$ be a family of symmetric matrices such that every difference of two different members of $\mathcal{S}$ is invertible. For instance, take a symmetric representation of the Galois field $\mathbb{F}_{p^n}$, which exists according to Theorem 3.3.11. Define a masa $\mathcal{M}_i = \mathcal{M}_{K_i} \subset M_d(\mathbb{C})$ as in Definition 3.3.9 for all $0 \leq i < d$. Then according to Proposition 3.3.10, the masas $\mathcal{D}_d, \mathcal{M}_0, \ldots, \mathcal{M}_{d-1} \subset M_d(\mathbb{C})$ form a complete quasi-orthogonal family in $M_d(\mathbb{C})$.

Remark. We propose the acronymic term "smid families" (symmetric matrices with invertible differences) for sets of matrices in $M_n(\mathbb{F}_p)$ like in Construction 3.3.12 and before. The study of such families is a subject of its own right, presenting a number of highly non-trivial difficulties. We shall investigate smid families in Chapter 5.

One advantage of the construction of Bandyopadhyay et al., compared to the one presented by Wootters and fields, is that the former works in practically the same way no matter whether the prime p is even or odd. We clarify this method by some examples.

Examples 3.3.13. (a) If n is one, a symmetric representation of the field $\mathbb{F}_p$ is just the field itself. The map $\mathcal{M}$ introduced in Definition 3.3.9 is of the most simple form.

$$\begin{aligned} \mathbb{F}_p \cong M_1(\mathbb{F}_p) &\xrightarrow{\mathcal{M}} \{\,^*\text{-subalgebras inside } M_p(\mathbb{C})\} \\ k &\longmapsto \mathcal{M}_k = \mathcal{A}^*\left(\mathrm{B}_0^k \mathrm{C}_0\right) \end{aligned}$$

By definition of the basis elements in $\mathfrak{E}_2^p$ (cf. Definition/Proposition 3.3.8), we compute

$$\mathcal{M}_k = \mathcal{A}^*\left(\mathrm{X}_p \mathrm{Z}_p^{k-1}\right).$$

You easily convince yourself that the masas $\mathcal{D}_p, \mathcal{M}_0, \ldots, \mathcal{M}_{p-1}$ are—up to the order of the $\mathcal{M}_k$—precisely the ones obtained by Popa's technique (see Construction 3.2.5).

(b) For $n = p = 2$, the unitaries $\mathrm{B}_0, \mathrm{B}_1, \mathrm{C}_0, \mathrm{C}_1$ are given by

$$\mathrm{B}_0 = \sigma_z \otimes \mathrm{I}_2, \quad \mathrm{B}_1 = \mathrm{I}_2 \otimes \sigma_z, \quad \mathrm{C}_0 = \mathrm{i}\, \sigma_x \sigma_z \otimes \mathrm{I}_2, \quad \text{and} \quad \mathrm{C}_1 = \mathrm{i}\, \mathrm{I}_2 \otimes \sigma_x \sigma_z.$$

Furthermore, it is straightforward to verify that the family containing the symmetric matrices

$$K_0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, K_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, K_2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \text{ and } K_3 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

in $M_2(\mathbb{F}_2)$ represents the Galois field $\mathbb{F}_4$. The masas associated with these matrices according to Definition 3.3.9 are given by

$$\begin{aligned} \mathcal{M}_{K_0} &= \mathcal{A}^*\left(\mathrm{C}_0, \mathrm{C}_1\right) &&= \mathcal{A}^*\left(\sigma_x\sigma_z \otimes \mathrm{I}_2, \mathrm{I}_2 \otimes \sigma_x\sigma_z\right), \\ \mathcal{M}_{K_1} &= \mathcal{A}^*\left(\mathrm{B}_0\mathrm{C}_0, \mathrm{B}_1\mathrm{C}_1\right) &&= \mathcal{A}^*\left(\sigma_x \otimes \mathrm{I}_2, \mathrm{I}_2 \otimes \sigma_x\right), \\ \mathcal{M}_{K_2} &= \mathcal{A}^*\left(\mathrm{B}_1\mathrm{C}_0, \mathrm{B}_0\mathrm{B}_1\mathrm{C}_1\right) &&= \mathcal{A}^*\left(\sigma_x\sigma_z \otimes \sigma_z, \sigma_z \otimes \sigma_x\right), \text{ and} \\ \mathcal{M}_{K_3} &= \mathcal{A}^*\left(\mathrm{B}_0\mathrm{B}_1\mathrm{C}_0, \mathrm{B}_0\mathrm{C}_1\right) &&= \mathcal{A}^*\left(\sigma_x \otimes \sigma_z, \sigma_z \otimes \sigma_x\sigma_z\right). \end{aligned}$$

Together with the diagonal masa $\mathcal{A}^*(\mathrm{B}_0, \mathrm{B}_1) = \mathcal{D}_4$, these masas form a complete quasi-orthogonal family in $M_4(\mathbb{C})$.

Reducing to prime powers

Definition 3.3.14. *For a prime decomposition $d = p_0^{n_0} \cdots p_m^{n_m}$ of the dimension d, where $p_0, \dots, p_m \in \mathbb{P}$ are pairwise different primes, $m \in \mathbb{N}_0$, and $n_0, \dots, n_m \in \mathbb{N}$, we call*

$$L_d = \min\left\{p_0^{n_0}, \dots, p_m^{n_m}\right\}$$

the smallest prime power in the prime factorisation of *d*.

As a consequence of the constructions presented above, we get the following lower bound for the number of pairwise quasi-orthogonal masas in arbitrary dimensions.

Corollary 3.3.15. *Let L_d be the smallest prime power in the prime factorisation of $d \in \mathbb{N}$, as defined directly above. Then there are families of $L_d + 1$ pairwise quasi-orthogonal masas in the matrix algebra $M_d(\mathbb{C})$.*

This assertion is an enhancement of Corollary 3.2.6, where we have used Popa's construction for prime dimensions to show that if $p_0 \in \mathbb{P}$ is the least prime dividing d, then there are at least $p_0 + 1$ pairwise quasi-orthogonal masas in $M_d(\mathbb{C})$. The proof is completely analogue, replacing the prime factors of d by their *powers* , and using the *-isomorphism

$$M_d(\mathbb{C}) \cong M_{p_0^{n_0}}(\mathbb{C}) \otimes \cdots \otimes M_{p_m^{n_m}}(\mathbb{C}).$$

An overview over existing prime power constructions

The literature concerning the subject of mutually unbiased bases growing more and more vast, we do not dare to claim to be aware of *all* methods which have so far been proposed for the construction of complete sets until today. The following list contains, to our best knowledge, the most important ones in their chronological order.

For the sake of completeness, the constructions described above are also included in that list. We have intentionally omitted some further publications that are, from our point of view, only minor variations of the construction principles above.

(1980) To all appearances, the first construction of complete MUB sets is due to W. O. Alltop, implicitly contained in an exposition concerning "Complex sequences with low periodic correlations" ([1]).

(1981) Ivanovic brings forward a method to obtain a complete set of MUBs in odd prime dimensions (Construction 3.3.4, [49]).

(1983) A paper on (general) quasi-orthogonal matrix algebras by Popa contains the standard construction in prime dimensions (Construction 3.2.5, [83]).

(1989) Besides Construction 3.3.3, Wootters and Fields also present a construction for powers of two in the article [114]. Their construction can be generalised to the planar function construction (Construction 3.3.6, [88, theorem 4.1]).

(1995) Robert Calderbank, Peter J. Cameron, William M. Kantor, and Johan J. Seidel publish an article concerning, among other aspects, so-called $\mathbb{Z}/4$-*Kerdock codes* and *orthogonal spreads* ([23]). The authors present—using a completely different terminology—constructions of complete MUB sets for all prime powers.

In 2011, Chris Godsil and Aidan Roy demonstrate that the constructions by Alltop, Wootters and Fields, Klappenecker and Rötteler, and Bandyopadhyay et al. are all special cases of the one developed in the exposition [23].

(2002a) Bandyopadhyay et al. present a construction of complete sets of MUBs in prime power dimensions, based on a partition of a unitary operator basis ([9]).

(2002b) For the case when p is odd, Subhash Chaturvedi rephrases the construction of Wootters and Fields in terms of the character vectors of the cyclic group of order p, which is helpful to explicitly write down the corresponding MUBs ([24]).

(2004a) Klappenecker and Rötteler develop alternative methods to construct complete sets of MUBs for powers of both even and odd primes in the paper [60].

(2004b) In the same year, Durt proposes an approach equivalent to the one of Wootters and Fields for odd prime powers, and a second one for even prime powers ([34]).

(2004c) Arthur O. Pittenger and Morton H. Rubin publish an article ([81]) concerning, inter alia, the construction of MUBs in prime power dimensions.

(2005) Kathleen S. Gibbons, Matthew J. Hoffman, and W. K. Wootters investigate Wigner functions over a discrete phase space, where the latter is described in terms of a Galois field ([38]).

(2007) Rod Gow presents a construction of complete sets of MUBs in even prime powers, and of certain smaller sets in the odd case, which is based on the theory of group representations ([42]). Concretely, he succeeds in constructing a matrix whose powers encode pairwise mutually unbiased bases as their columns.

(2009) Employing combinatorial designs known as (k, s)-nets, Tomasz Paterek, Borivoje Dakić, and Časlav Brukner construct complete families of pairwise quasi-orthogonal masas in the papers [79,80]. This approach is discussed in Section 3.5.

(2010) A special construction of complete sets of MUBs in (certain) Hilbert spaces of even prime power dimension $d = 2^n$ is presented by Oliver Kern, Kedar S. Ranade, and Ulrich Seyfarth in 2009 ([55], also see [95,96]). In this construction, all masas in a so-called *cyclic* complete set are obtained from one single member by conjugation with a unitary u fulfilling $u^{d+1} = \mathrm{I}_d$. (Note that this resembles the aforementioned technique of R. Gow.) An alternative representation of this approach, focussing on the implementation of MUBs in *quantum circuits* for qubits, is published in the same year ([95]).

3.4 A construction of quasi-orthogonal masa families in square dimensions

As we shall see in Chapter 4, all masa families constructed in the previous section belong to a subclass of quasi-orthogonal families called *nice.* We will further state a result of Michael Aschbacher, Andrew M. Childs and Pawel Wocjan ([3], also cf. Theorem 4.3.8), asserting that there are no nice quasi-orthogonal masa families in any dimension $d \in \mathbb{N}$ having more than $L_d + 1$ members, where the number L_d is defined according to Corollary 3.3.15.

A prominent feature of the next construction is that it allows to construct, in some dimensions, quasi-orthogonal masa families whose length *exceeds* $L_d + 1$. Notably, the quasi-orthogonal families obtained in this way are therefore *not* always nice.

We only need one new ingredient for this method, which is borrowed from a relatively young branch of mathematics dealing with so-called *combinatorial designs.* A (k, s)*-net* defined below is one example of a combinatorial design, more precisely of a so-called *block design.* Others are *finite projective planes* or *Latin squares,* which are both closely connected to (k, s)-nets. For both a good introduction and comprehensive disquisition on combinatorial designs, we refer the interested reader to either of the textbooks [26, 87].

For the rest of this section, fix a dimension $d \in \mathbb{N}$ being a square $d = s^2$ $(s \in \mathbb{N})$. We embed the elements of the field $\mathbb{F}_2$ into the integers in the usual manner, that is via the mapping $\iota : \mathbb{F}_2 \to \mathbb{Z}$, $0 \mapsto 0$, $1 \mapsto 1$. This permits to equip the d-dimensional column vector space $(\mathbb{F}_2)^d$ with a specific product $(\cdot \mid \cdot)_H : (\mathbb{F}_2)^d \times (\mathbb{F}_2)^d \to \{0, \ldots, d\}$, defined by

$$\left(\begin{pmatrix} a_0 \\ \vdots \\ a_{d-1} \end{pmatrix} \middle| \begin{pmatrix} b_0 \\ \vdots \\ b_{d-1} \end{pmatrix} \right)_H = \sum_{i=0}^{d-1} \iota(a_i b_i) \in \{0, \ldots, d\}.$$

Definition 3.4.1. *In the present context, a vector $X \in (\mathbb{F}_2)^d$ is called* incidence vector. *The number of entries of X being equal to one, that is $(X \mid X)_H$, is called* Hamming weight *of X, the set of coordinates equal to one is the* support *of X. A collection of ks incidence vectors*

$$\left\{ X_0^{(0)}, \ldots, X_{s-1}^{(0)}; X_0^{(1)}, \ldots, X_{s-1}^{(1)}; \ldots; X_0^{(k-1)}, \ldots, X_{s-1}^{(k-1)} \right\} \subset (\mathbb{F}_2)^d$$

*is called a (k, s)-*net *if it satisfies the following conditions.*

(i) The vectors in each section[*] $\{X_0^{(i)}, \ldots, X_{s-1}^{(i)}\}$ *of the net $(0 \leq i < k)$ have pairwise disjoint support, meaning that for all indices $0 \leq j_0, j_1 < s$, $j_0 \neq j_1$, we have*

$$\left(X_{j_0}^{(i)} \middle| X_{j_1}^{(i)} \right)_H = 0.$$

(ii) The supports of two vectors from different sections in the net intersect precisely in one coordinate, that is we have

$$\left(X_{j_0}^{(i_0)} \middle| X_{j_1}^{(i_1)} \right)_H = 1$$

whenever $i_0 \neq i_1$ for $0 \leq i_0, i_1 < k$, $0 \leq j_0, j_1 < s$.

[*] We replace the term *block,* used by Wocjan and Beth, by *section,* since a block in their language does not correspond to a block in the original definition of a (k, s)-net. This avoids confusion in Section 3.5.

$X_0^{(0)}$	$X_1^{(0)}$	$X_0^{(1)}$	$X_1^{(1)}$	$X_0^{(2)}$	$X_1^{(2)}$
1	0	1	0	1	0
1	0	0	1	0	1
0	1	1	0	0	1
0	1	0	1	1	0

Figure 3.5: *A* $(3,2)$*-net (a)*

The concept of a (k,s)-net is probably best understood by an example. The one you can find in the adjacent Figure 3.5 is taken from the article [112], published by Pawel Wocjan and Thomas Beth in 2004. Before we present their construction from that very article, we need one simple

Observation 3.4.2. Any column vector in a (k,s)-net has Hamming weight s.

In fact, considering the s vectors in one section $\{X_0^{(i)}, \dots, X_{s-1}^{(i)}\}$, you immediately see that condition (i) could not be satisfied if one of the vectors had support longer than s. If a vector in section number i_0 had *less* than s entries equal to one, then condition (ii) would imply that at least two vectors in any other section number $i_1 \neq i_0$ must have intersecting support, in contradiction to condition (i).

Construction 3.4.3 (Wocjan and Beth 2004)**.** Let $h = \sqrt{1/s}(\eta_{i,j})_{0\le i,j<s} \in M_s(\mathbb{C})$ denote a unitary Hadamard matrix and

$$\left\{X_0^{(0)}, \dots, X_{s-1}^{(0)}; X_0^{(1)}, \dots, X_{s-1}^{(1)}; \dots; X_0^{(k-1)}, \dots, X_{s-1}^{(k-1)}\right\} \subset (\mathbb{F}_2)^d$$

a (k,s)-net. Further label the standard basis vectors in $\mathbb{C}^d$ as $z_0, \dots, z_{d-1}$, and the ones in $(\mathbb{F}_2)^d$ as $Z_0, \dots, Z_{d-1}$.

A fixed vector in the net can then be written as $X_j^{(i)} = \sum_{r=0}^{s-1} Z_{t_r}$, where the indices $0 \le t_0, \dots, t_{s-1} < d$ are the positions of the entries being one in that vector. We thereby define s vectors

$$x_{j,m}^{(i)} = \sqrt{1/s} \sum_{r=0}^{s-1} \eta_{r,m} z_{t_r} \in \mathbb{C}^d$$

for $0 \le m < s$. Doing so for each member $X_j^{(i)}$ of the net, one obtains k orthonormal bases

$$\mathfrak{a}_i = \left(x_{0,0}^{(i)}, \dots, x_{0,s-1}^{(i)}; \dots; x_{s-1,0}^{(i)}, \dots, x_{s-1,s-1}^{(i)}\right)$$

for the Hilbert space $\mathbb{C}^d$. The bases $\mathfrak{a}_0, \dots, \mathfrak{a}_{k-1}$ are pairwise mutually unbiased.

The proof of the assertions made in this construction consists only of explicit computations of the involved scalar products and is therefore left as an exercise to the reader. As for the concept of nets, an explicit example might be the best way to clarify the method of Wocjan and Beth. The following one is also taken over from their article [112].

Example 3.4.4. We construct a family of 3 MUBs in $\mathbb{C}^4$, using the $(3,2)$-net from the table in Figure 3.5 and the unitary Hadamard matrix

$$\mathrm{F}_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \in M_2(\mathbb{C}).$$

From section number zero of our net, we obtain the basis vectors

$$x^{(0)}_{0,0} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \; x^{(0)}_{0,1} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix}, \; x^{(0)}_{1,0} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \text{ and } x^{(0)}_{1,1} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 0 \\ 1 \\ -1 \end{pmatrix}$$

in $\mathbb{C}^4$, which form an orthonormal basis $\mathfrak{a}_0$. The bases $\mathfrak{a}_1$ and $\mathfrak{a}_2$ associated with the respective sections of the net are

$$\mathfrak{a}_1 = \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ 0 \\ -1 \end{pmatrix} \right\} \quad \text{and}$$

$$\mathfrak{a}_2 = \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix} \right\}.$$

This instance is of course not very convincing, since we already know how to construct a *complete* family of five MUBs in $\mathbb{C}^4$. The crucial question is whether there are square dimensions $d = s^2$ which admit (k,s)-nets having *more* than $L_d + 1$ sections. Among several interesting aspects of the discussion of their construction, Wocjan and Beth cite two important facts in this direction (see [112, fact 2 and corollary 5]).

Facts 3.4.5. (a) There is a $(6, 26^2)$-net, implying that Construction 3.4.3 permits to construct a family of *six* MUBs in $M_{26^2}(\mathbb{C})$. Since the prime factors of 26 are 2 and 13, the prime power constructions introduced in Section 3.3 do not allow to produce more than $2 \cdot 2 + 1 = 5$ MUBs in this dimension.

(b) For all but finitely many natural numbers $s \in \mathbb{N}$, there are (k,s)-nets having $k \geq s^{1/14.8}$ sections. As a consequence, there are infinitely many dimensions s^2 (for instance, take $s \equiv 2 \bmod 4$, s large enough) where Construction 3.4.3 allows to construct more MUBs than the prime power constructions.

Both of these facts stem from results concerning *Latin squares*, some aspects of which we will discuss in the next section. For more details, we refer once more to [3] and [26].

3.5 *Excursion:* Mutually unbiased bases and design theory

Apart from the construction of Wocjan and Beth, outlined in the previous section, there are some more links between certain combinatorial designs and MUBs that are quite often alluded to in expositions on the latter. We spend some lines on these connections drawn in literature (specially in [79, 80]) in the first part of this section.

The second part concerns the important relation between MUBs and certain geometrical objects named spherical 2-designs, which was established by Klappenecker and Rötteler in 2005 ([58]).

MUBs and combinatorial designs

Roughly speaking, combinatorial designs are collections of subsets of finite sets meeting certain prescribed conditions. These conditions vary a lot for different types of designs, so that many combinatorial objects fall under this umbrella. Three of these are *nets, Latin squares,* and *projective planes.* For more details, facts, and many examples, we advise the aforementioned textbooks [26, 87].

We have already introduced (k, s)-nets in the previous section (see Definition 3.4.1). For the sequel, the following equivalent definition is more convenient.

Definition 3.5.1. *A* (k, s)-net *is a table having* s^2 *columns and k rows, with entries from a set S of* s^2 *elements, with the following properties. Each row* $0 \leq i < k$ *contains precisely all elements of S, and is divided into s (disjoint)* blocks $B_{i,0}, \ldots, B_{i,s-1} \subset S$ *of length s. A fixed block in one row intersects with each block from every other row in exactly one element.*

The definitions we have given for (k, s)-nets are equivalent to a more abstract definition that can for instance be found in [26, 3.15]. Nets are equivalent to so-called *transversal designs* (cf. [26, 3.16]), which are special instances of *group divisible designs* (cf. [87, 12.1.7]).

To kill two birds with one stone, we represent, as our first instance, the $(3, 2)$-net which has already served as an example in the previous section (see Figure 3.5) according to the definition above.

- First interpret the columns of the table in Figure 3.5 as characteristic functions on a set of $s^2 = 4$ elements, say $S = \mathbb{Z}/4$. Thereby each column corresponds to a subset of length $s = 2$, and the $ks = 3 \cdot 2$ columns are translated to the ks blocks in the alternative net definition. For instance, the two columns of the first section, i.e. the vectors $X_0^{(0)}$ and $X_1^{(0)}$, correspond to the blocks $\{0, 1\}$ and $\{2, 3\}$ respectively.

- Each section of the table in Section 3.4 becomes one row in the new representation. The order of rows, and of the blocks forming one row, is arbitrary in this process.

Translating sections to rows from left to right, one obtains the adjacent representation of the $(3,2)$-net from Figure 3.5, that is a table according to Definition 3.5.1. The blocks placed one below the other, i.e. the “columns of blocks”, are referred to as *cells.*

Nets are intimately linked to Latin squares, as we will explain in the sequel.

	$c=0$	$c=1$
	$\{0,1\}$	$\{2,3\}$
“block” →	$\{0,2\}$	$\{1,3\}$
	$\{0,3\}$	$\{1,2\}$
	↑ “cell”	

Figure 3.6: *A* $(3,2)$*-net (b)*

Definition 3.5.2. *A* Latin square *of order s is a $s \times s$-matrix with entries from a set M of cardinality s, e.g. $\mathbb{Z}/s$, such that each element of M occurs exactly once in each row and each column.*

There are Latin squares of any order, as the following standard example shows.

Example 3.5.3. Fix a natural number $s \in \mathbb{N}$ and coefficients $0 \neq q, r \in \mathbb{Z}/s$ which are coprime with s. Then a Latin square is given by the matrix

$$(qx + ry)_{0 \leq x,y < s} \in M_s(\mathbb{Z}/s).$$

For instance, one obtains the following Latin squares from this example (for the parameters $[s = 2, q = r = 1]$, $[s = 3, q = r = 1]$, and $[s = 3, q = 1, r = 2]$).

$$\begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \qquad \begin{array}{ccc} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{array} \qquad \begin{array}{ccc} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{array}$$

There is a natural orthogonality relation for Latin squares.

Definition 3.5.4. *Two Latin squares $A = (a_{i,j})$ and $B = (b_{i,j})$ of order s, with entries from a set M, are called* orthogonal *if all entries of the matrix*

$$\big(\, (a_{i,j}, b_{i,j}) \,\big)_{0 \leq i,j < s} \in M_s(M \times M)$$

are pairwise different. Such a matrix is called Graeco-Latin square *or* Euler square.

The following important standard example is checked without difficulty.

Example 3.5.5. Fix a prime $p \in \mathbb{P}$ and an element $q \in \mathbb{F}_p^\times$. All of the $p-1$ Latin squares in the family

$$\left\{ (\, qx + ry \,)_{x,y\in\mathbb{F}_p} \;\middle|\; r \in \mathbb{F}_p^\times \right\} \subset M_p(\mathbb{F}_p)$$

are mutually orthogonal.

In general, there are at most $s-1$ mutually orthogonal Latin squares, called MOLs in short, of order s, and such *complete* sets are known to exist for prime powers, whereas the maximal number of MOLs is not known for general dimensions, apart from the smallest cases (for $s = 6$, for instance, it equals one).

Given a set of Latin squares of order s with elements from a set M, each of them is orthogonal to both of the (non-Latin) squares $R = (i)_{i,j\in M}$ and $C = (j)_{i,j\in M}$, which are orthogonal to each other as well. Adding the matrices R and C to a set of MOLs, one obtains a so-called *augmented set of MOLs* .

An augmented set of MOLs of order s, containing k square matrices in all, gives rise to a (k, s)-net, as is for instance explained in [79].

Proposition 3.5.6. *For natural numbers $k, s \in \mathbb{N}$, $k \le s+1$, let $L_0, \ldots, L_{k-1}$ be an augmented set of MOLs of order s, with entries from the set $M = \mathbb{Z}/s$. In particular, label as L_0 the matrix $C = (j)_{i,j\in M}$. For each matrix $L_i = (l^i_{x,y})_{x,y\in M}$, define subsets $B_{i,0}, \ldots, B_{i,s-1}$ of $S = M \times M$ by*

$$\begin{aligned} B_{k-1,c} &= \left\{ \left(c, l^{k-1}_{c,0}\right), \ldots, \left(c, l^{k-1}_{c,s-1}\right) \right\} = \{(c,0), \ldots, (c, s-1)\} && \text{if } i = 0, \\ B_{i,c} &= \left\{ \left(0, l^{i}_{c,0}\right), \ldots, \left(s-1, l^{i}_{c,s-1}\right) \right\} && \text{for } 1 \le i \le k-1, \end{aligned}$$

where c ranges from 0 to $s-1$. Then the following table is a (k, s)-net.

$c = 0$	$\ldots$	$c = s-1$
$B_{0,0}$	$\cdots$	$B_{0,s-1}$
$\vdots$		$\vdots$
$B_{k-1,0}$	$\cdots$	$B_{k-1,s-1}$

For the proof, one solely has to check the defining properties of a (k, s)-net one after the other. What is more, the construction can be inverted, whence we get the following

Proposition 3.5.7. *The existence of $k-2$ MOLs of order s is equivalent to the existence of a (k, s)-net.*

We omit the computational proofs of the previous propositions in favour of another

Example 3.5.8. There are no two orthogonal Latin squares of order 2, so that the standard augmented set of MOLs in $M_2(\mathbb{F}_2)$ consists only of the three matrices

$$C = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \; R = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}, \; \text{and } L = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

This augmented set generates the $(3,2)$-net displayed in Figure 3.7 (where we omit the set braces for simplicity).

		$c = 0$	$c = 1$
$\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$	$\rightsquigarrow$	$(0,0),(0,1)$	$(1,0),(1,1)$
$\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$	$\rightsquigarrow$	$(0,0),(1,0)$	$(0,1),(1,1)$
$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\rightsquigarrow$	$(0,0),(1,1)$	$(0,1),(1,0)$

Figure 3.7: *A* $(3,2)$*-net (c)*

(Identifying the pairs $(m,n) \in \mathbb{F}_p^2$ with elements of the ring $\mathbb{Z}/4$ via the bijection $(m,n) \mapsto 2m+n$, this is once more the $(3,2)$-net displayed in Figures 3.5 and 3.6.)

While Wocjan an Beth interpret a (k,s)-net as an encoding scheme of k mutually unbiased bases in the Hilbert space of dimension $\mathbf{s^2}$ in [112], one can also construct sets of MUBs—or rather quasi-orthogonal masas—in the Hilbert space of dimensions $\mathbf{s}$ from certain (k,s)-nets, for the case when s is a prime power. This approach was brought forward by T. Paterek et al. in [79,80]. Here comes their construction for *prime* dimensions.

Construction 3.5.9 (Paterek et al. 2009)**.** For a prime number $p \in \mathbb{P}$, let $L_0, \dots, L_{p+1}$ be an augmented complete set of MOLs based on one of the sets in Example 3.5.5.

(a) Construct a $(p+2,p)$-net from the augmented set of MOLs $L_0, \dots, L_{p+1}$ as in Proposition 3.5.6, especially denote the blocks $B_{i,j}$ as is done there for indices $0 \le i \le p+1$ and $0 \le j < p$.

(b) For all $0 \le i \le p+1$, label the pairs in the block $B_{i,0}$ as $(m_{i,j}, n_{i,j}) \in \mathbb{F}_p^2$ for all $0 \le j < p$.

(c) Associate a *-subalgebra of the matrix algebra $M_p(\mathbb{C})$ with each of these blocks via the following assignment.

$$B_{i,0} \longmapsto \mathcal{M}_i = \mathcal{M}_{B_i} = \mathcal{A}^*\left(\mathrm{X}_p^{m_{i,0}}\mathrm{Z}_p^{n_{i,0}}, \dots, \mathrm{X}_p^{m_{i,p-1}}\mathrm{Z}_p^{n_{i,p-1}}\right)$$

Then the *-subalgebras $\mathcal{M}_0, \dots, \mathcal{M}_{p-1}$ are pairwise quasi-orthogonal masas in $M_p(\mathbb{C})$.

Applying this construction to the $(3, 2)$-net displayed in Figure 3.7, we end up with the standard family of quasi-orthogonal masas $\mathcal{A}^*(\sigma_z)$, $\mathcal{A}^*(\sigma_x)$, and $\mathcal{A}^*(\sigma_x\sigma_z)$, in other words with the standard family in $M_2(\mathbb{C})$ (see Construction 3.2.5). It is not too difficult to check that this analogously holds for all primes p.

The weak point of Construction 3.5.9 is that it does **not** connect general $(p + 2, p)$-nets to sets of MUBs, but only the ones induced by the regular family of MOLs introduced in Example 3.5.5.

The similar construction from Paterek et al. for general prime powers, which is omitted here, is subject to an analogue constraint—it also solely works for a certain "linear" standard construction of MOLs and nets respectively. It is known that there are (many) prime power dimensions where this construction is *not* unique (this follows e.g. from various instances in reference [26]).

Both in the prime and the prime power case, the underlying complete sets of MOLs encodes, in a way, the arithmetic of a Galois field. At the worst, one might therefore see Latin squares and nets on the one hand, and sets of MUBs on the other, as mathematical objects where the same field arithmetic shows through—in the most regular constructions—and nothing more. (Let us remark that the articles [79, 80] of Paterek et al. discuss, mainly from a physicist's perspective, many other interesting aspects of the relation between MUBs and MOLs.)

Last but not least, let us briefly mention that the existence of a complete set of $s - 1$ MOLs of order s is equivalent to the existence of a so-called *projective plane* of order n, and also to the existence of an *affine plane* of the same order (cf. [87, 12.3.2, fact 7]). Apart from that, the combinatorial designs considered in this section are intimately linked to *difference sets,* a topic which we have intentionally left aside. All combinatorial and geometrical objects mentioned here are discussed in the compendia [26, 87].

Complete sets of MUBs as complex projective 2-designs

In 2005, Klappenecker and Rötteler proved that a complete set of MUBs is a so-called *complex projective* 2*-design* ([58]). These designs belong to the class of *spherical t-designs,* which were introduced by Delsarte, Goethals and Seidel, and later extended by Neumaier to certain projective spaces (see e.g. [41, 46]). Although spherical t-designs owe their name to certain combinatorial designs called *t-(v, k, λ)-designs*, often named t-designs in short, they are defined in a fairly different, more geometrical spirit.

Before we can state the main result of [58], we have to recall the definition of the *projective unit sphere* in the complex Hilbert space $\mathbb{C}^d$. To this aim, we define the following equivalence relation on the unit sphere $S^{d-1} \subset \mathbb{C}^d$. We say two unit vectors $x, y \in S^{d-1}$ are equivalent, in signs $x \sim y$, if there is a factor $\lambda \in \mathbb{T}$ such that $x = \lambda y$. This is a well-defined equivalence relation, and the quotient $\mathbb{C}S^{d-1} = S^{d-1}/\sim$ is called projective unit sphere. (The manifold $\mathbb{C}S^{d-1}$ is in fact isomorphic to the projective space $\mathbb{C}P_{d-1}$.)

In the commutative polynomial ring $R = \mathbb{C}[X_0, \ldots, X_{d-1}; Y_0, \ldots, Y_{d-1}]$, we define, with Klappenecker and Rötteler, a subset Hom (k, k) as the set of all polynomials that are homogeneous of order k w.r.t. the indeterminates $X_0, \ldots, X_{d-1}$ *and* $Y_0, \ldots, Y_{d-1}$. In other words, a polynomial $p \in R$ belongs to Hom (k, k) if and only if all of its terms are of the form

$$X_0^{s_0} \cdots X_{d-1}^{s_{d-1}} \cdot Y_0^{t_0} \cdots Y_{d-1}^{t_{d-1}}$$

for exponents $s_0, \ldots, s_{d-1}, t_0, \ldots, t_{d-1} \in \mathbb{N}_0$ satisfying the equations $s_0 + \ldots + s_{d-1} = k$ and $t_0 + \ldots + t_{d-1} = k$.

As it is customary, we identify the ring of polynomials R with the associated polynomial functions. Writing vectors in $\mathbb{C}^d$ as columns (i.e. in particular fixing a basis), we can define a function $p_0 : S^{d-1} \to \mathbb{C}$ for every polynomial function $p \in$ Hom (k, k) via

$$p_0\left((\lambda_0, \ldots, \lambda_{d-1})\right) = p(\lambda_0, \ldots, \lambda_{d-1}, \bar{\lambda}_0, \ldots, \bar{\lambda}_{d-1})$$

for every vector $x = (\lambda_0, \ldots, \lambda_{d-1}) \in \mathbb{C}^d$. It is straightforward to see that we have $p_0(\mu x) = p_0(x)$ for all $\mu \in \mathbb{T}$, so that we can understand p_0 as a function on the projective unit sphere $\mathbb{C}S^{d-1}$. We denote the set of all functions obtained this way by Hom $(k, k)_0$.

Definition 3.5.10 (see [58, definition 2]). *Let μ be the unique Haar measures on the projective unit sphere $\mathbb{C}S^{d-1}$ which is invariant under unitary transformations. A finite set $X \subset \mathbb{C}S^{d-1}$ is a* complex projective t-design *if and only if the following identity holds for all functions $f \in$ Hom $(t, t)_0$.*

$$\frac{1}{|X|} \sum_{x \in X} f(x) = \frac{1}{\mu(\mathbb{C}S^{d-1})} \int_{x \in \mathbb{C}S^{d-1}} f(x) d\mu(x) \tag{3.12}$$

To put it another way, the mean of a function f in Hom $(t, t)_0$ over the points of X equals the mean of f over the whole projective unit sphere. Using elementary, very elegant arguments, Klappenecker and Rötteler prove the following

Theorem 3.5.11 (see [58, theorem 1]). *The following assertions are equivalent for any non-empty finite set $X \subset \mathbb{C}S^{d-1}$ and any integer $t \in \mathbb{N}_0$.*

(i) The set X is a complex projective t-design.

(ii) The following equation holds for all vectors $y \in \mathbb{C}^d$ and all $0 \leq k \leq t$.

$$\frac{(y \,|\, y)^k}{\binom{d+k-1}{k}} = \frac{1}{|X|} \sum_{x \in X} |(x \,|\, y)|^{2k}$$

(iii) The following equation holds for all $0 \leq k \leq t$.

$$\frac{1}{\binom{d+k-1}{k}} = \frac{1}{|X|^2} \sum_{x,y \in X} |(x \,|\, y)|^{2k} \tag{3.13}$$

Equation (3.13) says that a complex projective t-design attains *Welch's lower bounds* for all $0 \leq k \leq t$. In fact, L. Welch derived the following inequality for every non-empty finite set X of unit vectors in the Hilbert space $\mathbb{C}^d$ and all $k \geq 0$ in [105].

$$\frac{1}{\binom{d+k-1}{k}} \leq \frac{1}{|X|^2} \sum_{x,y \in X} |(x\,|\,y)|^{2k}$$

It is a matter of pure computation to check that the set of the $d(d+1)$ unit vectors contained in a complete set of MUBs satisfies equation (3.13) for $0 \leq k \leq 2$.

Corollary 3.5.12 (see [58, theorem 3])**.** *The set X of all vectors in a complete set of MUBs of the Hilbert space $\mathbb{C}^d$ is a complex projective* 2*-design.*

One crucial observation concerning this fact is that the left-hand side of equation (3.12) depends only on the function $f \in \text{Hom }(2,2)_0$, so that the right-hand side is the same for all complete sets of MUBs. We can thus record:

Corollary 3.5.13. *Every function $f \in$ Hom $(2,2)_0$ gives rise to an* invariant *for complete sets of MUBs in the Hilbert space $\mathbb{C}^d$, that is there is a constant $c_f \in \mathbb{C}$, specified by equation* (3.12)*, such that the identity*

$$\frac{1}{d(d+1)} \sum_{x \in X} f(x) = c_f$$

holds for all sets X of unit vectors defining a complete set of MUBs.

The fact that complete sets of MUBs are complex projective 2-designs has found applications for instance in the study of *entanglement* (e.g. [109]) and *entropic uncertainty relations* (e.g. [8]) of MUBs. In future, it may very well also serve as an important tool to exclude the existence of complete sets in certain dimensions.

One application is the *conservation of entanglement* for complete sets of MUBs. This is discussed by the physicists M. Wieśniak, T. Paterek, and A. Zeilinger in their paper [109]. We conclude the present section by outlining some of the aspects discussed in that exposition.

For natural numbers $a, b \geq 2$, consider the composite dimension $d = ab$. As in Convention 0.0.2, we make the following identification of Hilbert spaces.

$$\mathbb{C}^a \otimes \mathbb{C}^b \underset{\cong}{\xrightarrow{\Phi_0}} \mathbb{C}^d, \quad z_i \otimes z_j \longmapsto z_{bi+j}$$

From a physicist's viewpoint, the Hilbert space $\mathbb{C}^d$ may model a bipartite quantum system, composed of subsystems A corresponding to $\mathbb{C}^a$ and B corresponding to $\mathbb{C}^b$. Having fixed the isomorphism Φ_0 (or any other tensor product isomorphism), one says a vector $x \in \mathbb{C}^d$ is *entangled* if it cannot be written as a tensor product $x = x_0 \otimes x_1$.

Entanglement can be quantified, for instance with the help of the so-called *trace out* operation. If the considered global d-dimensional quantum system is in the (pure) state

$$x = \sum_{\substack{0 \le i < a \\ 0 \le j < b}} \lambda_{i,j} z_{bi+j} \in \mathbb{C}^d, \ \|x\| = 1,$$

one defines the so-called *reduced density matrix of x on the subsystem A* by the linear operation

$$\begin{aligned} &\mathrm{Tr}_B(x) : \mathbb{C}^a \longrightarrow \mathbb{C}^a, \\ &\quad z_{i'} \longmapsto \sum_{i=0}^{a-1} \left(\sum_{j=0}^{b-1} \left(x \mid z_{bi+j} \right) \left(z_{bi'+j} \mid x \right) \right) z_i = \sum_{i=0}^{a-1} \left(\sum_{j=0}^{b-1} \lambda_{i,j} \bar{\lambda}_{i',j} \right) z_i. \end{aligned} \tag{3.14}$$

You readily check that the operator $\mathrm{Tr}_B(x)$ corresponds to a self-adjoint and positive semi-definite matrix in $M_a(\mathbb{C})$ with (non-normalised) trace equal to one, thus to a density matrix (cf. Definition 3.1.1). As a matter of fact, $\mathrm{Tr}_B(x)$ is the density matrix of the subsystem A if the global system's state is x, i.e. it describes the observation of somebody whose observation is restricted to system A. Colloquially, physicists say the operation $x \mapsto \mathrm{Tr}_B(x)$ "traces out" the system B.

The following examples are quickly computed and may help to get a feeling for the trace out operation. As usual, we label the projection onto the line $\mathbb{C} \cdot y \subset \mathbb{C}^a$ as p_y for any vector $y \in \mathbb{C}^a$.

$$\mathrm{Tr}_B(x_0 \otimes x_1) = p_{x_0} \qquad \text{for unit vectors } x_0 \in \mathbb{C}^a, x_1 \in \mathbb{C}^b$$

$$\mathrm{Tr}_B\left(\sqrt{1/2}(x_0 \otimes y_0 + x_1 \otimes y_1)\right) = \frac{1}{2}\left(p_{x_0} + p_{x_1}\right) \qquad \begin{array}{l}\text{for orthogonal unit vectors} \\ x_0, x_1 \in \mathbb{C}^a \text{ and } y_0, y_1 \in \mathbb{C}^b\end{array}$$

$$\mathrm{Tr}_B(\sqrt{1/d} \sum_{\substack{0 \le i < a \\ 0 \le j < b}} z_{bi+j}) = \frac{1}{a} \sum_{i=0}^{a-1} p_{z_i} \tag{3.15}$$

As always, let τ be the *normalised* trace on the matrix algebra $M_a(\mathbb{C})$. We define a positive real-valued function

$$\psi : \mathbb{C}^d \longmapsto \mathbb{R}^+, \quad x \longmapsto \tau\left(\mathrm{Tr}_B(x)^2\right). \tag{3.16}$$

One easily verifies that ψ attains its maximum $1/a$ exactly on non-entangled (also called *separable*) unit vectors, and its minimum $1/a^2$ on *maximally entangled unit vectors,* that is on vectors having a reduced density matrix like the one in example (3.15) above. On that account, ψ measures the amount of entanglement for (unit) vectors in $\mathbb{C}^d$. Furthermore, a calculation reveals that the function ψ is an element of Hom $(2, 2)$, and can therefore be considered as an element of Hom $(2,2)_0$ as well. Elihu Lubkin proved in [67] that the average value of ψ over the projective unit sphere $\mathbb{C}S^{d-1}$ computes to

$$\frac{1}{\mu(\mathbb{C}S^{d-1})}\int_{x\in\mathbb{C}S^{d-1}}\psi(x)d\mu(x)=\frac{a+b}{a(d+1)}.$$

On the whole, Corollary 3.5.13 now allows to make the following

Observation 3.5.14. The entanglement function $\psi : S^{d-1} \to [1/a^2, 1/a]$, defined by the assignment (3.16), induces an *invariant* for complete sets of mutually unbiased bases in the following sense. If $X \subset S^{d-1}$ is the set of all unit vectors in a complete system of mutually unbiased bases for the Hilbert space $\mathbb{C}^d \cong \mathbb{C}^a \otimes \mathbb{C}^b$, then the following equation holds.

$$\frac{1}{d(d+1)}\sum_{x\in X}\psi(x)=\frac{a+b}{a(d+1)} \tag{3.17}$$

Assume that a number of $0 \leq s \leq d+1$ among the MUBs considered in this observation are *product bases,* i.e. consist of non-entangled vectors only. Let $Y \subset X$ denote the subset of X containing the vectors of these bases. Then Y has sd members, and equation (3.17) becomes

$$\frac{1}{d}\left(\frac{sd}{a}+\sum_{x\in X\setminus Y}\psi(x)\right)=\frac{a+b}{a}.$$

Knowing that ψ is bounded above by $1/a$, it takes a few steps to deduce from this equation that at most $s = a+1$ members of the considered set of MUBs are product bases. If this maximum is attained, then equation (3.17) leads to the identity

$$\sum_{x\in X\setminus Y}\psi(x)=\frac{b-1}{a}.$$

This last equation can only hold true if ψ attains its minimum $1/a^2$ on all vectors in the set $X \setminus Y$, that is to say, if all of these vectors are *maximally entangled.* Since we have not specified whether a exceeds b or vice versa, we can altogether record the following fact.

Observation 3.5.15 (Wieśniak et al. 2011, see [109, lemma 1])**.** For two natural numbers $2 \leq a \leq b$, fix an isomorphism of Hilbert spaces $\mathbb{C}^a \otimes \mathbb{C}^b \cong \mathbb{C}^d$. A complete set of MUBs in $\mathbb{C}^d$ contains at most $a+1$ product bases, and if this holds true, then all vectors of the remaining orthonormal bases are maximally entangled.

Although a proof has, to our best knowledge, not yet been found, it seems very unlikely that a set of $a+1$ mutually unbiased product bases like in the previous observation can be completed (or even extended?) at all.

Daniel McNulty and Stefan Weigert derived a couple of results pointing in this direction: they first demonstrated ([71,72]) that the existing sets of three mutually unbiased product bases in $\mathbb{C}^6$ are maximal, and later that even pairs of product bases in $\mathbb{C}^6$ cannot be extended to a complete set of MUBs ([73]).

Chapter 4

Nice masa families and the generalised Clifford algebra

From here on, we will mainly limit our considerations of quasi-orthogonal masa families to the subclass of *nice* masa families. These got their name from the so-called *nice unitary error bases,* which we will therefore introduce in Section 4.1.

In Section 4.2, we present a class of quasi-orthogonal masa pairs which we call *normal*. It generalises the class of standard pairs of masas on the one hand, and is compatible with a definition of nice families of MUBs given by Aschbacher et al. ([3]) in important cases on the other, as we shall demonstrate in Section 4.3.

Next, we show in Section 4.4 that the *generalised Clifford algebra* is an appropriate algebraic framework to construct any complete nice masa family. This rephrases a result of Boykin et al. in [16], where it is shown that any complete nice masa family stems from a partition of the basis $\mathfrak{F}_{p^n}$ introduced in Section 4.4.

Finally, we propose and shortly discuss another possible generalisation of standard masa pairs in Section 4.5. We show most notably that this class comprises *all* quasi-orthogonal masa families in dimension four. However, we do not further follow this line of investigation in the present work.

4.1 Nice unitary error bases

In 1996, Emanuel Knill established a concept of especially nice unitary operator bases for the matrix algebra $M_d(\mathbb{C})$ in the papers [61, 62].

Bases of unitaries for matrix algebras are often called *error bases* by physicists. This terminology stems from the fact that these bases play an important role in the construction of so-called *error correcting codes* in the area of quantum computing. We will explain this in a nutshell at the end of this section.

Proposition/Definition 4.1.1 (E. Knill 1996). *Let G be a (multiplicative) finite group of order d^2, e its neutral element, and $\mathfrak{E} = \{u_g \mid g \in G\} \subset \mathcal{U}_d$ a set of d^2 unitary $d \times d$-matrices indexed by G. If all members of $\mathfrak{E}$ besides u_e are trace-free and there are complex numbers $\omega_{g,h} \in \mathbb{C}$ for all $g, h \in G$ satisfying the equations*

$$u_g u_h = \omega_{g,h} u_{gh}, \tag{4.1}$$

then $\mathfrak{E}$ is a Hilbert-Schmidt orthonormal basis for $M_d(\mathbb{C})$, called nice (unitary) error basis.

The group G is the index group *of $\mathfrak{E}$ and $\{\omega_{g,h} \mid g, h \in G\}$ its* factor set. *The factors $w_{g,h}$ automatically have modulus one, further the unitary u_e equals the unit matrix up to a phase factor.*

Since the determinant of any unitary matrix is an element of the unit circle, there are factors $\lambda_g \in \mathbb{T}$ such that all elements in $\mathfrak{E}' = \{\lambda_g u_g \mid g \in G\}$ have determinant one. As a consequence, all factors $w'_{g,h}$ associated to $\mathfrak{E}'$ as above are dth roots of unity, and $\mathfrak{E}'$ contains the unit matrix. An error basis like $\mathfrak{E}'$ is called very nice.

Proof. The factors $\omega_{g,h}$ have modulus one by unitarity of the basis elements and equation (4.1), which further implies $u_e u_e = \omega_{e,e} u_e$ and thereby $u_e = \omega_{e,e} \mathrm{I}_d$. For all $g \in G$, it moreover leads to

$$u_g u_{g^{-1}} \;=\; \omega_{g,g^{-1}}\, u_e \;\sim_{\mathbb{T}}\; \mathrm{I}_d \;=\; u_g u_g^*$$

and thus to $u_{g^{-1}} \sim_{\mathbb{T}} u_g^*$. This ensures that

$$\left(u_g \mid u_h\right)_{\mathrm{HS}} = \tau(u_g u_h^*) \;\sim_{\mathbb{T}}\; \tau(u_g u_{h^{-1}}) \;\sim_{\mathbb{T}}\; \tau(u_{gh^{-1}}) = \begin{cases} \tau(u_e) \sim 1 & \text{if } h = g \\ 0 & \text{else} \end{cases}$$

for all $g, h \in G$, whence $\mathfrak{E}$ is a Hilbert-Schmidt orthonormal basis.

Now suppose all elements in $\mathfrak{E}$ have determinant one. From equation (4.1), we then deduce for all $g, h \in G$:

$$\begin{aligned} & & \det(u_g u_h) &= \det(\omega_{g,h} u_{gh}) \\ \Leftrightarrow & & \det(u_g)\det(u_h) &= \omega_{g,h}^d \det(u_{gh}) \\ \Leftrightarrow & & 1 &= \omega_{g,h}^d \end{aligned}$$

Hence all factors $\omega_{g,h}$ are dth roots of unity if $\mathfrak{E}$ is *very* nice. □

As a remark, it is an easy exercise to check that the index group for a given nice unitary error basis is *unique* (up to isomorphism).

Consider a *very* nice unitary error basis $\mathfrak{E} = \{u_g \mid g \in G\} \subset \mathcal{U}_d$ (which can always be gained from a nice error basis as in the proposition/definition above) with index group G. As explained before, the factor set Ω of $\mathfrak{E}$ is included in the set Z_d of d-roots of unity, hence the set

$$\{\omega\, u_g \mid \omega \in \Omega, g \in G\}$$

is a finite subgroup of the unitaries, named *error group*. A group isomorphic to an error group is usually called *abstract* error group. Knill characterised these groups in [61, theorem 2.1].

Theorem 4.1.2 (Knill 1996). *A finite group H is an (abstract) error group if and only if there is an irreducible character $\chi : H \to \mathbb{C}$ supported on the centre of H and such that the kernel of the irreducible representation associated to χ is trivial.*

The proof of implication "⇒" can be found in the Appendix on page 221. ▷

We have already come across a number of examples of nice error groups in the preceding chapters.

Examples 4.1.3. As before, let $Z_d \subset \mathbb{T}$ designate the set of all dth roots of unity and fix the primitive root $\zeta_d = \exp(2\pi\mathrm{i}/d) \in Z_d$ for all $d \in \mathbb{N}$. Further recall the d-dimensional Weyl matrices

$$\mathrm{x}_d = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & & \vdots & \vdots \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix} \in \mathcal{W}_d \quad \text{and} \quad \mathrm{z}_d = \begin{pmatrix} 1 & & & \\ & \zeta_d & & \\ & & \ddots & \\ & & & \zeta_d^{d-1} \end{pmatrix} \in \mathcal{W}_d.$$

(a) For all $0 \le i,j < d$, we define a unitary monomial matrix $u_{i,j} = \mathrm{x}_d^i \mathrm{z}_d^j \in \mathcal{U}_d$. We have seen in Example 2.2.16 that these elements are pairwise Hilbert-Schmidt orthogonal. Due to the commutation relation $\mathrm{z}_d\mathrm{x}_d = \zeta_d \mathrm{x}_d \mathrm{z}_d$, they obey the identities

$$u_{i,j}u_{k,l} = \zeta_d^{jk} u_{i+k,j+l},$$

where the indices are understood modulo d on the right-hand side, and i,j,k,l range from 0 to $d-1$. As a consequence, the set

$$\mathfrak{E} = \left\{ \mathrm{x}_d^i \mathrm{z}_d^j \;\middle|\; 0 \le i,j < d \right\} \subset \mathcal{U}_d$$

is a very nice error basis for $M_d(\mathbb{C})$ with abelian index group $\mathbb{Z}/d \times \mathbb{Z}/d$, factor set Z_d, and error group

$$H = \left\{ \zeta_d^k \mathrm{x}_d^i \mathrm{z}_d^j \;\middle|\; 0 \le i,j,k < d \right\}.$$

The (non-abelian) error group H is (an irreducible and faithful representation of) the finite Heisenberg group $N(\mathbb{Z}/d)$, also known as Heisenberg-Weyl group. An instructive discussion of these groups can be found in [4].

(b) Fix a factorisation $d = d_0 \cdots d_m$ ($m \in \mathbb{N}_0$, $d_0, \ldots, d_m \in \mathbb{N}$) of the dimension d. Then the product basis of monomial unitaries

$$\mathfrak{F}_{d_0,\ldots,d_m} = \left\{ \mathrm{X}_{d_0}^{i_0} \mathrm{Z}_{d_0}^{j_0} \otimes \cdots \otimes \mathrm{X}_{d_m}^{i_m} \mathrm{Z}_{d_m}^{j_m} \;\middle|\; 0 \le i_k, j_k \le d_k - 1 \text{ for all } 0 \le k \le m \right\}$$

inside $M_{d_0}(\mathbb{C}) \otimes \cdots \otimes M_{d_m}(\mathbb{C}) \cong M_d(\mathbb{C})$ is a very nice error basis with abelian index group

$$G = \bigoplus_{k=0}^{m} (\mathbb{Z}/d_k\mathbb{Z} \times \mathbb{Z}/d_k\mathbb{Z}) .$$

The basis $\mathfrak{F}_{d_0,\ldots,d_m}$ is indexed by G in the obvious way, namely via the assignment

$$G \ni (i_0, j_0, \ldots, i_m, j_m) \longmapsto \mathrm{X}_{d_0}^{i_0} \mathrm{Z}_{d_0}^{j_0} \otimes \cdots \otimes \mathrm{X}_{d_m}^{i_m} \mathrm{Z}_{d_m}^{j_m} .$$

The factor set Ω of $\mathfrak{F}$ is included in Z_d and depends on the given factorisation. For instance, if the dimension is a power $d = a^{m+1}$, and d_k equals a for all $0 \le k \le m$, the factor set is Z_a. It equals Z_d in case the greatest common divisor of $d_0, \ldots, d_m$ is one.

It is an exercise to check that in general, the following rule applies. For each prime $p \in \mathbb{P}$ which divides d, let $s_p \in \mathbb{N}$ denote the largest power of p dividing one of the factors $d_0, \ldots, d_m$, and label as d' the product of all powers s_p obtained this way. Then the factor set of $\mathfrak{F}_{d_0,\ldots,d_m}$ is given by $Z_{d'}$.

(c) If the dimension is a power $d = c^n$, and decomposed via $d_0 = \ldots = d_{n-1} = c$ ($c \in \mathbb{N}$), we write $\mathfrak{F}_{c^n}$ instead of $\mathfrak{F}_{c,\ldots,c}$. If $c = p$ is prime, the error basis

$$\mathfrak{F}_{p^n} = \left\{ \mathrm{X}_p^{i_0} \mathrm{Z}_p^{j_0} \otimes \cdots \otimes \mathrm{X}_p^{i_{n-1}} \mathrm{Z}_p^{j_{n-1}} \;\middle|\; 0 \le i_k, j_k < p \text{ for all } 0 \le k < n \right\} \tag{4.2}$$

coincides, up to phase factors, with the basis $\mathfrak{E}_{2n}^{p}$ employed for the construction of Bandyopadhyay et al. (see Definition/Proposition 3.3.8 and Construction 3.3.12).

We shall not leave unmentioned that there is a multitude of unitary error bases which are *not* nice. Consider for instance a nice error basis $\mathfrak{E} = \{u_g \mid g \in G\} \subset \mathcal{U}_d$. Then for any two unitaries $v, w \in \mathcal{U}_d$, the set

$$\mathfrak{E}' = \{v u_g w \mid g \in G\}$$

is certainly still a unitary error basis, but in general, the commutation relation (4.1) of a nice error basis does no longer hold. The basis $\mathfrak{E}'$ is, however, equivalent to a nice unitary error basis in the following sense.

Definition 4.1.4. *Two unitary error bases $\{u_i \mid 0 \leq i \leq d^2-1\}$, $\{u'_i \mid 0 \leq i \leq d^2-1\}$ of the $d\times d$-matrices are called equivalent if there are two unitaries $v, w \in \mathcal{U}_d$, a permutation $\sigma \in S_{d^2}$, and factors $\lambda_i \in \mathbb{T}$ such that $u'_i = \lambda_i v u_{\sigma(i)} w$ for all $0 \leq i \leq d^2-1$.*

One may ask whether every unitary error basis is, if not nice, at least *equivalent* to a nice unitary error basis. It is checked without difficulty that this holds for $M_2(\mathbb{C})$, since in this case all error bases are indeed equivalent to the (nice) basis of Pauli matrices (Example 4.1.3 (a)). The short proof can be found in the paper [59] by A. Klappenecker and M. Rötteler.

In the same exposition, the authors also present (a similar version of) the following example of an error basis for $M_4(\mathbb{C})$, showing that in general, the question raised above has negative answer. Bases which are not equivalent to any nice unitary error basis are often called *wicked.*

Example 4.1.5. Let $\alpha \in \mathbb{R}\setminus\mathbb{Q}$ be an irrational angle and define diagonal unitary matrices in $M_4(\mathbb{C})$ by

$$\begin{aligned} u_0 &= \mathrm{I}_4, \\ u_1 &= \operatorname{diag}(1, \quad 1, \quad\; -1, \quad\; -1), \\ u_2 &= \operatorname{diag}(1, -1, \quad \mathrm{e}^{2\pi\mathrm{i}\alpha}, -\mathrm{e}^{2\pi\mathrm{i}\alpha}) \\ \text{and}\quad u_3 &= \operatorname{diag}(1, -1, -\mathrm{e}^{2\pi\mathrm{i}\alpha}, \quad \mathrm{e}^{2\pi\mathrm{i}\alpha}). \end{aligned}$$

The Hilbert-Schmidt orthonormal family $\{u_0, \ldots, u_3\}$ can be completed to a unitary error basis (for instance by $\{\mathrm{x}_4^i \mathrm{z}_4^j \mid 1 \leq i \leq 3, 0 \leq j \leq 3\}$). Every such basis is wicked.

Proof. Suppose on the contrary that a unitary basis containing $\{u_0, \ldots, u_3\}$ is equivalent to a nice error basis $\mathfrak{E}$. Then there are unitaries $v, w \in \mathcal{U}_4$ and phases $\lambda, \mu \in \mathbb{T}$ such that the matrices $u'_0 = \lambda v u_0 w$ and $u'_2 = \mu v u_2 w$ belong to $\mathfrak{E}$.

Recall that due to equation (4.1), the product $u'_0 u'^*_2$ belongs, up to a phase factor, to $\mathfrak{E}$ as well (see the proof of Proposition/Definition 4.1.1). Since moreover the index group of $\mathfrak{E}$ is of order 16, there is thus a factor $n \in \mathbb{N}$ of 16 such that we have

$$\left(u'_0 u'^*_2\right)^n \sim_{\mathbb{T}} (v u_2^* v^*)^n = v(u_2^*)^n v^* \sim_{\mathbb{T}} \mathrm{I}_4,$$

so that we eventually obtain $u_2^n \sim_{\mathbb{T}} \mathrm{I}_4$. In view of the upper left entry of u_2, this leads to $u_2^n = \mathrm{I}_4$, contradicting the presumption that the angle α is irrational. □

At this point, we are able to add a criterion for the standardness of masa pairs to the list in Theorem 2.4.7, which mostly resembles item (iv) in that list.

Proposition 4.1.6. *The following assertions are equivalent for all masas $\mathcal{M}, \mathcal{N} \subset M_d(\mathbb{C})$ inside the matrix algebra $M_d(\mathbb{C})$.*

(i) The masas $\mathcal{M}$ and $\mathcal{N}$ form a standard (quasi-orthogonal) pair of masas.

(iv) There are unitary generators v_0 of $\mathcal{M}$ and v_1 of $\mathcal{N}$ having trace-free powers $v_0, \dots, v_0^{d-1}$, $v_1, \dots, v_1^{d-1}$, and commuting up to a primitive dth root of unity ω:

$$v_0 v_1 = \omega v_1 v_0 \tag{4.3}$$

(iv)′ There are unitary generators v_0 of $\mathcal{M}$ and v_1 of $\mathcal{N}$ such that a very nice error basis for $M_d(\mathbb{C})$ is given by $\mathfrak{E} = \{v_0^i v_1^j \mid 0 \le i, j < d\}$.

Proof. Suppose statement (i) holds. By definition of standard masa pairs, there is then a unitary $u \in \mathcal{U}_d$ such that the masas $\mathcal{M}$ and $\mathcal{N}$ are generated by elements $v_0 = u\mathrm{Z}_d u^*$ and $v_1 = u\mathrm{X}_d u^*$ respectively. Thereby the set $\mathfrak{E}$ defined in item $(iv)'$ equals the basis defined in Example 4.1.3 (a) up to unitary equivalence, and thus is a very nice unitary error basis.

Assertion $(iv)'$ almost immediately implies assertion (iv) by definition of very nice unitary error bases, up to the *primitivity* of the dth root ω in equation (4.3). Suppose ω were not primitive. Then you would find an exponent $0 < a < d$ such that v_1^a would commute with (all powers of) v_0. By maximality of the masa $\mathcal{M}$, this would impose v_1^a lies in $\mathcal{M} = \operatorname{span}(\mathrm{I}_d, v_0, \dots, v_0^{d-1})$, in contradiction to the linear independence of members of the basis $\mathfrak{E}$.

The implication $(iv) \Rightarrow (i)$ has been shown in the proof of Theorem 2.4.7. □

Remarks 4.1.7. (a) Although all index groups in Examples 4.1.3 are abelian, there are also nice error bases having non-abelian index groups. A method to find such nice error bases was presented by Knill in [61]. The smallest examples, occuring in dimension $d = 4$, can also be found in [56]. Pursuing our objectives, we will not come across explicit instances of non-abelian index groups in this thesis. Nevertheless, it is not necessary to limit our considerations to the abelian case in the present section.

(b) Apart from nice unitary error bases, there is a second very important construction of error bases, described by Reinhard Werner in [106], yielding the so-called *shift-and-multiply bases.* In 2003, Klappenecker and Rötteler proved in [59] that these classes of error bases are in fact different, which had not been clear from the beginning.

Nice error bases and projective unitary representations

It meets the eye that no requirements concerning the index group G are stated in Definition 4.1.1 above. At the same time, obviously not *every* group is appropriate to serve as an index group for a nice error basis (just as not any group can serve as an error group, cf. Theorem 4.1.2). To come to a better understanding of the nature of error bases and their index groups, we need to recollect a few ingredients from the theory of group representations (for finite groups). Detailed introductions to group representations can be found in many textbooks, for instance [29] and [94].

Definition 4.1.8. *The* projective unitary group $\mathcal{PU}_d$ *inside the* $d \times d$*-matrices is defined as the quotient group of the unitary group* $\mathcal{U}_d$ *by its centre* $\mathbb{T} \cdot \mathrm{I}_d$*, that is* $\mathcal{PU}_d = \mathcal{U}_d / \mathbb{T}$*. We denote the quotient map by* p*, and often write* $[u]$ *instead of* $p(u)$ *for a coset in* $\mathcal{PU}_d$ $(u \in \mathcal{U}_d)$*. Given a group* G*, a group homomorphism* $\rho : G \to \mathcal{PU}_d$ *is called* projective unitary representation *(of* G*) of order* d*.*

Informally speaking, the unitaries of a nice error basis "form a group up to phase factors". That is exactly what links them to projective representations.

Observation 4.1.9. Let G be the index group of a nice error basis $\mathfrak{E} = \{u_g \mid g \in G\}$ in $\mathcal{U}_d$. Then the mapping $G \to \mathcal{PU}_d$, $g \mapsto [u_g]$, defines a(n injective) projective unitary representation of G.

This assertion follows directly from Knill's definition of nice unitary error bases. At the same time, the trace-condition prevents that conversely, *every* projective unitary representation of a group of order d^2 gives rise to a nice unitary error basis in $M_d(\mathbb{C})$. Further requirements concerning the index group are needed.

A projective representation (in different mathematical areas) admits a so-called *pullback.* In the present context, this means the following. Given a *faithful*—that is injective—projective representation $\rho : G \to \mathcal{PU}_d$, there is a subgroup $\hat{G}$ of the unitary group $\mathcal{U}_d$ and a surjective group homomorphism $\hat{p} : \hat{G} \to G$ such that the adjacent diagram commutes. For finite groups, one can show more.

$$\begin{tikzcd}
\hat{G} \subset \mathcal{U}_d \arrow[d, "\hat{p}"'] \arrow[dr, "p"] & \\
G \arrow[r, hook, "\rho"'] & \mathcal{PU}_d
\end{tikzcd}$$

Figure 4.1: *Pullback*

Proposition 4.1.10. *Given a finite group* G *which admits a faithful projective unitary representation* $\rho : G \to \mathcal{PU}_d$*, there is a* finite *preimage* $\hat{G} \subset \mathcal{U}_d$ *(a subgroup of the unitary group* $\mathcal{U}_d$*) and a group homomorphism* $\hat{p} : \hat{G} \to G$ *such that the diagram in Figure 4.1 commutes.*

Proof. For each $g \in G$, there is a representative $u_g \in \mathcal{U}_d$ of the coset $\rho(g) \in \mathcal{PU}_d$ having determinant one. Since ρ is a projective representation, there furthermore is a factor set $\Omega = \{\omega_{g,h} \mid g, h \in G\} \subset \mathbb{T}$ such that the identity $u_g u_h = \omega_{g,h} u_{gh}$ holds for all $g, h \in G$. As explained in the proof of Proposition/Definition 4.1.1, the condition that all elements u_g have determinant one ensures that the factor set Ω is included in the group Z_d of dth roots of unity. It is therefore plain to see that

$$\hat{G} = \{\omega\, u_g \mid \omega \in Z_d, g \in G\} \subset \mathcal{U}_d$$

is a group of order at most $d \cdot \operatorname{ord}(G)$. By the faithfulness of ρ, the mapping $\hat{p} : \hat{G} \to G$, $\omega\, u_g \mapsto g$ for all $\omega \in Z_d$, is a well-defined group homomorphism, which obviously is surjective and fulfils $\rho \circ \hat{p}(\omega\, u_g) = \rho(g) = p(\omega\, u_g)$ for all $\omega \in Z_d$ and $g \in G$. □

Leaving apart the assumption that ρ is faithful in Proposition 4.1.10, one still obtains a finite preimage of $\rho(G)$ inside the unitary group, that is a finite subgroup $\hat{G} \subset \mathcal{U}_d$ with the property that $p(\hat{G})$ equals $\rho(G)$. (To see this, consider the quotient $G/\ker(\rho)$ instead of the group G in the proof above.) However, one will in general not find a well-defined group homomorphism $\hat{p}$ like in Figure 4.1.

Michael Aschbacher, Andrew M. Childs and Pawel Wocjan rephrased Knill's original definition of nice error bases in their paper [3]. (A similar reformulation had been published earlier by A. Klappenecker and M. Rötteler in [56].) This reformulation of Definition 4.1.1 reveals that nice error bases are associated to (groups admitting) projective representations of a special type. The following definition is essentially taken over from [3].

Proposition/Definition 4.1.11. *We say a subgroup $\hat{G}$ of the unitary group $\mathcal{U}_d$ is of* central type *if the image $p(\hat{G}) \subset \mathcal{PU}_d$ is of order d^2 and all unitaries in $\hat{G} \setminus \mathbb{T} \cdot \mathrm{I}_d$ are trace-free.*

A projective unitary representation $\rho : G \to \mathcal{PU}_d$ is said to be of central type if ρ is faithful *and some (and thereby each) preimage $\hat{G} \subset \mathcal{U}_d$ of $\rho(G)$ is of central type. Accordingly, the group G is of order d^2.*

Proof. For the second part, let us briefly demonstrate that the existence of one preimage $\hat{G}$ of central type for a faithful projective unitary representation $\rho : G \to \mathcal{PU}_d$ implies that every other preimage $\tilde{G} \subset \mathcal{U}_d$ of $\rho(G)$ is central as well. First of all, the images of $\hat{G}$ and $\tilde{G}$ are both of order d^2, since we have $|p(\hat{G})| = |p(\tilde{G})| = |\rho(G)|$ by diagram 4.1. (Clearly the injectivity of ρ then yields $|G| = d^2$.) What is more, there are elements $\hat{u} \in \hat{G}$ and $g \in G$ satisfying $p(\tilde{u}) = \rho(g) = p(\hat{u})$ for each unitary $\tilde{u} \in \tilde{G}$. Consequently, there is a phase factor $\lambda \in \mathbb{T}$ such that $\tilde{u} = \lambda\hat{u}$, and hence $\tilde{u}$ is trace-free if and only if the same is true for $\hat{u}$. This shows that $\tilde{G}$ is of central type as well. □

Here comes the description of nice error bases from [3].

Theorem 4.1.12 (Aschbacher et al. 2004). *A subset $\mathfrak{E}$ of the unitary matrices in $M_d(\mathbb{C})$ is a nice unitary error basis if and only if there is a group G (of order d^2) which admits a projective unitary representation $\rho : G \to \mathcal{PU}_d$* of central type *such that $\mathfrak{E}$ contains precisely one representative of $\rho(g) \in \mathcal{PU}_d$ for all $g \in G$.*

Proof. First suppose $\mathfrak{E}$ is a nice unitary error basis in the sense of Definition 4.1.1. There is then a group G of order d^2 such that we have $\mathfrak{E} = \{u_g \mid g \in G\}$, and the injective mapping

$$\rho : G \longrightarrow \mathcal{PU}_d, \quad g \longmapsto [u_g],$$

is a group homomorphism.

We choose representatives $u'_g \in [u_g] = \rho(g)$ in $\mathcal{U}_d$ having determinant one for all $g \in G$. As in the proof of Proposition 4.1.10, one sees that the factor set of the (very) nice error basis $\mathfrak{E}' = \{u'_g \mid g \in G\}$ is included in the group Z_d of dth roots of unity. The set

$$\hat{G} = \{\omega\, u'_g \mid \omega \in Z_d, g \in G\} \subset \mathcal{U}_d$$

is therefore a group and a finite preimage of $\rho(G)$. Since $\hat{G}$ is of central type by construction, the homomorphism ρ is a projective unitary representation of central type.

If conversely a projective unitary representation $\rho : G \to \mathcal{PU}_d$ of central type is given for a group G, then it directly follows $\operatorname{ord}(G) = d^2$. Fix a representative $u_g \in \rho(g)$ for all $g \in G$ and set $\mathfrak{E} = \{u_g \mid g \in G\}$. Since ρ is a group homomorphism, we know that $u_e \sim_{\mathbb{T}} \mathrm{I}_d$ and further have the identity $[u_g] \circ [u_h] = [u_{gh}]$ in $\mathcal{PU}_d$, hence $u_g u_h \sim_{\mathbb{T}} u_{gh}$ for all $g, h \in G$. Beyond that, all unitaries u_g for $e \neq g \in G$ are trace-free, because there is a preimage $\hat{G}$ of $\rho(G)$ of central type. As in the proof of Proposition/Definition 4.1.1, the last statement ensures that $\mathfrak{E}$ is actually a Hilbert-Schmidt orthonormal basis, whereas it is nice by the former assertion. □

Excursion: Nice error bases and quantum computing

In short, a quantum computer is a computational device based on quantum mechanical techniques and effects. At present, the only existing quantum computers are some small working prototypes, and the construction of such devices which can actually perform *useful* computations confronts both engineers and physicists with a number of highly non-trivial problems.

One of these obstacles is the phenomenon of *decoherence*, which is, loosely speaking, the interaction of the environment with the quantum system used for a computation. Another difficulty is the inevitable *inaccuracy* in the course of implementation of a quantum computational operation, especially if the latter depends on some non-discrete parameters.

Error correcting codes are (quantum) algorithms aiming to minimise the effects of decoherence and/or inaccuracy. Quantum algorithms are composed of a number of single unitary operations corresponding to manipulations of the quantum system (the so-called *quantum gates*), and that is where unitary error bases come into play. Without going into detail, one may guess that it makes things easier—both on a theoretical and a technical level—if the set of utilised gates enjoys some regularity properties. The term *nice* reflects this aspect.

For a concise introduction to both quantum computing and error correcting codes, we recommend the article *Fault-Tolerant Quantum Computation* by Peter W. Shor ([97]).

4.2 Normal pairs of quasi-orthogonal masas

In Sections 2.4 and 2.5, we have introduced the particularly regular *standard* quasi-orthogonal pairs of masas in $M_d(\mathbb{C})$. We have seen how a standard pair of masas in $M_d(\mathbb{C})$ "models" the action of $\mathbb{Z}/d$ on the group C*-algebra $C^*(\mathbb{Z}/d)$.

If the dimension d is a composite number, say $d = d_0 \cdots d_m$, one may more generally consider actions of the direct sum $\mathbb{Z}/d_0\mathbb{Z} \times \cdots \times \mathbb{Z}/d_m\mathbb{Z}$ on $C^*(\mathbb{Z}/d)$. We shall see that such actions are also linked to a class of quasi-orthogonal masa pairs, related to the nice error bases introduced in the previous section. Notice that we do *not* assume the factors $d_0, \dots, d_m$ to be relatively prime, so that the corresponding actions, which we will describe in detail in this section, do not in general coincide with the canonical action of $\mathbb{Z}/d$ on the group C*-algebra $C^*(\mathbb{Z}/d)$.

For a given dimension d and a factorisation $d = d_0 \cdots d_m$, we identify the matrix algebra $M_d(\mathbb{C})$ and the tensor product $M_{d_0}(\mathbb{C}) \otimes \cdots \otimes M_{d_m}(\mathbb{C})$ via the *-isomorphism defined in Convention 0.0.2 as usual. We define the matrix

$$\mathrm{F}_{d_0,\dots,d_m} = \mathrm{F}_{d_0} \otimes \cdots \otimes \mathrm{F}_{d_m} \in M_d(\mathbb{C}),$$

where the components $\mathrm{F}_{d_0} \in M_{d_0}(\mathbb{C}), \dots, \mathrm{F}_{d_m} \in M_{d_m}(\mathbb{C})$ are the Fourier matrices introduced in Definition 1.3.2. As a remark, the matrix $\mathrm{F}_{d_0,\dots,d_m}$ is an example of a *block-circulant Hadamard matrix with circulant blocks*, see Definition 1.4.5.

The following definition generalises the notion of standard masa pairs (see Definition 2.4.5).

Definition 4.2.1. *Let $d = d_0 \cdots d_m$ denote a factorisation of the dimension d ($m \in \mathbb{N}_0$, $d_0, \dots, d_m \in \mathbb{N}$). A pair $\{\mathcal{M}, \mathcal{N}\}$ of masas in $M_d(\mathbb{C})$ is called* normal *w.r.t. this factorisation if it is equivalent to the pair $\{\mathcal{D}_d, \mathrm{F}_{d_0,\dots,d_m}\mathcal{D}_d\mathrm{F}^*_{d_0,\dots,d_m}\}$. If the pair $\{\mathcal{M}, \mathcal{N}\}$ is normal w.r.t. some (unspecified) factorisation of d, we simply call it normal.*

We shall explain the name of the masa pairs so defined in the next section, more precisely by Proposition 4.3.11.

Remarks 4.2.2. Fix a factorisation $d = d_0 \cdots d_m$ of the dimension d.

(a) Observe that a normal pair is automatically quasi-orthogonal since $\mathrm{F}_{d_0,\ldots,d_m}$ is a unitary Hadamard matrix.

(b) Recall the unitary Hilbert-Schmidt basis $\mathfrak{w}_{d_0,\ldots,d_m}$ for the diagonal masa $\mathcal{D}_d$ (Example 1.4.2). It consists of all ordered products of the elements

$$w_k = \mathrm{I}_{d_0} \otimes \cdots \otimes \mathrm{I}_{d_{k-1}} \otimes \mathrm{Z}_{d_k} \otimes \mathrm{I}_{d_{k+1}} \otimes \cdots \otimes \mathrm{I}_{d_m}.$$

Due to the identity $\mathrm{X}_{d_k} = \mathrm{F}_{d_k} \mathrm{Z}_{d_k}^* \mathrm{F}_{d_k}^*$ (cf. Example 2.2.9), the masa $\mathrm{F}_{d_0,\ldots,d_m} \mathcal{D}_d \mathrm{F}_{d_0,\ldots,d_m}^*$ is generated by the monomial unitaries

$$v_k = \mathrm{F}_{d_0,\ldots,d_m}\, w_k^*\, \mathrm{F}_{d_0,\ldots,d_m}^* = \mathrm{I}_{d_0} \otimes \cdots \otimes \mathrm{I}_{d_{k-1}} \otimes \mathrm{X}_{d_k} \otimes \mathrm{I}_{d_{k+1}} \otimes \cdots \otimes \mathrm{I}_{d_m},$$

where k ranges from 0 to m. Consequently, the identity $\mathrm{F}_d \mathcal{D}_d \mathrm{F}_d^* = \mathcal{A}^*(\mathrm{X}_d)$ in the standard case is generalised to

$$\mathcal{A}^*(v_0, \ldots, v_m) = \mathrm{F}_{d_0,\ldots,d_m} \mathcal{D}_d \mathrm{F}_{d_0,\ldots,d_m}^*. \tag{4.4}$$

Be aware, however, that the masa $\mathrm{F}_{d_0,\ldots,d_m} \mathcal{D}_d \mathrm{F}_{d_0,\ldots,d_m}^*$ is in general **not** generated by the single unitary $v_0 \cdots v_m = \mathrm{X}_{d_0} \otimes \cdots \otimes \mathrm{X}_{d_m}$. In fact, one easily verifies that this product generates $\mathrm{F}_{d_0,\ldots,d_m} \mathcal{D}_d \mathrm{F}_{d_0,\ldots,d_m}^*$ if and only if the factors $d_0, \ldots, d_m$ are relatively prime.

(c) Every standard pair is of course normal (w.r.t. the trivial factorisation). For prime dimensions, the converse obviously holds as well. For composite dimensions, not all normal masa pairs are standard. For instance, we have proved in Example 2.4.9 that the diagonal masa $\mathcal{D}_4 \subset M_4(\mathbb{C})$ and the masa $\mathcal{N}$ generated by the matrices $\mathrm{I}_2 \otimes \sigma_x$ and $\sigma_x \otimes \mathrm{I}_2$ do not form a standard pair. Nevertheless, $\{\mathcal{D}_4, \mathcal{N}\}$ is normal by definition.

(d) We have already noted in Section 2.4 that all prime dimensions greater than five admit non-standard and hence non-normal pairs of quasi-orthogonal masas (cf. Fact 2.4.11). Given a composite dimension $d \in \mathbb{N}$, it lies at hand that there is only a finite number of different equivalence classes of normal masa pairs in $M_d(\mathbb{C})$, depending on the number of possible factorisations of d into prime powers. For this reason, the result by Haagerup (see Proposition 2.4.10), stating that there are uncountably many pairwise inequivalent quasi-orthogonal masa pairs in every composite dimension, gives evidence that by far not all quasi-orthogonal pairs are normal.

As for standard pairs, one may wonder whether the order of the masas $\mathcal{M}$ and $\mathcal{N}$ matters in the definition above in the following sense. Suppose there is a *-isomorphism ϕ of $M_d(\mathbb{C})$ such that

$$\phi\left(\mathcal{D}_d\right) = \mathcal{M} \quad \text{and} \quad \phi\left(\mathrm{F}_{d_0,\ldots,d_m} \mathcal{D}_d \mathrm{F}_{d_0,\ldots,d_m}^*\right) = \mathcal{N}. \tag{4.5}$$

Does this imply the existence of a second *-isomorphism ψ of $M_d(\mathbb{C})$ fulfilling

$$\psi\left(\mathcal{D}_d\right) = \mathcal{N} \quad \text{and} \quad \psi\left(\mathrm{F}_{d_0,\ldots,d_m}\mathcal{D}_d\mathrm{F}^*_{d_0,\ldots,d_m}\right) = \mathcal{M} \tag{4.6}$$

and vice versa? The answer is positive.

Lemma 4.2.3. *Given a pair $\{\mathcal{M},\mathcal{N}\}$ of masas in $M_d(\mathbb{C})$ and a factorisation $d = d_0 \cdots d_m$ of the dimension d, the existence of *-isomorphisms ϕ and ψ of $M_d(\mathbb{C})$ obeying the equations* (4.5) *and* (4.6) *respectively is equivalent.*

Proof. This statement is essentially verified analogously to the corresponding Lemma 2.4.4 for standard pairs. One only has to check that the equations $\mathrm{X}_d = \mathrm{F}_d\mathrm{Z}_d^*\mathrm{F}_d^*$ and $\mathrm{X}_d = \mathrm{F}_d^*\mathrm{Z}_d\mathrm{F}_d$, established in that very proof, generalise to

$$v_k = \mathrm{F}_{d_0,\ldots,d_m}(\mathrm{I}_{d_0} \otimes \cdots \otimes \mathrm{I}_{d_{k-1}} \otimes \mathrm{Z}^*_{d_k} \otimes \mathrm{I}_{d_{k+1}} \otimes \cdots \otimes \mathrm{I}_{d_m})\mathrm{F}^*_{d_0,\ldots,d_m} \tag{4.7}$$

$$\text{and} \quad v_k = \mathrm{F}^*_{d_0,\ldots,d_m}(\mathrm{I}_{d_0} \otimes \cdots \otimes \mathrm{I}_{d_{k-1}} \otimes \mathrm{Z}_{d_k} \otimes \mathrm{I}_{d_{k+1}} \otimes \cdots \otimes \mathrm{I}_{d_m})\mathrm{F}_{d_0,\ldots,d_m} \tag{4.8}$$

for all $0 \leq k < m$. Setting $\tilde{u} = u\mathrm{F}_{d_0,\ldots,d_m}$ for any unitary $u \in \mathcal{U}_d$, we obtain the following equivalences.

$$\begin{array}{rrlcrl}
 & u\mathcal{D}_d u^* = & \mathcal{M} & \text{and} & u\mathcal{A}^*\left(v_0,\ldots,v_m\right)u^* = & \mathcal{N} \\
\underset{(4.7)}{\Leftrightarrow} & \mathcal{D}_d & = u^*\mathcal{M}u & \text{and} & \mathrm{F}_{d_0,\ldots,d_m}\mathcal{D}_d\mathrm{F}^*_{d_0,\ldots,d_m} & = u^*\mathcal{N}u \\
\Leftrightarrow & \mathrm{F}^*_{d_0,\ldots,d_m}\mathcal{D}_d\mathrm{F}_{d_0,\ldots,d_m} & = \tilde{u}^*\mathcal{M}\tilde{u} & \text{and} & \mathcal{D}_d & = \tilde{u}^*\mathcal{N}\tilde{u} \\
\underset{(4.8)}{\Leftrightarrow} & \mathcal{A}^*\left(v_0,\ldots,v_m\right) & = \tilde{u}^*\mathcal{M}\tilde{u} & \text{and} & \mathcal{D}_d & = \tilde{u}^*\mathcal{N}\tilde{u} \\
\Leftrightarrow & \tilde{u}\mathcal{A}^*\left(v_0,\ldots,v_m\right)\tilde{u} = & \mathcal{M} & \text{and} & \tilde{u}\mathcal{D}_d\tilde{u}^* = & \mathcal{N}
\end{array}$$

Since all *-isomorphisms of $M_d(\mathbb{C})$ are inner, this proves our assertion. □

The next theorem is an analogue of Theorem 2.4.7 concerning standard masa pairs (where item (iv) corresponds to item $(iv)'$ of Proposition 4.1.6, the latter allowing a less technical generalisation than the original statement (iv) of Theorem 2.4.7).

Recall that $\mathcal{W}_d$ denotes the subgroup of monomial unitaries in $\mathcal{U}_d$. In Section 2.4, we have also defined the subgroup $\mathcal{W}(\mathcal{M},\mathcal{N}) \subset \mathcal{U}_d$, associated with a pair of masas $\{\mathcal{M},\mathcal{N}\}$, by

$$\mathcal{W}(\mathcal{M},\mathcal{N}) = \{v \in \mathcal{N} \cap \mathcal{U}_d \mid v\mathcal{M}v^* = \mathcal{M}\}\,.$$

Also recall the identity $\mathcal{W}(\mathcal{D}_d,\mathcal{N}) = \mathcal{N} \cap \mathcal{W}_d$.

Theorem 4.2.4 (Criteria for normal pairs of masas). *Let $d = d_0 \cdots d_m$ be a factorisation of the dimension d ($m \in \mathbb{N}_0$, $d_0, \ldots, d_m \in \mathbb{N}$). We define unitary monomials*

$$\begin{aligned} v_k &= \mathrm{I}_{d_0} \otimes \cdots \otimes \mathrm{I}_{d_{k-1}} \otimes \mathrm{X}_{d_k} \otimes \mathrm{I}_{d_{k+1}} \otimes \cdots \otimes \mathrm{I}_{d_m}, \\ w_k &= \mathrm{I}_{d_0} \otimes \cdots \otimes \mathrm{I}_{d_{k-1}} \otimes \mathrm{Z}_{d_k} \otimes \mathrm{I}_{d_{k+1}} \otimes \cdots \otimes \mathrm{I}_{d_m} \in \mathcal{W}_d \end{aligned}$$

for all $0 \leq k \leq m$ as before. For any unitary matrix $u \in \mathcal{U}_d$ and associated masa $\mathcal{M} = u\mathcal{D}_d u^*$ in $M_d(\mathbb{C})$, the following statements are equivalent.

(i) The pair $\{\mathcal{D}_d, \mathcal{M}\}$ is a normal pair of masas w.r.t. the factorisation $d = d_0 \cdots d_m$.

(iia) There is a *-automorphism $\phi : M_d(\mathbb{C}) \to M_d(\mathbb{C})$ satisfying the identities

$$\phi\left(\mathcal{D}_d\right) = \mathcal{D}_d \quad \text{and} \quad \phi\left(\mathcal{A}^*\left(v_0, \ldots, v_m\right)\right) = \mathcal{M}.$$

(iib) There is a *-automorphism $\psi : M_d(\mathbb{C}) \to M_d(\mathbb{C})$ satisfying the identities

$$\psi\left(\mathcal{D}_d\right) = \mathcal{M} \quad \text{and} \quad \psi\left(\mathcal{A}^*\left(v_0, \ldots, v_m\right)\right) = \mathcal{D}_d.$$

(iiia) The unitary u is a Hadamard matrix equivalent to $\mathrm{F}_{d_0,\ldots,d_m}$.

(iiib) The unitary u^* is a Hadamard matrix equivalent to $\mathrm{F}_{d_0,\ldots,d_m}$.

(iv) There are unitary generators $\tilde{w}_0, \ldots, \tilde{w}_m$ of $\mathcal{D}_d$ and $\tilde{v}_0, \ldots, \tilde{v}_m$ of $\mathcal{M}$ such that the set

$$\mathfrak{E} = \left\{ \tilde{v}_0^{i_0} \cdots \tilde{v}_m^{i_m} \tilde{w}_0^{j_0} \cdots \tilde{w}_m^{j_m} \;\middle|\; 0 \leq i_k, j_k < d_k \text{ for all } 0 \leq k \leq m \right\}$$

is a very nice unitary error basis for the matrix algebra $M_d(\mathbb{C})$, indexed by the abelian group $\bigoplus_{k=0}^m (\mathbb{Z}/d_k \times \mathbb{Z}/d_k)$ in the obvious manner (cp. Example 4.1.3 (b)).

(va) The masa $\mathcal{M}$ is quasi-orthogonal to $\mathcal{D}_d$ and generated by unitaries $\tilde{v}_0, \ldots, \tilde{v}_m \in \mathcal{U}_d$ such that $\tilde{v}_k^{d_k} = \mathrm{I}_d$ and $\tilde{v}_k \mathcal{D}_d \tilde{v}_k^* = \mathcal{D}_d$ for all $0 \leq k \leq m$.

(vb) The masa $\mathcal{D}_d$ is quasi-orthogonal to $\mathcal{M}$ and generated by unitaries $\tilde{w}_0, \ldots, \tilde{w}_m \in \mathcal{U}_d$ such that $\tilde{w}_k^{d_k} = \mathrm{I}_d$ and $\tilde{w}_k \mathcal{M} \tilde{w}_k^* = \mathcal{M}$ for all $0 \leq k \leq m$.

(via) The masas $\mathcal{D}_d$ and $\mathcal{M}$ are quasi-orthogonal, and there is an isomorphism of abelian groups

$$\mathcal{W}\left(\mathcal{D}_d, \mathcal{M}\right) / \left(\mathbb{T} \cdot \mathrm{I}_d\right) \cong \mathbb{Z}/d_0 \times \cdots \times \mathbb{Z}/d_m.$$

(vib) The masas $\mathcal{D}_d$ and $\mathcal{M}$ are quasi-orthogonal, and there is an isomorphism of abelian groups

$$\mathcal{W}\left(\mathcal{M}, \mathcal{D}_d\right) / \left(\mathbb{T} \cdot \mathrm{I}_d\right) \cong \mathbb{Z}/d_0 \times \cdots \times \mathbb{Z}/d_m.$$

Proof. Recall that we have $\mathcal{A}^*(v_0, \ldots, v_m) = \mathrm{F}_{d_0,\ldots,d_m}\mathcal{D}_d\mathrm{F}^*_{d_0,\ldots,d_m}$ by equation (4.4). By definition of equivalence for masa pairs (cf. Definition 2.4.1), condition (i) holds true if and only if at least one of the conditions (iia) and (iib) is fulfilled. As the latter are equivalent by Lemma 4.2.3, the equivalences $(i) \Leftrightarrow (iia) \Leftrightarrow (iib)$ are clear.

Replacing F_d by $\mathrm{F}_{d_0,\ldots,d_m}$ in the proof of Theorem 2.4.7, one proves the equivalences $(iia) \Leftrightarrow (iiia)$ and $(iib) \Leftrightarrow (iiib)$ in just the same way as the respective equivalences in that earlier proof.

The schemes below give an overview over the implications we shall demonstrate in the sequel.

$$\begin{tikzcd}
(a) & (iia) \arrow[r, Rightarrow] \arrow[d, Rightarrow] & (via) \arrow[d, Rightarrow] & (b) & (iib) \arrow[r, Rightarrow] & (vib) \arrow[d, Rightarrow] \\
 & (iv) \arrow[r, Rightarrow] & (va) \arrow[ul, Rightarrow] & & & (vb) \arrow[ul, Rightarrow]
\end{tikzcd}$$

Once the steps in diagram (a) are proved, it is straightforward to deduce the implications of diagram (b) from the analogues in (a). To this aim, one intermediately applies the unitary conjugation $u^* \cdot u$, precisely as done for the respective implications in the proof of Theorem 2.4.7.

$\boldsymbol{(iia) \Rightarrow (iv).}$ We define unitary matrices $\tilde{v}_k = \phi(v_k)$, $\tilde{w}_k = \phi(w_k)$ for all $0 \leq k \leq m$. The basis $\mathfrak{E}$ is thereby unitarily equivalent to the basis $\mathfrak{S}_{d_0,\ldots,d_m}$ introduced in Example 4.1.3 (b), and hence a very nice unitary error basis with the stated index group.

$\boldsymbol{(iv) \Rightarrow (va).}$ By assumption, the unitaries $\tilde{v}_0, \ldots, \tilde{v}_m$ generate the masa $\mathcal{M}$. The error basis $\mathfrak{E}$ being nice, they moreover commute with the generators $\tilde{w}_0, \ldots, \tilde{w}_m$ of the diagonal $\mathcal{D}_d$ up to phase factors, implying the identities $\tilde{v}_k\mathcal{D}_d\tilde{v}_k^* = \mathcal{D}_d$ for all $0 \leq k \leq m$. By the structure of the index group of $\mathfrak{E}$, we can further assume $\tilde{v}_k^{d_k} = \mathrm{I}_d$ for all indices $0 \leq k \leq m$ w.l.o.g.

Elements of $\mathfrak{E}$ being pairwise Hilbert-Schmidt orthogonal, we specially have

$$\left(\tilde{v}_0^{i_0} \cdots \tilde{v}_m^{i_m} \,\middle|\, \tilde{w}_0^{j_0} \cdots \tilde{w}_m^{j_m} \right)_{\mathrm{HS}} = 0$$

for all $0 \leq i_k, j_k < d_k$, $0 \leq k \leq m$, apart from the case that all exponents i_k, j_k equal zero. Put differently, the masas $\mathcal{D}_d$ and $\mathcal{M}$ are quasi-orthogonal.

$\boldsymbol{(iia) \Rightarrow (via).}$ Applying the *-isomorphism ϕ^{-1}, we first have

$$\begin{aligned}
\mathcal{W}\left(\mathcal{D}_d, \mathcal{M}\right) / \left(\mathbb{T} \cdot \mathrm{I}_d\right) &\cong \phi^{-1}\left(\mathcal{W}\left(\mathcal{D}_d, \mathcal{M}\right)\right) / \phi^{-1}\left(\mathbb{T} \cdot \mathrm{I}_d\right) \\
&= \mathcal{W}\left(\mathcal{D}_d, \mathcal{A}^*\left(v_0, \ldots, v_m\right)\right) / \left(\mathbb{T} \cdot \mathrm{I}_d\right).
\end{aligned}$$

As noticed directly before the present proposition, we furthermore know that

$$\mathcal{W}\left(\mathcal{D}_d, \mathcal{A}^*\left(v_0, \ldots, v_m\right)\right) = \mathcal{A}^*\left(v_0, \ldots, v_m\right) \cap \mathcal{W}_d,$$

i.e. $\mathcal{W}(\mathcal{D}_d, \mathcal{A}^*(v_0, \ldots, v_m))$ is the group of monomial unitaries inside $\mathcal{A}^*(v_0, \ldots, v_m)$. Clearly this group contains the subgroup of $\mathcal{U}_d$ generated by the matrices $v_0, \ldots, v_m$, which is easily seen to be isomorphic to $\mathbb{Z}/d_0 \times \cdots \times \mathbb{Z}/d_m$.

Now consider any unitary monomial matrix $u \in \mathcal{A}^*(v_0, \ldots, v_m)$. It can be written in the form

$$u = \sum_{0 \leq i_0 \leq d_0, \ldots, 0 \leq i_m \leq d_m} \lambda_{i_0, \ldots, i_m} v_0^{i_0} \cdots v_m^{i_m}$$

for some coefficients $\lambda_{i_0, \ldots, i_m} \in \mathbb{C}$. It presents no difficulty to specify the action of u in the tensor product picture. (Recall that we always presume the isomorphisms defined in Convention 0.0.2.) For the vector $z_0 \otimes \cdots \otimes z_0$, we compute

$$\begin{aligned} u\left(z_0 \otimes \cdots \otimes z_0\right) &= \sum_{0 \leq i_0 < d_0, \ldots, 0 \leq i_m < d_m} \lambda_{i_0, \ldots, i_m} v_0^{i_0} \cdots v_m^{i_m} \left(z_0 \otimes \cdots \otimes z_0\right) \\ &= \sum_{0 \leq i_0 < d_0, \ldots, 0 \leq i_m < d_m} \lambda_{i_0, \ldots, i_m} \mathrm{X}_{d_0}^{i_0} z_0 \otimes \cdots \otimes \mathrm{X}_{d_m}^{i_m} z_0 \\ &= \sum_{0 \leq i_0 < d_0, \ldots, 0 \leq i_m < d_m} \lambda_{i_0, \ldots, i_m} z_{i_0} \otimes \cdots \otimes z_{i_m}. \end{aligned}$$

Since u is monomial by assumption, the last line reveals that *exactly one* of the coefficients $\lambda_{i_0, \ldots, i_m}$ is non-zero. As u is unitary, this coefficient automatically has modulus one. We have thereby shown that the group of monomials in $\mathcal{A}^*(v_0, \ldots, v_m)$ is precisely given by

$$\left\{ \lambda v_0^{i_0} \cdots v_m^{i_m} \;\middle|\; \lambda \in \mathbb{T}, 0 \leq i_k < d_k, 0 \leq k \leq m \right\}.$$

In regard to the identities above, this is assertion (via).

$\boldsymbol{(via) \Rightarrow (va)}$. Let $\rho : \mathbb{Z}/d_0 \times \cdots \times \mathbb{Z}/d_m \to \mathcal{W}\left(\mathcal{D}_d, \mathcal{M}\right) / \left(\mathbb{T} \cdot \mathrm{I}_d\right)$ denote the group isomorphism existing by assumption. For each $0 \leq k \leq m$, pick a representative $\tilde{v}_k$ in $\mathcal{M} \cap \mathcal{W}_d$ of $\rho((0, \ldots, 0, 1, 0, \ldots, 0))$, where the non-zero entry stands at the kth position, such that $\tilde{v}^{d_k} = \mathrm{I}_d$. Being monomials, the unitaries $\tilde{v}_k$ obey the equalities

$$\tilde{v}_k \mathcal{D}_d \tilde{v}_k^* = \mathcal{D}_d,$$

where k ranges from 0 to m. What is more, each of the monomial products $\tilde{v}_0^{i_0} \cdots \tilde{v}_m^{i_m}$ in $\mathcal{M}$ is either of the form $\lambda \mathrm{I}_d$ for a factor $\lambda \in \mathbb{T}$ or has empty diagonal (that is, all diagonal elements are zero). This follows from the quasi-orthogonality of $\mathcal{M}$ and $\mathcal{D}_d$, cf. Corollary 2.2.15. As a consequence, the set

$$\left\{ \tilde{v}_0^{i_0} \cdots \tilde{v}_m^{i_m} \;\middle|\; 0 \leq i_k < d_k, 0 \leq k \leq m \right\}$$

forms a Hilbert-Schmidt orthonormal system inside $\mathcal{M}$. The fact that ρ is a bijection ensures that the this orthonormal system spans a space of dimension d, since the following implications hold for all $0 \le i_k, j_k < d_k$, $0 \le k \le m$.

$$\begin{aligned} & \left(\tilde{v}_0^{i_0} \cdots \tilde{v}_m^{i_m} \,\middle|\, \tilde{v}_0^{j_0} \cdots \tilde{v}_m^{j_m}\right)_{\mathrm{HS}} = \tau(\tilde{v}_0^{i_0-j_0} \cdots \tilde{v}_m^{i_m-j_m}) \sim_{\mathbb{T}} \mathrm{I}_d \\ \Rightarrow \quad & \rho((i_0 - j_0, \dots, i_m - j_m)) = [\mathrm{I}_d] \\ \underset{(\rho \text{ bij.})}{\Rightarrow} \quad & i_0 = j_0, \dots, i_m = j_m \end{aligned}$$

In other words, the elements $\tilde{v}_0, \dots, \tilde{v}_m$ generate the masa $\mathcal{M}$.
$(va) \Rightarrow (iia)$. For a moment, consider the diagonal masa $\mathcal{D}_d$ as a Hilbert space, endowed with the Hilbert-Schmidt scalar product. According to Lemma 1.2.5, the conjugations by the monomials $\tilde{v}_k$ define *-automorphisms of the masa $\mathcal{D}_d$, hence in particular bijective linear mappings. Since the trace of any diagonal matrix is preserved under unitary conjugations, the maps

$$\begin{aligned} L_k : \mathcal{D}_d &\longrightarrow \mathcal{D}_k, \\ x &\longmapsto \tilde{v}_k x \tilde{v}_k^*, \end{aligned}$$

are unitary transformations of the Hilbert space $(\mathcal{D}_d, (\cdot \mid \cdot)_{\mathrm{HS}})$ for $0 \le k \le m$. Their eigenvalues, lying in the unit circle, must be d_kth roots of unity, because we have

$$L_k^d(x) = \tilde{v}_k^{d_k} \, x \, (\tilde{v}_k^*)^{d_k} = x$$

for all $x \in \mathcal{D}_d$ by assumption. What is more, the operators $L_0, \dots, L_m$ pairwise commute since the unitaries $\tilde{v}_0, \dots, \tilde{v}_m$ do so. There is hence an orthonormal basis of common eigenvectors of the operators L_k, that is a set of pairwise Hilbert-Schmidt orthogonal diagonal matrices having unit (normalised) trace

$$\mathfrak{X} = \{x_s \mid 0 \le s < d\} \subset \mathcal{D}_d.$$

With each element $x_s \in \mathfrak{X}$, we can associate an $(m+1)$-tuple in $\bigoplus_{k=0}^m \{0, \dots, d_k - 1\}$ as follows. The vector x_s being an eigenvector of L_k, there is an exponent $0 \le i_{s,k} < d_k$ such that we have

$$L_k(x_s) = \zeta_{d_k}^{i_{s,k}} x_s,$$

where $0 \le s < d$ and $0 \le k \le m$. (As always, we set $\zeta_{d_k} = \exp(2\pi \mathrm{i}/d_k) \in \mathbb{T}$ for all $0 \le k \le m$.) We can thus assign to each basis matrix $x_s \in \mathfrak{X}$ an $(m+1)$-tuple via a mapping

$$\begin{aligned} \gamma : \mathfrak{X} &\longrightarrow \bigoplus_{k=0}^{m} \{0, \dots, d_k - 1\}, \\ x_s &\longmapsto T_s = (i_{s,0}, \dots, i_{s,m}). \end{aligned}$$

Consider two basis elements $x_s, x_t \in \boldsymbol{\mathfrak{X}}$ sharing the same index tuple $T_s = T_t$. This asserts the equations

$$\begin{aligned} L_k\left(x_s x_t^*\right) &= \tilde{v}_k\, x_s x_t^*\, \tilde{v}_k^* = \tilde{v}_k x_s \tilde{v}_k^*\ \left(\tilde{v}_k x_t^* \tilde{v}_k^*\right) \\ = \tilde{v}_k x_s \tilde{v}_k^*\ \left(\tilde{v}_k x_t \tilde{v}_k^*\right)^* &= \zeta_{d_k}^{i_{s,k}-i_{t,k}} x_s x_t^* \underset{(T_s=T_t)}{=} x_s x_t^*, \end{aligned}$$

and thereby $\tilde{v}_k\left(x_s x_t^*\right) = \left(x_s x_t^*\right)\tilde{v}_k$ for all $0 \leq k \leq m$. As a consequence, the matrix $x_s x_t^* \in \mathcal{D}_d$ belongs to the masa $\mathcal{M}$ at the same time. Since $\mathcal{M}$ and $\mathcal{D}_d$ are quasi-orthogonal, this means $x_s x_t^* = \lambda \mathrm{I}_d$ for a factor $\lambda \in \mathbb{C}$ clearly being non-zero, so we end up with

$$\left(x_s \mid x_t\right)_{\mathrm{HS}} = \tau\left(x_s x_t^*\right) = \lambda \neq 0.$$

As x_s and x_t belong to one and the same Hilbert-Schmidt orthonormal system, this leads to $x_s = x_t$. We have thereby shown that the mapping γ is a bijection, because $\boldsymbol{\mathfrak{X}}$ and $\bigoplus_{k=0}^{m}\{0,\ldots,d_k-1\}$ are both of cardinality d.

For all $0 \leq k \leq m$, the d_kth power of the basis element

$$\tilde{w}_k = \gamma^{-1}((0,\ldots,0,\underset{\substack{| \\ (k\text{th pos.})}}{1},0,\ldots,0)) \in \boldsymbol{\mathfrak{X}}$$

is invariant under all mappings $L_0,\ldots,L_m$, and hence a multiple of the unit matrix by the same argument as used for the element $x_s x_t^*$ above. We can assume $\tilde{w}_k^{d_k} = \mathrm{I}_d$ without loss of generality. It is no problem to check that the set

$$\left\{ \tilde{v}_0^{i_0}\cdots\tilde{v}_m^{i_m}\tilde{w}_0^{j_0}\cdots\tilde{w}_m^{j_m} \;\middle|\; 0 \leq i_k, j_k < d_k \ \text{ for all } \ 0 \leq k \leq m \right\}$$

is a Hilbert-Schmidt orthonormal basis for $M_d(\mathbb{C})$ (in fact, a very nice unitary error basis, proving (iv) as a byproduct). We can therefore define a linear bijection of $M_d(\mathbb{C})$ by

$$\phi : v_0^{i_0}\cdots v_m^{i_m} w_0^{j_0}\cdots w_m^{j_m} \longmapsto \tilde{v}_0^{i_0}\cdots\tilde{v}_m^{i_m}\tilde{w}_0^{j_0}\cdots\tilde{w}_m^{j_m} \quad (0 \leq i_k, j_k < d_k, 0 \leq k \leq m).$$

The crucial point now is that the elements $\tilde{w}_k, \tilde{v}_l$ fulfil the *same relations* as the elements w_k, v_l for all $0 \leq k, l \leq m$, that is

$$\tilde{w}_k^{d_k} = \tilde{v}_k^{d_k} = \mathrm{I}_d, \quad \tilde{w}_k\tilde{w}_l = \tilde{w}_l\tilde{w}_k, \quad \tilde{v}_k\tilde{v}_l = \tilde{v}_l\tilde{v}_k, \quad \text{and} \quad \tilde{w}_k\tilde{v}_l = \begin{cases} \zeta_{d_k}\tilde{w}_l\tilde{v}_k & \text{if } k = l, \\ \tilde{w}_k\tilde{v}_l & \text{else.} \end{cases}$$

(By the by, observe that these relations coincide with the ones fulfilled by the matrices B_i and C_i introduced in Definition/Proposition 3.3.8.) This identity of relations ensures that ϕ is not only linear, but also *multiplicative,* which is first checked on the (algebraic) generators v_k, w_k, then carried over to products, and eventually to arbitrary polynomials in the generators by linearity. What is more, the first of these relations yields the identities $(\tilde{w}_k^i)^* = \tilde{w}_k^{d_k-i}$ and $(\tilde{v}_k^i)^* = \tilde{v}_k^{d_k-i}$ for all $0 \leq k \leq m$, $0 \leq i \leq d_k$. As a consequence, the mapping ϕ is compatible with the involution, that is we have the identity $\phi(a^*) = \phi(a)^*$ for all $a \in M_d(\mathbb{C})$, which is again first checked on the generators and then deduced for arbitrary polynomials.

Altogether, we have shown that ϕ is in fact a **-isomorphism*of $M_d(\mathbb{C})$. Clearly the masas $\mathcal{D}_d$ and $\mathcal{M}$ are invariant under the action of ϕ. This completes our proof. □

As a remark, the arguments in the final paragraphs of the proof above are more elegantly expressed in the language of *generators and relations,* which we shall introduce in Section 4.4.

Recall the *Fundamental Theorem of Finite Abelian Groups,* stating that every such group can be decomposed into a direct sum of cyclic subgroups of prime power order (see e.g. [92, theorem 2.41]). In regard to item (*via*) of Theorem 4.2.4, normal masa pairs associated to different factorisations of the dimension d might thus still be isomorphic. For instance, the standard masa pair in $M_{15}(\mathbb{C})$ is isomorphic to the normal pair w.r.t. the factorisation $15 = 3 \cdot 5$, due to the isomorphism $\mathbb{Z}/15 \cong \mathbb{Z}/3 \times \mathbb{Z}/5$. In general, there are of course non-isomorphic finite abelian groups sharing the same order, the smallest example being the *Klein four-group* $\mathbb{Z}/2 \times \mathbb{Z}/2$ and the cyclic group $\mathbb{Z}/4$.

The following corollary is an immediate consequence of Theorem 4.2.4.

Corollary 4.2.5. *Let $\mathcal{M}, \mathcal{N}$ and $\mathcal{M}', \mathcal{N}'$ be two pairs of masas in $M_d(\mathbb{C})$ being normal with respect to factorisations $d = d_0 \cdots d_m$ and $d = d_0' \cdots d_n'$ respectively. Then these pairs are equivalent if and only if there is an isomorphism of abelian groups*

$$\mathbb{Z}/d_0 \times \cdots \times \mathbb{Z}/d_m \cong \mathbb{Z}/d_0' \times \cdots \times \mathbb{Z}/d_n'.$$

According to the Fundamental Theorem of Finite Abelian Groups, it is thus no loss of generality to consider only normal masa pairs corresponding to factorisations of d into (not necessarily maximal) prime powers.

Excursion: Normal masa pairs and crossed products

In the excursional Section 2.5, we have seen that the standard masa pair $\{\mathcal{D}_d, \mathcal{A}^*(\chi_d)\}$ "models" a group action $\alpha : \mathbb{Z}/d \to \operatorname{Aut} C^*(\mathbb{Z}/d)$, $i \mapsto \alpha(i) = \alpha_i$, of the cyclic group $\mathbb{Z}/d$ on the group C*-algebra $C^*(\mathbb{Z}/d)$. The latter is, as we have explained in detail at that point, just the convolution algebra of complex-valued L^1-functions on d different points.

For a general function $f \in C^*(\mathbb{Z}/d)$, the automorphism α_1 is given by the formula

$$(\alpha_1 f)(i) = f(i-1) \ \text{ for all } \ i \in \mathbb{Z}/d,$$

cf. equation (2.12) on page 67. The group action α is injective, and as we have discussed in Section 2.5, the crossed product $C^*(\mathbb{Z}/d) \rtimes_\alpha \mathbb{Z}/d$ is therefore isomorphic to the matrix algebra $M_d(\mathbb{C})$.

Roughly speaking, an isomorphic matrix representation of $C^*(\mathbb{Z}/d) \rtimes_\alpha \mathbb{Z}/d$ is obtained as follows. First embed the function algebra $C^*(\mathbb{Z}/d)$ into the $d{\times}d$-matrices as diagonal masa $\mathcal{D}_d$. On the matrix level, the *-automorphism α_1 on $C^*(\mathbb{Z}/d)$ then corresponds to the conjugation of $\mathcal{D}_d$ by the shift matrix X_d. For this reason, there is a surjective *-homomorphism (the integrated form computed in equation (2.13)) mapping the crossed product to the *-subalgebra $C^*(\mathcal{D}_d, \mathrm{X}_d)$ of $M_d(\mathbb{C})$. As we have seen at several points in this work, the latter *-subalgebra is the whole matrix algebra $M_d(\mathbb{C})$. The dimension of the crossed product $C^*(\mathbb{Z}/d) \rtimes_\alpha \mathbb{Z}/d$ being d^2, we thus end up with an isomorphic *-representation

$$C^*(\mathbb{Z}/d) \rtimes_\alpha \mathbb{Z}/d \cong C^*(\mathcal{D}_d, \mathrm{X}_d) = M_d(\mathbb{C}).$$

In the sequel, we will briefly outline how normal masa pairs generalise this situation. To this end, we fix a factorisation $d = d_0 \cdots d_m$ of the dimension and make the usual identification $M_d(\mathbb{C}) \cong M_{d_0}(\mathbb{C}) \otimes \cdots \otimes M_{d_m}(\mathbb{C})$ (cp. Convention 0.0.2).

For each factor $\mathcal{D}_{d_k}$ of the diagonal $\mathcal{D}_d \cong \mathcal{D}_{d_0} \otimes \cdots \otimes \mathcal{D}_{d_m}$, we denote the minimal diagonal projections generating $\mathcal{D}_{d_k}$ by $q_0, \ldots, q_{d_k-1}$ as before. The minimal projections on the diagonal masa $\mathcal{D}_d$ are then given by tensor products of the form $q_{i_0} \otimes \cdots \otimes q_{i_m}$ for indices $0 \le i_k < d_k$, $0 \le k \le m$.

An injective group action $\mathbb{Z}/d_0 \times \cdots \times \mathbb{Z}/d_m \hookrightarrow \mathrm{Aut}\,(\mathcal{D}_d)$ is defined as follows. First we denote *-automorphisms $\tilde{\beta}_{[k]} : \mathcal{D}_d \to \mathcal{D}_d$ for all $0 \le k \le m$ by the formula

$$\begin{aligned}\tilde{\beta}_{[k]}\left(q_{i_0} \otimes \cdots \otimes q_{i_k} \otimes \cdots \otimes q_{i_m}\right) &= v_k \left(q_{i_0} \otimes \cdots \otimes q_{i_k} \otimes \cdots \otimes q_{i_m}\right) v_k^* \\ &= \left(q_{i_0} \otimes \cdots \otimes \mathrm{X}_{d_k} q_{i_k} \mathrm{X}_{d_k}^* \otimes \cdots \otimes q_{i_m}\right) \\ &= \left(q_{i_0} \otimes \cdots \otimes q_{i_k+1} \otimes \cdots \otimes q_{i_m}\right),\end{aligned}$$

where the unitary matrices $v_0, \ldots, v_m \in \mathcal{U}_d$ are given by

$$v_k = \mathrm{I}_{d_0} \otimes \cdots \otimes \mathrm{I}_{d_{k-1}} \otimes \mathrm{X}_{d_k} \otimes \mathrm{I}_{d_{k+1}} \otimes \cdots \otimes \mathrm{I}_{d_m}$$

as in Theorem 4.2.4, and the indices $0 \le i_k < d_k$ are understood modulo d_k for all indices $0 \le k \le m$.

Now the following assignment induces a group action.

$$\begin{aligned}\tilde{\beta} : \mathbb{Z}/d_0 \times \cdots \times \mathbb{Z}/d_m &\longrightarrow \mathrm{Aut}\,(\mathcal{D}_d) \\ (0, \ldots, 0, \underset{\substack{| \\ (k\text{th pos.})}}{1}, 0, \ldots, 0) &\longmapsto \tilde{\beta}_{[k]}\end{aligned}$$

Notice that it is important that the unitaries $v_0, \ldots, v_m$—and thereby the actions $\tilde{\beta}_{[k]}$—commute, for the represented group is abelian. It is easily checked that the so-defined group action $\tilde{\beta}$ is injective.

The unitary matrices $v_0, \ldots, v_m \in \mathcal{U}_d$ generate the masa $\mathcal{M}$ of the normal pair $\{\mathcal{D}_d, \mathcal{M}\}$ considered in Theorem 4.2.4, and therefore we know (cf. for instance item (iv)) that the *-subalgebra $C^*(\mathcal{D}_d, v_0, \ldots, v_m)$ is in fact the whole matrix algebra $M_d(\mathbb{C})$.

Identifying the diagonal masa and the function algebra $C^*(\mathbb{Z}/d)$ as explained in Section 2.5, the group action $\tilde{\beta}$ on the diagonal masa corresponds to an action

$$\beta : \mathbb{Z}/d_0 \times \cdots \times \mathbb{Z}/d_m \hookrightarrow \operatorname{Aut} C^*(\mathbb{Z}/d).$$

The crucial point is that the action $\tilde{\beta}$ on the diagonal masa is *inner* in the *-algebra $C^*(\mathcal{D}_d, v_0, \ldots, v_m)$. This is precisely the basic idea behind the crossed product construction, and similar as in Section 2.5, one can now establish a surjective *-homomorphism

$$C^*(\mathbb{Z}/d) \rtimes_\beta \mathbb{Z}/d_0 \times \cdots \times \mathbb{Z}/d_m \longrightarrow C^*(\mathcal{D}_d, v_0, \ldots, v_m) = M_d(\mathbb{C}).$$

Since both of the involved C*-algebras are of dimension d^2, this *-homomorphism is actually an isomorphism. The details of this construction are left to the reader.

4.3 Nice families of pairwise quasi-orthogonal masas

Aschbacher, Childs, and Wocjan presented a notion of *nice (sets of) mutually unbiased bases* in the article [3]. In the present section, we shall introduce this concept—translated into the picture of quasi-orthogonal masas—, and moreover link it to our concept of normal masa pairs (see Definition 4.2.1).

The basic idea in the article of Aschbacher et al. is to gain sets of quasi-orthogonal masas from certain partitions of nice unitary error bases.

Definition 4.3.1. *Let G denote an index group with neutral element e, and consider a nice unitary error basis $\mathfrak{E} = \{u_g \mid g \in G\}$ for the matrix algebra $M_d(\mathbb{C})$. We say two subsets $E, F \subset \mathfrak{E}$ have trivial intersection if $E \cap F$ equals $\{u_e\}$.*

A quasi-partition *of the error basis $\mathfrak{E}$ is a family of subsets $E_0, \ldots, E_m \subset \mathfrak{E}$ ($m \in \mathbb{N}_0$) covering the basis $\mathfrak{E}$ and having pairwise trivial intersection, that is satisfying*

$$E_0 \cup \ldots \cup E_m = \mathfrak{E} \qquad \textit{and} \qquad E_i \cap E_j = \{u_e\} \ \textit{for all} \ 0 \leq i < j \leq m.$$

The following definition is essentially taken from the aforementioned article [3] by Aschbacher et al.

Definition 4.3.2 (Aschbacher et al. 2004). *For $n \leq d$, consider a family of pairwise quasi-orthogonal masas $\mathscr{F} = \{\mathcal{M}_0, \dots, \mathcal{M}_n\}$ in $M_d(\mathbb{C})$. The family $\mathscr{F}$ is said to be* nice *or to* stem from a quasi-partition of a nice error basis *if the following applies. There is a nice unitary error basis $\mathfrak{E}$, and a quasi-partition $\{E_0, \dots, E_m\}$ of $\mathfrak{E}$ of length $m \geq n$, such that the masas $\mathcal{M}_k$ are linearly spanned by the subsets $E_k \subset \mathfrak{E}$ for all $0 \leq k \leq n$. If G is the index group of the error basis $\mathfrak{E}$, we say that the family $\mathscr{F}$ is nice with index group G.*

A set of mutually unbiased bases is called nice if it corresponds to a nice family of masas (in the sense of Proposition 1.2.8).

Obviously, the masas in a nice family are automatically pairwise quasi-orthogonal, and each of the sets $E_0, \dots, E_n$ consists of d pairwise commuting unitaries (one of them being the unit matrix). Furthermore, it is plain to see that we have $m = n = d$ if the nice masa family $\mathscr{F}$ is complete.

Fix an index $0 \leq k \leq n$ in the definition above. The *-algebra $\mathcal{A}^*(E_k)$ being generated by commuting matrices, it is commutative and hence of dimension at most d. As it trivially contains the linear span of E_k on the other hand, we end up with the identities

$$\mathcal{M}_k = \operatorname{span}_{\mathbb{C}}(E_k) = \mathcal{A}^*(E_k).$$

Notice, however, that a proper subset of E_k will in general be sufficient to *algebraically* generate the masa $\mathcal{M}_k$.

Concerning the subsets of the index group G corresponding to the sets $E_0, \dots, E_n$, we can make the following

Observation 4.3.3. In the situation of Definition 4.3.2, set $H_k = \{g \in G \mid u_g \in E_k\}$ for all $0 \leq k \leq n$. Then each H_k is an *abelian subgroup* of order d inside the index group G. The subgroups $H_0, \dots, H_n$ have pairwise trivial intersections, i.e. we have $H_k \cap H_l = \{e\}$ for all indices $0 \leq k < l \leq n$.

The proof can be found in the Appendix on pages 221-222. ▷

We have already come across several instances of nice masa families.

Examples 4.3.4. (a) Every standard masa pair is at the same time a nice family (of length two) with index group $\mathbb{Z}/d \times \mathbb{Z}/d$ according to Proposition 4.1.6.

(b) More generally, let $d = d_0 \cdots d_m$ be a decomposition of the dimension $d \in \mathbb{N}$. Then by Theorem 4.2.4, condition (iv), every masa pair which is normal w.r.t. this decomposition is nice with index group $\bigoplus_{k=0}^{m}(\mathbb{Z}/d_k\mathbb{Z} \times \mathbb{Z}/d_k\mathbb{Z})$.

(c) Let the dimension $d = p^n$ be a prime power. The construction of complete sets of pairwise quasi-orthogonal masas inside $M_{p^n}(\mathbb{C})$ presented by Bandyopadhyay et al. (Construction 3.3.12) is explicitly based on quasi-partitions of the nice error basis $\mathfrak{E}^p_{2n}$ (or, equivalently, of $\mathfrak{S}_{p^n}$, cf. Example 4.1.3 (c)). Therefore all masa families obtained in this way, including the standard family of Popa (see Example 3.3.13 (a)), are nice.

The set of nice masa families (of arbitrary length) is particularly easy to describe in prime dimensions.

Proposition 4.3.5. *Every nice family of masas in a prime dimension is equivalent to a subset of the standard complete family (see Construction 3.2.5).*

Proof. Let $\mathscr{F} = \{\mathcal{M}_0, \dots, \mathcal{M}_n\}$ be a nice masa family in $M_p(\mathbb{C})$, where p is a prime number. Since the statement is trivial for $n = 0$, we assume $n \geq 1$.

The masas $\mathcal{M}_0$ and $\mathcal{M}_1$ are spanned by subsets E, F with trivial intersection of a nice unitary error basis $\mathfrak{E} = \{u_g \mid g \in G\}$ for $M_p(\mathbb{C})$, where G is the index group of order p^2. It is a well-known fact from group theory that all finite groups of prime square order are *abelian,* and so is thus the index group G. We may further assume w.l.o.g. that the basis $\mathfrak{E}$ is *very* nice.

The subsets $H_0 = \{g \in G \mid u_g \in E\}$ and $H_1 = \{g \in G \mid u_g \in F\}$ of G are abelian subgroups of order p according to Observation 4.3.3, and hence isomorphic to $\mathbb{Z}/p$. There are thus generators $g_0 \in H_0$ and $g_1 \in H_1$ of order p, so that u_{g_0} generates $\mathcal{M}_0$ and u_{g_1} generates $\mathcal{M}_1$. Furthermore, the subgroups H_0, H_1 have trivial intersection.

From the quasi-orthogonality of the masas $\mathcal{M}_0$ and $\mathcal{M}_1$ (or, equivalently, from the properties of a nice error basis) we can deduce that the p^2 products $u^i_{g_0} u^j_{g_1}$ are pairwise Hilbert-Schmidt orthogonal ($i, j \in \mathbb{Z}/p$). These products belong to the nice error basis $\mathfrak{E}$ up to phase factors, and consequently we can write

$$\mathfrak{E} = \left\{ \lambda_{i,j} u^i_{g_0} u^j_{g_1} \;\middle|\; i, j \in \mathbb{Z}/p \right\}$$

for certain coefficients $\lambda_{i,j} \in \mathbb{T}$.

Being elements of very a nice error basis with abelian index group, the unitaries u_{g_0} and u_{g_1} commute up to a pth root of unity $\omega \in \mathbb{T}$ that clearly cannot equal one. There is hence an exponent $0 < i_0 < p$ such that

$$u^{i_0}_{g_0} u_{g_1} = \zeta_p u_{g_1} u^{i_0}_{g_0}.$$

Moreover, there are coefficients $\mu_0, \mu_1 \in \mathbb{T}$ such that the unitaries $\tilde{w} = \mu_0 u^{i_0}_{g_0}$, $\tilde{v} = \mu_1 u_{g_1}$ fulfil the equalities $\tilde{v}^p = \tilde{w}^p = \mathrm{I}_d$. Using exactly the same arguments as in the last paragraph of the proof of Theorem 4.2.4, you convince yourself that a *-isomorphism

ϕ of $M_p(\mathbb{C})$ is given by assigning $\phi(\tilde{v}) = \mathrm{X}_p$ and $\phi(\tilde{w}) = \mathrm{Z}_p$. The definition of ϕ directly results in the identities $\phi(\mathcal{M}_0) = \mathcal{D}_p$ and $\phi(\mathcal{M}_1) = \mathcal{A}^*(\mathrm{X}_p)$.

If the family $\mathscr{F}$ has more than two members, any other masa $\mathcal{M}_k \in \mathscr{F}$, $1 < k \leq n$, must contain a product $u_{g_0}^{i_0} u_{g_1}^{i_k}$ for an exponent $0 < i_k < p$, since $\mathscr{F}$ stems from a quasi-partition of $\mathfrak{L}$ by assumption. It follows

$$\phi(\mathcal{M}_k) = \phi(\mathcal{A}^*(u_{g_0}^{i_0} u_{g_1}^{i_k})) = \mathcal{A}^*(\mathrm{Z}_p \mathrm{X}_p^{i_k}),$$

so $\mathscr{F}$ is equivalent to a subset of the standard family. □

If $\mathscr{F} = \{\mathcal{M}_0, \ldots, \mathcal{M}_n\}$ is a nice family of masas in $M_d(\mathbb{C})$, then obviously every subset of masas in $\mathscr{F}$ is nice as well. The converse is not always true, as is shown by the next

Example 4.3.6. In Section 3.2, we have proved that the family of masas

$$\mathscr{F}_0 = \{\mathcal{D}_5, \mathcal{A}^*(\mathrm{X}_5), \mathcal{A}^*(\mathrm{X}_5\tilde{w})\}, \text{ where } \tilde{w} = \mathrm{diag}(\zeta_5^0, \zeta_5^1, \zeta_5^2, \zeta_5^4, \zeta_5^3),$$

in the matrix algebra $M_5(\mathbb{C})$ is *not* equivalent to any subset of the standard family (see Example 3.2.10). By Proposition 4.3.5, the family $\mathscr{F}_0$ is therefore not nice, though each pair of masas in $\mathscr{F}_0$—actually every pair of quasi-orthogonal masas in $M_5(\mathbb{C})$ at all—is standard and hence nice.

Let us dwell on nice masa *pairs* for a moment. As these coincide with standard pairs in prime dimensions (cf. Examples 4.3.4), we know that not all pairs of quasi-orthogonal masas are nice in the matrix algebras $M_p(\mathbb{C})$ for all primes $p > 5$ (see Fact 2.4.11).

For composite dimensions, Proposition 2.4.10 tells us that the number of equivalence classes of quasi-orthogonal masa pairs is uncountable. On the other hand, it is a well-known fact from group theory that for each natural number $d \in \mathbb{N}$, there are only finitely many isomorphism classes of groups of order d (cf. for instance P. M. Neumann's article [78]). All the more, this holds true for the number of (isomorphism classes of) *index groups* of a given order d^2, and consequently for the number of inequivalent nice masa pairs, so that "most" of the existing quasi-orthogonal masa pairs are *not* nice.

While nice pairs can thus, loosely speaking, be thought of as "rare birds" in the set of all quasi-orthogonal masa pairs, it is quite unclear whether the situation is similar for *complete* masa families, as the following fact indicates.

Fact 4.3.7. All constructions included in the list on pages 99f. produce nice complete masa families. As far as items (1980), (1981), (1989), (1995), (2002*a*) and (2004*a*) are concerned, this was verified by Godsil and Roy ([40]), confirming inter alia a conjecture made by Boykin et al. in 2007 ([16]).

Beyond that, Godsil and Roy showed that the methods of Alltop (1980), Wootters and Fields (1989), Bandyopadhyay et al. (2002*a*), and Klappenecker and Rötteler (2004*a*) even lead to *equivalent* families, and that all these constructions are special cases of the technique by Calderbank et al. (1995).

For the remaining constructions, a look into the respective papers reveals that they explicitly employ quasi-partitions of nice error bases.

The following theorem is the main result of the aforementioned article by Aschbacher, Childs, and Wocjan ([3, theorem 3]).

Theorem 4.3.8 (Aschbacher et al. 2004)**.** *Let $d = p_0^{n_0} \cdots p_m^{n_m}$ be the prime factorisation of the dimension d, where $p_0, \ldots, p_m \in \mathbb{P}$ are pairwise different primes, $n_0, \ldots, n_m \in \mathbb{N}$, $m \in \mathbb{N}_0$. As in Definition 3.3.14, let*

$$L_d = \min\left\{p_0^{n_0}, \ldots, p_m^{n_m}\right\}$$

denote the smallest prime power in the prime decomposition of d. Then there are no nice families of masas in $M_d(\mathbb{C})$ having more than $L_d + 1$ members. In particular, complete *nice masa families exist only in prime power dimensions.*

Sketch of the proof. The key tool for this proof is the following

Group Theoretic Lemma. If G is a group of order d^2 and L_d is defined as in the theorem above, then there are at most $L_d + 1$ trivially intersecting abelian subgroups of order d inside G.

It would lead too far to verify this statement, for its proof employs a number of non-trivial insights from group theory, most notably concerning *(Sylow) p-groups.* We refer the reader to the paper [3] instead. Once this lemma is shown, one concludes as follows.

Let G be the index group of a nice unitary error basis $\mathfrak{E}$ for $M_d(\mathbb{C})$. Then G is of order d^2, and according to Observation 4.3.3, a family of pairwise quasi-orthogonal masas which stems from a quasi-partition of $\mathfrak{E}$ corresponds to a set of trivially intersecting *abelian* subgroups of order d inside G. Thus the lemma above applies, telling us that no more than $L_d + 1$ of such subgroups can exist. □

Non-trivial group theoretic considerations also permit Aschbacher et al. to develop certain constraints on the index groups of nice unitary bases. For our purposes, only the next corollary, which corresponds to [3, corollary 9], is of importance. Although labeled as a corollary, this statement is not an easy consequence of Theorem 4.3.8, but of several group theoretic lemmas also employed for the verification of the theorem.

Corollary 4.3.9 (Aschbacher et al. 2004). *For a prime $p \in \mathbb{P}$ and a natural number $n \in \mathbb{N}$, let $\mathfrak{E} = \{u_g \mid g \in G\}$ be a nice unitary error basis of the matrix algebra $M_{p^n}(\mathbb{C})$, with index group G. If $\mathfrak{E}$ admits a quasi-partition into $p^n + 1$ commuting subsets of of order p^n, then G is isomorphic to an* elementary abelian group*, that is to a direct sum of copies of $\mathbb{Z}/p$. By the order of G, this leads to the isomorphism*

$$G \cong \bigoplus_{2n} \mathbb{Z}/p.$$

Accordingly, every complete nice masa family in $M_{p^n}(\mathbb{C})$ has index group $\bigoplus_{2n} \mathbb{Z}/p$.

It had been a long-standing conjecture that the upper bound for nice masa families stated in the last preceding theorem applies to general families. This was falsified in 2004 by the construction of Wocjan and Beth.

Consequence 4.3.10. *As recorded in Fact 3.4.5 (a), the construction of quasi-orthogonal masa families by Wocjan and Beth (Construction 3.4.3) allows to construct a family of six pairwise quasi-orthogonal masas in $M_{26^2}(\mathbb{C})$. This family cannot be nice, because nice families in $M_{26^2}(\mathbb{C})$ have at most five members according to Theorem 4.3.8 above. It further gives evidence that there are composite dimensions in which the prime power constructions can be exceeded.*

Nice masa families and normal masa pairs

A normal masa pair is at the same time a nice masa family in the sense of Aschbacher et al., as we have recorded in Example 4.3.4 (b). Conversely, a certain "normality condition" must be fulfilled to ensure that a pair of two masas in a nice family is normal. This condition, motivating the term *normal masa pair,* is made precise in the next proposition.

Proposition 4.3.11. *The following statements are equivalent for masas $\mathcal{M}_0, \mathcal{M}_1 \subset M_d(\mathbb{C})$.*

(i) The pair of masas $\{\mathcal{M}_0, \mathcal{M}_1\}$ is normal.

(ii) The pair of masas $\{\mathcal{M}_0, \mathcal{M}_1\}$ is a nice family, that is there is a nice unitary error basis $\mathfrak{E} \subset \mathcal{U}_d$ and two trivially intersecting commutative subsets $E_0, E_1 \subset \mathfrak{E}$ of length d spanning the masas $\mathcal{M}_0$ and $\mathcal{M}_1$ respectively. What is more, at least one of the abelian subgroups $H_k = \{g \in G \mid u_g \in E_k\}$ of the index group G is normal $(0 \leq k \leq 1)$.

Proof. A masa pair which is normal stems from a quasi-partition of a nice unitary error basis with abelian index group by item (iv) of Theorem 4.2.4. All subgroups of abelian groups being normal, this proves that the first statement implies the second.

Conversely, suppose that statement (ii) applies. We may assume w.l.o.g. that the subgroup H_0 of G is normal, and further that the masa $\mathcal{M}_0$ is the diagonal masa $\mathcal{D}_d$. Due to the Fundamental Theorem of Finite Abelian Groups, the subgroup H_1 is isomorphic to a direct sum $\mathbb{Z}/d_0 \times \cdots \times \mathbb{Z}/d_m$, where $d = d_0 \cdots d_m$ is a decomposition of d. For each index $0 \leq k \leq m$, label the generator associated to $(0, \ldots, 0, 1, 0, \ldots, 0)$, where the non-zero entry is at position k, as $g_k \in H_1$. Furthermore, let $\tilde{v}_k = u_{g_k}$ denote a representative of g_k in $\mathfrak{E}$, which can w.l.o.g. be assumed to satisfy the equality $\tilde{v}_k^{d_k} = \mathrm{I}_d$. Clearly the elements $\tilde{v}_0, \ldots, \tilde{v}_m$ generate the masa $\mathcal{M}_1$.

Fix an element $h \in H_0$ and an index $0 \leq k \leq m$. By the normality of the subgroup H_0, there is an element $h' \in H_0$ subject to the identity $g_k h g_k^{-1} = h'$. On the matrix level, this is reflected by the equalities

$$\tilde{v}_k u_h \tilde{v}_k^* = u_{g_k} u_h u_{g_k}^* \sim_{\mathbb{T}} u_{g_k h g_k^{-1}} = u_{h'}.$$

Since the subset $E_0 \subset \mathfrak{E}$ generates the masa $\mathcal{M}_0 = \mathcal{D}_d$, this leads to the identities $\tilde{v}_k \mathcal{D}_d \tilde{v}_k^* = \mathcal{D}_d$ for all $0 \leq k \leq m$. All in all, the elements $\tilde{v}_0, \ldots, \tilde{v}_m$ thus obey the conditions of item (va) of Theorem 4.2.4, so $\{\mathcal{D}_d, \mathcal{M}\}$ is a normal pair in the sense of Definition 4.2.1. □

Remark 4.3.12. In statement (ii) of the previous proposition, the condition that at least one of the abelian subgroups $H_0, H_1 \subset G$ must be normal may be replaced by "one of the subgroups H_0, H_1 is contained in the normaliser of the other". It is an elementary exercise that these formulations are *equivalent* in the given situation.

All nice families of masas considered in the present work have *abelian* index groups. As every subgroup of an abelian index group is normal, these nice families are closely linked to normal pairs. The following corollary records this fact.

Corollary 4.3.13. *If $\mathscr{F}$ is a nice family of masas with* abelian *index group, then every pair of masas from $\mathscr{F}$ is normal. This applies in particular to*

- *all nice masa families obtained by the method of Bandyopadhyay et al. (cf. Examples 4.3.4 and 4.1.3 (c)), including the standard family and hence, according to Proposition 4.3.5, all nice masa families in prime dimensions.*

- *every complete nice masa family (see Corollary 4.3.9).*

We conclude the present subsection by a very short glance on the case of *non-abelian* index groups, which possibly allow the existence of nice masa pairs being not normal.

Remarks 4.3.14. (a) As we have mentioned earlier, many instances of *non-abelian* index groups can be found in the article [56] by Klappenecker and Rötteler. Among these examples, it is not hard to find non-abelian index groups of order d^2 which admit pairs of trivially intersecting abelian subgroups of order d, such that at least one of these subgroups is normal. These pairs of subgroups give thus rise to normal masa pairs according to Proposition 4.3.11.

(b) Since any normal masa pair which is nice with a non-abelian index group can at the same time be obtained from a quasi-partition of an *abelian* index group according to Theorem 4.2.4, normal pairs give evidence that one and the same nice masa family may in general have several non-isomorphic index groups.

(c) Going through the explicit list of small index groups in [56], one also finds index groups of order d^2 which contain pairs of *non-normal,* trivially intersecting abelian subgroups of order d. In regard to Proposition 4.3.11, masa pairs stemming from such pairs of subgroups *may* not be normal—on the other hand, this is not excluded either, as remark (b) shows. The question whether there actually *are* masa pairs being nice but not normal seems interesting and not trivial to us. Nevertheless, we do not follow this line of investigation in the present work.

A conjecture on complete families of quasi-orthogonal masas

Due to Theorem 4.3.8, complete nice masa families can only exist in prime power dimensions. At the same time, Fact 4.3.7 indicates that to all appearances, the class of nice masa families comprises *all* complete families known at present.

What is more, the authors Boykin et al. observe in [16] (and we shall verify it as well in the next section) that the only nice error basis which permits to construct complete nice masa families is, up to unitary equivalence, the basis $\mathfrak{S}_{p^n}$ (see Example 4.1.3 (b)). This basis consists only of monomials and is therefore called itself a *monomial error basis.*

On the whole, one may risk to make the following

Conjecture 4.3.15. *All complete families of pairwise quasi-orthogonal masas are* nice. *As a consequence, the only dimensions admitting complete quasi-orthogonal families are prime powers p^n, and up to equivalence, all complete families in $M_{p^n}(\mathbb{C})$ stem from a quasi-partition of the nice and monomial unitary error basis $\mathfrak{S}_{p^n}$ defined in Example 4.1.3 (b).*

4.4 Nice complete masa families in the generalised Clifford algebra

Since our aim is to introduce a generalisation of the usual Clifford algebra in terms of an abstract C*-algebra, we begin this section with two reminders. First we collect some very basic facts concerning (usual) Clifford algebras, then we sketch the concept of abstract C*-algebras.

Reminder: Clifford algebras

Clifford algebras are well-studied objects with important applications to various areas of mathematics and physics. Their definition is closely linked to vector spaces and quadratic forms on the latter.

Roughly speaking, the Clifford algebra associated with a vector space V over a field F, equipped with a quadratic form $q : V \to F$, is the smallest associative unital algebra $Cl(V, q)$ containing an isomorphic image of V and fulfilling the multiplication rule

$$v^2 = q(v)1$$

for all $v \in V$. (Some authors prefer the rule $v^2 = -q(v)1$ instead, which is the same as to replace the quadratic form q by $-q$, and hence essentially leads to the same results.) In case the quadratic form is constantly zero, the Clifford algebra coincides with the *exterior algebra* $\Lambda(V)$ associated with V.

Recall that for the d-dimensional complex vector space $\mathbb{C}^d$, all non-degenerated quadratic forms are equivalent to the standard diagonal form

$$\begin{aligned} q_0 : \mathbb{C}^d &\longrightarrow \mathbb{C}, \\ (z_0, \ldots, z_{d-1}) &\longmapsto z_0^2 + \ldots + z_{d-1}^2. \end{aligned}$$

This leads to the equivalence of all Clifford algebras associated with $\mathbb{C}^d$, justifying the notation $\mathbb{C}l_n = Cl(\mathbb{C}^d, q)$. The smallest cases are easily computed.

$$\mathbb{C}l_0 \cong \mathbb{C} \qquad \mathbb{C}l_1 \cong \mathbb{C} \oplus \mathbb{C} \qquad \mathbb{C}l_2 \cong M_2(\mathbb{C})$$

The first example is often set as a convention, though it also follows from the fact that Clifford algebras are unital by definition. For the third example, one finds an isomorphism mapping the generators $v_0, v_1 \in \mathbb{C}l_n$ to the Pauli spin matrices $\sigma_x, \sigma_z \in M_2(\mathbb{C})$, and the Pauli matrices also serve to find isomorphisms for all greater dimensions. Both in the real and the complex case, the isomorphic representation of Clifford algebras are fully determined and can be depicted in tables of 8-fold ($F = \mathbb{R}$) and 2-fold ($F = \mathbb{C}$) periodicity.

This periodicity is determined by the formula $\mathbb{C}l_{n+2} \cong \mathbb{C}l_n \otimes \mathbb{C}l_2$ in the complex case, so that the small examples above imply the isomorphisms

$$\mathbb{C}l_{2n} \cong \bigotimes_n M_2(\mathbb{C}) \cong M_{2^n}(\mathbb{C}) \quad \text{and} \quad \mathbb{C}l_{2n+1} \cong M_{2^n}(\mathbb{C}) \oplus M_{2^n}(\mathbb{C}). \tag{4.9}$$

Several textbooks provide a detailed discussion of Clifford algebras and their applications, see for instance [37,39].

In 1967, the mathematician A. O. Morris investigated representations of a generalised Clifford algebra, defined by generators and relations ([74,75]). This algebra had been introduced shortly before by Keijiro Yamazaki ([115]). As a remark, some foundations had also been laid earlier by R. Brauer and H. Weyl in [17] and [108]. Further generalisations of the Clifford algebra have been proposed, for instance by Ramakrishnan et al. in [84]. These are not regarded in the present work.

Although the generalised Clifford algebra was originally defined as an abstract algebra over a(n almost) *general* field F, we shall only consider the case $F = \mathbb{C}$ in the present thesis. On the other hand, we can therefore endow this algebra with an involution and a C*-norm, obtaining a universal abstract C*-algebra.

Reminder: C*-algebras defined by generators and relations

A *two-sided involutive ideal* $\mathcal{J}$ in a complex *-algebra $\mathcal{A}$ is a linear subspace of $\mathcal{A}$ which is closed under involution and under multiplication from either side (the latter meaning that for all elements $a \in \mathcal{A}$ and $b \in \mathcal{J}$, the products ab, ba lie in $\mathcal{J}$).

Definition 4.4.1 (Universal *-algebras). *Let $E := \{x_i, x_i^* \mid i \in I\}$ be a set of symbols, called* generators, *indexed by a set I. For each $i \in I$, we call the* symbol x_i^* *the* adjoint *of x_i. Further let $\mathcal{P} = \mathbb{C}[E]$ denote the ring of all non-commutative polynomials in generators E with coefficients from $\mathbb{C}$, which is at the same time a complex algebra.*

We define an antilinear mapping called involution $^* : \mathcal{P} \to \mathcal{P}$ first on monic terms by $^* : \alpha x_i \mapsto (\alpha x_i)^* = \bar{\alpha} x_i^*$ and $(\alpha x_i^*)^* = \bar{\alpha} x_i$ for all $\alpha \in \mathbb{C}, i \in I$, then (inductively) for general polynomials $p, q \in \mathcal{P}$ by $(p \cdot q)^* = q^* \cdot p^*$.

Let R be a subset of $\mathcal{P}$, called set of relations *in the sequel. Then $\mathcal{J} = \mathcal{P}R\mathcal{P} + (\mathcal{P}R\mathcal{P})^*$ is the smallest two-sided involutive ideal in $\mathcal{P}$ containing R. The quotient of $\mathcal{P}$ by $\mathcal{J}$ inherits the operations from $\mathcal{P}$ in a well-defined manner, and is thereby (again) a *-algebra*

$$\mathcal{A} = \mathcal{A}^*(E, R) := \mathcal{P}/\mathcal{J},$$

called the universal *-algebra with generators E and relations R.

By a *homomorphism of involutive algebras $\mathcal{A}$, $\mathcal{B}$*, we mean an algebra homomorphism $\phi : \mathcal{A} \to \mathcal{B}$ which fulfils the identity $\phi(a^*) = \phi(a)^*$ for all $a \in \mathcal{A}$. This notion allows us to describe the universal property from which universal *-algebras got their name.

Proposition 4.4.2. *Let $\mathcal{A} = \mathcal{A}^* (E, R)$ be a universal *-algebra with relations R and set of generators $E := \{x_i, x_i^* \mid i \in I\}$. Further denote the quotient map $p : P \to P/J = \mathcal{A}$. Then $\mathcal{A}$ fulfils the following universal property, depicted in the adjacent commuting diagram.*

If $\mathcal{B}$ is a *-algebra containing a set of elements $F = \{y_i, y_i^* \mid i \in I\}$ subject to the relations R (i.e. $p(F) = 0$ for all polynomials $p \in J$), then there exists a unique homomorphism of *-algebras $\phi_0 : \mathcal{A} \to \mathcal{B}$ such that $\phi_0(x_i \text{ mod } J) = y_i$ holds for all $i \in I$.

$$\begin{tikzcd}
\mathcal{P} \arrow[d, "p"'] \arrow[drr, "x_i \mapsto y_i"] & & \\
\mathcal{A}^*(E,R) \arrow[rr, dashed, "\phi_0"'] & & \mathcal{B}
\end{tikzcd}$$

It is an easy exercise to verify the universal property above. Recall that a *Banach algebra $\mathcal{B}$* is a (real or complex) normed algebra being a complete vector space at the same time, so that especially the triangle inequality $\|a + b\| \leq \|a\| + \|b\|$ holds for all $a, b \in \mathcal{B}$. Apart from that, the Banach algebra norm is required to be *submultiplicative,* i.e. to fulfil the inequality

$$\|ab\| \leq \|a\| \, \|b\| \quad \text{for all} \;\; a, b \in \mathcal{B}. \tag{4.10}$$

A *C*-algebra*$\mathcal{A}$ is a complex Banach algebra endowed with an involution * that satisfies the *C*-condition,* that is

$$\|a^* a\| = \|a\|^2 \quad \text{for all} \;\; a \in \mathcal{A}. \tag{4.11}$$

Conversely, any submultiplicative norm on a *-algebra obeying equation (4.11) is called *C*-norm.* One can show that the C*-norm on any C*-algebra is *unique.* We will also need the notion of a *C*-seminorm,* which is a submultiplicative seminorm obeying equation (4.11).

A standard example of a C*-algebra is the set of bounded operators $\mathcal{B}(H)$ on a Hilbert space H, endowed with the involution given by taking adjoints, and the operator norm. The C*-algebra $\mathcal{B}(H)$ and its sub-C*-algebras are usually named *concrete* C*-algebras. Constructions like the one we present directly below yield, by contrast, *abstract* C*-algebras.

A **-homomorphism*is a norm-bounded involutive homomorphism of C*-algebras $\mathcal{A}$, $\mathcal{B}$; one defines *-isomorphisms etc. by analogy. An injective *-homomorphism $\phi : \mathcal{A} \to \mathcal{B}$ is automatically *isometric,* i.e. fulfils the identity $\|\phi(a)\| = \|a\|$ for all elements $a \in \mathcal{A}$. A *-homomorphism $\pi : \mathcal{A} \to \mathcal{B}(H)$ is called **-representation* of the C*-algebra $\mathcal{A}$. The famous Gelfand-Naimark Theorem tells us that every C*-algebra admits an isomorphic representation as a sub-C*-algebra of the bounded linear operators on a Hilbert space. For these and other basic and advanced results concerning C*-algebras, see e.g. the textbooks [15, 30, 77]. Universal C*-algebras in particular are studied at length in [15, II.8.3].

Definition 4.4.3 (Universal C*-algebras)**.** *Consider a universal *-algebra $\mathcal{A}^*(E,R)$ with generators E and relations R. If the supremum of $\{h(a) \mid h$ C*-seminorm on $\mathcal{A}\}$ is* finite *for all $a \in \mathcal{A}$, then a C*-seminorm on $\mathcal{A}$ is defined by*

$$\|a\|_s = \sup \{h(a) \mid h \ \textit{C}^*\textit{-seminorm on } \mathcal{A}\} .$$

The set $\mathcal{N} = \{a \in \mathcal{A} \mid \|a\|_s = 0\}$ is an involutive ideal in $\mathcal{A}$. The quotient *-algebra $\mathcal{A}/\mathcal{N}$ can be endowed with the quotient norm, which is a C*-norm. As a consequence, the closure w.r.t. this norm,

$$C^*(E,R) = \overline{\mathcal{A}/\mathcal{N}}^{\|\cdot\|},$$

is a C*-algebra, called the universal C*-algebra with generators E and relations R.

Notice that the set of C*-seminorms on any given *-algebra is never empty, because it always contains the trivial norm (i.e. the norm which is constantly zero). However, the supremum taken over all C*-seminorms might happen to be infinite for some elements of a given *-algebra. That is why universal C*-algebras do *not* always exist. In fact, examples of generators and relations which do not admit the definition of a C*-seminorm are not even hard to find. In case the universal C*-algebra exists, it enjoys a universal property analogue to the one above. Again we omit the short proof.

Proposition 4.4.4. *Let $\mathcal{C} = C^*(E,R)$ be the universal C*-algebra with relations R and set of generators $E := \{x_i, x_i^* \mid i \in I\}$. Set $\mathcal{P} = \mathbb{C}[E]$ and define ideals $\mathcal{J} \subset \mathcal{P}$ and $\mathcal{N} \subset \mathcal{A}^*(E,R)$ as in the definitions above. Further let $\tilde{p} : P \to \mathcal{C}$ denote the (double) quotient map, i.e. $\tilde{p}$ acts via $\tilde{p}(q) = (q \bmod \mathcal{J}) \bmod \mathcal{N}$ for all $q \in \mathcal{P}$. Then $\mathcal{C}$ fulfils the following universal property.*

If $\mathcal{B}$ is a C*-algebra containing a set of elements $F = \{y_i, y_i^* \mid i \in I\}$ subject to the relations R (i.e. $p(F) = 0$ for all polynomials $p \in J$), then there exists a unique *-homomorphism $\phi : \mathcal{C} \to \mathcal{B}$ such that $\phi(\tilde{p}(x_i)) = y_i$ holds for all $i \in I$.

$$\begin{tikzcd}
\mathcal{P} \arrow[d, "\tilde{p}"'] \arrow[drr, "x_i \mapsto y_i"] & & \\
C^*(E,R) \arrow[rr, dashed, "\phi"'] & & \mathcal{B}
\end{tikzcd}$$

The generalised Clifford algebra

Bringing the definitions above to life, we will now define the generalised Clifford algebra in terms of a universal C*-algebra. On an algebraic level, the definition coincides with the one stated by Morris ([74,75]).

Proposition/Definition 4.4.5. *Let $c \in \mathbb{N}$, $m \in \mathbb{N}_0$ be two natural numbers, and fix a primitive cth root of unity $\omega \in \mathbb{T}$. Consider a set $E = \{1, e_0, \ldots, e_{m-1}; e_0^*, \ldots, e_{m-1}^*\}$ of generators, subject to the relations*

$$e_i^c = 1, \qquad e_i^* = e_i^{c-1}, \quad \text{and} \quad e_i e_j = \omega e_j e_i \tag{4.12}$$

for all $i, j \in \{0, \ldots, m-1\}$, $i < j$. Put differently, the set of relations is given by

$$R = \{e_i^c - 1, e_i^* - e_i^{c-1}, e_i e_j - \omega e_j e_i \mid 0 \leq i, j < m, i < j\}.$$

The universal C-algebra $C^*(E, R)$ exists and is called* generalised (complex) Clifford algebra, *denoted $\mathbb{C}l_m^c$.*

Proof. If m equals zero, the algebra $\mathcal{A}^*(E, R)$ is generated by the unit element and thereby isomorphic to the complex numbers. The C*-condition ensures that there is only one seminorm h on this *-algebra, which coincides with the modulus of complex numbers, since the equality $h(1) = h(1 \cdot 1^*) = h(1)^2$ yields $h(1) = 1$. So $\mathbb{C}l_0^c$ is just the set of complex numbers, endowed with complex conjugation as involution and the modulus as C*-norm. In the sequel, we assume $m > 0$.

In order to verify the existence of the universal C*-algebra $C^*(E, R)$, we only need to check, according to Definition 4.4.3, that the supremum

$$\sup \{h(a) \mid h \text{ C}^*\text{-seminorm on } \mathcal{A}^*(E, R)\}$$

is finite for all $a \in \mathcal{A}^*(E, R)$.

Now any C*-seminorm h is at the same time a Banach algebra seminorm and thus fulfils the inequalities $h(ab) \leq h(a)h(b)$ and $h(a + b) \leq h(a) + h(b)$ for all elements $a, b \in \mathcal{A}^*(E, R)$. Due to these inequalities, it suffices to show that the sets

$$\{h(e_i) \mid h \text{ C}^*\text{-seminorm on } \mathcal{A}^*(E, R)\}$$

are bounded for all $0 \leq i < m$, because every element in $\mathcal{A}^*(E, R)$ is a polynomial in the generators $e_0, \ldots, e_{m-1}$ (taken into account the second of the relations (4.12)).

The relations $e_i^c = 1$ and $e_i^* = e_i^{c-1}$ together ensure that the elements e_i are all unitaries, and since any C*-seminorm h obeys the C*-condition (4.11), this leads to the identities $h(e_i)^2 = h(e_i e_i^*) = h(1)$ for all $0 \leq i < m$. The same condition also implies $h(1)^2 = h(1)$, thus $h(1) = 1$, and eventually $h(e_i) = 1$ for all $0 \leq i < m$, so that the suprema above are finite for all elements in $\mathcal{A}^*(E, R)$. □

It meets the eye that the notation $\mathbb{C}l_m^c$ does not reflect the choice of the primitive cth root of unity ω involved in the definition of the generalised Clifford algebra. The reason is given by Theorem 4.4.6 below, which especially implicates the independence of the C*-algebra $\mathbb{C}l_m^c$ of that choice.

The generalised Clifford algebras $\mathbb{C}l_n^2$ are algebraically isomorphic to the conventional Clifford algebras $\mathbb{C}l_n$ for all $n \in \mathbb{N}_0$. Endowed with an appropriate involution and a C*-norm, the latter are also isomorphic to the former as C*-algebras. This directly follows from a comparison of the *-representations (4.9) on page 143 and those stated in the following theorem. These have been presented by Morris, although he does not consider an involution in his articles [74,75].

Theorem 4.4.6 (Morris 1967)**.** *The following *-isomorphisms exist for all natural numbers $c \in \mathbb{N}$ and $n \in \mathbb{N}_0$.*

$$\mathbb{C}l_{2n}^c \cong M_{c^n}(\mathbb{C}) \qquad \mathbb{C}l_{2n+1}^c \cong \bigoplus_c M_{c^n}(\mathbb{C})$$

Accordingly, the definition of the C-algebra $\mathbb{C}l_m^c$ is independent of the choice of the primitive cth root of unity ω in Proposition/Definition 4.4.5, and the dimension of $\mathbb{C}l_m^c$ equals c^m for all $c \in \mathbb{N}$, $m \in \mathbb{N}_0$.*

Proof. We fix a primitive cth root of unity $\omega_c \in \mathbb{T}$ in the relations (4.12) of the generalised Clifford algebra, and define a diagonal matrix

$$\tilde{\mathrm{Z}}_c = \operatorname{diag}(1, \omega_c, \dots, \omega_c^{c-1}) \in M_c(\mathbb{C}),$$

which is a power of the standard clock matrix Z_c. Therefore the commutation rule

$$\tilde{\mathrm{Z}}_c \mathrm{X}_c = \omega_c \mathrm{X}_c \tilde{\mathrm{Z}}_c$$

is immediate. Furthermore, let $\omega_{2c} \in \mathbb{T}$ denote an element of the unit circle satisfying the identity $\omega_{2c}^2 = \omega_c$.

Let us first address the case when $m = 2n$ is pair. We define a unitary matrix $\mathrm{R} \in M_c(\mathbb{C})$ by

$$\mathrm{R} = \begin{cases} \omega_{2c}\,\mathrm{X}_c \tilde{\mathrm{Z}}_c^* & \text{if } c \text{ is pair,} \\ \mathrm{X}_c \tilde{\mathrm{Z}}_c^* & \text{else,} \end{cases}$$

and thereby unitaries

$$\begin{aligned} \mathrm{E}_{2i} &= \mathrm{R} \otimes \cdots \otimes \mathrm{R} \otimes \tilde{\mathrm{Z}}_c \otimes \mathrm{I}_c \otimes \cdots \otimes \mathrm{I}_c, \\ \mathrm{E}_{2i+1} &= \mathrm{R} \otimes \cdots \otimes \mathrm{R} \otimes \underset{\substack{| \\ (i\text{th pos.})}}{\mathrm{X}_c} \otimes \mathrm{I}_c \otimes \cdots \otimes \mathrm{I}_c \in \bigotimes_n M_c(\mathbb{C}) \cong M_{c^n}(\mathbb{C}) \end{aligned}$$

for all $0 \le i < n$. As plain calculations show, these elements fulfil the relations (4.12) of the generalised Clifford algebra, that is

$$\mathrm{E}_i^c = 1, \qquad \mathrm{E}_i^* = \mathrm{E}_i^{c-1} \quad \text{and} \quad \mathrm{E}_i \mathrm{E}_j = \omega_c \mathrm{E}_j \mathrm{E}_i \qquad \text{for all } i, j \in \{0, \dots, 2n-1\}, i < j.$$

Due to the universal property of the generalised Clifford algebra $\mathbb{C}l^c_{2n}$, there is thus a *-homomorphism

$$\begin{aligned} \rho : \mathbb{C}l^c_{2n} &\longrightarrow M_{c^n}(\mathbb{C}), \\ e_i &\longmapsto \mathrm{E}_i. \end{aligned}$$

One quickly checks that the ordered products of (powers of) the unitaries $\mathrm{E}_0, \dots, \mathrm{E}_{2n-1}$ form a Hilbert-Schmidt orthonormal basis

$$\left\{ \mathrm{E}_0^{k_0} \cdots \mathrm{E}_{2n-1}^{k_{2n-1}} \;\middle|\; 0 \leq k_0, \dots, k_{2n-1} < c \right\}$$

for the matrix algebra $M_{c^n}(\mathbb{C})$. (It corresponds to the nice unitary error basis $\mathfrak{S}_{c^n}$ up to phase factors, see Example 4.1.3 (c).) As a direct consequence, the *-homomorphism ρ is surjective.

On the other hand, the relations for the generators of $\mathbb{C}l^c_{2n}$ ensure that any element in this C*-algebra is a (finite) linear combination of ordered products of the form $e_0^{k_0} \cdots e_{2n-1}^{k_{2n-1}}$, where $0 \leq k_0, \dots, k_{2n-1} < c$. Put differently, the generalised Clifford algebra $\mathbb{C}l^c_{2n}$ is linearly spanned by the set

$$\mathfrak{B}^c_{2n} = \left\{ e_0^{k_0} \cdots e_{2n-1}^{k_{2n-1}} \;\middle|\; 0 \leq k_0, \dots, k_{2n-1} < c \right\},$$

and thereby the dimension of $\mathbb{C}l^c_{2n}$ is at most c^{2n}. This being the dimension of $M_{c^n}(\mathbb{C})$, the *-epimorphism ρ must be injective and thus a *-isomorphism.

If $m = 2n+1$ is odd, it suffices, with regard to what we have just demonstrated, to prove that there is a *-isomorphism

$$\rho' : \mathbb{C}l^c_{2n+1} \longrightarrow \bigoplus_c \mathbb{C}l^c_{2n}.$$

To this end, we define an element

$$f = \begin{cases} \omega_{2c}^n \, e_0 e_1^* \, e_2 e_3^* \cdots e_{2n-2} e_{2n-1}^* & \text{if } c \text{ is pair} \\ \quad e_0 e_1^* \, e_2 e_3^* \cdots e_{2n-2} e_{2n-1}^* & \text{else,} \end{cases}$$

in $\mathbb{C}l^c_{2n}$, and then elements in $\bigoplus_c \mathbb{C}l^c_{2n}$ by

$$\tilde{e}_i = \begin{cases} (e_i, \dots, e_i) & \text{for } 0 \leq i < 2n, \\ (f, \omega_c f, \dots, \omega_c^{c-1} f) & \text{if } i = 2n. \end{cases}$$

Again a straightforward computation reveals that the elements $\tilde{e}_0, \dots, \tilde{e}_{2n} \in \bigoplus_c \mathbb{C}l^c_{2n}$ are subject to the same relations as the generators of the generalised Clifford algebra $\mathbb{C}l^c_{2n+1}$, so that the assignment $\rho'(e_i) = \tilde{e}_i$ for $0 \leq i \leq 2n$ defines a *-homomorphism. We only have to verify that ρ' is surjective, because then its injectivity follows, as above, by dimension. (The C*-algebra $\mathbb{C}l^c_{2n+1}$ is spanned by the set $\mathfrak{B}^c_{2n+1}$, defined by analogy with $\mathfrak{B}^c_{2n}$ above, which implies $\dim \mathbb{C}l^c_{2n+1} \leq c^{2n+1} = \dim \bigoplus_c \mathbb{C}l^c_{2n}$.)

To put it another way, our task is to check that the elements $\tilde{e}_0, \ldots, \tilde{e}_{2n}$ generate the direct sum $\bigoplus_c \mathbb{C}l^c_{2n}$. First observe that we have

$$\tilde{e}_{2n} \cdot \underbrace{(\tilde{e}_0\tilde{e}_1^* \, \tilde{e}_2\tilde{e}_3^* \cdots \tilde{e}_{2n-2}\tilde{e}_{2n-1}^*)^*}_{\sim_{\mathbb{T}}(f^*,\ldots,f^*)} = \lambda(1, \omega_c, \ldots, \omega_c^{c-1}),$$

where the factor $\lambda \in \mathbb{T}$ depends on whether c is even or odd. The tuple on the right-hand side is therefore generated by $\tilde{e}_0, \ldots, \tilde{e}_{2n}$, and so are the elements

$$\begin{aligned}\left(\frac{1}{c}\sum_{k=0}^{c-1} \omega_c^{-jk} \left(1, \omega_c, \ldots, \omega_c^{c-1}\right)^k\right) \tilde{e}_i &= \frac{1}{c}\sum_{k=0}^{c-1} \left(\omega_c^{-jk}, \omega_c^{k(1-j)}, \omega_c^{k(2-j)}, \ldots, \omega_c^{k(c-1-j)}\right) \tilde{e}_i \\ &= (0, \ldots, 0, \underset{\substack{|\\(j\text{th pos.})}}{1}, 0, \ldots, 0) \cdot (e_i, \ldots, e_i) \\ &= (0, \ldots, 0, \overset{|}{e_i}, 0, \ldots, 0)\end{aligned}$$

for all $0 \leq i < 2n$ and $0 \leq j < c$. The direct sum $\bigoplus_c \mathbb{C}l^c_{2n}$ is clearly generated by these elements, and thus by $\tilde{e}_0, \ldots, \tilde{e}_{2n}$, so we are done. □

Convention 4.4.7. From here on, we shall always presume that the primitive cth root of unity $\omega \in \mathbb{T}$, involved in the defining relations (4.12) of the generalised Clifford algebra $\mathbb{C}l^c_m$, equals $\zeta_c = \exp(2\pi\mathrm{i}/c)$.

Equipped with the Hilbert-Schmidt scalar product, the finite-dimensional C*-algebras $M_{c^n}(\mathbb{C})$ and $\bigoplus_c M_{c^n}(\mathbb{C})$ are at the same time Hilbert spaces. More precisely, they are examples of so-called *Hilbert algebras.* A unital *-algebra is a Hilbert algebra if endowed with an inner product $(\cdot \,|\, \cdot) : \mathcal{A} \times \mathcal{A} \to \mathbb{C}$ such that

- $(x \,|\, y) = (y^* \,|\, x^*)$ for all $x, y \in \mathcal{A}$,
- $(zx \,|\, y) = (x \,|\, z^*y)$ for all $x, y, z \in \mathcal{A}$, and
- for each fixed element $x \in \mathcal{A}$, the left-multiplication $y \mapsto xy$ is a bounded linear map, i.e. there is a constant $C \geq 0$ such that $\|xy\|_2 \leq C\,\|y\|_2$ for all $y \in \mathcal{A}$, where $\|\cdot\|_2$ labels the norm induced by the scalar product.

Hilbert algebras often occur in the context of von Neumann algebras. They are for instance defined in the Dixmier's textbook [33].

Notice that for a Hilbert algebra which happens to be a C*-algebra as well, the norm induced by the inner product does, in general, **not** coincide with the C*-norm.

For the matrix algebras above, for instance, the latter is the standard operator norm, whereas the former is the Hilbert-Schmidt norm. Generalised Clifford algebras are Hilbert algebras with a very nice orthonormal basis.

Definition/Proposition 4.4.8. *For all natural numbers $c \in \mathbb{N}$ and $m \in \mathbb{N}_0$, denote the set of all ordered products of the generators of the generalised Clifford algebra $\mathbb{C}l^c_m$ by*

$$\mathfrak{B}^c_m = \left\{ e_0^{k_0} \cdots e_{m-1}^{k_{m-1}} \,\middle|\, 0 \le k_0, \ldots, k_{m-1} < c \right\}$$

as in the proof of Theorem 4.4.6. A well-defined inner product $(\cdot \,|\, \cdot)$ on $\mathbb{C}l^c_m$ is given by the rule that elements in $\mathfrak{B}^c_m$ shall be pairwise orthonormal, making $\mathbb{C}l^c_m$ into a Hilbert algebra. We call $\mathfrak{B}^c_m$ the standard basis *of the generalised Clifford algebra $\mathbb{C}l^c_m$.*

The *-isomorphisms declared in the proof of Theorem 4.4.6 are at the same time isomorphisms of Hilbert algebras, where the respective matrix algebras are endowed with the Hilbert-Schmidt scalar product.

If $m = 2n$ is even, then $\mathfrak{B}^c_{2n}$ corresponds—under the *-isomorphism ρ defined in the proof of Theorem 4.4.6, and up to phase factors—to the very nice unitary error bases $\mathfrak{C}^c_{2n}$ and $\mathfrak{S}_{c^n}$ respectively for the matrices $M_{c^n}(\mathbb{C})$ (cf. Definition/Proposition 3.3.8 and Example 4.1.3 (c)).

Proof. We employ the *-isomorphisms ρ and ρ' as defined in the proof of the last preceding theorem. If $m = 2n+1$ is odd, we moreover define an isomorphic *-representation $\rho'' : \mathbb{C}l^c_{2n+1} \to \bigoplus_c M_{c^n}(\mathbb{C})$ according to the following diagram.

$$\begin{tikzcd}
\mathbb{C}l^c_{2n+1} \arrow[r, "\rho'"] \arrow[rr, bend right, "\rho''=(\bigoplus_c \rho)\circ\rho'"'] & \bigoplus_c \mathbb{C}l^c_{2n} \arrow[r, "\bigoplus_c \rho"] & \bigoplus_c M_{c^n}(\mathbb{C})
\end{tikzcd}$$

Furthermore, the normalised trace—and thus the Hilbert-Schmidt scalar product—on the direct sum $\bigoplus_c M_{c^n}(\mathbb{C})$ is defined as the renormalised direct sum of the normalised traces on the summands $M_{c^n}(\mathbb{C})$, that is by the formula

$$\tau : \bigoplus_c M_{c^n}(\mathbb{C}) \longrightarrow \mathbb{C}, \quad (a_0, \ldots, a_{c-1}) \longmapsto \frac{1}{c} \sum_{k=0}^{c-1} \tau(a_k).$$

Depending on whether m is even or odd, one now defines an inner product $(\cdot \,|\, \cdot)$ on $\mathbb{C}l^c_m$ via the Hilbert-Schmidt scalar product for the respective matrix representation, i.e. for all $x, y \in \mathbb{C}l^c_m$, one sets

$$(x \,|\, y) := \begin{cases} (\rho(x) \,|\, \rho(y))_{\mathrm{HS}} & \text{if } m \text{ is even,} \\ (\rho''(x) \,|\, \rho''(y))_{\mathrm{HS}} & \text{if } m \text{ is odd.} \end{cases}$$

As already checked in the proof of Theorem 4.4.6, the basis $\mathfrak{B}^c_m$ is mapped to the Hilbert-Schmidt orthonormal basis $\mathfrak{S}_{c^n}$ up to phase factors by the *-isomorphism ρ in case m is even. If m is odd, an analogue result is ensured by the definition of ρ'', as a computation shows. As a consequence, the set $\mathfrak{B}^c_m$ is an orthonormal basis for the inner product $(\cdot \mid \cdot)$ introduced above. Defining an inner product on $\mathbb{C}l^c_m$ by the *rule* that $\mathfrak{B}^c_m$ shall be an orthonormal basis obviously yields the same scalar product, so that we do not have to worry about well-definedness in this context.

What is more, we have already mentioned that the matrix algebras $M_d(\mathbb{C})$, endowed with the Hilbert-Schmidt scalar product, are examples of Hilbert algebras. As the inner products on $\mathbb{C}l^c_m$ and its matrix representation (in both the even and the odd case) are compatible by definition of the inner product on $\mathbb{C}l^c_m$, the latter C*-algebra is a Hilbert algebra as well. For the same reason, the *-isomorphisms ρ and ρ'' are isomorphisms of Hilbert algebras at the same time. □

Nice complete masa families in the generalised Clifford algebra picture

For the investigation of (complete) nice masa families in prime power dimensions, that is inside the generalised Clifford algebras $\mathbb{C}l^p_{2n} \cong M_{p^n}(\mathbb{C})$, it proves useful to replace the unitaries $e_0, \ldots, e_{2n-1}$ by an alternative set of generators.

Definition/Proposition 4.4.9. *Fix a prime $p \in \mathbb{P}$ and a natural number $n \in \mathbb{N}$. Consider a set of generators $\tilde{E} = \{1, \tilde{b}_0, \ldots, \tilde{b}_{n-1}; \tilde{b}^*_0, \ldots, \tilde{b}^*_{n-1}; \tilde{c}_0, \ldots, \tilde{c}_{n-1}; \tilde{c}^*_0, \ldots, \tilde{c}^*_{n-1}\}$, subject to the relations $\tilde{R}$ given by*

$$\tilde{b}_i^p = 1, \quad \tilde{b}_i^* = \tilde{b}_i^{p-1}, \quad \tilde{b}_i\tilde{b}_j = \tilde{b}_j\tilde{b}_i, \qquad \tilde{c}_i^p = 1, \quad \tilde{c}_i^* = \tilde{c}_i^{p-1}, \quad \tilde{c}_i\tilde{c}_j = \tilde{c}_j\tilde{c}_i,$$
$$\text{and} \quad \tilde{b}_i\tilde{c}_j = \begin{cases} \zeta_p \tilde{c}_j \tilde{b}_i & \text{if } i = j, \\ \tilde{c}_j\tilde{b}_i & \text{else,} \end{cases} \tag{4.13}$$

for all $0 \le i, j < n$, where we set $\zeta_p = \exp(2\pi i/p)$ as before. The universal C*-algebra $C^*(\tilde{E}, \tilde{R})$ exists and is isomorphic to the generalised Clifford algebra $\mathbb{C}l^p_{2n}$. For all indices $0 \le i < n$, we define elements

$$b_i = (e_0 e_1^*) \cdots (e_{2i-2} e_{2i-1}^*) e_{2i} \quad \text{and} \quad c_i = \begin{cases} i\, e_{2i}^* e_{2i+1} & \text{if } p = 2, \\ e_{2i}^* e_{2i+1} & \text{else,} \end{cases} \tag{4.14}$$

in $\mathbb{C}l^p_{2n}$. Then a *-isomorphism $\phi : C^*(\tilde{E}, \tilde{R}) \to \mathbb{C}l^p_{2n}$ is given by setting $\phi(\tilde{b}_i) = b_i$ and $\phi(\tilde{c}_i) = c_i$ for all $0 \le i < n$.

Proof. The existence of the universal C*-algebra $C^*(\tilde{E}, \tilde{R})$ is verified in just the same way as in the case of the (standard picture of the) generalised Clifford algebra, see the proof of Proposition/Definition 4.4.5.

Once the existence is ensured, it is a matter of computation to verify that the elements $b_i, c_i \in \mathbb{C}l_{2n}^p$, defined in equation (4.14), satisfy the relations (4.13), so that, according to the universal property of $C^*(\tilde{E}, \tilde{R})$, the assignment ϕ is a well-defined *-homomorphism. (We leave the computational details to the reader.)

What is more, it is not hard to see that the dimension of the universal C*-algebra $C^*(\tilde{E}, \tilde{R})$ is at most p^{2n} on the one hand, and that the elements b_i, c_i generate the generalised Clifford algebra $\mathbb{C}l_{2n}^p$ on the other. Taken together, these assertions show that the proposed *-homomorphism ϕ is in fact a *-isomorphism. □

Remarks 4.4.10. (a) In Definition/Proposition 3.3.8, we have defined unitary matrices $\mathrm{B}_i, \mathrm{C}_i \in M_{p^n}(\mathbb{C})$ for all $0 \leq i < n$ by

$$\mathrm{B}_i = \quad \mathrm{I}_p \otimes \cdots \otimes \mathrm{I}_p \otimes \overset{(i\text{th pos.})}{\mathrm{Z}_p} \otimes \mathrm{I}_p \otimes \cdots \otimes \mathrm{I}_p$$

$$\text{and} \quad \mathrm{C}_i = \begin{cases} \mathrm{i}\,\mathrm{I}_p \otimes \cdots \otimes \mathrm{I}_p \otimes \sigma_x \sigma_z \otimes \mathrm{I}_p \otimes \cdots \otimes \mathrm{I}_p & \text{if } p = 2, \\ \mathrm{I}_p \otimes \cdots \otimes \mathrm{I}_p \otimes \mathrm{X}_p \mathrm{Z}_p^* \otimes \mathrm{I}_p \otimes \cdots \otimes \mathrm{I}_p & \text{else.} \end{cases}$$

It is an exercise to check that the matrices $\mathrm{B}_i, \mathrm{C}_i \in M_{p^n}(\mathbb{C})$ satisfy the relations (4.13), and they are easily seen to generate the matrix algebra $M_d(\mathbb{C})$. For this reason, we obtain a well-defined *-isomorphism $\rho : \mathbb{C}l_{2n}^p \to M_{p^n}(\mathbb{C})$ by setting $\rho(b_i) = \mathrm{B}_i$ and $\rho(c_i) = \mathrm{C}_i$ for all $0 \leq i < n$. (As a matter of fact, this is precisely the *-representation ρ defined by $\rho(e_i) = \mathrm{E}_i$ in the proof of Theorem 4.4.6.)

(b) Since the pth powers of all of all elements $b_i, c_i \in \mathbb{C}l_{2n}^p$ equal one, we can consider exponents of these unitaries as elements of the prime field $\mathbb{F}_p$, as we do for the standard generators e_i. Obviously, the set of all ordered products

$$\left\{ b_0^{k_0} \cdots b_{n-1}^{k_{n-1}} c_0^{l_0} \cdots c_{n-1}^{l_{n-1}} \,\middle|\, k_0, \ldots, k_{n-1}, l_0, \ldots, l_{n-1} \in \mathbb{F}_p \right\}$$

coincides with the standard basis $\mathfrak{B}_{2n}^p$ of $\mathbb{C}l_{2n}^p$ up to phase factors (see Definition/Proposition 4.4.8). Under the *-representation ρ, it precisely corresponds to the matrix basis $\mathfrak{E}_{2n}^p$ introduced in Definition/Proposition 3.3.8.

We will use the alternative generators $b_i, c_i \in \mathbb{C}l_{2n}^p$ to prove the next assertion, which slightly generalises a statement by Boykin et al. (see [16, theorem 2.4, last part]). They showed that all complete nice masa families inside the matrix algebras $M_{p^n}(\mathbb{C})$ can be obtained from a quasi-partition (cf. Definition 4.3.1) of the nice error basis $\mathfrak{F}_{p^n}$ introduced in Example 4.1.3 (c), where $p \in \mathbb{P}$ and $n \in \mathbb{N}$ are arbitrary. Recall that the matrix bases $\mathfrak{F}_{p^n}$ and $\mathfrak{E}_{2n}^p$ coincide up to phase factors (see Example 4.1.3 (c)).

The following theorem is the first of three steps towards the unifying construction result for complete nice masa families which we establish in the present work (see Main Theorem, page 178).

Theorem 4.4.11. *For a prime $p \in \mathbb{P}$ and a natural number $n \in \mathbb{N}$, set $d = p^n$. Further let $\mathscr{F}$ be a nice masa family with index group $\bigoplus_{2n} \mathbb{Z}/p$ inside the matrix algebra $M_d(\mathbb{C})$. Then there is a faithful *-representation $\tilde{\rho} : \mathbb{C}l^p_{2n} \to M_d(\mathbb{C})$ such that the family of quasi-orthogonal masas $\tilde{\rho}^{-1}(\mathscr{F})$ stems from a quasi-partition of the standard basis $\mathfrak{B}^p_{2n}$. As a consequence, the family $\mathscr{F}$ corresponds, up to unitary equivalence, to a quasi-partition of the error basis $\mathfrak{E}^p_{2n}$.*

What is more, if the family $\mathscr{F}$ contains at least two quasi-orthogonal masas $\mathcal{M}, \mathcal{N}$ in $M_d(\mathbb{C})$, one can always arrange that $\tilde{\rho}$ obeys the identities

$$\tilde{\rho}\left(\mathcal{A}^*(b_0, \dots, b_{n-1})\right) = \mathcal{N} \quad \textit{and} \quad \tilde{\rho}\left(\mathcal{A}^*(c_0, \dots, c_{n-1})\right) = \mathcal{M}.$$

Proof. The assertions are trivial if the family $\mathscr{F}$ contains only one single masa, so we presume $|\mathscr{F}| \geq 2$ in the sequel.

We can further assume without loss of generality that $\mathfrak{E}$ is *very* nice, compare Proposition/Definition 4.1.1. The index group being $\bigoplus_{2n} \mathbb{Z}/p$, the error basis $\mathfrak{E}$ then exclusively contains, besides the unit matrix, unitaries $v \in \mathcal{U}_d$ whose powers $v, \dots, v^{p-1}$ are all trace-free, and which moreover satisfy the equality $v^p = \mathrm{I}_d$. We can therefore consider the exponents of basis elements in $\mathfrak{E}$ as elements of the prime field $\mathbb{F}_p$.

Let $\mathcal{M}, \mathcal{N}$ be two different masas in the family $\mathscr{F}$. By the structure of $\mathfrak{E}$, there are elements $v_0, \dots, v_{n-1}, \tilde{w}_0, \dots, \tilde{w}_{n-1} \in \mathfrak{E} \setminus \{\mathrm{I}_d\}$ such that we can write

$$\mathcal{N} = \mathcal{A}^*\left(v_0, \dots, v_{n-1}\right) \quad \text{and} \quad \mathcal{M} = \mathcal{A}^*\left(\tilde{w}_0, \dots, \tilde{w}_{n-1}\right).$$

As always, set $\zeta_p = \exp({}^{2\pi\mathrm{i}}/_{p})$. Since the elements of $\mathfrak{E}$ commute up to pth roots of unity, there is, for each pair of indices $0 \leq i, j < n$, an exponent $k_{i,j} \in \mathbb{F}_p$ satisfying the commutation relation

$$v_i \tilde{w}_j = \zeta_p^{k_{i,j}} \tilde{w}_j v_i.$$

Next, we demonstrate by contradiction that the matrix $K = (k_{i,j})_{0 \leq i,j < n} \in M_n(\mathbb{F}_p)$ is invertible. Suppose on the contrary that the rows of K are linearly dependent, so that they allow a non-trivial linear combination of the zero vector,

$$\sum_{i=0}^{n-1} t_i (k_{i,0}, \dots, k_{i,n-1}) = (0, \dots, 0),$$

for some coefficients $t_0, \dots, t_{n-1} \in \mathbb{F}_p$. A plain calculation shows that thereby the element $v_0^{t_0} \cdots v_{n-1}^{t_{n-1}} \in \mathcal{N} \ominus \mathbb{C} \cdot \mathrm{I}_d$ commutes with each of the generators $\tilde{w}_0, \dots, \tilde{w}_{n-1}$ of the masa $\mathcal{M}$. By maximality of the latter, it thus contains the product $v_0^{t_0} \cdots v_{n-1}^{t_{n-1}}$, in contradiction to the quasi-orthogonality of $\mathcal{M}$ and $\mathcal{N}$.

So K is regular; let $L = (l_{i,j})_{0 \leq i,j < n} \in M_n(\mathbb{F}_p)$ denote its inverse. For all $0 \leq j < n$, we define elements

$$w_j = \tilde{w}_0^{l_{0,j}} \cdots \tilde{w}_{n-1}^{l_{n-1,j}} \in \mathcal{U}_d,$$

which belong to the error basis $\mathfrak{E}$ up to phase factors. One readily checks the equations

$$v_i w_j = \begin{cases} \zeta_p w_j v_i & \text{if } i = j, \\ w_j v_i & \text{else,} \end{cases}$$

for $0 \leq i, j < n$. The unitary matrices v_i and w_i also obey all remaining relations (4.13) of the alternative generators $b_i, c_i \in \mathbb{C}l_{2n}^p$. That is why there is a (unique) *-homomorphism $\tilde{\rho} : \mathbb{C}l_{2n}^p \to M_d(\mathbb{C})$ satisfying the identities

$$\tilde{\rho}(b_i) = v_i \quad \text{and} \quad \tilde{\rho}(c_i) = w_i$$

for all indices $0 \leq i < n$. As the range of $\tilde{\rho}$ contains all elements of the basis $\mathfrak{E}$, it is surjective, and thus a *-isomorphism by dimension. By construction, we have ensured that $\tilde{\rho}$ maps the masas $\mathcal{A}^*(b_0, \ldots, b_{n-1})$ and $\mathcal{A}^*(c_0, \ldots, c_{n-1})$ as proposed in the assertion.

The inverse $\tilde{\rho}^{-1}$ carries the elements of the nice error basis $\mathfrak{E}$ to elements of the standard basis $\mathfrak{B}_{2n}^p$ of $\mathbb{C}l_{2n}^p$ up to phase factors, cf. Remark 4.4.10 (b). Consequently, the nice masa family $\tilde{\rho}^{-1}(\mathscr{F})$ in $\mathbb{C}l_{2n}^p$ stems from a quasi-partition of $\mathfrak{B}_{2n}^p$.

Finally, recall the standard *-representation $\rho : \mathbb{C}l_{2n}^p \to M_d(\mathbb{C})$ defined in the proof of Theorem 4.4.6 or, alternatively, in Remark 4.4.10 (a). The masa family $\rho \circ \tilde{\rho}^{-1}(\mathscr{F})$ in $M_d(\mathbb{C})$ is unitarily equivalent to the original family $\mathscr{F}$, and stems from a quasi-partition of $\mathfrak{E}_{2n}^p$ by construction—this completes our proof. □

Combining the theorem above and Corollary 4.3.9, and bearing in mind that the error bases $\mathfrak{S}_{p^n}$ and $\mathfrak{E}_{2n}^p$ coincide up to phase factors, we literally obtain the aforementioned result by Boykin et al.

Corollary 4.4.12 (Boykin et al. 2007). *Up to unitary equivalence, every nice complete masa family in the matrix algebra $M_{p^n}(\mathbb{C})$ stems from a quasi-partition of the error basis $\mathfrak{S}_{p^n}$.*

4.5 *Excursion:* Concatenated normal pairs of masas

Fix a dimension d and a factorisation $d = d_0 \cdots d_m$. A pair of masas $\{\mathcal{D}_d, \mathcal{M}\}$ in the matrix algebra $M_d(\mathbb{C})$ which is normal w.r.t. this factorisation models, as we have seen in Section 4.2, an action of the abelian group $\mathbb{Z}/d_0 \times \cdots \times \mathbb{Z}/d_m$ on the function algebra $C^*(\mathbb{Z}/d) \cong \mathbb{C}[\mathbb{Z}/d]$. More precisely, the masa $\mathcal{M}$ is generated by monomial unitaries $v_0, \ldots, v_m \in \mathcal{W}_d$ fulfilling $v_k^{d_k} = \mathrm{I}_d$ for all $0 \leq k \leq m$, and each unitary v_k thereby induces an action of $\mathbb{Z}/d_k$ on the diagonal masa $\mathcal{D}_d$ via conjugation (cf. items (va) and (via) of Theorem 4.2.4, and the excursional part at the end of Section 4.2).

In the present section, we introduce a type of masa pairs generalising this concept in the following way. Consider a quasi-orthogonal pair of masas $\{\mathcal{D}_d, \mathcal{M}\}$ in $M_d(\mathbb{C})$, and suppose $\mathcal{M}$ contains a unitary monomial matrix v_0. Then v_0 acts by conjugation on the diagonal $\mathcal{D}_d$. If $d_0 \in \mathbb{N}$ is a factor of d such that we have $v_0^{d_0} \sim_{\mathbb{T}} \mathrm{I}_d$, then this conjugation models a group action $\beta_{[0]}$ of $\mathbb{Z}/d_0$ on $C^*(\mathbb{Z}/d)$. Similarly as in Section 2.5, one shows that if the action $\beta_{[0]}$ is injective and the dimension of $\mathcal{A}^*(\mathcal{D}_d, v_0)$ equals $d_0 \cdot d$, then there is an isomorphism

$$C^*(\mathbb{Z}/d) \rtimes_{\beta_{[0]}} \mathbb{Z}/d_0 \cong \mathcal{A}^*(\mathcal{D}_d, v_0) \subset M_d(\mathbb{C}).$$

Now assume $\mathcal{M}$ contains another unitary matrix v_1 that is not necessarily monomial, but nevertheless induces an injective group action $\beta_{[1]}$ of $\mathbb{Z}/d_1$ on the *-subalgebra $\mathcal{A}^*(\mathcal{D}_d, v_0)$, where d_1 is another factor of d. If furthermore the dimension of the *-subalgebra $\mathcal{A}^*(\mathcal{D}_d, v_0, v_1)$ is $d \cdot d_0 \cdot d_1$, then by analogy with the argument above, this leads to an isomorphism

$$(C^*(\mathbb{Z}/d) \rtimes_{\beta_{[0]}} \mathbb{Z}/d_0) \rtimes_{\beta_{[1]}} \mathbb{Z}/d_1 \cong \mathcal{A}^*(\mathcal{D}_d, v_0, v_1) \subset M_d(\mathbb{C}).$$

One can proceed in the same way until a complete set of generators of $\mathcal{M}$ is involved. This leads to the following definition.

Definition 4.5.1. *Let $d = d_0 \cdots d_m$ be a factorisation of the dimension d, where the order of the factors $d_0, \ldots, d_m \in \mathbb{N}$ is of importance. Consider a masa $\mathcal{M}$ in $M_d(\mathbb{C})$ which is quasi-orthogonal to $\mathcal{D}_d$, and generated by unitary matrices $v_0, \ldots, v_m \in \mathcal{U}_d$ such that the following conditions hold.*

(i) For all $0 \leq k \leq m$, the unitary v_k obeys the equality $v_0^{d_k} = \mathrm{I}_d$.

(ii) The unitary matrix v_0 is monomial, so that $v_0 \mathcal{D}_d v_0^* = \mathcal{D}_d$.

(iii) For all $0 \leq k < m$, the unitary matrix v_{k+1} induces a conjugation on the *-subalgebra $\mathcal{A}^*(\mathcal{D}_d, v_0, \ldots, v_k) \subset M_d(\mathbb{C})$, that is

$$v_{k+1} \mathcal{A}^* \left(\mathcal{D}_d, v_0, \ldots, v_k\right) v_{k+1}^* = \mathcal{A}^* \left(\mathcal{D}_d, v_0, \ldots, v_k\right).$$

We then say the pair of masas $\{\mathcal{D}_d, \mathcal{M}\}$ is concatenated normal *w.r.t. the factorisation above (in that particular order of the factors). More generally, we call any pair of masas in $M_d(\mathbb{C})$ concatenated normal if it is equivalent to a pair fulfilling the conditions of $\{\mathcal{D}_d, \mathcal{M}\}$.*

As in the case of normal masa pairs, we do not just postulate that concatenated normal masa pairs shall induce arbitrary (e.g. trivial) actions of the groups $\mathbb{Z}/d_k$, but *injective* ones. This is already encoded in the definition above.

Proposition 4.5.2. *In the situation of Definition 4.5.1, set $\mathcal{A}_k = \mathcal{A}^*(\mathcal{D}_d, v_0, \dots, v_k)$ for all $0 \leq k \leq m$, and $\mathcal{A}_{-1} = \mathcal{D}_d$ for convenience. Each of the *-subalgebras $\mathcal{A}_k \subset M_d(\mathbb{C})$ has dimension $d \cdot d_0 \cdots d_k$, and for each $0 \leq k \leq m$, there is an injective group homomorphism*

$$\beta_{[k]} : \mathbb{Z}/d_k \hookrightarrow Aut\ (\mathcal{A}_{k-1}), \\ i \longmapsto \beta_{[k],i}\,, \quad \beta_{[k],i}(a) = v_k^i a v_k^{-i} \text{ for all } a \in \mathcal{A}_{k-1}.$$

This induces the isomorphisms of C^*-algebras

$$\mathcal{A}_k \cong \mathcal{A}_{k-1} \rtimes_{\beta_{[k]}} \mathbb{Z}/d_k \cong \left(\left(\cdots\left(C^*\left(\mathbb{Z}/d\right) \rtimes_{\beta_{[0]}} \mathbb{Z}/d_0\right)\cdots\right) \rtimes_{\beta_{[k-1]}} \mathbb{Z}/d_{k-1}\right) \rtimes_{\beta_{[k]}} \mathbb{Z}/d_k$$

for all $0 \leq k \leq m$, where we identify the group actions $\beta_{[k]}$ on the *-subalgebras of $M_d(\mathbb{C})$ and the respective actions on the isomorphic crossed products.

Proof. Since the commuting unitary matrices $v_0, \dots, v_m \in \mathcal{U}_d$ generate the masa $\mathcal{M}$, the latter is linearly spanned by the set of ordered products

$$\mathfrak{B} = \left\{ v_0^{i_0} \cdots v_m^{i_m} \;\middle|\; 0 \leq i_k < d_k, 0 \leq k \leq m \right\}.$$

At the same time, condition (i) of Definition 4.5.1 ($v_k^{d_k} = \mathrm{I}_d$) implies $|\mathfrak{B}| \leq d$, so that $\mathfrak{B}$ is a basis for $\mathcal{M}$ by dimension.

To begin with, we show that for each $0 \leq k \leq m$, a basis for the *-subalgebra $\mathcal{A}_k$ is given by

$$\mathfrak{B}_k = \left\{ \mathrm{z}_d^i v_0^{i_0} \cdots v_k^{i_k} \;\middle|\; 0 \leq i < d, 0 \leq i_s < d_s, 0 \leq s \leq k \right\},$$

where $\mathrm{z}_d \in \mathcal{D}_d$ is the clock matrix as always. Counting the elements in $\mathfrak{B}_k$, it then follows immediately that the dimension of each $\mathcal{A}_k$ equals $d \cdot d_0 \cdots d_k$.

We first show by induction that the sets $\mathfrak{B}_k$ *span* the *-algebras $\mathcal{A}_k$ for all $0 \leq k \leq m$, starting with $k = 0$. We know that z_d generates the diagonal and that $\mathrm{z}_d^d = \mathrm{I}_d$. By condition (i) of Definition 4.5.1, we further have $v_0^{d_0} = \mathrm{I}_d$. As a consequence, the *-subalgebra $\mathcal{A}_0 = \mathcal{A}^*(\mathcal{D}_d, v_0) = \mathcal{A}^*(\mathrm{z}_d, v_0)$ is surely spanned by products of the form

$$\mathrm{z}_d^{i_0} v_0^{j_0} \cdots \mathrm{z}_d^{i_t} v_0^{j_t},$$

where $t \in \mathbb{N}_0$, $0 \leq i_0, \dots, i_t < d$, and $0 \leq j_0, \dots, j_t < d_k$. From condition (ii) of Definition 4.5.1, we deduce that there is a polynomial $p_0 \in \mathbb{C}[X]$, of degree less than d, satisfying the equality $v_0 \mathrm{z}_d v_0^* = p_0(\mathrm{z}_d)$ and thus $v_0 \mathrm{z}_d = p_0(\mathrm{z}_d) v_0$. Exploiting this fact finitely many times, one can write the product above in the form

$$\mathrm{z}_d^{i_0} v_0^{j_0} \cdots \mathrm{z}_d^{i_t} v_0^{j_t} = p(\mathrm{z}_d) v_0^{j_0} \cdots v_0^{j_t}$$

for a certain polynomial $p \in \mathbb{C}[X]$ of degree at most $d - 1$. The right-hand side expression is clearly a linear combination of elements of the set $\mathfrak{B}_0$, so that the latter spans

$\mathcal{A}_0$. (As a remark, we have started our induction with the case $k = 0$ for clarity; we could as well have taken $k = -1$ as base case.)

For the inductive step, presume that $\mathcal{A}_{k-1}$ is spanned by the set $\mathfrak{B}_{k-1}$ for an index $k \geq 1$. Just as in the base case, elements in $\mathcal{A}_k = \mathcal{A}^*(\mathcal{D}_d, v_0, \dots, v_k) = \mathcal{A}^*(\mathfrak{B}_{k-1}, v_k)$ are, a priori, linear combinations of products of the form

$$a_0 v_k^{j_0} a_1 v_k^{j_1} \cdots a_t v_k^{j_t} \tag{4.15}$$

for $t \in \mathbb{N}_0$, elements $a_0, \dots, a_t \in \mathfrak{B}_{k-1}$, and exponents $0 \leq j_0, \dots, j_t < d_k$. Since the powers of v_k act by conjugation on $\mathcal{A}_{k-1} = \operatorname{span} \mathfrak{B}_{k-1}$ according to condition (iii) of Definition 4.5.1, there is—by analogy with the base step—a linear combination a_1' of elements of the set $\mathfrak{B}_{k-1}$ such that $v_k^{j_0} a_1 v_k^{-j_0} = a_1'$ and hence $v_k^{j_0} a_1 = a_1' v_k^{j_0}$. The product (4.15) can thereby be rewritten as

$$a_0 a_1' v_k^{j_0 + j_1} a_2 v_k^{j_2} \cdots a_t v_k^{j_t}.$$

After finitely many analogue steps, one sees that the product (4.15) can in fact be expressed as $a v_k^j$ for an element $a \in \mathcal{A}_{k-1}$ and an exponent $0 < j < d_k$. Now a is again a linear combination of matrices of $\mathfrak{B}_{k-1}$, and consequently $a v_k^j$—and thus each element in $\mathcal{A}_k$—is a linear combination of elements of $\mathfrak{B}_k$.

Next we show that each of the spanning sets $\mathfrak{B}_k$ is linearly independent. For the rest of the proof, fix an index $0 \leq k \leq m$. First observe that due to the quasi-orthogonality of the masas $\mathcal{D}_d$ and $\mathcal{M}$, we have

$$\begin{aligned}
\left(\mathrm{Z}_d^i v_0^{i_0} \cdots v_k^{i_k} \,\middle|\, \mathrm{Z}_d^j v_0^{j_0} \cdots v_k^{j_k} \right)_{\mathrm{HS}} &= \tau\left(\mathrm{Z}_d^i v_0^{i_0} \cdots v_k^{i_k} v_k^{-j_k} \cdots v_0^{-j_0} \mathrm{Z}_d^{-j} \right) \\
&= \tau\left(\mathrm{Z}_d^{i-j} v_0^{i_0 - j_0} \cdots v_k^{i_k - j_k} \right) \\
&= \tau\left(\mathrm{Z}_d^{i-j} \right) \tau\left(v_0^{i_0 - j_0} \cdots v_k^{i_k - j_k} \right)
\end{aligned}$$

for all indices $0 \leq i, j < d$ and $0 \leq i_s, j_s < d_s$ for $0 \leq s \leq k$, where we have used criterion (vi) of Theorem 2.2.14 in the last step. It follows that the set $\mathfrak{B}_k$ can be divided into pairwise orthogonal subsets

$$\left\{ v_0^{i_0} \cdots v_k^{i_k} \,\middle|\, 0 \leq i_s < d_s, 0 \leq s \leq k \right\}, \left\{ \mathrm{Z}_d v_0^{i_0} \cdots v_k^{i_k} \,\middle|\, 0 \leq i_s < d_s, 0 \leq s \leq k \right\},$$
$$\dots, \left\{ \mathrm{Z}_d^{d-1} v_0^{i_0} \cdots v_k^{i_k} \,\middle|\, 0 \leq i_s < d_s, 0 \leq s \leq k \right\}.$$

Up to multiplication by a power of Z_d, i.e. by a fixed unitary, each of these disjoint sets is a subset of the basis $\mathfrak{B}$ of $\mathcal{M}$ and hence linearly independent. Orthogonality implying linear independence, we have shown that $\mathfrak{B}_k$ is in fact a *basis* for the *-subalgebra $\mathcal{A}_k$.

For the injectivity of the group homomorphisms $\beta_{[k]}$, suppose that the *-automorphism $\beta_{[k],i_0}$ of $\mathcal{A}_{k-1}$—which exists according to conditions (ii) and (iii) respectively of Definition 4.5.1—is trivial for an exponent $0 < i_0 \leq d_k$. This especially implies

$$v_k^{i_0} a v_k^{-i_0} = a$$

for all $a \in \mathcal{D}_d \subset \mathcal{A}_{k-1}$, whence the unitary $v_k^{i_0}$ is a diagonal matrix. The masas $\mathcal{M}$ and $\mathcal{D}_d$ being quasi-orthogonal, the element $v_k^{i_0} \in \mathcal{M}$ is thereby a multiple of the unit matrix I_d (cf. Corollary 2.2.15). Supposing $i_0 < d_k$ would immediately imply $|\mathfrak{B}| < d$ and thus contradict the fact that $\mathfrak{B}$ is a basis for $\mathcal{M}$.

Combined with condition (i) of Definition 4.5.1, this shows that the *-automorphisms $\beta_{[k],0}, \dots, \beta_{[k],d_k-1}$ are pairwise different (on the diagonal $\mathcal{D}_d$, and thus on $\mathcal{A}_{k-1}$). In other words, the group homomorphism $\beta_{[k]} : \mathbb{Z}/d_k \to \mathrm{Aut}\,(\mathcal{A}_{k-1})$ is injective.

At last, let us verify the proposed isomorphisms $\mathcal{A}_{k-1} \rtimes_{\beta_{[k]}} \mathbb{Z}/d_k \cong \mathcal{A}_k$. The triple $(\mathcal{A}_{k-1}, \mathbb{Z}/d_k, \beta_{[k]})$ is a C*-dynamical system (see Section 2.5). A covariant representation (cf. Definition 2.5.1) of this system lies at hand: let $\pi : \mathcal{A}_{k-1} \to M_d(\mathbb{C})$ label the identity operator, restricted to $\mathcal{A}_{k-1}$, and take as (faithful) unitary group representation $u : \mathbb{Z}/d_k \to \mathcal{U}_d$, $i \mapsto u_i = v_k^i$. Then the covariance relation $\pi(\beta_{[k],i}(a)) = u_i \pi(a) u_i^*$ is trivially satisfied.

Recall that the crossed product $\mathcal{A}_{k-1} \rtimes_{\beta_{[k]}} \mathbb{Z}/d_k$ is originally defined as the *-algebra $\mathcal{C}(\mathbb{Z}/d_k, \mathcal{A}_{k-1})$, endowed with multiplication and involution twisted by the automorphism $\beta_{[k]}$ (see equations (2.11) on page 64), and endowed with the universal norm defined in Proposition 2.5.3. (We do not have to care about completion, since the involved algebras are finite-dimensional.) Proposition 2.5.2 tells us that a *-representation of $\mathcal{A}_{k-1} \rtimes_{\beta_{[k]}} \mathbb{Z}/d_k$ (the integrated form of the covariant representation (π, u)) is given by

$$\begin{aligned} \pi \rtimes u : \mathcal{C}(\mathbb{Z}/d_k, \mathcal{A}_{k-1}) &\longrightarrow M_d(\mathbb{C}), \\ (a_0, \dots, a_{k-1}) &\longmapsto \sum_{i=0}^{d_k-1} \pi\,(a_i)\, u_i = \sum_{i=0}^{d_k-1} a_i v_k^i. \end{aligned}$$

By construction, the integrated form $\pi \rtimes u$ maps the crossed product $\mathcal{A}_{k-1} \rtimes \mathbb{Z}/d_k$ into $\mathcal{A}_k$. As we have seen above, the fact that the set $\mathfrak{B}_k$ is a basis for $\mathcal{A}_k$ in particular implicates that every element in $\mathcal{A}_k$ is of the form $a v_k^i$ for an element $a \in \mathcal{A}_{k-1}$ and an exponent $0 \leq i < d_k$. This shows that the representation $\pi \rtimes u$ maps *surjectively* onto $\mathcal{A}_k$. At the same time, both $\mathcal{C}(\mathbb{Z}/d_k, \mathcal{A}_{k-1})$ and $\mathcal{A}_k$ are of dimension $d \cdot d_0 \cdots d_k$ by what we have already shown, so that $\pi \rtimes u$ is injective as well. All in all, we have thus obtained the *-isomorphism $\mathcal{A}_k \cong \mathcal{A}_{k-1} \rtimes_{\beta_{[k]}} \mathbb{Z}/d_k$. The second proposed isomorphism immediately follows by induction, so we are done. □

In the situation of Proposition 4.5.2, we notably have the equality $\mathcal{A}_m = M_d(\mathbb{C})$ by dimension, which also follows from the quasi-orthogonality of the masas $\mathcal{D}_d$ and $\mathcal{M}$ (see for instance implication (2.3) on page 40). There is thus a *-isomorphism

$$M_d(\mathbb{C}) \cong (\cdots((C^*(\mathbb{Z}/d) \rtimes_{\beta_{[0]}} \mathbb{Z}/d_0) \rtimes_{\beta_{[1]}} \mathbb{Z}/d_1) \cdots) \rtimes_{\beta_{[m]}} \mathbb{Z}/d_m,$$

which generalises the isomorphism $M_d(\mathbb{C}) \cong C^*(\mathbb{Z}/d) \rtimes_{\tilde{\beta}} (\mathbb{Z}/d_0 \times \cdots \times \mathbb{Z}/d_m)$, stated at the very end of Section 4.2.

For prime dimensions, every concatenated normal pair (just like every normal pair) is automatically standard. As there are non-standard pairs of quasi-orthogonal masas in $M_p(\mathbb{C})$ for all $p \geq 7$ (cp. Fact 2.4.11), the class of concatenated normal pairs does not in general comprise all quasi-orthogonal pairs of masas.

We shall not go into a more detailed study of concatenated normal masa pairs in the present work. Instead, we confine ourselves to presenting the following motivating example.

Proposition 4.5.3. *All pairs of quasi-orthogonal masas in $M_4(\mathbb{C})$ are concatenated normal.*

Proof. It is an elementary exercise to check that all unitary complex Hadamard matrices in $M_4(\mathbb{C})$ are equivalent (in the sense of Definition 1.3.4) to the Hadamard matrix

$$h_\lambda = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & \lambda & -\lambda \\ 1 & -1 & -\lambda & \lambda \end{pmatrix}$$

for some element of the unit circle $\lambda \in \mathbb{T}$ (see for instance [44, 103]). As a consequence, every pair of quasi-orthogonal masas in $M_4(\mathbb{C})$ is equivalent to one of the pairs $\{\mathcal{D}_4, h_\lambda \mathcal{D}_4 h_\lambda^*\}$, $\lambda \in \mathbb{T}$ (cf. Lemma 2.4.2).

Fix an element $\lambda \in \mathbb{T}$ and set $\mathcal{M}_\lambda = h_\lambda \mathcal{D}_4 h_\lambda^*$. As one easily computes, the masa $\mathcal{M}_\lambda$ contains the unitary matrices

$$v_0 = h_\lambda \mathrm{diag}(1,1,-1,-1) h_\lambda^* = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \in \mathcal{W}_4$$

and

$$v_1 = h_\lambda \mathrm{diag}(1,-1,1,-1) h_\lambda^* = \frac{1}{2}\begin{pmatrix} 0 & 0 & 1+\bar{\lambda} & 1-\bar{\lambda} \\ 0 & 0 & 1-\bar{\lambda} & 1+\bar{\lambda} \\ 1+\lambda & 1-\lambda & 0 & 0 \\ 1-\lambda & 1+\lambda & 0 & 0 \end{pmatrix} \in \mathcal{U}_4.$$

Looking at the diagonalisations of v_0 and v_1, you immediately see that $v_0^2 = v_1^2 = \mathrm{I}_4$, and that $\{v_0, v_1, v_0 v_1, \mathrm{I}_4\}$ is a Hilbert-Schmidt orthonormal basis for the masa $\mathcal{M}_\lambda$. The unitary v_0 is monomial, so all that is left to show in regard to Definition 4.5.1 is that v_1 induces a conjugation on the *-subalgebra $\mathcal{A}^*(\mathcal{D}_4, v_0)$, i.e.

$$v_1 \mathcal{A}^*(\mathcal{D}_4, v_0) v_1^* = \mathcal{A}^*(\mathcal{D}_4, v_0).$$

The *-subalgebra $\mathcal{A}^*(\mathcal{D}_4, v_0)$ is generated by the unitaries Z_4 and v_0. Since v_0 and v_1 commute, it suffices to show that the element $v_1 \mathrm{Z}_4 v_1^*$ belongs to $\mathcal{A}^*(\mathcal{D}_4, v_0)$. Setting

$$\begin{aligned} \mu &= -\frac{1}{4}\left(|1+\lambda|^2 + \mathrm{i}\,|1-\lambda|^2\right) & \text{and} \qquad \nu &= -{}^1\!/\!_4\left(1+\bar{\lambda}\right)(1-\lambda) \\ &= \frac{\mathrm{i}-1}{2}\mathrm{Re}\,\lambda - \frac{\mathrm{i}+1}{2} & &= \frac{\mathrm{i}}{2}\mathrm{Im}\,\lambda, \end{aligned}$$

one computes

$$v_1 \mathrm{Z}_4 v_1^* = \begin{pmatrix} \mu & 0 & 0 & 0 \\ 0 & \mathrm{i}\bar{\mu} & 0 & 0 \\ 0 & 0 & -\mu & 0 \\ 0 & 0 & 0 & -\mathrm{i}\bar{\mu} \end{pmatrix} + \begin{pmatrix} \nu + \mathrm{i}\bar{\nu} & 0 & 0 & 0 \\ 0 & \bar{\nu} + \mathrm{i}\nu & 0 & 0 \\ 0 & 0 & -\bar{\nu} - \mathrm{i}\nu & 0 \\ 0 & 0 & 0 & -\nu - \mathrm{i}\nu \end{pmatrix} \circ \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

which obviously is an element of the *-algebra $\mathcal{A}^*(\mathcal{D}_4, v_0)$. □

It is straightforward to check that the Hadamard matrices h_λ are equivalent to the Fourier matrix F_4 if and only if $\lambda \in \{\pm \mathrm{i}\}$. On the other hand, one directly sees that the unitary matrix v_1 in the proof above is monomial precisely if $\lambda \in \{\pm 1\}$. This determines the normal pairs among the quasi-orthogonal masa pairs $\{\mathcal{D}_4, h_\lambda \mathcal{D}_4 h_\lambda^*\}$.

Observation 4.5.4. For all $\lambda \in \mathbb{T}$, let $h_\lambda \in M_4(\mathbb{C})$ denote the complex Hadamard matrix as defined in the proof of Proposition 4.5.3.

- The pair $\{\mathcal{D}_4, h_\lambda \mathcal{D}_4 h_\lambda^*\}$ is a standard pair—that is normal w.r.t. the trivial decomposition—exactly if $\lambda \in \{\pm \mathrm{i}\}$.
- The pair $\{\mathcal{D}_4, h_\lambda \mathcal{D}_4 h_\lambda^*\}$ is normal w.r.t. the factorisation $4 = 2 \cdot 2$ if and only if $\lambda \in \{\pm 1\}$.

We conclude our discussion of concatenated normal masa pairs with the following important

Remarks 4.5.5. (a) Lengthy calculations reveal that the masa pair $\{\mathcal{D}_4, h_\lambda \mathcal{D}_4 h_\lambda^*\}$ is nice if and only if the parameter $\lambda \in \mathbb{T}$ is a fourth root of unity. Comparing this to Observation 4.5.4, we see that every nice masa pair is normal in $M_4(\mathbb{C})$. Using Proposition 4.3.11, a look at the list of all (isomorphism classes) of index groups of order four (see for instance [56]) allows come to the same conclusion.

(b) One checks without much effort that uncountably many of the quasi-orthogonal masa pairs $\{\mathcal{D}_4, h_\lambda \mathcal{D}_4 h_\lambda^*\}$ are pairwise inequivalent, as predicted by Proposition 2.4.10. With regard to the previous remark and Proposition 4.5.3, this gives evidence that there are concatenated normal masa pairs which are not nice.

Chapter 5

Smid families

As we have seen in Theorem 4.4.11, every nice complete masa family in the matrix algebra $M_{p^n}(\mathbb{C})$ stems, up to unitary equivalence, from a quasi-partition of the nice unitary error basis $\mathfrak{E}^p_{2n}$ (or, equivalently, $\mathfrak{S}_{p^n}$). Such partitions can be encoded by families of symmetric matrices in $M_n(\mathbb{F}_p)$ with pairwise invertible differences—for which we propose the acronymic expression *smid families*—, as was first done by Bandyopadhyay et al. (cf. Construction 3.3.12).

In the first section of this chapter, we show that *all* nice complete masa families are encoded by smid families. We further define an equivalence relation for the latter that is compatible with the equivalence of the corresponding masa families. Combining the results above, we obtain the main theorem of the present thesis, which states that there is a one-to-one correspondence between nice complete sets of masas in $M_{p^n}(\mathbb{C})$ and complete smid families in $M_n(\mathbb{F}_p)$ for all $n \in \mathbb{N}$ and $p \in \mathbb{P}$.

A coherent next step towards a better understanding of complete nice masa families is, in regard to our main result, the study of complete smid families in $M_n(\mathbb{F}_p)$. To all appearances, the classification of the latter is quite a hard task. To get a grip of this problem, we first investigate complete smid families which are linear subspaces of $M_2(\mathbb{F}_p)$ in Section 5.2.

In Section 5.3, we address the question whether $M_2(\mathbb{F}_p)$ admits *non-linear* complete smid families. To this aim, we study connections between general complete smid families in $M_2(\mathbb{F}_p)$, Latin squares, and permutation polynomials. While this allows us to conclude that no non-linear complete smid families exist in $M_2(\mathbb{F}_3)$ and $M_2(\mathbb{F}_5)$, the question above remains undecided for general primes in this work.

Using computer algebraic methods, we have investigated the structure of smid families of arbitrary length in the smallest prime power dimensions. The results are collected in Section 5.4.

5.1 Equivalence classes of smid families and nice sets of masas

We establish the relation between smid families and nice complete masa families in this section. Although we have already introduced the term *smid family*, let us start with a proper definition.

Definition 5.1.1. *Let F be a finite field and n a natural number. A* smid family*is a set $\mathcal{S} \subset M_n(F)$ of symmetric matrices with invertible differences. Precisely, this means that the difference $A - B$ is either invertible or zero for each pair of matrices $A, B \in \mathcal{S}$.*

A smid family $\mathcal{S}$ is called maximal *if there is no symmetric matrix $C \in M_n(F) \setminus \mathcal{S}$ such that the union $\mathcal{S} \cup \{C\}$ is a smid family. A maximal smid family is said to be* complete *if there are no smid families in $M_n(F)$ containing a greater number of matrices. A smid family which is included in a complete smid family is called* completable.

Obviously, the length of all complete smid families in $M_n(F)$ is the same. According to our aim, we will mostly limit our investigation to smid families in $M_n(\mathbb{F}_p)$ in the sequel.

Proposition 5.1.2. *For all numbers $n \in \mathbb{N}$, $p \in \mathbb{P}$, complete smid families in $M_n(\mathbb{F}_p)$ consist of p^n elements. One example of a complete smid family in $M_n(\mathbb{F}_p)$ is provided by a symmetric representation of the field $\mathbb{F}_{p^n}$ which exists for all $n \in \mathbb{N}$, $p \in \mathbb{P}$, according to Theorem 3.3.11.*

Proof. A rather simple combinatorial argument proves the first part. The difference of two matrices sharing the same first row can doubtlessly not be regular, hence each two matrices inside one and the same smid family must differ in their first row. Obviously, there are only p^n different choices for the first row of a matrix in $M_n(\mathbb{F}_p)$. □

Here are some examples of smid families in the smallest non-trivial prime power dimension, that is in the matrix algebra $M_2(\mathbb{F}_2)$. You easily convince yourself of the proposed assertions.

Examples 5.1.3. (i) The subsets

$$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \quad \text{and} \quad \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

of $M_2(\mathbb{F}_2)$ are smid families which are neither complete nor maximal.

(ii) A complete smid family in $M_2(\mathbb{F}_2)$ is given by the subset

$$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}.$$

(iii) The following subset of $M_2(\mathbb{F}_2)$ is a maximal smid family.

$$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

Remark 5.1.4. Note that according to Definition 5.1.1, the *empty set* is a smid family of length zero. This will prove convenient in the following discussion. We will not always explicitly consider the trivial case that a smid family of unspecified length is empty, but nevertheless, no contradictions will arise from allowing this case.

Encoding nice masa families in $\mathbb{C}l^{\mathbf{p}}_{\mathbf{2n}}$ by smid families

As a next step, we rephrase the method of Bandyopadhyay et al. to obtain complete nice masa families (Construction 3.3.12), using the picture of the generalised Clifford algebra. For the rest of this section, fix a natural number $n \in \mathbb{N}$, a prime number $p \in \mathbb{P}$, and set $d = p^n$.

The alternative generators b_i, c_i of the generalised Clifford algebra $\mathbb{C}l^p_{2n}$, introduced in Definition/Proposition 4.4.9, are once more a valuable tool in the present context.

First recall that in Section 3.3, we have defined unitaries $\mathrm{B}_i, \mathrm{C}_i \in M_d(\mathbb{C})$ for all indices $0 \leq i < n$ by

$$\mathrm{B}_i = \quad \mathrm{I}_p \otimes \cdots \otimes \mathrm{I}_p \otimes \overset{(i\text{th pos.})}{\mathrm{Z}_p} \otimes \mathrm{I}_p \otimes \cdots \otimes \mathrm{I}_p$$

$$\text{and} \quad \mathrm{C}_i = \begin{cases} \mathrm{i}\, \mathrm{I}_p \otimes \cdots \otimes \mathrm{I}_p \otimes \sigma_x \sigma_z \otimes \mathrm{I}_p \otimes \cdots \otimes \mathrm{I}_p & \text{if } p = 2, \\ \mathrm{I}_p \otimes \cdots \otimes \mathrm{I}_p \otimes \mathrm{X}_p \mathrm{Z}_p^* \otimes \mathrm{I}_p \otimes \cdots \otimes \mathrm{I}_p & \text{else,} \end{cases}$$

see Definition/Proposition 3.3.8. The set of all ordered products of these unitaries, denoted $\mathfrak{E}^p_{2n}$, is a nice unitary error basis with index group $\bigoplus_{2n} \mathbb{Z}/p$, cf. Definition/Proposition 3.3.8 and Example 4.1.3 (c).

Furthermore, we have checked in Proposition 3.3.10 (items (ii) to (iv)) that

- for each symmetric matrix $K = (k_{i,j}) \in M_n(\mathbb{F}_p)$, a masa $\mathcal{M}_K \subset M_d(\mathbb{C})$ is algebraically generated by the n products

$$\mathrm{B}_0^{k_{0,0}} \cdots \mathrm{B}_{n-1}^{k_{0,n-1}} \mathrm{C}_0,\ \mathrm{B}_0^{k_{1,0}} \cdots \mathrm{B}_{n-1}^{k_{1,n-1}} \mathrm{C}_1, \ldots,\ \mathrm{B}_0^{k_{n-1,0}} \cdots \mathrm{B}_{n-1}^{k_{n-1,n-1}} \mathrm{C}_{n-1},$$

- two masas $\mathcal{M}_K$ and $\mathcal{M}_L$ obtained in this way are quasi-orthogonal if and only if the difference $K - L \in M_n(\mathbb{F}_p)$ is regular,
- and any masa of the form $\mathcal{M}_K$ is quasi-orthogonal to the diagonal masa

$$\mathcal{N} = \mathcal{A}^*(\mathrm{B}_0, \ldots, \mathrm{B}_{n-1}) = \mathcal{D}_d.$$

These are the key ingredients for the construction of Bandyopadhyay et al., which produces nice masa families $\{\mathcal{N}, \mathcal{M}_{K_0}, \ldots, \mathcal{M}_{K_{m-1}}\}$ in the complex $d\times d$-matrices from sets $\{K_0, \ldots, K_{m-1}\} \subset M_n(\mathbb{F}_p)$ of symmetric matrices with pairwise invertible differences—that is to say, from smid families.

As we have observed in Remark 4.4.10 (a), the unitaries $b_i, c_i \in \mathbb{C}l_{2n}^p$ correspond to the matrices $\mathrm{B}_i, \mathrm{C}_i \in M_d(\mathbb{C})$ under the standard *-representation of the generalised Clifford algebra $\mathbb{C}l_{2n}^p$ specified in the proof of Theorem 4.4.6 (page 148f.). That is why the following construction is just a literal translation of the construction of Bandyopadhyay et al. into the picture of the generalised Clifford algebra. (Strictly speaking, we have only defined quasi-orthogonality for matrix algebras in Definition 2.2.1, but clearly this notion can be generalised to arbitrary unital C*-algebras in the obvious way. We presuppose this generalisation in the sequel.)

Construction 5.1.5 (Reformulation of Bandyopadhyay et al. 2002)**.** For any symmetric matrix $K = (k_{i,j})_{0\le i,j<n} \in M_n(\mathbb{F}_p)$, a masa in $\mathbb{C}l_{2n}^p$ is defined by

$$\begin{aligned}\mathcal{M}_K = \mathcal{A}^*(&b_0^{k_{0,0}} \;\cdots\; b_{n-1}^{k_{0,n-1}} c_0,\\ &b_0^{k_{1,0}} \;\cdots\; b_{n-1}^{k_{1,n-1}} c_1,\\ &\qquad\vdots\\ &b_0^{k_{n-1,0}} \cdots b_{n-1}^{k_{n-1,n-1}} c_{n-1}).\end{aligned}$$

If $L \in M_n(\mathbb{F}_p)$ is another symmetric matrix, and $\mathcal{M}_L \subset \mathbb{C}l_{2n}^p$ the associated masa, then $\mathcal{M}_K$ and $\mathcal{M}_L$ are quasi-orthogonal if and only if the difference $K - L$ is an invertible matrix. What is more, every masa $\mathcal{M}_K$ defined as above is quasi-orthogonal to the masa $\mathcal{N} = \mathcal{A}^*(b_0, \ldots, b_{n-1}) \subset \mathbb{C}l_{2n}^p$.

As a consequence, each smid family $\mathcal{S} = \{K_0, \ldots, K_{m-1}\}$ inside $M_n(\mathbb{F}_p)$ of length $0 \le m \le p^n$ induces a nice masa family of length $m+1$ (with index group $\bigoplus_{2n} \mathbb{Z}/p$)

$$\mathscr{F}(\mathcal{S}) = \{\mathcal{N}, \mathcal{M}_{K_0}, \ldots, \mathcal{M}_{K_{m-1}}\}.$$

The next theorem is the second step (succeeding Theorem 4.4.11) towards a full classification of nice complete masa families in terms of smid families.

Theorem 5.1.6. *Let $0 \leq m < p^n$ be a natural number and $\mathscr{F} = \{\mathcal{A}_{-1}, \mathcal{A}_0, \dots, \mathcal{A}_{m-1}\}$ a nice family of $m+1$ pairwise quasi-orthogonal masas in the matrix algebra $M_{p^n}(\mathbb{C})$ with index group $\bigoplus_{2n} \mathbb{Z}/p$. Then $\mathscr{F}$ can be encoded by a smid family of length m in $M_n(\mathbb{F}_p)$.*

More precisely, one finds an isomorphic matrix representation $\tilde{\rho} : \mathbb{C}l_{2n}^p \to M_{p^n}(\mathbb{C})$ of the generalised Clifford algebra and a smid family $\mathcal{S} = \{K_0, \dots, K_{m-1}\} \subset M_n(\mathbb{F}_p)$ satisfying the identities

$$\tilde{\rho}(\mathcal{N}) = \mathcal{A}_{-1} \quad \textit{and} \quad \tilde{\rho}(\mathcal{M}_{K_i}) = \mathcal{A}_i \ \textit{for all} \ 0 \leq i < m,$$

where the masas $\mathcal{M}_{K_i} \subset \mathbb{C}l_{2n}^p$ are defined as in Construction 5.1.5. Unless the smid family $\mathcal{S}$ is empty, it can always be arranged that the matrix $K_0 \in M_n(\mathbb{F}_p)$ is zero.

Proof. If m happens to be zero, the nice family $\mathscr{F}$ contains only the masa $\mathcal{A}_{-1}$ and the proposed smid family $\mathcal{S}$ is empty. Thereby the only condition required from the *-representation $\tilde{\rho}$ is given by the identity $\tilde{\rho}(\mathcal{N}) = \mathcal{A}_{-1}$. This can doubtlessly be arranged, since all masas are unitarily equivalent.

From here one, let us suppose $m \geq 1$. By assumption, the family $\mathscr{F}$ stems from a (partial) quasi-partition of a very nice unitary error basis $\mathfrak{E}$ for matrix algebra $M_d(\mathbb{C})$, with index group $\bigoplus_{2n} \mathbb{Z}/p$. Beyond that, we have convinced ourselves in Theorem 4.4.11 that for an arbitrary pair of masas in the nice family $\mathscr{F}$—here we pick $\mathcal{A}_{-1}$ and $\mathcal{A}_0$ for convenience—, one can arrange the following.

- One finds unitary matrices $v_0, \dots, v_{n-1} \in \mathcal{U}_d$ generating the masa $\mathcal{A}_{-1}$, and unitaries $w_0, \dots, w_{n-1} \in \mathcal{U}_d$ generating $\mathcal{A}_0$, such that w.l.o.g. the nice error basis $\mathfrak{E}$ is given by

  $$\mathfrak{E} = \left\{ v_0^{k_0} \cdots v_{n-1}^{k_{n-1}} w_0^{l_0} \cdots w_{n-1}^{l_{n-1}} \;\middle|\; k_i, l_i \in \mathbb{F}_p \text{ for all } 0 \leq i < n \right\}.$$

- The unitaries $v_i, w_i \in \mathcal{U}_d$ are subject to the relations for the alternative generators $b_i, c_i \in \mathbb{C}l_{2n}^p$ of the generalised Clifford algebra (cf. Definition/Proposition 4.4.9). That is why a *-representation $\tilde{\rho} : \mathbb{C}l_{2n}^p \to M_d(\mathbb{C})$ is given by setting $\tilde{\rho}(b_i) = v_i$ and $\tilde{\rho}(c_i) = w_i$ for all $0 \leq i < n$. By definition, this *-representation obeys the identities

  $$\tilde{\rho}\left(\mathcal{A}^*(b_0, \dots, b_{n-1})\right) = \mathcal{A}_{-1} \quad \text{and} \quad \tilde{\rho}\left(\mathcal{A}^*(c_0, \dots, c_{n-1})\right) = \mathcal{A}_0.$$

  Using the notation of Construction 5.1.5, the last identities become $\tilde{\rho}(\mathcal{N}) = \mathcal{A}_{-1}$ and $\tilde{\rho}(\mathcal{M}_0) = \mathcal{A}_0$.

If m equals one, we just set $\mathcal{S} = \{0\}$ and have completed our proof. Otherwise, fix an index $1 \leq i_0 < m$. We aim at demonstrating that the preimage $\mathcal{M} = \tilde{\rho}^{-1}(\mathcal{A}_{i_0})$ equals a masa $\mathcal{M}_K \subset \mathbb{C}l_{2n}^p$, defined as in Construction 5.1.5, for a symmetric matrix $K = (k_{i,j}) \in M_n(\mathbb{F}_p)$.

Since $\mathcal{A}_{i_0}$ is generated by elements of the error basis $\mathfrak{E}$, the masa $\mathcal{M}$ is generated by elements of the standard orthonormal basis $\mathfrak{B}_{2n}^p$ of the generalised Clifford algebra $\mathbb{C}l_{2n}^p$, that is by elements of the form

$$\begin{aligned} \tilde{g}_0 &= \quad b_0^{\tilde{k}_{0,0}} \cdots b_{n-1}^{\tilde{k}_{0,n-1}} \cdot c_0^{l_{0,0}} \cdots c_{n-1}^{l_{0,n-1}}, \\ &\vdots \\ \tilde{g}_{n-1} &= b_0^{\tilde{k}_{n-1,0}} \cdots b_{n-1}^{\tilde{k}_{n-1,n-1}} \cdot c_0^{l_{n-1,0}} \cdots c_{n-1}^{l_{n-1,n-1}} \end{aligned}$$

for indices $\tilde{k}_{i,j}, l_{i,j} \in \mathbb{F}_p$, $0 \leq i,j < n$. The matrix of indices $L = (l_{i,j}) \in M_n(\mathbb{F}_p)$ is invertible, for otherwise there would be a non-trivial linear combination of rows

$$\sum_{i=0}^{n-1} t_i(l_{i,0}, \ldots, l_{i,n-1}) = 0$$

for some coefficients $t_0, \ldots, t_{n-1} \in \mathbb{F}_p$, and thereby $\mathcal{M}$ would contain the element

$$\tilde{g}_0^{t_0} \cdots \tilde{g}_{n-1}^{t_{n-1}} \sim_{\mathbb{T}} b_0^{\sum_{i=0}^{n-1} t_i \tilde{k}_{i,0}} \cdots b_{n-1}^{\sum_{i=0}^{n-1} t_i \tilde{k}_{i,n-1}} \cdot \underbrace{c_0^{\sum_{i=0}^{n-1} t_i l_{i,0}} \cdots c_{n-1}^{\sum_{i=0}^{n-1} t_i l_{i,n-1}}}_{=c_0^0 \cdots c_{n-1}^0 = 1}.$$

This would be contradictory:

- If all of the exponents of the factors $b_0, \ldots, b_{n-1}$ were equal to zero in the right-hand side expression, then the products of the generators $\tilde{g}_0, \ldots, \tilde{g}_{n-1}$ would not span the whole masa $\mathcal{M}$ as presumed.
- If some of the exponents $\sum_{i=0}^{n-1} t_i \tilde{k}_{i,i}$ were *non-zero,* then $\mathcal{M}$ would contain an element of the space $\mathcal{N} \ominus \mathbb{C} \cdot 1$, contradicting the quasi-orthogonality of the masas $\mathcal{M}$ and $\mathcal{N}$.

So the matrix L has an inverse $L^{-1} = M = (m_{i,j}) \in M_n(\mathbb{F}_p)$. Having this at our disposal, we can define another index matrix K by setting

$$k_{i,j} = \sum_{s=0}^{n-1} m_{i,s} \tilde{k}_{s,j}$$

for all $0 \leq i,j < n$. The masa $\mathcal{M}$ contains the following elements for all $0 \leq j < n$.

$$\begin{aligned} g_i &= \tilde{g}_0^{m_{i,0}} \cdots \tilde{g}_{n-1}^{m_{i,n-1}} \\ &\sim_{\mathbb{T}} b_0^{\sum_{s=0}^{n-1} m_{i,s} \tilde{k}_{s,0}} \cdots b_{n-1}^{\sum_{s=0}^{n-1} m_{i,s} \tilde{k}_{s,n-1}} \cdot \underbrace{c_0^{\sum_{s=0}^{n-1} m_{i,s} l_{s,0}} \cdots c_{n-1}^{\sum_{s=0}^{n-1} m_{i,s} l_{s,n-1}}}_{=c_i} \\ &= b_0^{k_{i,0}} \cdots b_{n-1}^{k_{i,n-1}} c_i \end{aligned}$$

It is straightforward that the elements $g_0, \dots, g_{n-1}$ generate the masa $\mathcal{M}$. Following the lines of the proof of Proposition 3.3.10, item *(ii)* (where we just have to replace the matrices $\mathtt{B}_i, \mathtt{C}_i \in M_d(\mathbb{C})$ by the respective generators $b_i, c_i \in \mathbb{C}l_{2n}^p$ in the whole statement), we moreover see that the matrix $K = (k_{i,j}) \in M_n(\mathbb{F}_p)$ must be symmetric. We thus end up with the identity $\mathcal{M} = \mathcal{M}_K$.

Proceeding as above for all masas $\mathcal{A}_1, \dots, \mathcal{A}_{m-1}$, we obtain symmetric matrices $K_1, \dots, K_{m-1} \in M_n(\mathbb{F}_p)$ so that we can write $\tilde{\rho}^{-1}(\mathcal{A}_i) = \mathcal{M}_{K_i}$ for all indices $1 \leq i < m$. The masas $\mathcal{M}_{K_i}$ are pairwise quasi-orthogonal as preimages of quasi-orthogonal masas w.r.t. a *-isomorphism, so we deduce from Proposition 3.3.10 *(iii)*—again translated to the picture of the generalised Clifford algebra—that each of the differences $K_i - K_j$ is either regular or zero, where i, j range from 1 to $m-1$. As each masa $\mathcal{M}_{K_i}$ is quasi-orthogonal to the masa $\mathcal{M}_0$, we moreover know that all of the matrices $K_1, \dots, K_{m-1}$ are invertible.

All in all, we have shown that the masas $\mathcal{N}, \mathcal{M}_0, \mathcal{M}_{K_1}, \dots, \mathcal{M}_{K_{m-1}} \subset \mathbb{C}l_{2n}^p$ are preimages of the masas $\mathcal{A}_{-1}, \dots, \mathcal{A}_{m-1} \subset M_d(\mathbb{C})$ w.r.t. the *-isomorphism $\tilde{\rho}$, and that the set of matrices $\{0, K_1, \dots, K_{m-1}\}$ is a smid family in $M_n(\mathbb{F}_p)$. □

Mind that Theorem 5.1.6 does *not* apply to *all* nice masa families in $M_d(\mathbb{C})$. For instance, we know that the standard pair $\{\mathcal{D}_d, \mathcal{A}^*(\mathtt{X}_d)\}$ is nice (cf. Example 4.3.4 *(a)*). However, it is not normal w.r.t. the full prime decomposition of d if the latter is a non-trivial prime power p^n, $n \geq 2$, see Corollary 4.2.5. It can therefore not stem from a quasi-partition of the nice error basis $\mathfrak{B}_{2n}^p$ in this case.

Equivalence classes of smid families and nice masa families

Let F denote any field. At first sight, one may expect that a natural notion of equivalence for smid families in the $n \times n$-matrices $M_n(F)$ should be formulated in terms of affine linear transformations, that is to say, one may want to consider two smid families $\mathcal{S}, \mathcal{T} \subset M_n(F)$ as equivalent if they fulfil the equality $\mathcal{T} = cA\mathcal{S}A^T + B$ for a matrix $A \in \mathrm{GL}_n(F)$, a symmetric matrix $B \in M_n(F)$, and a constant $c \in F^\times$.

However, it turns out that this notion is *not* appropriate for our purposes. To obtain compatibility of the equivalence of smid families on the one hand, and the equivalence of the associated nice masa families on the other, a kind of *"two-component-equivalence"* is needed. It involves the following simple

Observation 5.1.7. Let $m, n \in \mathbb{N}$ be two natural numbers. If the set of symmetric matrices $\mathcal{S} = \{0, K_1, \dots, K_{m-1}\}$ is a smid family in the matrix algebra $M_n(F)$, then so is the set

$$\mathcal{S}^{-1} = \{0, K_1^{-1}, \dots, K_{m-1}^{-1}\},$$

which we call the *inverse smid family to* $\mathcal{S}$.

Proof. Just observe that since $\mathcal{S}$ contains the zero matrix, all non-zero matrices in $\mathcal{S}$ are regular, so that we can write down the equations

$$(K_i - K_j)K_i^{-1}K_j^{-1} = K_j^{-1} - K_jK_i^{-1}K_j^{-1} = K_j(K_j^{-1} - K_i^{-1})K_j^{-1}$$

for all $1 \leq i, j < m$. The left-hand term in this calculation is known to be invertible if $i \neq j$, and therefore the same applies to the conjugated right-hand side

$$K_j^{-1}\left(K_j(K_j^{-1} - K_i^{-1})K_j^{-1}\right)K_j = K_j^{-1} - K_i^{-1}.$$

This proves that $\mathcal{S}^{-1}$ is a smid family, for the inverse of any symmetric matrix is again symmetric. □

Definition 5.1.8. *For all matrices $A \in GL_n(\mathbb{F}_p)$, $B \in M_n(\mathbb{F}_p)$, we define an affine linear transformation*

$$T_{A,B} : M_n(\mathbb{F}_p) \longrightarrow M_n(\mathbb{F}_p), \quad K \longmapsto AKA^T + B.$$

Furthermore, we declare a mapping $X : GL_n(\mathbb{F}_p) \cup \{0\} \to GL_n(\mathbb{F}_p) \cup \{0\}$ by $X(0) = 0$ and

$$X(K) = -K^{-1} \text{ for all } K \in GL_n(\mathbb{F}_p).$$

We call smid families $\mathcal{S}, \mathcal{T} \subset M_n(\mathbb{F}_p)$ of the same length equivalent if one of the following identities holds for some matrices $A, A' \in GL_n(\mathbb{F}_p)$, $B, B' \in M_n(\mathbb{F}_p)$ (the matrices B and B' are then automatically symmetric).

$$(i) \qquad \mathcal{T} = T_{A,B}(\mathcal{S}) \qquad\qquad (ii) \qquad \mathcal{T} = T_{A',B'} \circ X \circ T_{A,B}(\mathcal{S})$$

For the second equality, the choice of the matrix B must ensure that the smid family $T_{A,B}(\mathcal{S})$ contains the zero matrix.

Observe that the transformation X sends any smid family $\mathcal{S}$ which is contained in $\mathrm{GL}_n(\mathbb{F}_p) \cup \{0\}$ to its negative inverse $-\mathcal{S}^{-1}$. Also notice that one can always arrange—by an appropriate choice of the matrix A—that the matrix A' in item (ii) equals the unit matrix.

It is an exercise to verify that the equivalence of smid families defined above positively is an equivalence relation. In particular, it is redundant to concatenate transformations of type (i) and (ii), that is to say, any concatenation of such transformations is again of type (i) or (ii). These facts will also be confirmed by the following considerations.

We aim at demonstrating that the equivalence of smid families in $M_n(\mathbb{F}_p)$ corresponds to the equivalence of the associated nice masa families inside the generalised Clifford algebra $\mathbb{C}l_{2n}^{p}$ (w.r.t. the mapping specified in Construction 5.1.5). This goal is achieved by the two following lemmas.

Lemma 5.1.9. *As in Construction 5.1.5, associate with any symmetric matrix $K \in M_n(\mathbb{F}_p)$ a masa $\mathcal{M}_K$ in the generalised Clifford algebra $\mathbb{C}l_{2n}^p$, and define a masa $\mathcal{N} = \mathcal{A}^*(b_0, \ldots, b_{n-1})$.*

(i) Given an invertible matrix $A \in GL_n(\mathbb{F}_p)$ and a symmetric matrix $B \in M_n(\mathbb{F}_p)$, there is a *-automorphism $\phi_{A,B}$ of $\mathbb{C}l_{2n}^p$ fulfilling the identity $\phi_{A,B}(\mathcal{N}) = \mathcal{N}$ and, for all symmetric matrices $K \in M_n(\mathbb{F}_p)$,

$$\phi_{A,B}(\mathcal{M}_K) = \mathcal{M}_{T_{A,B}(K)}.$$

(ii) There is a *-automorphism χ of the generalised Clifford algebra $\mathbb{C}l_{2n}^p$ that satisfies the identities $\chi(\mathcal{N}) = \mathcal{M}_0$, $\chi(\mathcal{M}_0) = \mathcal{N}$, and, for all invertible *symmetric matrices $K \in GL_n(\mathbb{F}_p)$,*

$$\chi(\mathcal{M}_K) = \mathcal{M}_{X(K)} = \mathcal{M}_{-K^{-1}}.$$

It follows that equivalent smid families $\mathcal{S} = \{K_0, \ldots, K_{m-1}\}$ and $\mathcal{T} = \{L_0, \ldots, L_{m-1}\}$ in $M_n(\mathbb{F}_p)$ induce equivalent nice masa families

$$\mathscr{F}(\mathcal{S}) = \{\mathcal{N}, \mathcal{M}_{K_0}, \ldots, \mathcal{M}_{K_{m-1}}\} \quad \text{and} \quad \mathscr{F}(\mathcal{T}) = \{\mathcal{N}, \mathcal{M}_{L_0}, \ldots, \mathcal{M}_{L_{m-1}}\}.$$

inside the generalised Clifford algebra $\mathbb{C}l_{2n}^p$ ($0 \leq m \leq d$).

Proof. The assertion is trivial if m is zero, for then both of the smid families $\mathcal{S}$ and $\mathcal{T}$ are empty and the masa families $\mathscr{F}(\mathcal{S})$ and $\mathscr{F}(\mathcal{T})$ obviously coincide. We therefore assume $m > 0$ from here on.

It is elementary that every symmetric matrix in $M_n(\mathbb{F}_p)$ is a finite sum of matrices of the type

$$B_{i,j} = \begin{array}{cc} \begin{matrix} i\text{th col.} & j\text{th col.} \\ | & | \end{matrix} & \\ \begin{pmatrix} & 1 \\ 1 & \end{pmatrix} & \begin{matrix} \text{— } i\text{th row} \\ \text{— } j\text{th row} \end{matrix} \end{array},$$

where i and j range from 0 to $n-1$.

Likewise, every invertible matrix in $M_n(\mathbb{F}_p)$ is the product of a finite number of matrices of the form

$$M_{i,a} = \begin{array}{c} \begin{array}{ccccccc} &&& i\text{th column} &&& \\ &&& | &&& \end{array} \\ \begin{pmatrix} 1 &&&&&& \\ & \ddots &&&&& \\ && 1 &&&& \\ &&& a &&& \\ &&&& 1 && \\ &&&&& \ddots & \\ &&&&&& 1 \end{pmatrix} \end{array}, \qquad A_{i,j} = \begin{array}{cc} \begin{array}{cccccc} &&&& j\text{th column} & \\ &&&& | & \end{array} & \\ \begin{pmatrix} 1 &&&&& \\ & \ddots &&&& \\ && 1 && 1 & \\ &&& \ddots && \\ &&&& \ddots & \\ &&&&& 1 \end{pmatrix} & \begin{array}{l} \\ \\ \text{— } i\text{th row} \\ \\ \\ \\ \end{array} \end{array},$$

$$\text{and} \quad F_{i,j} = \begin{array}{cc} \begin{array}{ccccccccccc} &&& i\text{th col.} &&&& j\text{th col.} &&& \\ &&& | &&&& | &&& \end{array} & \\ \begin{pmatrix} 1 &&&&&&&&&& \\ & \ddots &&&&&&&&& \\ && 1 &&&&&&&& \\ &&& 0 &&&& 1 &&& \\ &&&& 1 &&&&&& \\ &&&&& \ddots &&&&& \\ &&&&&& 1 &&&& \\ &&& 1 &&&& 0 &&& \\ &&&&&&&& 1 && \\ &&&&&&&&& \ddots & \\ &&&&&&&&&& 1 \end{pmatrix} & \begin{array}{l} \\ \\ \\ \text{— } i\text{th row} \\ \\ \\ \\ \text{— } j\text{th row} \\ \\ \\ \\ \end{array} \end{array}$$

for indices $0 \leq i, j < n$ and a non-zero field element $a \in \mathbb{F}_p^\times$.

On that account, every affine linear transformation $T_{A,B}$, as introduced in Definition 5.1.8 (for a *symmetric* matrix B), is a concatenation of transformations of the following "elementary" types, for indices $0 \leq i, j < n$ and field elements $a \in \mathbb{F}_p^\times$ ($K \in M_n(\mathbb{F}_p)$).

$$T_{\mathrm{I}_n, B_{i,j}} : K \longmapsto K + B_{i,j} \qquad\qquad T_{A_{i,j},0} : K \longmapsto A_{i,j} K A_{i,j}^T$$
$$T_{M_{i,a},0} : K \longmapsto M_{i,a} K M_{i,a} \qquad\qquad T_{F_{i,j},0} : K \longmapsto F_{i,j} K F_{i,j}$$

(i). We fix indices $0 \leq i_0, j_0 < n$ and a non-zero field element $a \in \mathbb{F}_p^\times$, and explicitly define *-automorphisms of the generalised Clifford algebra $\mathbb{C}l_{2n}^p$ of "elementary type", satisfying the conditions of item (i). The general statement then immediately follows by concatenation of the obtained elementary *-automorphisms. Concretely, we have to establish the following *-automorphisms of the generalised Clifford algebra $\mathbb{C}l_{2n}^p$.

$$T_{\mathrm{I}_n, B_{i_0,j_0}} \rightsquigarrow \phi_0 = \phi_{1, B_{i_0,j_0}} \qquad\qquad T_{A_{i_0,j_0},0} \rightsquigarrow \phi_2 = \phi_{A_{i_0,j_0},0}$$
$$T_{M_{i_0,a},0} \rightsquigarrow \phi_1 = \phi_{M_{i_0,a},0} \qquad\qquad T_{F_{i_0,j_0},0} \rightsquigarrow \phi_3 = \phi_{F_{i_0,j_0},0}$$

Construction of ϕ_0. On the generators $b_0, \dots, b_{n-1}, c_0, \dots, c_{n-1} \in \mathbb{C}l^p_{2n}$, we set

$$\begin{aligned} \phi_0(b_i) &= b_i \text{ for all } 0 \le i < n, \qquad & \phi_0(c_i) &= c_i \qquad \text{for all } 0 \le i < n,\ i \notin \{i_0, j_0\}, \\ & & \phi_0(c_{i_0}) &= b_{j_0} c_{i_0}, \\ & & \phi_0(c_{j_0}) &= b_{i_0} c_{j_0}. \end{aligned}$$

It is obvious that the unitary images $\phi(b_0), \dots, \phi(b_{n-1})$, $\phi(c_0), \dots, \phi(c_{n-1})$ generate $\mathbb{C}l^p_{2n}$, and you readily verify that they satisfy the relations of the generators b_i and c_i (cf. Definition/Proposition 4.4.9), thus ϕ_0 is a *-automorphism. What is more, ϕ_0 maps the masa $\mathcal{N}$ to itself by definition. (Observe that we do not need to consider the cases $i_0 = j_0$, $i_0 \ne j_0$ separately.)

Let $K = (k_{i,j})$ denote a symmetric matrix in $M_n(\mathbb{F}_p)$, further set $K_0 = K + B_{i_0,j_0}$. The generators of the masa $\mathcal{M}_K$ are given by

$$\begin{aligned} g_0(k_{0,0}, \dots, k_{0,n-1}) &= b_0^{k_{0,0}} \cdots b_{n-1}^{k_{0,n-1}}\, c_0, \\ &\vdots \\ g_{n-1}(k_{n-1,0}, \dots, k_{n-1,n-1}) &= b_0^{k_{n-1,0}} \cdots b_{n-1}^{k_{n-1,n-1}}\, c_{n-1} \end{aligned}$$

according to Construction 5.1.5. Only two of these generators are *not* invariant under the action of ϕ_0—namely, we have

$$\begin{aligned} \phi_0\left(g_{i_0}(k_{i_0,0}, \dots, k_{i_0,n-1})\right) &= \phi_0\left(b_0^{k_{i_0,0}} \cdots b_{n-1}^{k_{i_0,n-1}}\, c_{i_0}\right) \\ &= b_0^{k_{i_0,0}} \cdots b_{n-1}^{k_{i_0,n-1}}\, b_{j_0} c_{i_0} \\ &= b_0^{k_{i_0,0}} \cdots b_{j_0-1}^{k_{i_0,j_0-1}}\, b_{j_0}^{\boldsymbol{k_{i_0,j_0}+1}}\, b_{j_0+1}^{k_{i_0,j_0+1}} \cdots b_{n-1}^{k_{i_0,n-1}}\, c_{i_0} \\ &= g_{i_0}(k_{i_0,0}, \dots, k_{i_0,j_0-1}, \boldsymbol{k_{i_0,j_0}+1}, k_{i_0,j_0+1}, \dots k_{i_0,n-1}) \\ \text{and} \quad \phi_0\left(g_{j_0}(k_{j_0,0}, \dots, k_{j_0,n-1})\right) &= g_{j_0}(k_{j_0,0}, \dots, k_{j_0,i_0-1}, \boldsymbol{k_{j_0,i_0}+1}, k_{j_0,i_0+1}, \dots k_{j_0,n-1}). \end{aligned}$$

Comparing the exponents of these generators immediately yields the identity

$$\phi_0\left(\mathcal{M}_K\right) = \mathcal{M}_{K_0}.$$

Construction of ϕ_1. We declare ϕ_1 on the generators by

$$\begin{aligned} \phi_1(b_i) &= b_i, \qquad & \phi_1(c_i) &= c_i \qquad \text{for all } 0 \le i < n,\ i \ne i_0, \\ \phi_1(b_{i_0}) &= b_{i_0}^a, & \phi_1(c_{i_0}) &= c_{i_0}^{(a^{-1})}. \end{aligned}$$

As in the previous step, you convince yourself that the images $\phi_1(c_i)$, $\phi_1(b_i)$ obey the relations of the generators b_i and c_i and generate the generalised Clifford algebra $\mathbb{C}l^p_{2n}$, so that the assignment above induces a well-defined *-automorphism ϕ_1 of $\mathbb{C}l_{2n}^p$. What is more, the masa $\mathcal{N}$ is clearly invariant under ϕ_1.

For a matrix $K = (k_{i,j}) \in M_n(\mathbb{F}_p)$, one computes

$$T_{M_{i_o,a},0}(K) = M_{i_0,a} K M_{i_0,a} = \begin{pmatrix} & & & ak_{0,i_o} & & & \\ & & & \vdots & & & \\ & & & ak_{i_o-1,i_o} & & & \\ ak_{i_o,0} & \cdots & ak_{i_o,i_o-1} & a^2 k_{i_o,i_o} & ak_{i_o,i_o+1} & \cdots & ak_{i_o,n-1} \\ & & & ak_{i_o+1,i_o} & & & \\ & & & \vdots & & & \\ & & & ak_{n-1,i_o} & & & \end{pmatrix} =: K_1,$$

where all entries of the matrix K_1 that are not shown coincide with the respective entries of K.

The action of ϕ_1 on the generators of the masa $\mathcal{M}_K \subset \mathbb{C}l_{2n}^p$ is given by

$$\phi_1 \left(g_i(k_{i,0}, \ldots, k_{i,n-1}) \right) = g_i(k_{i,0}, \ldots, k_{i,i_0-1}, ak_{i,i_0}, k_{i,i_0+1}, \ldots, k_{i,n-1}) \quad \text{for } i \neq i_0$$

and

$$\begin{aligned} \phi_1 \left(g_{i_0}(k_{i_0,0}, \ldots, k_{i_0,n-1}) \right) &= b_0^{k_{i_0,0}} \cdots b_{i_0-1}^{k_{i_0,i_0-1}} \, b_{i_0}^{ak_{i_0,i_0}} \, b_{i_0+1}^{k_{i_0,i_0+1}} \cdots b_{n-1}^{k_{i_0,n-1}} \, c_{i_0}^{(a^{-1})} \\ &\sim_{\mathbb{T}} g_{i_0}(ak_{i_0,0}, \ldots, ak_{i_0,i_0-1}, a^2 k_{i_0,i_0}, ak_{i_0,i_0+1}, \ldots, ak_{i_0,n-1})^{(\boldsymbol{a^{-1}})}. \end{aligned}$$

Replacing the generator $\phi_1(g_{i_0}(\ldots))$ by its ath power in the masa $\phi_1(\mathcal{M}_K)$, and comparing the exponents of the factors b_i afterwards, we end up with the identity

$$\phi_1 \left(\mathcal{M}_K \right) = \mathcal{M}_{K_1}.$$

Construction of ϕ_2. Given a matrix $K = (k_{i,j}) \in M_n(\mathbb{F}_p)$, one readily computes that $T_{A_{i_o,j_o},0}(K)$ equals the matrix

$$K_2 = \begin{array}{cc} \begin{array}{c} i_0\text{th column} \\ | \end{array} & \\ \begin{pmatrix} & & & k_{0,i_o}+k_{0,j_o} & & & \\ & & & \vdots & & & \\ & & & k_{i_o-1,i_o} k_{i_o-1,j_o} & & & \\ k_{i_o,0}+k_{j_o,0} & \cdots & k_{i_o,i_o-1}+k_{j_o,i_o-1} & x & k_{i_o,i_o+1}+k_{j_o,i_o+1} & \cdots & k_{i_o,n-1}+k_{j_o,n-1} \\ & & & k_{i_o+1,i_o}+k_{i_o+1,j_o} & & & \\ & & & \vdots & & & \\ & & & k_{n-1,i_o}+k_{n-1,j_o} & & & \end{pmatrix} & \text{— } i_0\text{th row} \end{array} ,$$

where we set $x = k_{i_0,i_0} + k_{i_0,j_0} + k_{j_0,i_0} + k_{j_0,j_0}$, and all entries not shown coincide with those of the matrix K as before.

Similar as above, you check that the images of the map ϕ_2, defined below, obey the relations of the elements b_i and c_i and generate $\mathbb{C}l_{2n}^p$, so that ϕ_2 is a well-defined *-automorphism.

$$\begin{aligned} &\phi_2(b_i) = b_i \quad \text{for all } 0 \leq i < n,\ i \neq j_0 && \phi_2(c_i) = c_i \quad \text{for all } 0 \leq i < n,\ i \neq i_0, \\ &\phi_2(b_{j_0}) = b_{i_0} b_{j_0}, && \phi_2(c_{i_0}) = c_{i_0} c_{j_0}^* \end{aligned}$$

The action of ϕ_2 on the generators of the masa $\mathcal{M}_K$ computes to

$$\phi_2\left(g_i(k_{i,0},\ldots,k_{i,n-1})\right) = \begin{cases} b_0^{k_{i,0}} \cdots b_{i_0-1}^{k_{i,i_0-1}}\ b_{i_0}^{\boldsymbol{k_{i,i_0}+k_{i,j_0}}}\ b_{i_0+1}^{k_{i,i_0+1}} \cdots b_{n-1}^{k_{i,n-1}}\ c_i & \text{if } i \neq i_0, \\ b_0^{k_{i_0,0}} \cdots b_{i_0-1}^{k_{i_0,i_0-1}}\ b_{i_0}^{k_{i_0,i_0}+k_{i_0,j_0}}\ b_{i_0+1}^{k_{i_0,i_0+1}} \cdots b_{n-1}^{k_{i_0,n-1}}\ c_{i_0}\boldsymbol{c_{j_0}^*} & \text{if } i = i_0. \end{cases}$$

The image $\phi_2(g_{i_0}(\ldots))$ is, as you notice, not one of the standard generators for the masas of the form $\mathcal{M}_K$ we consider here. To obtain the "missing" generator for the masa $\phi_2(\mathcal{M}_K)$, we take the product $\phi_2(g_{i_0}(\ldots)) \cdot \phi_2(g_{j_0}(\ldots))$:

$$\begin{aligned} &\phi_2\left(g_{i_0}(k_{i_0,0},\ldots,k_{i_0,n-1})\right) \cdot \phi_2\left(g_{j_0}(k_{j_0,0},\ldots,k_{j_0,n-1})\right) \\ &\quad \sim_{\mathbb{T}} g_{i_0}\left(k_{i_0,0}+k_{j_0,0},\ldots,k_{i_0,i_0-1}+k_{j_0,i_0-1},x,k_{i_0,i_0+1}+k_{j_0,i_0+1},\ldots,k_{i_0,n-1}+k_{j_0,n-1}\right) \end{aligned}$$

Now a look at the indices of the matrix K_2 reveals the equality

$$\phi_2\left(\mathcal{M}_K\right) = \mathcal{M}_{K_2}.$$

Construction of ϕ_3. As in the preceding steps, one checks that the following assignment defines a *-automorphism ϕ_3 of $\mathbb{C}l_{2n}^p$.

$$\begin{aligned} \phi_3(b_i) &= b_i, & \phi_3(c_i) &= c_i \quad \text{for all } 0 \leq i < n,\ i \notin \{i_0, j_0\}, \\ \phi_3(b_{i_0}) &= b_{j_0}, & \phi_3(c_{i_0}) &= c_{j_0}, \\ \phi_3(b_{j_0}) &= b_{i_0}, & \phi_3(c_{j_0}) &= c_{i_0} \end{aligned}$$

The masa $\mathcal{N}$ is clearly invariant under the action of ϕ_3, and setting $K_3 = F_{i_0,j_0} K F_{i_0,j_0}$ for a symmetric matrix $K \in M_n(\mathbb{F}_p)$, a straightforward calculation reveals the equality

$$\phi_3\left(\mathcal{M}_K\right) = \mathcal{M}_{K_3}.$$

(ii). We declare the "crossing automorphism" χ of the generalised Clifford algebra $\mathbb{C}l_{2n}^p$ on the generators by

$$\chi(b_i) = c_i \quad \text{and} \quad \chi(c_i) = b_i^*$$

for all indices $0 \leq i < n$. Well-definedness of the *-automorphism χ is quickly checked, moreover it clearly maps the masa $\mathcal{N}$ to $\mathcal{M}_0 = \mathcal{A}^*(c_0,\ldots,c_{n-1})$ and vice versa. Given an invertible matrix $K = (k_{i,j}) \in M_n(\mathbb{F}_p)$, the standard generators of the associated masa $\mathcal{M}_K$ are mapped as follows for all $0 \leq i < n$.

$$\chi\left(g_i(k_{i,0}, \dots, k_{i,n-1})\right) = c_0^{k_{i,0}} \cdots c_{n-1}^{k_{i,n-1}} b_i^*$$

Let $L = (l_{i,j}) \in M_n(\mathbb{F}_p)$ denote the inverse matrix to K. Then one computes, for each fixed index $0 \leq j_0 < n$, that the masa $\chi(\mathcal{M}_K)$ contains the product

$$\begin{aligned} \prod_{i=0}^{n-1} \chi\left(g_i(k_{i,0}, \dots, k_{i,n-1})\right)^{l_{i,jo}} &\sim_{\mathbb{T}} c_0^{\sum_{i=0}^{n-1} k_{i,0} l_{i,jo}} \cdots c_{n-1}^{\sum_{i=0}^{n-1} k_{i,n-1} l_{i,jo}} b_0^{-l_{0,jo}} \cdots b_{n-1}^{-l_{n-1,jo}} \\ &\sim_{\mathbb{T}} b_0^{-l_{0,jo}} \cdots b_{n-1}^{-l_{n-1,jo}} c_{j_0}, \end{aligned}$$

where the second step is deduced from the matrix identity $KL = \mathrm{I}_n$. Consequently, the image $\chi(\mathcal{M}_K)$ coincides with the masa $\mathcal{M}_{-K^{-1}}$. Our proof is complete. □

Lemma 5.1.10. *Let $\mathcal{S} = \{K_0, \dots, K_{m-1}\}$ and $\mathcal{T} = \{L_0, \dots, L_{m-1}\}$ be two smid families of equal length in $M_n(\mathbb{F}_p)$ ($0 \leq m \leq d$). If the associated nice masa families*

$$\mathscr{F}(\mathcal{S}) = \left\{\mathcal{N}, \mathcal{M}_{K_0}, \dots, \mathcal{M}_{K_{m-1}}\right\} \quad \textit{and} \quad \mathscr{F}(\mathcal{T}) = \left\{\mathcal{N}, \mathcal{M}_{L_0}, \dots, \mathcal{M}_{L_{m-1}}\right\}$$

in the generalised Clifford algebra $\mathbb{C}l_{2n}^p$ are equivalent (in the sense of Definition 3.2.1), then so are the smid families $\mathcal{S}$ and $\mathcal{T}$ (according to Definition 5.1.8).

Proof. The smid families $\mathcal{S}$ and $\mathcal{T}$ are both empty if m is zero, and of length one if m equals one. In both cases, they are trivially equivalent, so that we assume $m \geq 2$ in the sequel.

By definition, the masa families $\mathscr{F}(\mathcal{S})$ and $\mathscr{F}(\mathcal{T})$ are equivalent if and only if there is a *-automorphism ψ of $\mathbb{C}l_{2n}^p$ mapping each masa of the former family to a member of the latter. (We generalise the respective Definition 3.2.1, genuinely formulated for matrix algebras, to the generalised Clifford algebra in the obvious way.)

We have to consider two distinct cases.

(i) The *-automorphism ψ maps the masa $\mathcal{N}$ to itself.

(ii) The *-automorphism ψ maps the masa $\mathcal{N}$ to one of the masas $\mathcal{M}_{L_k}$ ($0 \leq k < m$).

(It will turn out that these cases correspond to the respective items of Definition 5.1.8.)

We can apply Lemma 5.1.9 to facilitate the situation. First of all, we can assume w.l.o.g. that both smid families $\mathcal{S}$ and $\mathcal{T}$ contain the zero matrix. In case (i), we can moreover assume w.l.o.g. that ψ sends $\mathcal{M}_0$ to $\mathcal{M}_0$. (Suppose ψ initially maps $\mathcal{M}_{K_0}$

to $\mathcal{M}_{L_k}$ for some index $0 \leq k < m$. Then we can replace the masa family $\mathcal{S}$ by the equivalent family $\mathcal{S}' = \mathcal{S} - K_0$, and likewise replace $\mathcal{T}$ by $\mathcal{T}' = \mathcal{T} - L_k$.) Similarly, we can presume that ψ maps $\mathcal{N}$ to $\mathcal{M}_0$ and and vice versa in case (ii). After possibly renumerating the matrices in the smid families $\mathcal{S}$ and $\mathcal{T}$, we are thus (w.l.o.g.) faced with one of the situations depicted in the following diagrams, where we rename the *-automorphism ψ to distinguish the two cases.

$$\begin{tikzcd}
\mathcal{N}, \arrow[d] & \mathcal{M}_0, \arrow[d] & \mathcal{M}_{K_1}, \arrow[d] & \ldots, \arrow[d, phantom, "\psi_0"] & \mathcal{M}_{K_{m-1}} \arrow[d] \\
\mathcal{N}, & \mathcal{M}_0, & \mathcal{M}_{L_1}, & \ldots, & \mathcal{M}_{L_{m-1}}
\end{tikzcd}$$

Case (i)

$$\begin{tikzcd}
\mathcal{N}, \arrow[dr] & \mathcal{M}_0, \arrow[dl] & \mathcal{M}_{K_1}, \arrow[d] & \ldots, \arrow[d, phantom, "\psi_1"] & \mathcal{M}_{K_{m-1}} \arrow[d] \\
\mathcal{N}, & \mathcal{M}_0, & \mathcal{M}_{L_1}, & \ldots, & \mathcal{M}_{L_{m-1}}
\end{tikzcd}$$

Case (ii)

We set $d = p^n$ as usual. At one step of our proof, it will be useful to identify the generalised Clifford algebra $\mathbb{C}l_{2n}^p$ and the matrix algebra $M_d(\mathbb{C})$, using the *-representation ρ introduced in the proof of Theorem 4.4.6 (page 148f.). Recall that we have the following identities for all indices $0 \leq i < n$.

$$\rho(b_i) = \mathrm{B}_i = \quad \mathrm{I}_p \otimes \cdots \otimes \mathrm{I}_p \otimes \overset{(i\text{th pos.})}{\mathrm{Z}_p} \otimes \mathrm{I}_p \otimes \cdots \otimes \mathrm{I}_p$$

$$\rho(c_i) = \mathrm{C}_i = \begin{cases} \mathrm{i}\,\mathrm{I}_p \otimes \cdots \otimes \mathrm{I}_p \otimes \sigma_x\sigma_z \otimes \mathrm{I}_p \otimes \cdots \otimes \mathrm{I}_p & \text{if } p = 2, \\ \mathrm{I}_p \otimes \cdots \otimes \mathrm{I}_p \otimes \mathrm{X}_p\mathrm{Z}_p^* \otimes \mathrm{I}_p \otimes \cdots \otimes \mathrm{I}_p & \text{else} \end{cases}$$

According to Construction 5.1.5, we further have the identities

$$\mathcal{N} = \mathcal{A}^*\left(b_0, \ldots, b_{n-1}\right) \quad \text{and} \quad \mathcal{M}_0 = \mathcal{A}^*\left(c_0, \ldots, c_{n-1}\right),$$

and so these masas correspond to the masas

$$\begin{aligned} \rho(\mathcal{N}) &= \mathcal{A}^*\left(\mathrm{Z}_p \otimes \mathrm{I}_p \otimes \cdots \otimes \mathrm{I}_p, \ldots, \mathrm{I}_p \otimes \cdots \otimes \mathrm{I}_p \otimes \mathrm{Z}_p\right) \\ &= \mathcal{D}_d \\ \text{and} \quad \rho(\mathcal{M}_0) &= \mathcal{A}^*\left(\mathrm{X}_p\mathrm{Z}_p^* \otimes \mathrm{I}_p \otimes \cdots \otimes \mathrm{I}_p, \ldots, \mathrm{I}_p \otimes \cdots \otimes \mathrm{I}_p \otimes \mathrm{X}_p\mathrm{Z}_p^*\right) \end{aligned}$$

in the matrix picture.

Case (i). On the matrix level, ψ_0 induces a *-automorphism $\tilde{\psi}_0 = \rho \circ \psi_0 \circ \rho^{-1}$ of $M_d(\mathbb{C})$. The identity $\tilde{\psi}_0(\mathcal{D}_d) = \mathcal{D}_d$ ensures that $\tilde{\psi}_0$ corresponds to a conjugation by a *monomial* unitary matrix in $M_d(\mathbb{C})$ (cf. Lemma 1.2.5). The masa $\rho(\mathcal{M}_0)$ is invariant under $\tilde{\psi}_0$ and generated by monomials, and so $\tilde{\psi}_0$ sends each of its monomial generators to a monomial element of $\rho(\mathcal{M}_0)$.

Here comes the reason why we have switched to the matrix picture: as we have discussed at length in the proof of Theorem 4.2.4 (implication $(iia) \Rightarrow (via)$ on page

128), the only monomials inside $\rho(\mathcal{M}_0)$ are products of the form

$$(\mathrm{X}_p\mathrm{Z}_p^*)^{s_0} \otimes \cdots \otimes (\mathrm{X}_p\mathrm{Z}_p^*)^{s_{n-1}},$$

where we as usually consider the exponents $s_0, \dots, s_{n-1}$ as elements of the prime field $\mathbb{F}_p$. There is thus a matrix $A = (a_{i,j}) \in M_n(\mathbb{F}_p)$ such that $\tilde{\psi}_0$ maps the generators of $\rho(\mathcal{M}_0)$ according to the rule

$$\tilde{\psi}_0(\mathrm{I}_p \otimes \cdots \otimes \mathrm{I}_p \otimes \underset{\substack{|\\ (i\text{th pos.})}}{\mathrm{X}_p\mathrm{Z}_p^*} \otimes \mathrm{I}_p \otimes \cdots \otimes \mathrm{I}_p) = (\mathrm{X}_p\mathrm{Z}_p^*)^{a_{i,0}} \otimes \cdots \otimes (\mathrm{X}_p\mathrm{Z}_p^*)^{a_{i,n-1}} \quad (0 \leq i < n).$$

On the level of the generalised Clifford algebra $\mathbb{C}l_{2n}^p$, this results in

$$\psi_0(b_i) = b_0^{a_{i,0}} \cdots b_0^{a_{i,n-1}} \text{ for all } 0 \leq i < n.$$

This information, combined with the identity $\psi_0(\mathcal{M}_0) = \mathcal{M}_0$, completely determines the *-automorphism ψ_0, as we shall see further below.

The matrix A must be regular, because if its rows were linearly dependent, then one of the images specified above would be a product of powers of the others (up to a phase factor), which would immediately contradict the fact that $\tilde{\psi}$ is a *-automorphism. As a consequence, $A \in M_n(\mathbb{F}_p)$ is a product of elementary regular matrices of type $M_{i,a}$, $A_{i,j}$, and $F_{i,j}$, defined as in the proof of Lemma 5.1.9. It therefore suffices to show that ψ_0 induces the equivalence of the smid families $\mathcal{S}$ and $\mathcal{T}$ in the special cases that A is one of these elementary matrices. The general assertion then follows by concatenation of the respective "elementary" linear transformations on the side of the smid families.

First suppose that A equals the diagonal matrix $M_{i_0,a}$ for an index $0 \leq i_0 < n$ and a non-zero field element $a \in \mathbb{F}_p^\times$, so that the images of the generators $b_0, \dots, b_{n-1}$ under the action of ψ_0 are given by

$$\psi_0(b_i) = \begin{cases} b_i^a & \text{if } i = i_0, \\ b_i & \text{else.} \end{cases}$$

As the commutation relations for the generators b_i and c_i of $\mathbb{C}l_{2n}^p$ (see Definition/Proposition 4.4.9) carry over to their images under the *-homomorphism ψ_0, and since moreover ψ_0 maps $\mathcal{M}_0 = \mathcal{A}^*(c_0, \dots, c_{n-1})$ to itself, it is an easy exercise to verify that the generators $c_0, \dots, c_{n-1}$ are mapped by ψ_0 as follows.

$$\psi_0(c_i) = \begin{cases} c_i^{a^{-1}} & \text{if } i = i_0 \\ c_i & \text{else} \end{cases}$$

A comparison yields that ψ_0 coincides with the *-automorphism ϕ_1 defined in the proof of Lemma 5.1.9, whence we deduce the identity

$$\psi_0(\mathcal{M}_K) = \mathcal{M}_{M_{i_0,a}KM_{i_0,a}}$$

for all symmetric matrices $K \in M_n(\mathbb{F}_p)$. By definition of ψ_0 (see the diagram for case (i) above), we thus obtain the equalities

$$\mathcal{M}_{L_i} = \mathcal{M}_{M_{i_o,a}K_i\, M_{i_o,a}}$$

for all $0 \leq i < m$.

It is immediate that two masas $\mathcal{M}_K, \mathcal{M}_L \subset \mathbb{C}l_{2n}^p$ coincide exactly if the same holds true for the symmetric matrices $K, L \in M_n(\mathbb{F}_p)$, and so the equations above yield the matrix identities $L_i = M_{i_0,a}K_i\, M_{i_0,a}$ for all $0 \leq i < m$. Accordingly, we end up with $\mathcal{T} = M_{i_o,a}\mathcal{S}\, M_{i_o,a}$, that is with the equivalence of the masa families $\mathcal{S}$ and $\mathcal{T}$.

Completely analogue arguments allow to tackle the cases $A = A_{i_0,j_0}$ and $A = F_{i_0,j_0}$ for indices $0 \leq i_0, j_0 < n$. In the former case, one easily computes that ψ_0 equals the *-automorphism ϕ_2 defined in the proof of Lemma 5.1.9, which finally leads to $\mathcal{T} = A_{i_0,j_0}\mathcal{S}\, A_{i_0,j_0}$. In the latter case, ψ_0 coincides with the *-automorphism ϕ_3, which asserts the identity $\mathcal{T} = F_{i_0,j_0}\mathcal{S}\, F_{i_0,j_0}$. The details are left to the reader.

Case (ii). Concatenating the *-automorphism ψ_1 and the crossing automorphism χ of $\mathbb{C}l_{2n}^p$ defined in the proof of Lemma 5.1.9 (part (ii)), we obtain a *-automorphism $\psi_2 = \chi \circ \psi_1$ as depicted in the following diagram.

$$\begin{tikzcd}
\mathcal{N}, \arrow[dr] & \mathcal{M}_0, \arrow[dl] & \mathcal{M}_{K_1}, \arrow[d] & \ldots, \arrow[d, phantom, "\psi_1"] & \mathcal{M}_{K_{m-1}} \arrow[d] \arrow[dd, bend left, "\psi_2"] \\
\mathcal{N}, \arrow[dr] & \mathcal{M}_0, \arrow[dl] & \mathcal{M}_{L_1}, \arrow[d] & \ldots, \arrow[d, phantom, "\chi"] & \mathcal{M}_{L_{m-1}} \arrow[d] \\
\mathcal{N}, & \mathcal{M}_0, & \mathcal{M}_{-L_1^{-1}}, & \ldots, & \mathcal{M}_{-L_{m-1}^{-1}}
\end{tikzcd}$$

Since the *-automorphism ψ_2 preserves the masas $\mathcal{N}$ and $\mathcal{M}_0$, we can apply the same arguments as in case (i) to see that we have the identities $\mathcal{M}_{-L_i^{-1}} = \mathcal{M}_{AK_i\, A}$ for a regular matrix A—which depends on the *-automorphism ψ_1—and all $1 \leq i < m$. This implies the equalities

$$-L_i^{-1} = X(L_i) = AK_i\, A = T_{A,0}(K_i),$$

and thereby, since the transformation X is obviously self-inverse, the identity

$$\mathcal{T} = X \circ T_{A,0}(\mathcal{S}),$$

that is the equivalence of $\mathcal{S}$ and $\mathcal{T}$. (Recall that we have presumed that both of the smid families $\mathcal{S}$ and $\mathcal{T}$ contain the zero matrix. Leaving aside this restriction, we clearly end up with a more general equality of the form $\mathcal{T} = T_{A',B'} \circ X \circ T_{A,B}(\mathcal{S})$, where one may set $A' = \mathrm{I}_d$ w.l.o.g.) □

The following theorem is a direct consequence of the preceding lemmas, and completes our main goal to fully classify complete sets of nice masas by complete smid families.

Theorem 5.1.11. *Let $\mathcal{S}, \mathcal{T}$ be two smid families in $M_n(\mathbb{F}_p)$. The associated nice sets of quasi-orthogonal masas $\mathscr{F}(\mathcal{S})$ and $\mathscr{F}(\mathcal{T})$ in $\mathbb{C}l^p_{2n}$ are equivalent if and only if the smid families $\mathcal{S}$ and $\mathcal{T}$ are equivalent in the sense of Definition 5.1.1.*

The unique encoding of complete nice masa families

Let $p \in \mathbb{P}$ denote a prime and $n \in \mathbb{N}$ a natural number, and set $d = p^n$. Further let $\mathscr{F}$ be a nice masa family with index group $\bigoplus_{2n} \mathbb{Z}/p$ inside the matrix algebra $M_d(\mathbb{C})$. Then according to Theorem 4.4.11, there is a unitary $u \in \mathcal{U}_d$ such that the family $u\mathscr{F}u^*$ stems from a quasi-partition of the nice unitary error basis

$$\mathfrak{E}^p_{2n} = \left\{ \mathrm{B}_0^{i_0} \cdots \mathrm{B}_{n-1}^{i_{n-1}} \mathrm{C}_0^{i_n} \cdots \mathrm{C}_{n-1}^{i_{2n-1}} \;\middle|\; i_0, \ldots, i_{2n-1} \in \mathbb{F}_p \right\}$$

introduced in Definition/Proposition 3.3.8.

In a next step, Theorem 5.1.6 tells us that the smid family $u\mathscr{F}u^*$—that is, the respective quasi-partition of the basis $\mathfrak{E}^p_{2n}$—is encoded by a smid family in $M_n(\mathbb{F}_p)$.

Finally two nice masa families in $M_d(\mathbb{C})$ with index group $\bigoplus_{2n} \mathbb{Z}/p$ are equivalent if and only if the smid families assigned to them (according to Theorem 5.1.6) are equivalent, as we have seen in Theorem 5.1.11 just before.

The following Main Theorem recapitulates our results concerning the classification of nice masa families in $M_{p^n}(\mathbb{C})$, focussing on *complete* families for clarity. (As in the preceding summary, the statements apply analogously for general nice masa families in $M_{p^n}(\mathbb{C})$ with index group $\bigoplus_{2n} \mathbb{Z}/p$.)

Main Theorem. *Fix a natural number $n \in \mathbb{N}$ and a prime $p \in \mathbb{P}$.*

(I) Up to unitary equivalence, all complete nice masa families in $M_{p^n}(\mathbb{C})$ stem from quasi-partitions of the nice monomial error basis $\mathfrak{E}^p_{2n}$. (Theorem 4.4.11)

(II) Every quasi-partition of the error basis $\mathfrak{E}^p_{2n}$ that induces a nice complete masa family is encoded by a complete smid family. (Theorem 5.1.6)

(III) Two quasi-partitions like in item (II) yield equivalent masa families if and only if the corresponding smid families are equivalent. (Theorem 5.1.11)

There is hence a one-to-one correspondence between equivalence classes of complete nice masa families in $M_{p^n}(\mathbb{C})$ and equivalence classes of complete smid families in $M_n(\mathbb{F}_p)$.

Admittedly, it had escaped the author's notice for a long time that the result above is in fact *not new.* It had been stated earlier—albeit in quite different terms—in a very remarkable paper by Calderbank et al. ([23]), concerning error correcting codes, discrete geometry, and representations of certain finite groups. (We have mentioned this article before, see item (1995) on page 99 and Fact 4.3.7.) The Main Theorem above, and the steps leading towards it, may therefore be seen as an alternative approach to obtain the result of Calderbank et al., based on more or less elementary techniques of finite-dimensional (linear) algebra. We collect the essential

Facts 5.1.12. In the paper [23], Calderbank et al. investigate, among many other issues, special *orthogonal frames*—for our purposes, one may as well think of orthonormal bases of the Hilbert space $\mathbb{C}^{p^n}$—which correspond to MUBs (lemma 5.5 if p equals two, lemma 11.3 else). They gain sets of orthogonal frames corresponding to *complete* sets of MUBs from so-called *symplectic spreads* (combine lemma 5.5 and theorem 5.6 if p is two, otherwise lemma 11.3 and theorem 11.4; see the beginning of the fifth chapter for the definition of a symplectic spread).

Going through the details, one finds that the sets of MUBs obtained by the technique of Calderbank et al. are *nice* (to see this, keep an eye on the operators X and Y defined in chapter 2 for the odd case, and at the beginning of chapter 11 for the even case).

Furthermore, Calderbank et al. prove that the obtained complete sets of nice MUBs (i.e. the corresponding orthogonal frames) are equivalent (in the same sense as defined in the present work) if and only if the underlying symplectic spreads fulfil a certain equivalence condition (proposition 5.11 if p is two, corollary 11.6 else).

The application of the results by Calderbank et al. to the subject of MUBs is due to Godsil and Roy, who also collected the facts mentioned above in [40, chapter 6].

One missing piece must be added to these facts, namely that the explained correspondence between (equivalence classes) of symplectic spreads and nice complete sets of MUBs is *one-to-one,* i.e. one conversely receives a symplectic spread from every nice complete set of MUBs. This is not hard to see, once one has worked oneself through the many technical details in reference [23].

As a consequence, the mentioned equivalence of symplectic spreads must be compatible with our equivalence relation for smid families, and the result of Calderbank et al., adopted by Godsil and Roy, is equivalent to our Main Theorem above.

Finally, let us remark that Calderbank et al. even literally mention smid families—though of course not under this very name—as a special (symmetric) case of so-called *spread sets,* see [23, equation (5.1)].

Inequivalent smid families

Speaking of smid families of arbitrary length, the existence of inequivalent families is apparently not a rare phenomenon. For instance, take the first and the last family presented in Examples 5.1.3. Since the former is not maximal by contrast to the latter, these families in $M_2(\mathbb{F}_2)$ cannot be equivalent.

Already in the trivial matrix algebras $M_1(\mathbb{F}_p) \cong \mathbb{F}_p$, there are in general many instances of inequivalent incomplete smid families, as the examples further below shall demonstrate. Smid families in prime dimensions are just subsets of the field $\mathbb{F}_p$, and you readily convince yourself that according to Definition 5.1.8, the equivalence of smid families in $\mathbb{F}_p$ can be described as follows.

Proposition 5.1.13. *Two smid families $\{k_0, \ldots, k_{m-1}\}, \{l_0, \ldots, l_{m-1}\} \subset \mathbb{F}_p$ of the same length $1 \leq m \leq p$ are equivalent if there are elements $a \in \mathbb{F}_p^\times$, $b \in \mathbb{F}_p$, and a permutation $\sigma \in S_m$, such that one of the following statements applies.*

(i) The identity $l_{\sigma(i)} = a^2 k_i + b$ holds for all $0 \leq i < m$.

(ii) There is an index $0 \leq i_0 < m$ such that the element $l_{\sigma(i_0)}$ equals b and the identity $l_{\sigma(i)} = a^2(k_{i_0} - k_i)^{-1} + b$ holds for all $i \neq i_0$ $(0 \leq i < m)$.

Recall that a *quadratic residue* q in a prime field $\mathbb{F}_p$ is an element which is a square modulo p, that is there is an element $s \in \mathbb{F}_p$ subject to the equation $s^2 = q$ in $\mathbb{F}_p$. For all odd primes p, the field $\mathbb{F}_p$ contains exactly $(p+1)/2$ quadratic residues (including zero), which we shall sometimes refer to as *squares* in $\mathbb{F}_p$ for short.

Examples 5.1.14. (a) Let p be a prime number. In $M_1(\mathbb{F}_p) \cong \mathbb{F}_p$, consider the smid family $\mathscr{F}_0 = \{0, 1\}$. Following the lines of Proposition 5.1.13, you effortlessly check that a smid family $\{0, a\} \subset \mathbb{F}_p$ is equivalent to $\mathscr{F}_0$ if and only if a or $-a$ is a quadratic residue modulo p. Now assume that p is congruent $1 \bmod 4$. According to the first supplement of Gauss' famous *Law of Quadratic Reciprocity*, this is equivalent to -1 being a quadratic residue modulo p. As a consequence, each element $a \in \mathbb{F}_p$ is a square if and only if the same applies for $-a$. There are thus $m = (p-1)/2$ elements $b_0, \ldots, b_{m-1}$ in $\mathbb{F}_p$ being neither a square nor the negative of one. This asserts that none of the smid families $\{0, b_i\}$ is equivalent to $\mathscr{F}_0$.

(b) Applying the first example to the case $p = 13 \equiv 1 \bmod 4$, we see that the smid families $\{0, 1\}$ and $\{0, 5\}$ in $\mathbb{F}_{13}$ are inequivalent, since the set of quadratic residues in $\mathbb{F}_{13}$ equals $\mathcal{Q} = -\mathcal{Q} = \{0, 1, 3, 4, 9, 10, 12\}$. After switching from the smid family $\{0, 5\}$ to the equivalent family $\{2, 7\}$, one applies (the contraposition of) Lemma 5.1.10 to conclude that the nice masa families $\{\mathcal{D}_{13}, \mathcal{M}_0, \mathcal{M}_1\}$ and $\{\mathcal{D}_{13}, \mathcal{M}_2, \mathcal{M}_7\}$ in the matrix algebra $M_{13}(\mathbb{C})$, considered in Example 3.2.10 (*b*), are inequivalent.

(c) Reversing the arguments of example (a), it follows that if a prime p is congruent $3 \bmod 4$, then all smid families of length two inside the prime field $\mathbb{F}_p$ are equivalent.

Further above, we have stressed the fact that the equivalence relation for smid families does—maybe somewhat surprisingly—not involve scalar multiplication. Observe how this is crucial for the examples above.

As far as *complete* smid families are concerned, it turns out to be much harder to find inequivalent instances. As a matter of fact, the smallest matrix algebra $M_n(\mathbb{F}_p)$ (w.r.t. the prime power p^n) admitting inequivalent complete smid families is $M_3(\mathbb{F}_3)$.

In the aforementioned article [23], Calderbank et al. point out that there are, however, many dimensions which admit inequivalent orthogonal frames, of the type corresponding to complete sets of MUBs, in the Hilbert space $\mathbb{C}^{p^n}$. There are thus many matrix algebras $M_n(\mathbb{F}_p)$ admitting inequivalent complete smid families.

For the even case (see [23, corollary 10.9]), Calderbank et al. apply an earlier result by W. M. Kantor ([51]), concerning *inequivalent Preparata codes,* which are a special kind of error correcting codes. For the odd case (see [23, paragraph after corollary 11.6]), the authors explain that there are examples of *non-desarguesian symplectic spreads*, as was shown by L. Bader et al. ([6]) and, once again, by Kantor ([52]). These cannot be equivalent to the desarguesian symplectic spreads (which correspond to the more common *desarguesian planes*).

Calderbank et al. also remark that the smallest case where inequivalent orthogonal frames occur is $p = n = 3$. This follows from the fact that the so-called *Hering plane* of order 27 is, as Bader et al. show in [6], a non-regular symplectic spread, and can therefore not be equivalent to the existing regular symplectic spreads.

Translating the observations of Calderbank et al. into the picture of smid families, we can record the following

Facts 5.1.15 (Calderbank et al. 1997)**.** If $n \in \mathbb{N}$ is an odd composite number, then there are more than $2^{\sqrt{n}/2}$ pairwise inequivalent smid families in $M_n(\mathbb{F}_2)$. There are also *odd* primes $p \in \mathbb{P}$ and natural numbers $n \in \mathbb{N}$ such that $M_n(\mathbb{F}_p)$ contains inequivalent smid families.

Calderbank et al. state that "*[...] in spite of the small numbers known, there must be large numbers of inequivalent examples*" for the case when p is odd ([23, paragraph after corollary 11.6]). This was recently made more precise by Kantor, whose article [53] gives an exhaustive overview over results implying the existence of inequivalent nice sets of MUBs, also correcting some faults made in other papers on the subject.

In Section 5.4, we present the numbers of inequivalent smid families of any possible length for all prime power dimensions less than $p^n = 32$ that we have obtained by computer algebraic methods (Computer Algebraic Results 5.4.3 and 5.4.4). We also give an explicit matrix representation of the Hering plane in $M_3(\mathbb{F}_3)$ in the Computer Algebraic Result 5.4.1.

5.2 Complete linear smid families in the matrix algebras $\mathbf{M_2(\mathbb{F}_p)}$

Throughout this section, let p be a prime number. Be aware that most of the computations are performed inside the prime field $\mathbb{F}_p$, as will be clear from the context. In particular, we sometimes notate the multiplication with an inverse element as a fraction, i.e. we write s/t for $s \cdot t^{-1}$ for field elements $s \in \mathbb{F}_p$, $t \in \mathbb{F}_p^\times$.

As a technical preparation, we need the following assertion concerning certain subsets of $\mathbb{F}_p$, which will occur at several points in the sequel.

Technical Lemma 5.2.1. *Let p be odd. For each non-zero element $q \in \mathbb{F}_p^\times$, we define a subset*

$$N_q = \left\{ k - k^{-1}q \;\middle|\; k \in \mathbb{F}_p^\times \right\} \subset \mathbb{F}_p.$$

The cardinality of N_q is $\frac{p+1}{2}$ if $-q$ is a quadratic residue and $\frac{p-1}{2}$ otherwise.

Proof. The multiplicative group $\mathbb{F}_p^\times$ of any prime field $\mathbb{F}_p$ is cyclic, so we can pick a *primitive element* $g \in \mathbb{F}_p^\times$, that is an element such that $\{1, g, g^2, \ldots, g^{p-2}\} = \mathbb{F}_p^\times$ (cf. [65, theorem 2.8]). We denote the elements of N_q by

$$n_q(i) = g^i - g^{-i}q.$$

A computation reveals the following equivalences for all $i, j \in \mathbb{F}_p^\times$.

$$\begin{aligned} n_q(i) = n_q(j) \quad &\Leftrightarrow \quad g^{i+j}(g^{-i} - g^{-j}) = -q(g^{-i} - g^{-j}) \\ \\ &\Leftrightarrow \quad \Big(i = j \text{ or } g^{i+j} = -q\Big) \end{aligned} \tag{5.1}$$

First suppose that $-q \in \mathbb{F}_p^\times$ is a square, so that there is an index $m \in \mathbb{N}_0$ such that $-q = g^{2m}$. We first show that the set N_q equals

$$N_q' = \left\{ n_q(i+m) \mid 0 \le i \le {}^{(p-1)}/_2 \right\}$$

in this case. By definition, N_q includes N_q'. For the converse inclusion, we only have to show that N_q' also contains the elements $n_q(j+m)$ for ${}^{(p-1)}/_2 < j < p-1$, since the map $g^i \mapsto g^{i+m}$ permutes $\mathbb{F}_p^\times$. For each such integer j, the difference $i = p-1-j$ belongs to $\{0, \ldots, {}^{(p-1)}/_2\}$. For this reason, the element

$$\begin{aligned} n_q(j+m) = n_q(p-1-i+m) &\underset{g^{\pm(p-1)}=1}{=} g^{-i+m} + g^{i+m} = g^{i+m} + g^{-(i+m)}g^{2m} \\ &= n_q(i+m) \end{aligned}$$

belongs to N_q, so that we obtain the inclusion $N_q \subset N'_q$.

To see that N'_q has cardinality ${}^{(p+1)}/_2$, we compare two elements $n_q(i+m), n_q(j+m)$ for integers $0 \leq i, j \leq {}^{(p-1)}/_2$, $i \neq j$, and apply equation (5.1).

$$n_q(i+m) = n_q(j+m) \underset{(5.1)}{\Leftrightarrow} g^{i+j+2m} = -q = g^{2m} \underset{(g \text{ generator})}{\Leftrightarrow} i+j \equiv 0 \bmod p-1$$

The last condition is never satisfied by choice of i and j, and consequently we end up with $|N_q| = {}^{(p+1)}/_2$.

In case $-q$ is *no* square modulo p, we can assume $-q = g^{2n-1}$ for some element $n \in \mathbb{N}$. Similarly as above, one verifies the identity $n_q(p - \mathbf{2} - i + n) = n_q(i+n)$, and concludes that N_q equals the set $N''_q = \{n_q(i+n) \mid 0 \leq i \mathbf{<} {}^{(p-1)}/_2\}$.

Furthermore, one checks the following equivalences for all $0 \leq i, j < {}^{(p-1)}/_2$, $i \neq j$.

$$n_q(i+n) = n_q(j+n) \underset{(5.1)}{\Leftrightarrow} g^{i+j+2n} = g^{2n-1} \Leftrightarrow i+j \equiv p-2 \bmod p-1$$

The last of these conditions is never fulfilled, so that we end up with $|N_q| = {}^{(p-1)}/_2$. □

It suggests itself to call a smid family *(affine) linear* if it is a(n affine) linear subspace. Linear smid families inside the matrix algebra $M_n(\mathbb{F}_p)$ are (discrete) planes in the three-dimensional space of symmetric 2×2-matrices over the field $\mathbb{F}_p$.

Obviously, all smid families in $M_n(\mathbb{F}_p)$ which are equivalent—in the sense of Definition 5.1.8—to a symmetric representation of the finite field $\mathbb{F}_{p^n}$ are affine linear subspaces. The theorem below states that indeed all affine linear smid families in $M_2(\mathbb{F}_p)$ are of this type, and gives a complete classification of these families.

Theorem 5.2.2. *There are exactly $\frac{p(p-1)}{2}$ different complete linear smid families in $M_2(\mathbb{F}_p)$. They are given by*

$$\mathcal{S}_{q,r} = \left\{ \begin{pmatrix} x & y \\ y & qx+ry \end{pmatrix} \middle| \, x, y \in \mathbb{F}_p \right\}$$

for field elements $q \in \mathbb{F}_p^\times$ and $r \notin N_q = \{k - k^{-1}q \mid k \in \mathbb{F}_p^\times\}$. All of these smid families are pairwise equivalent, and this carries over to all affine *linear complete smid families in $M_2(\mathbb{F}_p)$.*

Proof. Before we start, notice that the statement is correct for $p = 2$. One checks without effort that the only existing complete smid family in $M_2(\mathbb{F}_p)$ is, in the notation defined above, the family $\mathcal{S}_{1,1}$ (also see Example 5.1.3 (*ii*)). Let us therefore suppose $p \geq 3$ during this proof. Furthermore, note that it suffices to prove that all *linear* smid families are pairwise equivalent, because this immediately implies the same for all *affine* linear smid families by Definition 5.1.8.

Step 1. First we show that a set $\mathcal{S}_{q,r}$ as defined in our assertion is a complete linear smid family if and only if $q \neq 0$ and $r \notin N_q$. For convenience, we denote the matrices in $\mathcal{S}_{q,r}$ by

$$K_{q,r}(x,y) = \begin{pmatrix} x & y \\ y & qx + ry \end{pmatrix} \quad (x, y \in \mathbb{F}_p).$$

To begin with, $\mathcal{S}_{q,r}$ contains exactly p^2 elements including the zero matrix. It is furthermore fairly clear that it is a (two-dimensional) linear subspace of the symmetric matrices in $M_2(\mathbb{F}_p)$.

Suppose $q \neq 0$ and $r \notin N_q$. Since $\mathcal{S}_{q,r}$ is a subspace, it suffices to show that each non-zero element is invertible to prove that $\mathcal{S}_{q,r}$ is a smid family. It is obvious that for all $y \in \mathbb{F}_p^\times$, the matrix $K_{q,r}(0,y)$ is invertible; the same applies for $x \in \mathbb{F}_p^\times$ and $K_{q,r}(x,0)$. For $x, y \in \mathbb{F}_p^\times$, there is always an element $s \in \mathbb{F}_p^\times$ such that $y = sx$. Supposing the matrix $K_{q,r}(x,sx)$ is irregular, i.e. $\det K_{q,r}(x,sx) = 0$, yields the following implications.

$$x^2(q + rs - s^2) = 0 \quad \Rightarrow \quad qs^{-1} + r - s = 0 \quad \Rightarrow \quad r = s - s^{-1}q \in N_q$$

This contradicts the assumption $r \notin N_q$, so all elements in $\mathcal{S}_{q,r}$ are regular and the latter is a complete linear smid family.

Next suppose a pair $(q,r) \in \mathbb{F}_p^2$ does not meet the conditions stated above. If q is zero, the space $\mathcal{S}_{q,r}$ contains the non-invertible element

$$K_{0,r}(1,0) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

and is thus no smid family. If $q \neq 0$ and $r \in N_q$, there is an element $s \in \mathbb{F}_p^\times$ such that we have $r = s - s^{-1}q$. Thereby we get

$$\det K_{q,r}(1,s) = q + rs - s^2 = -s(s - s^{-1}q - r) = 0,$$

so $\mathcal{S}_{q,r}$ is not a smid family in this case either.

Step 2. Next, we count all linear smid families in $M_2(\mathbb{F}_p)$. First of all, you convince yourself that any complete smid family $\mathcal{S} \subset M_2(\mathbb{F}_p)$ is of the form

$$\mathcal{S} = \left\{ \begin{pmatrix} x & y \\ y & L(x,y) \end{pmatrix} \,\middle|\, x, y \in \mathbb{F}_p \right\}$$

for a mapping $L : \mathbb{F}_p^2 \to \mathbb{F}_p$. This is implied by the regularity of all non-trivial differences in $\mathcal{S}$. If moreover $\mathcal{S}$ is a linear subspace, then L must be linear too, and hence declared via $(x, y) \mapsto qx + ry$ $(x, y \in \mathbb{F}_p)$ for some constants $q, r \in \mathbb{F}_p$. According to step 1, we further have $q \in \mathbb{F}_p^\times$ and $r \notin N_q$.

Let us count all pairs $(q, r) \in \mathbb{F}_p^2$ which meet these conditions. Applying the Technical Lemma 5.2.1, and taking into account that there are exactly ${}^{(p-1)}/_2$ non-zero squares modulo p for all $p \geq 3$, the number of all such pairs $(q, r) \in \mathbb{F}_p^2$ sums up to

$$\underbrace{\frac{p-1}{2}}_{-q\in\mathbb{F}_p^\times \text{ a square}} \underbrace{\left(p - \frac{p+1}{2}\right)}_{|\mathbb{F}_p\backslash N_q|} + \underbrace{\frac{p-1}{2}}_{-q\in\mathbb{F}_p^\times \text{ no square}} \underbrace{\left(p - \frac{p-1}{2}\right)}_{|\mathbb{F}_p\backslash N_q|} = \frac{p-1}{2}p$$

Although it lies quite at hand, let us mention for completeness that the ${}^{p(p-1)}/_2$ linear smid families $\mathcal{S}_{q,r}$ found above are in fact *pairwise different*. To see this, consider two different pairs $(q_0, r_0), (q_1, r_1) \in \mathbb{F}_p^2$. We then get

$$\begin{aligned} K_{q_0,r_0}(1,0) &\neq K_{q_1,r_1}(1,0) \quad \text{if } q_0 \neq q_1, \text{ or} \\ K_{q_0,r_0}(0,1) &\neq K_{q_1,r_1}(0,1) \quad \text{if } r_0 \neq r_1. \end{aligned}$$

By the form of complete linear smid families in $M_2(\mathbb{F}_p)$ stated above, this implies $\mathcal{S}_{q_0,r_0} \neq \mathcal{S}_{q_1,r_1}$.

Step 3. At last we prove the equivalence of all linear smid families $\mathcal{S}_{q,r}$. To this aim, we fix a linear smid family $\mathcal{S}_{1,a}$, where we not only presume $a \notin N_1$ (which especially implies $a \neq 0$ since we know that N_1 contains zero), but moreover $a^2 \neq -4$. We will need the second condition further below, and it can always be achieved:

- It holds true if p is three, as $-4 \equiv 2 \bmod 3$ is not a square modulo three.
- If p is five, one computes e.g. $2 \notin N_1 = \{0, 1, 4\}$ and $2^2 \equiv 4 \not\equiv -4 \bmod 5$.
- According the Technical Lemma 5.2.1, the cardinality of the set N_1 is at most ${}^{(p+1)}/_2$. For $p \geq 7$, there are thus at least $p - {}^{(p+1)}/_2 = {}^{(p-1)}/_2 \geq 3$ elements $a \in \mathbb{F}_p$ such that $\mathcal{S}_{1,a}$ is a smid family. We can therefore always pick one different from the two square roots of -4.

For all elements $b, c \in \mathbb{F}_p$, we define a matrix

$$A_{b,c} = \begin{pmatrix} 1 & 0 \\ b & c \end{pmatrix} \in M_2(\mathbb{F}_p).$$

We shall investigate the following set of pairwise equivalent linear smid families.

$$\Sigma = \left\{ A_{b,c}\, \mathcal{S}_{1,a}\, A_{b,c}^T \;\middle|\; b, c \in \mathbb{F}_p, c \in \{1, \ldots, {}^{(p-1)}/_2\} \right\}$$

Our strategy is to show that Σ contains ${}^{p(p-1)}/_2$ pairwise different—and hence all—linear smid families in $M_2(\mathbb{F}_p)$.

Take elements $b_0, b_1 \in \mathbb{F}_p$ and $c_0, c_1 \in \{1, \ldots, {}^{(p-1)}/_2\}$, and set

$$\mathcal{T}_0 = A_{b_0,c_0}\, \mathcal{S}_{1,a}\, A_{b_0,c_0}^T \quad \text{and} \quad \mathcal{T}_1 = A_{b_1,c_1}\, \mathcal{S}_{1,a}\, A_{b_1,c_1}^T.$$

We already know that there must be elements $q_0, r_0 \in \mathbb{F}_p$ such that $\mathcal{T}_0 = \mathcal{S}_{q_0,r_0}$. Now the family $\mathcal{T}_0$ contains the matrices

$$\begin{pmatrix} 1 & 0 \\ b_0 & c_0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix} \begin{pmatrix} 1 & b_0 \\ 0 & c_0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 2b_0 + ac_0 \end{pmatrix}$$

$$\text{and} \quad \begin{pmatrix} 1 & 0 \\ b_0 & c_0 \end{pmatrix} \left(a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix} \right) \begin{pmatrix} 1 & b_0 \\ 0 & c_0 \end{pmatrix} = \begin{pmatrix} a & ab_0 - c_0 \\ ab_0 - c_0 & ab_0^2 - 2b_0c_0 \end{pmatrix},$$

which immediately tells us

$$q_0 = c_0^2 - b_0^2 - ab_0c_0 \quad \text{and} \quad r_0 = 2b_0 + ac_0.$$

Likewise, setting $\mathcal{T}_1 = \mathcal{S}_{q_1,r_1}$, we obtain the equalities

$$q_1 = c_1^2 - b_1^2 - ab_1c_1 \quad \text{and} \quad r_1 = 2b_1 + ac_1.$$

Suppose $\mathcal{T}_0$ and $\mathcal{T}_1$ coincide. According to step 2, this implies $q_0 = q_1$ and $r_0 = r_1$, which leads to the equations

$$c_0^2 - c_1^2 = b_0^2 - b_1^2 + a(b_0c_0 - b_1c_1) \quad \text{and} \quad b_0 - b_1 = -\frac{a}{2}(c_0 - c_1).$$

Inserting the second of these identities into the first (two times), we come to

$$\begin{aligned} c_0^2 - c_1^2 &= {}^{-a}/_2(b_0 + b_1)(c_0 - c_1) + a(b_0c_0 - b_1c_1) \\ &= {}^{a}/_2(b_0c_0 - b_1c_0 + b_0c_1 - b_1c_1) = {}^{a}/_2(b_0 - b_1)(c_0 + c_1) = {}^{-a^2}/_4(c_0^2 - c_1^2). \end{aligned}$$

Since we have ${}^{a^2}/_4 \neq -1$ by assumption, this implies $c_0^2 = c_1^2$. Now the key point is that the identity $c_0 = -c_1$ is excluded by definition of the set Σ:

$$c_0, c_1 \in \{1, \ldots, {}^{(p-1)}/_2\} \quad \Rightarrow \quad c_0 + c_1 \in \{2, \ldots, p-1\} \quad \Rightarrow \quad c_0 + c_1 \neq 0$$

Consequently, the matrix entries c_0 and c_1 coincide, which immediately implies, by the equations above, that also b_0 equals b_1. We have thus shown that two smid families $\mathcal{T}_0, \mathcal{T}_1 \in \Sigma$ coincide only if the corresponding conjugating matrices do so. Since there are ${}^{p(p-1)}/_2$ of these matrices by definition of the set Σ, our proof is complete. □

Some of the smid families $\mathcal{S}_{q,r}$ are isomorphic to the field $\mathbb{F}_{p^2}$, as we shall make precise in the following corollary. In particular, this implies the general result by Seroussi and Lempel (see Theorem 3.3.11) on symmetric field representations for the (simplest) case $n = 2$.

Corollary 5.2.3. *All symmetric representations of the Galois field $\mathbb{F}_{p^2}$ inside the matrix algebra $M_2(\mathbb{F}_p)$ are equivalent. They are given by the complete linear smid families $\mathcal{S}_{1,r}$, where $r \notin N_1$ (cf. Theorem 5.2.2). These field representations are precisely all* commutative *complete linear smid families in $M_2(\mathbb{F}_p)$.*

For odd primes p, the number of symmetric representations of the field $\mathbb{F}_{p^2}$ in $M_2(\mathbb{F}_p)$ is given by the following rule. If -1 is a square modulo p, then there are exactly ${}^{(p-1)}/{}_2$ such representations. Otherwise, there are ${}^{(p+1)}/{}_2$ of them.

Proof. For all $n \in \mathbb{N}$, a symmetric representation of the field $\mathbb{F}_{p^n}$ in $M_n(\mathbb{F}_p)$ is a linear complete smid family (cp. Theorem 3.3.11) and thus of the form $\mathcal{S}_{q,r}$ by Theorem 5.2.2. For this reason, our task is to decide which of the smid families $\mathcal{S}_{q,r} \subset M_2(\mathbb{F}_p)$ are field representations.

Each smid family $\mathcal{S}_{q,r}$ ($q \in \mathbb{F}_p^\times$, $r \notin N_q$) is an additive group, and all of its non-zero elements are invertible. Hence $\mathcal{S}_{q,r}$ is a field whenever $\mathcal{S}_{q,r} \setminus \{0\}$ is a *commutative group* with respect to matrix multiplication.

As before, we denote the elements of $\mathcal{S}_{q,r}$ by

$$K_{q,r}(x,y) = \begin{pmatrix} x & y \\ y & qx+ry \end{pmatrix}.$$

To check under which conditions the family $\mathcal{S}_{q,r}$ is commutative, we calculate the commutator of two matrices $K_{q,r}(x_0,y_0)$ and $K_{q,r}(x_1,y_1)$ in $\mathcal{S}_{q,r}$.

$$\begin{aligned} \big[K_{q,r}(x_0,y_0), K_{q,r}(x_1,y_1)\big] &= K_{q,r}(x_0,y_0)K_{q,r}(x_1,y_1) - K_{q,r}(x_1,y_1)K_{q,r}(x_0,y_0) \\ &= \begin{pmatrix} 0 & (1-q)(x_1y_0 - x_0y_1) \\ (q-1)(x_0y_1 - x_1y_0) & 0 \end{pmatrix} \end{aligned}$$

This shows that $\mathcal{S}_{q,r}$ is commutative if and only if q equals one, in which case the product $K_{1,r}(x_0,y_0)K_{1,r}(x_1,y_1)$ computes to

$$\begin{pmatrix} x_0x_1 + y_0y_1 & x_0y_1 + x_1y_0 + ry_0y_1 \\ x_0y_1 + x_1y_0 + ry_0y_1 & 1(x_0x_1 + y_0y_1) + r(x_0y_1 + x_1y_0 + ry_0y_1) \end{pmatrix}.$$

The last matrix is not only symmetric, but an element of $\mathcal{S}_{1,r}$, so the latter is closed under multiplication. The same applies for $\mathcal{S}_{1,r} \setminus \{0\}$, since the product of two invertible matrices is of course not zero. We have thus shown that $\mathcal{S}_{1,r} \setminus \{0\}$ is a *commutative semigroup* (containing the neutral element $K_{1,r}(1,0)$, so that we actually have a *monoid*).

Consisting solely of invertible matrices, the semigroup $\mathcal{S}_{1,r} \setminus \{0\}$ trivially has the *cancellation property,* that is we have the implication

$$KL = KM \ \text{ or } \ LK = MK \quad \Rightarrow \quad L = M$$

for all $K, L, M \in \mathcal{S}_{1,r} \setminus \{0\}$. It is an elementary fact from group theory that every finite semigroup which has the cancellation property is a group at the same time. Altogether, we have thus shown that $\mathcal{S}_{1,r} \setminus \{0\}$ is a commutative group.

Consequently, all smid families of the form $\mathcal{S}_{1,r}$ are fields. Simply by their cardinality, they are symmetric representations of the field $\mathbb{F}_{p^2}$. Besides that, it follows from our proof that all other complete linear smid families in $M_2(\mathbb{F}_p)$ are *not* commutative. The remaining statements in the assertion follow from the Technical Lemma 5.2.1 and Theorem 5.2.2. □

Recall that according to the first supplement of Gauss' Law of Quadratic Reciprocity, the element $-1 \in \mathbb{F}_p$ is a quadratic residue if and only if $p \equiv 1 \bmod 4$.

If the prime p is odd, the sets N_q contain zero if and only if $q \in \mathbb{F}_p^\times$ is a square:

$$0 \in N_q \quad \Leftrightarrow \quad \underset{k \in \mathbb{F}_p^\times}{\exists} \ k - k^{-1}q = 0 \quad \Leftrightarrow \quad \underset{k \in \mathbb{F}_p^\times}{\exists} \ k^2 = q$$

For this reason, there are linear smid families of the particularly simple form $\mathcal{S}_{q,0}$ for all primes $p > 2$.

Observation 5.2.4. For all odd primes p, a smid family in $M_2(\mathbb{F}_p)$ is given by $\mathcal{S}_{q,0}$ if and only if $q \in \mathbb{F}_p^\times$ is not a square, hence for exactly $(p-1)/2$ elements in $q \in \mathbb{F}_p^\times$.

We conclude this section with an explicit list of the complete linear smid families in the matrix algebra $M_2(\mathbb{F}_3)$.

Example 5.2.5. Set $p = 3$. There are $p(p-1)/2 = 3$ complete linear smid families in $M_2(\mathbb{F}_3)$, namely $\mathcal{S}_{1,1}, \mathcal{S}_{1,2}$, and $\mathcal{S}_{2,0}$. As predicted by Corollary 5.2.3, $(p+1)/2 = 2$ of them (the first and the second) are representations of the field $\mathbb{F}_9$, because -1 is not a square modulo 3. The third is of the type described in Observation 5.2.4.

$$\begin{aligned}
\mathcal{S}_{1,1} \;=\; & \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix}, \right. \\
& \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix}, \\
& \left. \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix} \right\}
\end{aligned}$$

$$\begin{aligned}
\mathcal{S}_{1,2} \;=\; & \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 2 & 1 \end{pmatrix}, \right. \\
& \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}, \\
& \left. \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 2 & 0 \end{pmatrix} \right\}
\end{aligned}$$

$$\begin{aligned}
\mathcal{S}_{2,0} \;=\; & \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}, \right. \\
& \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}, \\
& \left. \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix} \right\}
\end{aligned}$$

5.3 Smid families in $\mathbf{M_2(\mathbb{F}_p)}$, permutation polynomials, and Latin squares

Let p denote an **odd** prime number for the whole section (we exclud the rather trivial case $p = 2$ to avoid some technical inconveniences). The guideline of this section is the following

Question 5.3.1. Are all complete smid families in $M_2(\mathbb{F}_p)$ affine linear subspaces?[*]

The answer is positive for $M_2(\mathbb{F}_2)$ according to Example 5.1.3 (ii). We shall give a positive answer for $p = 3$ at the end of this section, and for $p = 5$ and $p = 7$ in the next section. For primes $p > 7$, we have to leave the question above undecided.

Some basic observations

As pointed out in the previous section, linear smid families in $M_2(\mathbb{F}_p)$ are planes in the three-dimensional vector space of symmetric 2×2-matrices over the field $\mathbb{F}_p$. This geometric picture is the background of our first observation, which tells us that a smid family in $M_2(\mathbb{F}_p)$ is either an affine plane or, loosely speaking, "extremely non-linear".

Observation 5.3.2. Let $\mathcal{S} \subset M_2(\mathbb{F}_p)$ be a (not necessarily complete) smid family. Then $\mathcal{S}$ can neither contain

- a pair of skew lines of matrices,
- nor three different lines of matrices which do not belong to the same plane.

Proof. For the first item, let $A, B, X, Y \in M_2(\mathbb{F}_p)$ be symmetric matrices such that the affine lines $X + \langle A \rangle$ and $Y + \langle B \rangle$ are skew.

Suppose these skew lines belong to one and the same smid family. Then the same applies to the line $\langle A \rangle$ and the affine line $C + \langle B \rangle$, where we set $C = Y - X$. Accordingly, the sum

$$kA + C + lB = (C + lB) - (-k)A$$

is invertible as a non-zero difference of elements of a smid family for all coefficients $k, l \in \mathbb{F}_p$. The differences are not only non-zero, but moreover *pairwise different*, because since the (affine) lines $\langle A \rangle$ and $C + \langle B \rangle$ are skew lines, the matrices A, B, C are linearly independent.

[*] *Addendum:* Directly before this thesis had to be submitted, it came to our knowledge that the answer to this question is actually *positive.* The author has learned from W. M. Kantor ([50]) that this follows from results established by S. Ball et al. in [7]. The author is very grateful for this information.

This is a contradiction, for it asserts the existence of far too many invertible symmetric matrices in $M_2(\mathbb{F}_p)$ (in fact, since A is regular as well, it actually implies the regularity of *all* non-zero symmetric matrices in $M_2(\mathbb{F}_p)$). Consequently, a smid family cannot contain two different skew lines.

The second item requires some technicalities. First we check that, given any invertible symmetric matrix

$$A = \begin{pmatrix} x & y \\ y & z \end{pmatrix} \in M_2(\mathbb{F}_p),$$

either A is a multiple of the "flip matrix"

$$F = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

or there is a regular symmetric matrix $T \in M_2(\mathbb{F}_p)$ such that TAT is diagonal. If y equals zero, there is nothing to check, and the same holds true for the case $x = z = 0$. Otherwise set

$$T = \begin{cases} \begin{pmatrix} -yx^{-1} & 1 \\ 1 & 0 \end{pmatrix} & \text{if } z = 0 \text{ and } x \neq 0, \\[2ex] \begin{pmatrix} 0 & 1 \\ 1 & -yz^{-1} \end{pmatrix} & \text{if } z \neq 0. \end{cases}$$

You easily convince yourself that TAT is a diagonal matrix in each of the two cases.

Now let $\mathcal{S}$ denote a smid family containing three different lines (and thereby in particular the zero matrix). According to what we have just shown, it is no loss of generality to assume that one of these lines consists either of diagonal matrices or of multiples of the flip matrix F. Since at most one line is spanned by the flip matrix, we can apply the same argument once more, and hence always presume that one of the lines included in $\mathcal{S}$ is spanned by the diagonal matrix

$$A = \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix}$$

for some entry $q \in \mathbb{F}_p^{\times}$. Then no other line in the family $\mathcal{S}$ can contain diagonal non-zero matrices, for this would produce irregular non-zero differences. On that account, we can suppose w.l.o.g. that the two remaining lines lying in $\mathcal{S}$ by assumption are spanned by matrices

$$B = \begin{pmatrix} s & 1 \\ 1 & sq + r_0 \end{pmatrix} \quad \text{and} \quad C = \begin{pmatrix} t & 1 \\ 1 & tq + r_1 \end{pmatrix}$$

for elements $s, t, r_0, r_1 \in \mathbb{F}_p$, where we have chosen a form for the lower right entries that is convenient for our purposes.

In fact, since all of the differences $kA - lB$ and $kA - lC$ are invertible or zero for $k, l \in \mathbb{F}_p$, both of the planes $\langle A, B\rangle$ and $\langle A, C\rangle$ are complete linear smid families in $M_2(\mathbb{F}_p)$. Having identified all these families in Theorem 5.2.2, we know $\langle A, B\rangle = \mathcal{S}_{q,r_0}$ and $\langle A, C\rangle = \mathcal{S}_{q,r_1}$.

The clue is that by the same argument as used before, the plane $\langle B, C\rangle$ is a complete linear smid family as well, and it is readily seen that this smid family simultaneously equals $\mathcal{S}_{q,r_0}$ *and* $\mathcal{S}_{q,r_1}$, implying that r_0 and r_1 coincide. All in all, each of the lines $\langle A\rangle$, $\langle B\rangle$, and $\langle C\rangle$ is included in the smid family $\mathcal{S}_{q,r_0}$, that is in one and the same plane. □

The statement above can be slightly reinforced, e.g. by replacing the term "line" in turn by "set of at least $p - 1$ matrices on a line". For the sake of clarity, we omit some technical details of this kind at some points of the present section.

If non-linear smid families in $M_2(\mathbb{F}_p)$ exist, then they are maximally unstable under linear conjugations. This is the main assertion of the next observation.

Observation 5.3.3. Let $\mathcal{S}$ be a complete smid family in the matrix algebra $M_2(\mathbb{F}_p)$. Then the following assertions are equivalent.

(i) The family $\mathcal{S}$ is a (two-dimensional) linear subspace of $M_2(\mathbb{F}_p)$.

(ii) The identity $A\mathcal{S}A^T = \mathcal{S}$ holds for a matrix $\mathrm{I}_2 \neq A \in M_2(\mathbb{F}_p)$.

(iii) The identity $a\mathcal{S} = \mathcal{S}$ holds for a coefficient $1 \neq a \in \mathbb{F}_p^\times$.

Proof. It goes without saying the the first statement implies the others. If the second assertion holds, then $\mathcal{S}$ lies in the kernel of the linear map

$$T_A : M_2(\mathbb{F}_p) \longrightarrow M_2(\mathbb{F}_p), \quad K \longmapsto AKA^T - K,$$

for some matrix $\mathrm{I}_2 \neq A \in M_2(\mathbb{F}_p)$. The kernel is a linear subspace of dimension at most two, because otherwise we would end up with $AKA^T = K$ for all symmetric matrices $K \in M_2(\mathbb{F}_p)$. The cardinality of $\mathcal{S}$ leads to $\ker T_A = \mathcal{S}$ and thereby to statement (i).

Replacing the mapping T_A by

$$T_a : M_2(\mathbb{F}_p) \longrightarrow M_2(\mathbb{F}_p), \quad K \longmapsto aK - K,$$

for some coefficient $1 \neq a \in \mathbb{F}_p^\times$, the same argument proves that item (iii) asserts (i). □

Recall that item (iii) in the observation above is *not* a priori a special case of item (ii), as we have seen in the proof of Lemma 5.1.9.

The defining condition that all differences in a smid family are either zero or invertible directly leads to the next, rather technical

Observation 5.3.4. Every smid family $\mathcal{S} \subset M_2(\mathbb{F}_p)$ is of the form

$$\mathcal{S} = \left\{ \begin{pmatrix} x & y \\ y & \Phi(x,y) \end{pmatrix} \;\middle|\; (x,y) \in I \right\},$$

where I is a subset of $\mathbb{F}_p^2$ and Φ maps from I to the field $\mathbb{F}_p$. Defining maps $\phi_y : I_y \to \mathbb{F}_p$ by $\phi_y(x) = \Phi(x,y)$ whenever the subset $I_y = \{x \in \mathbb{F}_p \mid (x,y) \in I\}$ is not empty, we can as well write

$$\mathcal{S} = \left\{ \begin{pmatrix} x & y \\ y & \phi_y(x) \end{pmatrix} \;\middle|\; (x,y) \in I \right\}$$

By regularity of all non-zero differences in $\mathcal{S}$, we then get

$$(x_1 - x_2)(\phi_{y_1}(x_1) - \phi_{y_2}(x_2)) \neq (y_1 - y_2)^2$$

whenever $(x_1, y_1), (x_2, y_2) \in I$ do not coincide. Especially, the maps ϕ_y are *injective.*

The following statement is a consequence of this observation, and sheds light on the close link between permutations of the field $\mathbb{F}_p$ and complete smid families in $M_2(\mathbb{F}_p)$.

Lemma 5.3.5. *Consider a smid family $\mathcal{S} \subset M_2(\mathbb{F}_p)$. We keep the notations of the previous observation, and define maps $\Psi_{(x_0,y_0,k)} : \mathbb{F}_p \to \mathbb{F}_p$ for all triples $(x_0, y_0, k) \in \mathbb{F}_p^3$ by*

$$\Psi_{(x_0,y_0,k)} : l \longmapsto \phi_{y_0+lk}(x_0 + l) - lk^2,$$

whenever $(y_0 + lk, x_0 + l)$ belongs to I. Then all of these maps are injective.

If $\mathcal{S}$ happens to be complete and hence I equals $\mathbb{F}_p^2$, then all maps $\Psi_{(x_0,y_0,k)}$, notably the maps $\phi_y = \Psi_{(0,y,0)}$, are permutations.

Proof. Fix a triple $(x_0, y_0, k) \in \mathbb{F}_p^3$ and consider elements $l_0, l_1 \in \mathbb{F}_p$ such that the pairs $(y_0 + l_0k, x_0 + l_0)$ and $(y_0 + l_1k, x_0 + l_1)$ belong to I. We then have the following equivalences.

$$\begin{aligned} & \Psi_{(x_0,y_0,k)}(l_0) = \Psi_{(x_0,y_0,k)}(l_1) \\ \Leftrightarrow \quad & \phi_{y_0+l_0k}(x_0 + l_0) - \phi_{y_0+l_1k}(x_0 + l_1) - (l_0 - l_1)k^2 = 0 \\ \Leftrightarrow \quad & (l_0 - l_1)\left(\phi_{y_0+l_0k}(x_0 + l_0) - \phi_{y_0+l_1k}(x_0 + l_1)\right) - (l_0 - l_1)^2k^2 = 0 \end{aligned}$$

The left-hand side of the last line is precisely the determinant of the difference

$$\begin{pmatrix} x_0 + l_0 & y_0 + l_0k \\ y_0 + l_0k & \phi_{y_0+l_0k}(x_0 + l_0) \end{pmatrix} - \begin{pmatrix} x_0 + l_1 & y_0 + l_1k \\ y_0 + l_1k & \phi_{y_0+l_1k}(x_0 + l_1) \end{pmatrix},$$

which is zero if and only if l_0 equals l_1 by regularity of all differences in $\mathcal{S}$. Thus, the mapping $\Psi_{(x_0,y_0,k)}$ is injective. If the smid family $\mathcal{S}$ is complete, then we have $I = \mathbb{F}_p^2$. As a consequence, the map $\Psi_{(x_0,y_0,k)}$ is defined over the whole field $\mathbb{F}_p$, and hence a permutation of the latter. □

The next lemma states, roughly speaking, that a complete smid family in $M_2(\mathbb{F}_p)$ is already determined by any choice of $p^2 - p$ of its members.

Lemma 5.3.6. *Consider a smid family $\mathcal{S} \subset M_2(\mathbb{F}_p)$ containing $m \geq p^2 - p$ elements, which is* completable, *i.e. there is a set $\mathcal{C}$ of $p^2 - m$ symmetric matrices such that $\mathcal{S} \cup \mathcal{C}$ is a complete smid family. Then the following assertions hold:*

(i) If $\mathcal{S} \cup \{C\}$ is a smid family for any symmetric matrix $C \in M_2(\mathbb{F}_p)$, it follows $C \in \mathcal{C}$. As a consequence, the completing set $\mathcal{C}$ is unique.

(ii) If the smid family $\mathcal{S}$ is included in a (two-dimensional) plane $\mathcal{T} \subset M_2(\mathbb{F}_p)$, then $\mathcal{T}$ is a linear smid family and the unique completion of $\mathcal{S}$.

(iii) The completion $\mathcal{S} \cup \mathcal{C}$ of $\mathcal{S}$ lies in the span of $\mathcal{S}$, that is we have $\langle \mathcal{S} \rangle = \langle \mathcal{S} \cup \mathcal{C} \rangle$.

The elementary but a bit lengthy proof is provided in the Appendix on pages 222-224. ▷

We deduce two easy corollaries from this lemma.

Corollary 5.3.7. *If $\mathcal{S} \subset M_2(\mathbb{F}_p)$ is a complete smid family and $D \in M_2(\mathbb{F}_p)$ is any symmetric matrix, then either D is a member of $\mathcal{S}$, or there are exactly $p + 1$ elements $K_0, \ldots, K_p \in \mathcal{S}$ such that $K_i - D$ is neither invertible nor zero for all $0 \leq i \leq p$.*

The proof can be found in the Appendix on page 224. ▷

Corollary 5.3.8. *Every matrix $A \neq 0$ in a complete smid family $\mathcal{S} \subset M_2(\mathbb{F}_p)$ is a linear combination of linearly independent matrices in $\mathcal{S}$, each of which is linearly independent of A.*

The proof can be found in the Appendix on page 225. ▷

Complete smid families in $\mathbf{M_2(\mathbb{F}_p)}$ and permutation polynomials

Observation 5.3.2 tells us that a non-linear complete smid family in $M_2(\mathbb{F}_p)$—if there is one—is not a union of lines of matrices. It does not exclude that a non-linear smid family may be composed of a family of *parallel affine* lines, which do not belong to a single plane. This gap is filled by Lemma 5.3.10 further below, whose proof requires some work. In particular, it borrows a fact from the theory of *permutation polynomials over finite fields.*

It is a basic algebraic fact that *all* functions mapping a finite field F to itself are given by polynomials in the ring $F[X]$ (or, more precisely, by the associated polynomial functions on F). This can for instance be deduced from the *Lagrange interpolation formula* (cf. [65, theorem 1.71]).

Of special interest in many contexts are polynomial functions which are at the same time permutations of the field F. If q is the order of F, then such permutation polynomials correspond to elements of the symmetric group S_q. In general, it is a non-trivial task to decide whether a given polynomial in $F[X]$ induces a permutation of F or not. A collection of criteria is stated in [65, chapter 7].

The following technical lemma tells us that if a map $f : \mathbb{F}_p \to \mathbb{F}_p$ differs from "many" permutation polynomials only by linear terms, then f must be linear itself (and hence especially a permutation). This is a direct consequence of a more general theorem published in 1992 by Ronald J. Evans, John Greene and Harald Niederreiter in [36]. The direct proof presented in the Appendix is more than inspired by their theorem's proof.

Technical Lemma 5.3.9. *Consider a map $f : \mathbb{F}_p \to \mathbb{F}_p$ such that $f(0) = 0$ and define mappings $g_c : \mathbb{F}_p \to \mathbb{F}_p$ by $g_c(x) = f(x) + cx$ for all $c \in \mathbb{F}_p$. If there are at least $(p-1)/2$ different values $c \in \mathbb{F}_p$ such that g_c is a permutation of the field $\mathbb{F}_p$, then f is linear.*

The proof can be found in the Appendix on pages 225-229. ▷

The statement above enables us to add the following criterion for the linearity of complete smid families in $M_2(\mathbb{F}_p)$ to our list.

Lemma 5.3.10. *Let $\mathcal{S} \subset M_2(\mathbb{F}_p)$ be a complete smid family containing the zero matrix. The following assertions are equivalent.*

(i) The family $\mathcal{S}$ is a linear subspace of $M_2(\mathbb{F}_p)$.

(ii) There is a symmetric matrix $A \in M_2(\mathbb{F}_p) \setminus \{0\}$ such that $\mathcal{S} + A$ equals $\mathcal{S}$.

Proof. The first statement trivially implies the second, so that we only have to prove the converse implication.

Let $\mathcal{S} \subset M_2(\mathbb{F}_p)$ be a smid family containing zero, and $A \in M_2(\mathbb{F}_p)$ a non-zero symmetric matrix like in statement (ii). Then we have $0 + A \in \mathcal{S} + A = \mathcal{S}$ by assumption, so that A must be a regular matrix. According to our considerations in the proof of Observation 5.3.2, we can assume w.l.o.g. that A is either a diagonal matrix or the flip matrix F defined in that proof.

Case 1 ($A = F$). Consider the diagonal elements

$$\begin{pmatrix} x & 0 \\ 0 & \phi_0(x) \end{pmatrix} \quad (x \in \mathbb{F}_p)$$

in the smid family $\mathcal{S}$, where $\phi_0 : \mathbb{F}_p \to \mathbb{F}_p$ is a permutation fulfilling $\phi_0(0) = 0$ (cf. Observation 5.3.4). As a consequence of the assumption $\mathcal{S} + A = \mathcal{S}$, the elements

$$\begin{pmatrix} x & 0 \\ 0 & \phi_0(x) \end{pmatrix} + j \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

belong to the family $\mathcal{S}$ for all $x, j \in \mathbb{F}_p$. Thereby $\mathcal{S}$ is a disjoint union of p parallel lines.

$$\mathcal{S} = \dot{\bigcup_{x \in \mathbb{F}_p}} \left(\begin{pmatrix} x & 0 \\ 0 & \phi_0(x) \end{pmatrix} + \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \right) \tag{5.2}$$

The regularity of all differences in $\mathcal{S}$ asserts that the determinant

$$\det\left(\begin{pmatrix} x_0 - x_1 & 0 \\ 0 & \phi_0(x_0) - \phi_0(x_1) \end{pmatrix} - m \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right) = (x_0 - x_1)(\phi_0(x_0) - \phi_0(x_1)) - m^2$$

is non-zero, which leads to the inequality

$$\frac{\phi_0(x_0) - \phi_0(x_1)}{x_0 - x_1} \neq \frac{m^2}{(x_0 - x_1)^2} \qquad \text{for all } m, x_0, x_1 \in \mathbb{F}_p,\ x_0 \neq x_1.$$

Let $\mathcal{Q} \subset \mathbb{F}_p$ denote the set of quadratic residues (i.e. squares) modulo p, and fix a square $c \in \mathcal{Q}$. The inequalities above allow to draw the following conclusions for every pair $x_0, x_1 \in \mathbb{F}_p$ with $x_0 \neq x_1$.

$$\begin{array}{rrcl} & \dfrac{\phi_0(x_0) - \phi_0(x_1)}{x_0 - x_1} & \notin & \mathcal{Q} \\ \Rightarrow & \dfrac{\phi_0(x_0) - \phi_0(x_1)}{x_0 - x_1} - c & \notin & \mathcal{Q} - c \\ \Rightarrow & \dfrac{(\phi_0(x_0) - cx_0) - (\phi_0(x_1) - cx_1)}{x_0 - x_1} & \notin & \mathcal{Q} - c \\ \Rightarrow & \dfrac{(\phi_0(x_0) - cx_0) - (\phi_0(x_1) - cx_1)}{x_0 - x_1} & \neq & 0 \end{array}$$

The last inequality shows that the maps $g_c : x \mapsto \phi_0(x) - cx$ are *permutations* for all squares $c \in \mathbb{F}_p$. As there are $(p+1)/2$ squares in $\mathbb{F}_p$, the Technical Lemma 5.3.9 applies, telling us that the map ϕ_0 must be linear (recall that we assume that p is odd). In other words, the set of diagonal matrices inside $\mathcal{S}$ is a *line*, which immediately implies that the smid family $\mathcal{S}$ is a plane by equation (5.2).

Case 2 (A diagonal). Without loss of generality, we can assume

$$A = \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix}$$

for an element $q \in \mathbb{F}_p^\times$. By analogy with case 1, we can write

$$\mathcal{S} = \dot{\bigcup_{y \in \mathbb{F}_p}} \left(\begin{pmatrix} 0 & y \\ y & f(y) \end{pmatrix} + \left\langle \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix} \right\rangle \right)$$

for a map $f : \mathbb{F}_p \to \mathbb{F}_p$ with $f(0) = 0$. Notice that a priori, f is not necessarily a permutation (we have $f(y) = \phi_y(0)$ in the notation of Observation 5.3.2).

The regularity of all non-zero differences in $\mathcal{S}$ yields

$$0 \neq \det \left(\begin{pmatrix} -m & y_0 - y_1 \\ y_0 - y_1 & f(y_0) - f(y_1) - mq \end{pmatrix} \right) = m^2 q - m(f(y_0) - f(y_1)) - (y_0 - y_1)^2,$$

whereby we obtain the inequality

$$\frac{f(y_0) - f(y_1)}{y_0 - y_1} \neq \frac{m}{y_0 - y_1} q - \frac{y_0 - y_1}{m}$$

for all $m, y_0, y_1 \in \mathbb{F}_p$, provided $y_0 \neq y_1$ and $m \neq 0$. If we fix a pair $y_0 \neq y_1$ and vary through $m \in \mathbb{F}_p^\times$, the right-hand side of the previous inequality takes all values in the set $\{k^{-1}q - k \mid k \in \mathbb{F}_p^\times\} = -N_q = N_q$, which is already familiar to us from Section 5.2. For any element $c \in N_q$, this leads to the following conclusions.

$$\begin{aligned} & \frac{f(y_0) - f(y_1)}{y_0 - y_1} && \notin N_q \\ \Rightarrow \quad & \frac{(f(y_0) - cy_0) - (f(y_1) - cy_1)}{y_0 - y_1} && \notin N_q - c \\ \Rightarrow \quad & \frac{(f(y_0) - cy_0) - (f(y_1) - cy_1)}{y_0 - y_1} && \neq 0. \end{aligned}$$

On that account, the maps $g_c : y \mapsto f(y) - cy$ are permutations for all $c \in N_q$. As we have calculated in the Technical Lemma 5.2.1, the cardinality of N_q is either $(p+1)/2$ or $(p-1)/2$. At any rate, N_q contains enough elements to satisfy the conditions of the Technical Lemma 5.3.9, so that we can conclude, as in case 1, that the map f is linear. Consequently, the set of all matrices

$$\begin{pmatrix} 0 & y \\ y & f(y) \end{pmatrix} \quad (y \in \mathbb{F}_p)$$

is a line, and hence $\mathcal{S}$ is plane. Our proof is complete. □

As a consequence of the last preceding lemma and Observation 5.3.2, we get the following

Corollary 5.3.11. *If a complete smid family in $M_2(\mathbb{F}_p)$ is a union of (affine) lines of symmetric matrices, then it is an affine linear subspace.*

Linear transformations of smid families and automorphism groups of MUBs

We define an affine linear transformation of $M_2(\mathbb{F}_p)$ for matrices $A, B \in M_2(\mathbb{F}_p)$ and a factor $c \in \mathbb{F}_p$ by

$$T_{A,B,c} : K \longmapsto cAKA^T + B \quad (K \in M_2(\mathbb{F}_p)). \tag{5.3}$$

Let $\mathcal{S}$ be a complete smid family in $M_2(\mathbb{F}_p)$. The set of all affine linear transformations $T_{A,B,c}$ which *fix* $\mathcal{S}$, i.e. fulfil the identity $T_{A,B,c}(\mathcal{S}) = \mathcal{S}$, clearly is a group. We say this group is trivial if it contains only the identity.

It is a subject of its own to investigate the group of all affine linear transformations which fix a given smid family $\mathcal{S}$. Such transformations correspond to unitary conjugations (of the matrix algebra $M_{p^2}(\mathbb{C})$) fixing the set of masas associated with the family $\mathcal{S}$ (up to a permutation; also cf. Section 5.1). The group of unitaries meeting this condition is sometimes referred to as the *automorphism group* of the respective set of MUBs. The study of these automorphism groups is left out in the present work. For prime dimensions, it is considered at length in the dissertation of Daniel P. May, see [70].

It is straightforward to check that the group of linear transformations of the form $T_{A,B,c}$ is trivial for an affine linear smid family unless the latter is linear. On the other hand, Observation 5.3.3 implies that this group is never trivial for linear smid families.

Combining Observation 5.3.3 and Lemma 5.3.10, we obtain the following

Corollary 5.3.12. *Let $\mathcal{S} \subset M_2(\mathbb{F}_p)$ be a smid family containing the zero matrix, and define linear transformations $T_{A,B,c}$ as in equation* (5.3) *for all matrices $A, B \in M_2(\mathbb{F}_p)$ and factors $c \in \mathbb{F}_p$. Then the following assertions are equivalent.*

(i) The family $\mathcal{S}$ is a linear subspace of $M_2(\mathbb{F}_p)$.

(ii) The group of linear transformations $\{T_{A,B,c} \mid T_{A,B,c}(\mathcal{S}) = \mathcal{S}\}$ is not trivial.

Complete smid families in $\mathbf{M_2(\mathbb{F}_p)}$ and Latin squares

We have already come across Latin squares in Section 3.5. However, since that section is marked as an excursion, we repeat the basics at this point. A few more facts are mentioned in Section 3.5. A collection of all the basics and the most important results concerning Latin squares, as well as an exhaustive overview over the many related combinatorial topics (e.g. block designs), can be found in both of the textbooks [26, 87].

Definition 5.3.13. *A* Latin square *of order m is a $m \times m$-matrix with entries from a set M of cardinality m, e.g. from $M = \mathbb{Z}/m$, such that each element of M occurs exactly once in each row and each column.*

There are Latin squares of any order, as the following standard example shows.

Example 5.3.14. Fix a natural number $m \in \mathbb{N}$ and an element $s \in \mathbb{Z}/m$, further let $q, r \in \mathbb{Z}/m$ be elements which are coprime with m. Then a Latin square is given by the $m\times m$-matrix

$$(qx + ry + s)_{0\leq x,y<m} \,.$$

Setting for instance $m = 3$, $q = 1$, and $s = 0$, we get the following Latin squares.

$$\begin{array}{ccc} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{array} \qquad \begin{array}{ccc} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{array} \tag{5.4}$$

There is a natural orthogonality relation for Latin squares.

Definition 5.3.15. *Two Latin squares $A = (a_{i,j})$ and $B = (b_{i,j})$ of order m, with entries from the set $\mathbb{Z}/m$, are called* orthogonal *if all entries of the matrix*

$$\big(\, (a_{i,j}, b_{i,j})\,\big)_{0\leq i,j<m} \in M_m(\mathbb{Z}/m \times \mathbb{Z}/m)$$

are pairwise different. Such a matrix is called Graeco-Latin square *or* Euler square.

In the sequel, we will only consider Latin squares of prime order $p \in \mathbb{P}$, and consider their entries as elements of the respective prime field $\mathbb{F}_p$ for convenience. It is easy to verify the following standard example by hand.

Example 5.3.16. Fix an element $q \in \mathbb{F}_p^\times$. All of the $p - 1$ Latin squares in the family

$$\Big\{ (\, qx + ry\,)_{x,y\in\mathbb{F}_p} \;\Big|\; r \in \mathbb{F}_p^\times \Big\}$$

are mutually orthogonal.

As a general result, there are at most $m - 1$ mutually orthogonal Latin squares of order m. Families as in the example above are therefore called *complete.*

$$\begin{array}{ccc} (0,0) & (1,1) & (2,2) \\ (1,2) & (2,0) & (0,1) \\ (2,1) & (0,2) & (1,0) \end{array}$$

For $p = 3$ and $q = 1$, the example above yields the orthogonal Latin squares explicitly displayed in Example 5.3.14, which thus form a complete orthogonal set of order 3. Consequently, the adjacent 3×3-matrix with entries from $\mathbb{F}_p \times \mathbb{F}_p$ is a Graeco-Latin square.

Here comes the connection between Latin squares of order p and complete smid families in $M_2(\mathbb{F}_p)$.

Observation 5.3.17. For a map $\Phi : \mathbb{F}_p \times \mathbb{F}_p \to \mathbb{F}_p$, define a set of symmetric matrices in $M_2(\mathbb{F}_p)$ by

$$\mathcal{S} = \left\{ \begin{pmatrix} x & y \\ y & \Phi(x,y) \end{pmatrix} \middle| \; x, y \in \mathbb{F}_p \right\}.$$

Furthermore, declare maps $\Phi_k : \mathbb{F}_p \times \mathbb{F}_p \to \mathbb{F}_p$ for all $k \in \mathbb{F}_p^\times$ by

$$\Phi_k(x,y) = \Phi(x+ky, y) - k^{-1}y \quad (x, y \in \mathbb{F}_p). \tag{5.5}$$

Then the set $\mathcal{S}$ is a complete smid family precisely if the $p{\times}p$-matrices

$$L_k = (\, \Phi_k\,(x,y)\,)_{x,y \in \mathbb{F}_p}$$

are Latin squares for all $k \in \mathbb{F}_p^\times$.

Proof. Recall that according to Lemma 5.3.5, the set $\mathcal{S}$ is a complete smid family if and only if the mappings

$$\Psi_{(x_0,y_0,k)} : \mathbb{F}_p \longrightarrow \mathbb{F}_p, \quad l \longmapsto \Phi(x_0 + l, y_0 + lk) - lk^2,$$

defined for $x_0, y_0, k \in \mathbb{F}_p$, are all permutations.
$\Rightarrow$. If $\mathcal{S}$ is a smid family, then in particular the maps $\Psi_{(x_0,0,k^{-1})}$ and $\Psi_{(ky_0,y_0,0)}$ are permutations for all $x_0, y_0 \in \mathbb{F}_p$ and $k \in \mathbb{F}_p^\times$, and one readily computes the identities

$$\Psi_{(x_0,0,k^{-1})}(ky) = \Phi_k(x_0,y) \quad \text{and} \quad \Psi_{(ky_0,y_0,0)}(x) = \Phi(x+ky_0,y_0) = \Phi_k(x,y_0) + k^{-1}y_0.$$

This shows that all rows and columns of the matrix $(\Phi_k(x,y))$ are permutations for each index $k \in \mathbb{F}_p^\times$.
$\Leftarrow$. If conversely all of the $p{\times}p$-matrices L_k are Latin squares, consider two different matrices

$$K_0 = \begin{pmatrix} x_0 & y_0 \\ y_0 & \Phi(x_0,y_0) \end{pmatrix}, \quad \text{and} \quad K_1 = \begin{pmatrix} x_1 & y_1 \\ y_1 & \Phi(x_1,y_1) \end{pmatrix}$$

in the set $\mathcal{S}$. Our goal is to demonstrate that the determinant

$$\det(K_0 - K_1) = (x_0 - x_1)\,(\Phi\,(x_0,y_0) - \Phi\,(x_1,y_1)) - (y_0 - y_1)^2$$

is non-zero.

If x_0 equals x_1, then it follows $y_0 \neq y_1$ and thereby the regularity of the difference $K_0 - K_1$. If the difference $l = x_1 - x_0$ is non-zero, we can assume w.l.o.g. that x_0 is non-zero as well. In case y_0 equals y_1, one computes

$$\det(K_0 - K_1) = -l\,(\Phi\,(x_0,y_0) - \Phi\,(x_0 + l, y_0)) = -l\left(\Psi_{(x_0,y_0,0)}\,(0) - \Psi_{(x_0,y_0,0)}\,(l)\right) \neq 0.$$

If by contrast y_0 differs from y_1, then there is a coefficient $k \in \mathbb{F}_p^\times$ such that we can write $y_1 = y_0 + lk$, since we know $l \neq 0$. The determinant of the difference $K_0 - K_1$ is non-zero in this case as well, as the following calculation shows.

$$-l\left(\Phi\left(x_0, y_0\right) - \Phi\left(x_0 + l, y_0 + lk\right)\right) - l^2k^2 = -l\left(\Psi_{(x_0,y_0,k)}\left(0\right) - \Psi_{(x_0,y_0,k)}\left(l\right)\right) \neq 0.$$

□

It lies at hand that the Latin squares associated with a complete smid family $\mathcal{S}$ in $M_2(\mathbb{F}_p)$ incorporate the information whether $\mathcal{S}$ is an affine linear subspace or not.

Lemma 5.3.18. *We keep all notations of Observation 5.3.17. The following assertions are equivalent.*

(i) The smid family $\mathcal{S}$ is an affine linear subspace.

(ii) The rows and the columns of each of the Latin squares L_k ($k \in \mathbb{F}_p^\times$) are given by affine linear functions.

(iii) There is an index $k_0 \in \mathbb{F}_p^\times$ such that the rows of the Latin square L_{k_0} are given by affine linear functions.

(iv) There is an index $k_0 \in \mathbb{F}_p^\times$ such that the columns of the Latin square L_{k_0} are given by affine linear functions.

Proof. If $\mathcal{S}$ is an affine linear subspace, then the function Φ is affine linear, and thereby also all functions Φ_k defined by equation (5.5). On that account, item (i) implies item (ii), which trivially implies both of the remaining assertions. We demonstrate that each of the latter is a sufficient condition for statement (i).
$\boldsymbol{(iii) \Rightarrow (i)}$. If the rows of L_{k_0} are affine linear functions, then there are, for all $x \in \mathbb{F}_p$, coefficients $s_x \in \mathbb{F}_p$ and $t_x \in \mathbb{F}_p^\times$ such that the entries of the xth row are given by $\Phi_{k_0}(x, y) = s_x + t_x y$ for all $y \in \mathbb{F}_p$. By Definition of the map Φ_{k_0}, this yields the identity

$$\Phi(x + k_0 y, y) = s_x + (t_x + k_0^{-1})y$$

for all $x, y \in \mathbb{F}_p$. For this reason, the smid family $\mathcal{S}$ contains all of the elements

$$\begin{pmatrix} x + k_0 y & y \\ y & s_x + (t_x + k_0^{-1})y \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & s_x \end{pmatrix} + y \begin{pmatrix} k_0 & 1 \\ 1 & t_x + k_0^{-1} \end{pmatrix},$$

and therefore, for all $x \in \mathbb{F}_p$, the affine lines

$$\begin{pmatrix} x & 0 \\ 0 & s_x \end{pmatrix} + \left\langle \begin{pmatrix} k_0 & 1 \\ 1 & t_x + k_0^{-1} \end{pmatrix} \right\rangle.$$

You immediately convince yourself that these affine lines do not intersect. Observation 5.3.2 ensures that they are not skew, hence all of them must be parallel. At this point, Corollary 5.3.11 comes into play, telling us that $\mathcal{S}$ is an affine linear subspace of $M_2(\mathbb{F}_p)$.

***(iv)* ⇒ *(i)*.** In case the *columns* of L_{k_0} are assumed to be affine linear functions, there are coefficients $s_y \in \mathbb{F}_p$ and $t_y \in \mathbb{F}_p^\times$ such that the entries of the yth column are given by $\Phi_{k_0}(x,y) = s_y + t_y x$ for all $x \in \mathbb{F}_p$. Proceeding as above, we use equation (5.5) to compute

$$\Phi(x + k_0 y, y) = s_y + t_y x + k_0^{-1} y,$$

whereby we deduce that $\mathcal{S}$ contains the affine lines

$$\begin{pmatrix} k_0 y & y \\ y & s_y \end{pmatrix} + \left\langle \begin{pmatrix} 1 & 0 \\ 0 & t_y \end{pmatrix} \right\rangle .$$

These affine lines are parallel and pairwise different, whence we conclude as in the previous step that $\mathcal{S}$ is an affine linear subspace. □

Corollary 5.3.19. *All complete smid families in $M_2(\mathbb{F}_3)$ are affine linear subspaces.*

Proof. It suffices to observe that all permutations in S_3 correspond to affine linear mappings. Hence each and every Latin square has affine linear rows and columns. Each complete smid family in $M_2(\mathbb{F}_3)$ must therefore be an affine linear subspace according to Lemma 5.3.18. □

We make the following observation with regard to the Latin squares defined in Observation 5.3.17. The easy proof is left as an exercise to the reader.

Observation 5.3.20. We still keep all notations of Observation 5.3.17. Suppose the smid family $\mathcal{S} \subset M_2(\mathbb{F}_p)$ is linear, say $\mathcal{S} = \mathcal{S}_{q,r}$ for some indices $q \in \mathbb{F}_p^\times$, $r \in \mathbb{F}_p \setminus N_q$. Then the family of Latin squares $\{L_k \mid k \in \mathbb{F}_p^\times\}$ has precisely $|N_q|$ different members, all of which are mutually orthogonal. (For the cardinality of N_q, see the Technical Lemma 5.2.1.)

It did not escape our notice that if $\mathcal{S}_{q,r}$ is a complete linear smid family in $M_2(\mathbb{F}_p)$, as introduced in Definition 5.2.2, then the entries in the lower right corner of its matrices induce a Latin square if r is non-zero (which is, in a way, "missing" in the list $L_1, \ldots, L_{p-1}$). However, we do not see interesting mathematical aspects in this direction.

Summary: Criteria for (non-)linear smid families in $\mathbf{M_2(\mathbb{F}_p)}$

Let us collect the conditions found for the linearity of complete smid families in the matrix algebra $M_2(\mathbb{F}_p)$. Items (ii) to $(viii)$ in the following theorem are labeled with references to the statements which imply their equivalence to item (i).

Theorem 5.3.21 (Criteria for the linearity of smid families in $M_2(\mathbb{F}_p)$)**.** *Let $\mathcal{S} \subset M_2(\mathbb{F}_p)$ be a complete smid family containing the zero matrix, and define the associated Latin squares $L_1, \ldots, L_{p-1}$ as in Observation 5.3.17. The following assertions are equivalent.*

(i) The family $\mathcal{S}$ is a linear subspace of $M_2(\mathbb{F}_p)$.

(ii) The identity $A\mathcal{S}A^T = \mathcal{S}$ holds for a matrix $\mathrm{I}_2 \neq A \in M_2(\mathbb{F}_p)$. (Observation 5.3.3)

(iii) The identity $a\mathcal{S} = \mathcal{S}$ holds for a coefficient $1 \neq a \in \mathbb{F}_p^\times$. (Observation 5.3.3)

(iv) At least $p^2 - p$ elements of $\mathcal{S}$ belong to the same two-dimensional subspace of $M_2(\mathbb{F}_p)$. (Lemma 5.3.6)

(v) There is a symmetric matrix $A \in M_2(\mathbb{F}_p) \setminus \{0\}$ satisfying the identity $\mathcal{S} + A = \mathcal{S}$. (Lemma 5.3.10)

(vi) The family $\mathcal{S}$ is a union of (affine) lines of matrices. (Corollary 5.3.11)

(vii) The group of affine linear transformations $\{T_{A,B,c} \mid T_{A,B,c}(\mathcal{S}) = \mathcal{S}\}$ is not trivial. (Corollary 5.3.12)

(viii) At least one of the Latin squares L_k ($k \in \mathbb{F}_p^\times$) has affine linear rows or affine linear columns. (Lemma 5.3.18)

From Lemma 5.3.18, we moreover obtain the following connection between complete smid families in $M_2(\mathbb{F}_p)$ and Latin squares of order p.

Proposition 5.3.22. *The following assertions are equivalent.*

(i) There is a complete smid family in $M_2(\mathbb{F}_p)$ which is no affine linear subspace.

(ii) For all elements $k_0 \in \mathbb{F}_p^\times$, there is a Latin square $(\Psi_{k_0}(x, y))$ of order p that is not of the "linear type" introduced in Example 5.3.14, such that the matrices

$$\left(\Psi_{k_0}\left(x + sy, y\right) + s\left(sk_0 + k_0^2\right)^{-1} y \right)_{x,y \in \mathbb{F}_p}$$

are Latin squares for all $s \in \mathbb{F}_p \setminus \{-k_0\}$.

Proof. Let $\mathcal{S}$ be a complete smid family in $M_2(\mathbb{F}_p)$. We overtake the notations of Observation 5.3.17 for the proof.

First observe that fixing an index $k_0 \in \mathbb{F}_p^\times$ in equation (5.5), all functions Φ_k $(k \in \mathbb{F}_p^\times)$ can be expressed in the form

$$\Phi_k(x,y) = \Phi_{k_0}(x + (k - k_0)\, y, y) + \left(k_0^{-1} - k^{-1}\right) y \quad (x, y \in \mathbb{F}_p).$$

We set $\Psi_{k_0} = \Phi_{k_0}$ and $s = k - k_0 \neq -k_0$. Then a computation yields the identity

$$\Phi_{k_0+s}(x,y) = \Psi_{k_0}(x + sy, y) + s\left(sk_0 + k_0^2\right)^{-1} y \tag{5.6}$$

for all $x, y \in \mathbb{F}_p$. The functions on either side of this equation induce Latin squares by Observation 5.3.17.

If the smid family $\mathcal{S}$ is no affine linear subspace, then $\Psi_{k_0} = \Phi_{k_0} : \mathbb{F}_p \times \mathbb{F}_p \to \mathbb{F}_p$ is not an affine linear function. Consequently, the Latin square $(\Psi_{k_0}(x,y))$ is not of the "linear type" introduced in Example 5.3.14.

If conversely a family of Latin squares like in item (ii) is given for some $k_0 \in \mathbb{F}_p^\times$, we can regain the functions Φ_k by equation (5.6), and thereby the function Φ, defining a complete smid family, due to equation (5.5). Obviously, this smid family is not (affine) linear. □

In spite of all the collected criteria, we are unable to prove or disprove that all complete smid families in $M_2(\mathbb{F}_p)$ are linear for $p \geq 7$.[*] Even for the case $p = 5$, we have only found a proof based more or less on "brute force": for a start, observe that any complete smid family in $M_2(\mathbb{F}_p)$ w.l.o.g. contains the zero and the unit matrix, or the zero and only such non-zero diagonal matrices which have precisely one diagonal entry being a quadratic residue. This at hand, it is not completely beyond reason to write down the possibly involved permutations (beginning with the diagonal matrices) and exclude non-linear combinations one by one. At the same time, it is not very illustrative either. On that account, we omit this proof and refer the reader to the respective computer algebraic result in the next section instead.

5.4 Smid families in small dimensions—some computer algebraic results

At the beginning of our investigation of smid families, we have used computer algebra to explore the smallest dimensions. We present the results we have obtained this way in this section.

[*] Recall, however, the footnote on page 190.

We have implemented the algorithms for the investigation of smid families in the programming language C. Apart from counting the equivalence classes, they also output the found smid families. The source codes only use the C standard library—in other words, it should be possible to compile and run them on almost every modern computer. However, apart from the smallest dimensions ($p^n \leq 16$), it is inevitable to perform parallel computations in order to come to results within a reasonable length of time.

We have described the functionality of our programs in more detail in the Appendix, see pages 230-233. Feel free to contact us* if you are interested in the source codes.

Complete smid families

As far as complete smid families are concerned, the programs we have developed in the course of our investigations give evidence that these are unique in all matrix algebras $M_n(\mathbb{F}_p)$ where the power p^n is less than 27. The matrix algebra $M_3(\mathbb{F}_3)$ admits two inequivalent complete linear smid families, as we have already mentioned in Section 5.1 (see paragraphs directly before the Facts 5.1.15).

Computer Algebraic Result 5.4.1. *The only prime power p^n ($p \in \mathbb{P}$, $n \in \mathbb{N}$) less than* 32 *which admits inequivalent complete smid families in the matrix algebra $M_n(\mathbb{F}_p)$ is 3^3. There are exactly two inequivalent complete linear smid families inside the matrix algebra $M_3(\mathbb{F}_3)$, namely the linear spans*

$$\mathcal{S}_0 = \left\langle \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \right\rangle$$

$$\textit{and} \quad \mathcal{S}_1 = \left\langle \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix} \right\rangle.$$

The smid family $\mathcal{S}_0$ is an isomorphic representation of the field $\mathbb{F}_{27}$. Being inequivalent to $\mathcal{S}_0$, the family $\mathcal{S}_1$ must be a matrix representation of the Hering plane mentioned directly after the Facts 5.1.15.

* `mail@sebastian-krusekamp.de`

Once the families $\mathcal{S}_0$ and $\mathcal{S}_1$ above are computed, one can verify by hand that the smid family $\mathcal{S}_1$ is inequivalent to any field representation and thus inequivalent to $\mathcal{S}_0$. However, we do not see a way to avoid fairly extensive matrix computations to prove this assertion.

The dimension 7^2 is the largest accessible dimension for our programs, and computer says…

Computer Algebraic Result 5.4.2. *There are no inequivalent complete smid families in the matrix algebra $M_2(\mathbb{F}_7)$.*

Already for the algebras $M_5(\mathbb{F}_2)$ and $M_2(\mathbb{F}_{11})$, we have not come to any useful results.

Smid families of arbitrary length

Our programs also detect non-complete smid families, and are able to count the number of equivalence classes of the latter. Having these data at our disposal for all prime powers $p^n < 32$ (except for the case $p^n = 3^3$, where we have not been able to determine all of the respective values), we would not wish to deprive the reader thereof, in particular since the sequences of numbers may show similarities to other sequences, in combinatorics or elsewhere.

For all prime powers $1 < p^n < 32$, the numbers of inequivalent smid families of length $1 < m \leq p^n$ in the matrix algebras $M_n(\mathbb{F}_p)$ are listed in the tables on the following pages.

Computer Algebraic Result 5.4.3 (Equivalence classes of smid families in small dimensions, $n = 1$)**.** *The following table shows the numbers of inequivalent smid families of length* $2 \leq m \leq p$ *in the prime fields* $\mathbb{F}_p$ *specified in the first row.*

m	$\mathbb{F}_3$	$\mathbb{F}_5$	$\mathbb{F}_7$	$\mathbb{F}_{11}$	$\mathbb{F}_{13}$	$\mathbb{F}_{17}$	$\mathbb{F}_{19}$	$\mathbb{F}_{23}$	$\mathbb{F}_{29}$	$\mathbb{F}_{31}$
2	1	2	1	1	2	2	1	1	2	1
3	1	1	3	2	4	4	5	5	6	8
4		1	1	2	5	8	6	7	19	15
5		1	1	6	7	15	19	34	68	83
6			1	2	10	20	26	57	194	233
7			1	2	7	27	49	143	531	769
8				1	5	34	52	220	1255	1893
9				1	4	27	74	356	2576	4490
10				1	2	20	52	412	4628	8683
11				1	1	15	49	494	7294	15444
12					1	8	26	412	10047	23373
13					1	4	19	356	12171	32054
14						2	6	220	13004	38039
15						1	5	143	12171	40843
16						1	1	57	10047	38039
17						1	1	34	7294	32054
18							1	7	4628	23373
19							1	5	2576	15444
20								1	1255	8683
21								1	531	4490
22								1	194	1893
23								1	68	769
24									19	233
25									6	83
26									2	15
27									1	8
28									1	1
29									1	1
30										1
31										1

Computer Algebraic Result 5.4.4 (Equivalence classes of smid families in small dimensions, $n > 1$)**.** *The following table shows the numbers of inequivalent smid families of length $2 \leq m \leq p^n$ in the matrix algebras $M_n(\mathbb{F}_p)$ specified in the first row. The missing entries for the matrix algebra $M_3(\mathbb{F}_3)$ are due to computational limitations.*

m	$\mathbf{M_2(\mathbb{F}_2)}$	$\mathbf{M_2(\mathbb{F}_3)}$	$\mathbf{M_2(\mathbb{F}_5)}$	$\mathbf{M_3(\mathbb{F}_2)}$	$\mathbf{M_3(\mathbb{F}_3)}$	$\mathbf{M_4(\mathbb{F}_2)}$
2	2	2	2	1	1	2
3	1	5	8	1	8	4
4	1	6	44	2	46	22
5		4	213	1	831	39
6		3	994	1	7911	84
7		2	3560	1	?	65
8		1	9429	1	?	51
9		1	17755		?	11
10			24329		?	8
11			24674		?	4
12			19439		?	3
13			12520		?	1
14			6952		?	1
15			3404		?	1
16			1493		?	1
17			598		?	
18			212		?	
19			77		?	
20			28		?	
21			12		?	
22			3		?	
23			2		?	
24			1		?	
25			1		?	
26					?	
27					2	

Conclusion

Starting from basic geometric and algebraic aspects of quasi-orthogonal masas in complex matrix algebras, we have focussed our attention on nice masa families in the course of the present work. All known constructions of complete sets of quasi-orthogonal masa produce nice families.

On our way, we have introduced normal masa pairs, which are linked to representations of certain group actions and generalise standard masa pairs in a natural way. Each pair of masas in a complete nice family is normal.

We have shown that all complete nice families of masas are encoded by certain sets of symmetric matrices (smid families) with entries from a prime field. Although this result is effectively not new (see Facts 5.1.12), we have established it, at least from our own point of view, in a more elementary fashion compared to the analogue result known before.

So far, so good. But although one may consider the encoding of nice complete masa families by smid families as a satisfactory result to some degree, it is at the same time merely the starting point of another, seemingly much more challenging investigation, namely the classification of (complete) smid families.

This task seems to be related to deep questions both of combinatorial and algebraic nature, as we have tried to outline in the last chapter of this thesis. Let us point out that we are not at all convinced that the picture of smid families is appropriate to tackle the underlying classification problem.

If the classification of nice masa families is already a task presenting extraordinary difficulties, the same holds a fortiori for the complex of questions related to the MUB-Problem. Are there complete families of quasi-orthogonal masas which are *not* nice? In particular, are there complete quasi-orthogonal families in dimensions which are no prime powers? How are geometric or physical concepts like entanglement related to more algebraic structures underlying MUBs? These are only a few of the many open questions in this field.

The study of quasi-orthogonal masas, or MUBs, or unbiased Hadamard matrices, or complementary observables, fuses aspects of algebra, geometry, combinatorics and physics to an exceptional and tantalising degree. After all, research has still just begun in this fascinating area.

Appendix

Proof of Proposition 1.2.4 (page 15)

It is straightforward that every monomial matrix is invertible and that its inverse is monomial as well. Moreover, the identity matrix I_d is of course monomial and so is the product of two monomial matrices. Hence, the set of all monomial matrices in $M_d(\mathbb{C})$ is a subgroup of the general linear group GL_d. It is also clear that a monomial matrix is unitary if and only if all of its non-zero entries have modulus one, and that the set $\mathcal{W}_d$ of all unitary monomial matrices is a subgroup of the unitary group $\mathcal{U}_d$.

We need to check that for $d \geq 2$, the subgroup $\mathcal{W}_d \subset \mathcal{U}_d$ is not normal, i.e. there is a unitary $u \in \mathcal{U}_d$ and a monomial matrix $w \in \mathcal{W}_d$ such that uwu^* does not belong to $\mathcal{W}_d$.

For any fixed dimension $d \geq 2$, one such pair u, w is given by the matrices

$$u = \frac{1}{\sqrt{d}} \left(\zeta_d^{ij}\right)_{0 \leq i,j < d} \in \mathcal{U}_d \quad \text{and} \quad w = \operatorname{diag}(\zeta_d, 1, 1, \ldots, 1) \in \mathcal{W}_d,$$

where $\zeta_d \in \mathbb{T}$ denotes a primitive dth root of unity. In fact, one calculates

$$\begin{aligned} uwu^*\, z_0 = uw \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} z_i &= u \frac{1}{\sqrt{d}} \left(\zeta_d z_0 + \sum_{i=1}^{d-1} z_i \right) \\ &= \frac{1}{d} \left(\zeta_d \sum_{j=0}^{d-1} z_j + \sum_{i=1}^{d-1} \sum_{j=0}^{d-1} \zeta_d^{ij} z_j \right) \\ &= \frac{1}{d} \sum_{j=0}^{d-1} \left(\zeta_d + \sum_{i=1}^{d-1} \zeta_d^{ij} \right) z_j \\ &= \frac{1}{d} \sum_{j=0}^{d-1} \left(\zeta_d - 1 + \sum_{i=0}^{d-1} \zeta_d^{ij} \right) z_j \\ &= \frac{1}{d} (\zeta_d - 1 + d) z_0 + \frac{1}{d} \sum_{j=1}^{d-1} (\zeta_d - 1)\, z_j. \end{aligned}$$

The last term is clearly not a vector of the standard basis $\mathfrak{e}$, so that uwu^* is not a monomial unitary matrix; our proof is complete. □

Proof of Lemma 1.2.5 (page 15)

Let $\phi : \mathcal{D}_d \to \mathcal{D}_d$ be a *-automorphism, moreover define minimal projections

$$q_i = \operatorname{diag}(0, \ldots, 0, \underset{\substack{| \\ (i\text{th pos.})}}{1}, 0, \ldots, 0) \in \mathcal{D}_d$$

for all $0 \le i < d$. Since ϕ is a *-automorphism, the images $\phi(q_0), \ldots, \phi(q_{d-1})$ are projections as well, and also pairwise orthogonal like the projections $q_0, \ldots, q_{d-1}$. Now d pairwise orthogonal (non-zero) diagonal projections must be minimal, and the only minimal diagonal projections are $q_0, \ldots, q_{d-1}$.

There is thus a mapping $\sigma : \{0, \ldots, d-1\} \to \{0, \ldots, d-1\}$ such that ϕ acts by

$$\phi(q_i) = q_{\sigma(i)}$$

for all $0 \le i < d$, and the injectivity of ϕ ensures that σ is a permutation. Defining the permutation matrix w_σ as before, we get

$$w_\sigma q_{i_0} w_\sigma^* \, z_i = w_\sigma q_{i_0} \, z_{\sigma^{-1}(i)} = \left\{ \begin{array}{ll} z_{\sigma(i_0)} & \text{if } i_0 = \sigma^{-1}(i) \\ 0 & \text{else} \end{array} \right\} = q_{\sigma(i_0)} \, z_i = \phi(q_{i_0}) \, z_i$$

for all indices $i_0, i \in \{0, \ldots, d-1\}$. This shows the first part of our assertion.

The implication "$\Leftarrow$" of the stated equivalence relation is straightforward. For the converse implication, first observe that for any unitary $u \in \mathcal{U}_d$ fulfilling $u\mathcal{D}_d u^* = \mathcal{D}_d$, the mapping

$$\mathcal{D}_d \ni a \mapsto uau^* \in \mathcal{D}_d$$

is a *-automorphism. According to the first part of the lemma, there is thus a permutation matrix $w \in \mathcal{W}_d$ such that

$$uau^* = waw^* \ \text{ for all } a \in \mathcal{D}_d.$$

In order to prove that u is monomial, let us denote the orthonormal basis given by the columns of u by $\mathfrak{a} = (x_0, \ldots, x_{d-1})$. We have to show that the basis $\mathfrak{a}$ is—up to order and phase factors—the same as the standard basis $\mathfrak{e} = (z_0, \ldots, z_{d-1})$. To this aim, let us fix an index $0 \le i_0 < d$ and represent the vector z_{i_0} with respect to the orthonormal basis $\mathfrak{a}$:

$$z_{i_0} = \sum_{j=0}^{d-1} \lambda_j x_j$$

For a diagonal matrix $a = \operatorname{diag}(\mu_0, \ldots, \mu_{d-1})$, one computes

$$\begin{aligned} uau^* \, z_{i_0} &= ua \sum_{j=0}^{d-1} \lambda_j u^* \, x_j \\ &= u \sum_{j=0}^{d-1} \lambda_j a \, z_j = u \sum_{j=0}^{d-1} \lambda_j \mu_j z_j = \sum_{j=0}^{d-1} \lambda_j \mu_j x_j \end{aligned}$$

By assumption, we have $uau^* z_{i_0} = waw^* z_{i_0} = \mu_{\sigma^{-1}(i_0)} z_{i_0}$, where $\sigma \in S_d$ denotes the permutation associated with w. Writing $x \sim y$ for linear dependent vectors x, y in the Hilbert space $\mathbb{C}^d$, we hence get

$$uau^* z_{i_0} = \sum_{j=0}^{d-1} \lambda_j \mu_j x_j \sim z_{i_0}.$$

Suppose that two of the coefficients in the representation of z_{i_0} were non-zero, say λ_{j_1} and λ_{j_2}, where $j_1 \neq j_2$. Then, comparing the equation above for $a = q_{j_1}$ and $a = q_{j_2}$, we would end up with

$$\lambda_{j_1} x_{j_1} \sim z_{j_0} \sim \lambda_{j_2} x_{j_2}.$$

This would of course contradict the linear independence of x_{j_1} and x_{j_2}, so that only *one* of the coefficients $\lambda_0, \ldots, \lambda_{d-1}$ can be non-zero. Therefore z_{i_0} is a non-zero multiple of one basis element of $\mathfrak{a}$. Applying the same argumentation for the remaining basis vectors of $\mathfrak{e}$, we see that the bases $\mathfrak{e}$ and $\mathfrak{a}$ coincide up to order and phase factors, which implies $u \in \mathcal{W}_d$. □

Proof of Proposition 1.4.6 (page 26)

First observe that we automatically have $n \leq d$, because the powers $v, v^2, \ldots, v^n$ are pairwise orthogonal by assumption and span the abelian *-algebra generated by v.

Let $w \in \mathcal{D}_d$ be a diagonalisation of v, i.e. we have $v = uwu^*$ for a unitary matrix $u \in \mathcal{U}_d$. Then we deduce from $w^n = v^n = \mathrm{I}_d$ that all (diagonal) entries of the unitary w are nth roots of unity. There is hence a primitive nth root of unity $\zeta_n \in \mathbb{T}$ and indices $i_0, \ldots, i_{d-1} \in \{0, \ldots, n-1\}$ such that the matrix w equals $\mathrm{diag}(\zeta_n^{i_0}, \ldots, \zeta_n^{i_{d-1}})$.

For all $1 \leq k < n$, the trace of the power w^k equals zero:

$$0 = \tau(v^k) = \tau(w^k) = \frac{1}{d} \sum_{l=0}^{d-1} \zeta_n^{i_l k}$$

Let $\eta_l \in \mathbb{N}_0$ denote the number of occurrences of the power ζ_n^l in the diagonal of w for all $0 \leq l < n$. From the equation above, we get

$$\sum_{l=0}^{\mathbf{n}-1} \eta_l \zeta_n^{lk} = 0 \text{ for all } 1 \leq k < n.$$

Our goal is to show that all of the numbers $\eta_0, \ldots, \eta_{n-1}$ coincide, implying $\eta_0 \cdot n = d$ (because obviously the sum $\eta_0 + \ldots + \eta_{n-1}$ equals d).

Fix an exponent $0 \leq s < n$ and set $\tilde{w} = \zeta_n^s w$. The powers $\tilde{w}, \ldots, \tilde{w}^{n-1}$ are of course trace-free as well, so that we end up with the equations

$$\sum_{l=0}^{n-1} \eta_l \zeta_n^{k(l+s)} = 0 \text{ for all } 1 \leq k < n \tag{A.7}$$

Let $\mathbb{Z}[X]$ be the polynomial ring over the integers and define polynomials

$$p_s(X) = \sum_{l=0}^{n-1} \eta_l X^{[l+s]} \in \mathbb{Z}[X]$$

for all $0 \leq s < n$. Here $[l+s]$ stands for the (unique) representative of $l+s \mod n$ in $\{0, \dots, n-1\}$ for the moment, so that each of the polynomials p_s is of degree at most $n-1$. Actually each polynomial p_s *is* of degree $n-1$, because it has $n-1$ different zeros in the complex numbers due to equation (A.7), namely

$$p_s(\zeta_n) = p_s(\zeta_n^2) = \dots = p_s(\zeta_n^{n-1}) = 0.$$

Now let $\zeta_n^{l_0}$ denote a power of ζ_n having a minimal number of occurrences in w, that is

$$\eta_{l_0} = \min\{\eta_0, \dots, \eta_n\},$$

and denote polynomials

$$q_s(X) = \sum_{l=0}^{n-1} (\eta_l - \eta_{l_0}) X^{[l+s]} \in \mathbb{Z}[X]$$

for $0 \leq s < n$. These polynomials also have zeros in $\zeta_n, \dots, \zeta_n^{n-1} \in \mathbb{T}$. In fact, one computes

$$q_s(\zeta_n^k) = \sum_{l=0}^{n-1} (\eta_l - \eta_{l_0}) \zeta_n^{k(l+s)} = p_s(\zeta_n^k) - \eta_{l_0} \underbrace{\sum_{l=0}^{n-1} \zeta_n^{k(l+s)}}_{=0} = 0$$

for all $1 \leq k < n$. In particular, the polynomial q_{n-l_0-1} has $n-1$ complex zeros, although its degree is at most $n-2$, as the following computation demonstrates.

$$\begin{aligned} q_{n-l_0-1}(X) &= \sum_{l=0}^{n-1} (\eta_l - \eta_{l_0}) X^{[l+n-l_0-1]} \\ &= \sum_{l \neq l_0} \underbrace{(\eta_l - \eta_{l_0}) X^{[l+n-l_0-1]}}_{\text{terms of degree } 0,\dots,n-2} + (\eta_{l_0} - \eta_{l_0}) X^{n-1} \end{aligned}$$

It follows that $q_{n-l_0-1} \in \mathbb{Z}[X]$ equals zero and hence $\eta_0 = \dots = \eta_{n-1}$. This implies $n \cdot \eta_0 = d$ and completes our proof. □

Proof of Technical Lemma 2.3.2 (page 45)

We will apply the *method of Lagrange multipliers* to determine the extrema of the function f_d. Before all, we therefore recall this method in a simplified form, which is convenient for our purposes. It predicts, to a certain extend, possible extremal points of a real-valued function in several real variables, when restricted to a generalised contour line (i.e. a manifold) given by another function. Verifications of the following theorem can be found in many introductory textbooks on (multivariable) analysis.

Lagrange Multiplier Theorem. *For $d \in \mathbb{N}$, consider functions $g, r : \mathbb{R}^d \to \mathbb{R}$ having continuous first partial derivates, and define a set*

$$R = \left\{ t \in \mathbb{R}^d \,\middle|\, r(t) = 0 \right\} \subset \mathbb{R}^d$$

We say that g has a constrained local maximum *in a point $t_0 \in R$ if there is some $\delta > 0$ such that $g(t) \leq g(t_0)$ for all $t \in R$ fulfilling $\|t - t_0\| < \delta$. A constrained local minimum is defined analogously.*

If g has a constrained local extremum in a point $t_0 \in R$, and the gradient $\nabla r(t_0)$ is not zero, then there is a coefficient $\lambda \in \mathbb{R}$ such that

$$\nabla g(t_0) = \lambda \nabla r(t_0). \tag{A.8}$$

For our purposes, we declare the functions $g, r : \mathbb{R}^d \to \mathbb{R}$ in the theorem above as follows.

$$g : (t_j) \longmapsto \sum_{j=0}^{d-1} t_j^4 \qquad\qquad r : (t_j) \longmapsto \sum_{j=0}^{d-1} t_j^2 - 1$$

These functions meet the conditions of the Lagrange Multiplier Theorem, and the zero set R of the function r is the unit sphere S^{d-1}. By definition, the function f declared in our assertion is the restriction of g to the unit sphere, so that the local extrema of f are precisely the constrained local extrema of g on $R = S^{d-1}$. Since the unit sphere is compact, we moreover know that f *attains* its maximum and minimum on S^{d-1}, so that its global extrema are at the same time local. Our aim is thus to determine the least and the largest constrained extrema of g on R.

The gradient of r does not vanish on the unit sphere, because assuming that

$$\frac{\partial g}{\partial t_j} = 2t_j = 0$$

for all $0 \leq j < d$ contradicts the condition $g((t_0, \ldots, t_{d-1})^T) = 0$. Therefore the Lagrange Multiplier Theorem tells us that constrained local extrema of g can only lie at points $t = (t_0, \ldots, t_{d-1})^T \in S^{d-1}$ satisfying equation (A.8), which holds true if and only if

$$t_j^3 = \frac{\lambda}{2} t_j \quad \text{for all } 0 \leq j < d.$$

Accordingly, each component t_j equals either zero or $\sqrt{{}^{\lambda}/_{2}}$ (in particular, we get $\lambda \geq 0$). From the equation $r(t) = 0$, we deduce that the number n of components t_j being nonzero is at least one, moreover the multiplier λ equals ${}^{2}/_{n}$. The value of g at such a point t then computes to $g(t) = n({}^{\lambda}/_{2})^2 = {}^{1}/_{n}$ for $0 < n \leq d$. The global maximum of g and hence f on S^{d-1} thereby equals 1, and the minimum ${}^{1}/_{d}$. The former is attained if and only if $n = 1$, the latter if and only if $n = d$. It is straightforward that these global extrema lie precisely at the asserted points, so that our proof is complete. □

Sketch of the proof of Proposition 2.4.10 (page 62)

It is straightforward to prove that the commuting unitaries

$$v_0 = \mathrm{X}_a \otimes \mathrm{I}_b \quad \text{and} \quad v_1 = \mathrm{I}_a \otimes \mathrm{X}_b$$

generate a masa $\mathcal{M} = \mathcal{A}^*(v_0, v_1) \subset M_d(\mathbb{C})$ which is quasi-orthogonal to the diagonal masa $\mathcal{D}_d$. The unitary Hadamard matrix $h \in \mathcal{U}_d$ associated with $\mathcal{M} = \mathcal{M}_{[h]}$ is given by

$$h = \mathrm{F}_a \otimes \mathrm{F}_b = \sqrt{\frac{1}{b}} \begin{pmatrix} \mathrm{F}_a & \mathrm{F}_a & \mathrm{F}_a & \cdots & \mathrm{F}_a \\ \mathrm{F}_a & \zeta_b^1 \mathrm{F}_a & \zeta_b^2 \mathrm{F}_a & \cdots & \zeta_b^{b-1} \mathrm{F}_a \\ \mathrm{F}_a & \zeta_b^2 \mathrm{F}_a & \zeta_b^4 \mathrm{F}_a & \cdots & \zeta_b^{2(b-1)} \mathrm{F}_a \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathrm{F}_a & \zeta_b^{b-1} \mathrm{F}_a & \zeta_b^{2(b-1)} \mathrm{F}_a & \cdots & \zeta_b^{(b-1)(b-1)} \mathrm{F}_a \end{pmatrix} \in M_d(\mathbb{C}),$$

which is a direct consequence of Example 2.2.9.

For every $\lambda \in \mathbb{T}$, we define a matrix $\mathrm{F}_a[\lambda] = \mathrm{F}_a \operatorname{diag}(\lambda, 1, \dots,, 1) \in M_a(\mathbb{C})$, and thereby

$$h_\lambda = \sqrt{\frac{1}{b}} \begin{pmatrix} \mathrm{F}_a[\lambda] & \mathrm{F}_a[\lambda] & \mathrm{F}_a[\lambda] & \cdots & \mathrm{F}_a[\lambda] \\ \mathrm{F}_a & \zeta_b^1 \mathrm{F}_a & \zeta_b^2 \mathrm{F}_a & \cdots & \zeta_b^{b-1} \mathrm{F}_a \\ \mathrm{F}_a & \zeta_b^2 \mathrm{F}_a & \zeta_b^4 \mathrm{F}_a & \cdots & \zeta_b^{2(b-1)} \mathrm{F}_a \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathrm{F}_a & \zeta_b^{b-1} \mathrm{F}_a & \zeta_b^{2(b-1)} \mathrm{F}_a & \cdots & \zeta_b^{(b-1)(b-1)} \mathrm{F}_a \end{pmatrix}.$$

It goes without saying that the matrices h_λ are still Hadamard matrices for all indices $\lambda \in \mathbb{T}$. Moreover, you immediately convince yourself that they are unitaries. Our goal is to show that there is an uncountable subset I of the unit circle $\mathbb{T}$ such that

$$h_{\lambda_0} \not\sim h_{\lambda_1} \quad \text{and } h_{\lambda_0} \not\sim h_{\lambda_1}^*$$

whenever $\lambda_0 \neq \lambda_1$ for elements $\lambda_0, \lambda_1 \in I$. The associated pairs $\{\mathcal{D}_d, h_{\lambda_0} \mathcal{D}_d h_{\lambda_0}^*\}$ and $\{\mathcal{D}_d, h_{\lambda_1} \mathcal{D}_d h_{\lambda_1}^*\}$ of quasi-orthogonal masas are then inequivalent according to Lemma 2.4.2.

Let $Z_d \subset \mathbb{T}$ denote the set of all dth roots of unity and let $\emptyset \neq I \subset \mathbb{T}$ be a segment of the unit circle which contains *no* dth root of unity and has the following property: if $\lambda_0 \neq \lambda_1$ holds for $\lambda_0, \lambda_1 \in I$, then the products $\lambda_0\lambda_1$ and $\bar{\lambda}_0\lambda_1$ are no dth roots of unity either. (For instance, take the open subset $\{\exp(\mathrm{i}\lambda) \mid \lambda \in (0, {}^{\pi}\!/\!{}_{d})\} \subset \mathbb{T}$.)

Pick two elements $\lambda_0, \lambda_1 \in I$ and suppose the associated Hadamard matrices are equivalent. We write this in the form

$$h_{\lambda_1} = \underbrace{\operatorname{diag}(\rho_0, \ldots, \rho_{d-1})}_{=:r} w h_{\lambda_0} w' \underbrace{\operatorname{diag}(\gamma_0, \ldots, \gamma_{d-1})}_{=:c} \tag{A.9}$$

for unweighted monomial unitaries $w, w' \in \mathcal{W}_d$ and weights $\rho_i, \gamma_i \in \mathbb{T}$ $(0 \leq i < d)$.

The rest of the proof is a matter of pure (and rather lengthy) computations. A careful comparison of the columns and rows of the matrix equation (A.9) reveals that no matter which permutations are performed by the matrices $w, w' \in \mathcal{W}_d$, one always ends up in a contradiction. The same holds true if one replaces the matrix h_{λ_1} by its adjoint $h^*_{\lambda_1}$.

Concretely, once the weights γ_i and ρ_i are adjusted to fulfil the equations imposed for a certain column in equation (A.9), one always finds a row in the same matrix equation which can not be satisfied, simply because there are always some coefficient equations where one side belongs to the set Z_d while the other does not. The details are left to the reader. □

Proof of Corollary 3.2.6 (page 82)

Let $d = \prod_{k=0}^{m} p_k$ be the prime factorisation of the dimension d ($m \in \mathbb{N}_0, p_k \in \mathbb{P}$ for all $0 \leq k \leq m$), where we assume $p_0 \leq p_1 \leq \ldots \leq p_m$. Further let

$$\left\{\mathcal{D}_{p_k}, \mathcal{M}_0^{(k)}, \ldots, \mathcal{M}_{p_k-1}^{(k)}\right\}$$

denote the standard masa family inside the matrix algebra $M_{p_k}(\mathbb{C})$ for each $0 \leq k \leq m$. Since p_0 is a minimal prime factor of d, each of these families contains at least $p_0 + 1$ members, so we can define *-subalgebras

$$\mathcal{N}_i = \mathcal{M}_i^{[0]} \otimes \mathcal{M}_i^{[1]} \otimes \cdots \otimes \mathcal{M}_i^{[m]} \subset \bigotimes_{k=0}^{m} M_{p_k}(\mathbb{C}) \cong M_d(\mathbb{C})$$

for $0 \leq i \leq p_0 - 1$. The $\mathcal{N}_i$ are commutative and hence masas by dimension.

Recall that the (normalised) trace $\tau : M_d(\mathbb{C}) \to \mathbb{C}$ factorises w.r.t. the tensor product: if $\tau^{(k)}$ designates the normalised trace on $M_{p_k}(\mathbb{C})$ and $a_k \in M_{p_k}(\mathbb{C})$ are any matrices for all $0 \leq k \leq m$, one computes

$$\tau(a_0 \otimes \cdots \otimes a_m) = \prod_{k=0}^{m} \tau^{(k)}(a_k).$$

The quasi-orthogonality of two masas $\mathcal{N}_i$, $\mathcal{N}_j$ ($i \neq j$) thereby follows directly from the quasi-orthogonalities

$$\mathcal{M}_i^{(0)} \perp_q \mathcal{M}_j^{(0)}, \ldots, \mathcal{M}_i^{(m)} \perp_q \mathcal{M}_j^{(m)}.$$

The same argument shows that each of the masas $\mathcal{N}_i$ ($0 \leq i \leq p_0 - 1$) is quasi-orthogonal to the diagonal masa $\mathcal{D}_d = \bigotimes_{k=0}^{m} \mathcal{D}_{p_k}$. □

Proof of Examples 3.2.10 (b) (page 84)

Let us start with an unspecified subfamily $\{\mathcal{M}_{k_0}, \mathcal{M}_{k_1}, \mathcal{M}_{k_2}\}$ of the standard family in $M_{13}(\mathbb{C})$ which is equivalent to $\mathscr{F}_1$ via a *-automorphism ϕ. Using arguments from part (a), we can then find a second *-automorphism ψ such that we get the following diagram.

$$\begin{tikzcd}
\mathcal{D}_{13} \arrow[d, "\phi"] \arrow[dd, bend right=60, "w \cdot w^*"'] & \mathcal{M}_0 \arrow[d, "\phi"] \arrow[dd, bend right=60, "w \cdot w^*"'] & \mathcal{M}_1 \arrow[d, "\phi"] \arrow[dd, bend right=60, "w \cdot w^*"'] \\
\mathcal{M}_{k_0} \arrow[d, "\psi"] & \mathcal{M}_{k_1} \arrow[d, "\psi"] & \mathcal{M}_{k_2} \arrow[d, "\psi"] \\
\mathcal{D}_{13} & \mathcal{M}_{k_1 - k_0} & \mathcal{M}_{k_2 - k_0}
\end{tikzcd} \tag{A.10}$$

(Note that this is also ensured if $\mathcal{M}_{k_0} = \mathcal{M}_{13} = \mathcal{D}_{13}$, since ψ is the identity in in this case and we understand the subscripts $k_1 - k_0, k_2 - k_0$ modulo 13.) Similarly as in part (a), the first two columns of this diagram permit to conclude that the monomial w acts (up to a scalar) by

$$w\, z_i = \mu^i \zeta_{13}^{ks \sum_{t=0}^{i-1}(m+it)} z_{m+ik}$$

on the standard orthonormal basis of the Hilbert space $\mathbb{C}^{13}$ ($0 \leq i \leq 12$), where we set $k = k_1 - k_0$ and $m, s \in \mathbb{Z}, \mu \in \mathbb{T}$ are constants. According to diagram (A.10), conjugation by w maps $\mathcal{M}_1$ to $\mathcal{M}_l$, where we set $l = k_2 - k_0$. Again the same argumentation as in part (a)—adjusting the dimension and replacing $\tilde{w}$ by z_{13}, i.e. setting $\rho(i) = i$ in equation (3.5)—shows that there is a constant $n \in \mathbb{Z}$ such that $\zeta_{13}^{i+ks^2 i} = \zeta_{13}^{ls^2 i + n}$ for all $0 \leq i \leq 12$. As a consequence, we get

$$i\left(1 + (k-l)s^2\right) \equiv n \mod 13$$

for all $0 \leq i \leq 12$, which implies $n \equiv 0 \mod 13$ and thus

$$(k-l)s^2 \equiv (k_1 - k_2)s^2 \equiv -1 \mod 13.$$

For this reason, the difference $k_2 - k_1$ is a *quadratic residue* modulo 13.

As a matter of fact, the set of indices $\{0,2,7\}$ of the masa family $\mathscr{F}_2$ admits no differences which are quadratic residues modulo 13: one computes

$$\{k_2 - k_1 \bmod 13 \mid k_1, k_2 \in \{0,2,7\}, k_1 \neq k_2\} = \{2,5,6,7,8,11\},$$

whereas the non-zero quadratic residues modulo 13 are precisely $1,3,4,9,10,12$.

Consequently, a *-automorphism ϕ like in diagram (A.10) cannot exist for any tuple (k_0, k_1, k_2) of (pairwise different) indices taken from the set $\{0,2,7\}$. □

Proof of Proposition 3.2.13 (page 88)

Fix a Hilbert-Schmidt orthonormal basis $(b_0^{(k)}, \dots, b_{d-1}^{(k)})$ for each masa $\mathcal{M}_k$ $(0 \leq k < d)$, where $b_0^{(k)} = \mathrm{I}_d$. The orthonormal system

$$(\mathrm{I}_d, b_1^{(0)}, \dots, b_{d-1}^{(0)}, b_1^{(1)}, \dots, b_{d-1}^{(1)}, \dots, b_{d-1}^{(d-1)})$$

contains $1 + d(d-1) = d^2 - (d-1)$ elements. It can hence be extended to an orthonormal basis of the Hilbert space $M_d(\mathbb{C})$ by another orthonormal system $(c_1, \dots, c_{d-1})$ of length $d-1$. For convenience, we set $c_0 = \mathrm{I}_d$. Our goal is to show that the subspace $\mathcal{N} = \langle c_0, \dots, c_{d-1} \rangle$ of $M_d(\mathbb{C})$ is a masa.

First we combine two results of Section 2.2: Proposition 2.2.12 tells us that the projection on each masa $\mathcal{M}_k$ equals the *conditional expectation* given by

$$\mathcal{P}_{\mathcal{M}_k}(a) = \mathcal{E}_{\mathcal{M}_k}(a) = \frac{1}{d} \sum_{i=0}^{d-1} b_i^{(k)} a (b_i^{(k)})^*$$

for all $a \in M_d(\mathbb{C})$. Furthermore, the conditional expectation of the line $\mathbb{C} \cdot \mathrm{I}_d$ is given by

$$\mathcal{E}_{\mathbb{C}\cdot \mathrm{I}_d}(a) = \tau(a)\mathrm{I}_d = \frac{1}{d^2} \left(\sum_{k=0}^{d-1} \sum_{i=\mathbf{1}}^{d-1} b_i^{(k)} a (b_i^{(k)})^* + \sum_{i=0}^{d-1} c_i a c_i^* \right)$$

according to Fact 2.2.13. From these formulas, we deduce for the projection onto the subspace $\mathcal{N} = \langle c_0, \dots, c_{d-1} \rangle$:

$$\begin{aligned} \mathcal{P}_{\mathcal{N}}(a) &= a - \sum_{k=0}^{d-1} \overbrace{\mathcal{P}_{\mathcal{M}_k \ominus \mathbb{C}\cdot \mathrm{I}_d}(a)}^{=\mathcal{E}_{\mathcal{M}_k}(a) - (a \,|\, \mathrm{I}_d)\mathrm{I}_d} \\ &= a - \frac{1}{d} \sum_{k=0}^{d-1} \sum_{i=0}^{d-1} b_i^{(k)} a (b_i^{(k)})^* + d\tau(a)\mathrm{I}_d \\ &= -\underbrace{\frac{1}{d} \sum_{k=0}^{d-1} \sum_{i=\mathbf{1}}^{d-1} b_i^{(k)} a (b_i^{(k)})^*}_{=d\tau(a)\mathrm{I}_d - \frac{1}{d}\sum_{i=0}^{d-1} c_i a c_i^*} + d\tau(a)\mathrm{I}_d \end{aligned}$$

$$\Rightarrow \quad \mathcal{P}_{\mathcal{N}}(a) = \frac{1}{d} \sum_{i=0}^{d-1} c_i a c_i^* \ \text{ for all } \ a \in M_d(\mathbb{C}) \tag{A.11}$$

In the second part of the proof, we demonstrate that the equation above implies that the subspace $\mathcal{N}$ is a masa. This is precisely the converse of Proposition 2.2.12. To this aim, it suffices to prove that all elements inside $\mathcal{N}$ commute (since thereby $\mathcal{N}$ can be diagonalised; by dimension, it is thus isomorphic to the diagonal masa $\mathcal{D}_d$).

It is no loss of generality to assume that all elements $c_0, \ldots, c_{d-1}$ are *self-adjoint*: recall that the set of self-adjoint matrices $\mathcal{S}(M_d(\mathbb{C})) \subset M_d(\mathbb{C})$ is a real vector space of dimension d^2, inheriting the Hilbert-Schmidt scalar product. The self-adjoint part of a masa $\mathcal{M} \subset M_d(\mathbb{C})$ is clearly a d-dimensional real subspace in $\mathcal{S}(M_d(\mathbb{C}))$. By construction, this carries over to the real part $\mathcal{S}(\mathcal{N})$ of the subspace $\mathcal{N}$, and any orthonormal basis of self-adjoints for $\mathcal{S}(\mathcal{N})$ is then also a basis for $\mathcal{N}$.

It is furthermore enough to demonstrate that a *positive* element $a \in \mathcal{N}$ (i.e. a positive semidefinite matrix, $\operatorname{sp}(a) \subset \mathbb{R}_0^+$) commutes with all generators $c_0, \ldots, c_{d-1}$: once this is shown, fix an index $0 \leq i_0 < d$ and consider the positive matrix $a = c_{i_0} + \mu_{i_0} \mathrm{I}_d$ in $\mathcal{N}$, where $\mu_{i_0} \in \mathbb{R}$ denotes the smallest spectral value of c_{i_0}. Since a commutes with all elements $c_0, \ldots, c_{d-1}$, so does c_{i_0}, and consequently $\mathcal{N}$ is generated by commuting matrices.

So let $a \in \mathcal{N}$ be a positive element, $0 \leq \lambda_0 < \ldots < \lambda_{n-1}$ the different spectral values of a and $p_0, \ldots, p_{n-1} \in M_d(\mathbb{C})$ the associated spectral projections ($n \leq d$).

Clearly the matrix $a_0 = a - \lambda_0 \mathrm{I}_d \in \mathcal{N}$ is still positive. By equation (A.11), we can write

$$a_0 = \frac{1}{d} \sum_{i=0}^{d-1} c_i a_0 c_i .$$

It is elementary that all summands $c_i a_0 c_i$ are positive as well. Recall the assertions

$$\begin{aligned} &\ker(g+h) = ker(g) \cap \ker(h) \\ &(gx \,|\, x) = 0 \quad \Leftrightarrow \quad x \in \ker(g) \quad (x \in \mathbb{C}^d) \end{aligned}$$

for positive matrices $g, h \in M_d(\mathbb{C})$. Thereby we deduce

$$x \in \ker(a_0) \quad \Rightarrow \quad x \in \ker(c_i a_0 c_i) \quad \Rightarrow \quad (a_0 c_i x \,|\, c_i x) = 0 \quad \Rightarrow \quad c_i \, x \in \ker(a_0)$$

for all vectors $x \in \mathbb{C}^d$ and all $0 \leq i < d$. This gives us

$$\begin{aligned} c_i \, x = c_i p_0 \, x &= p_0 c_i p_0 \, x \quad \text{if } x \in \ker(a_0) \text{ and hence } c_i \, x \in \ker(a_0), \\ \text{and} \quad 0 = c_i p_0 \, x &= p_0 c_i p_0 \, x \quad \text{if } x \in (\ker(a_0))^{\perp} . \end{aligned}$$

As a consequence, the projection p_0 commutes with all matrices c_i, where i ranges from 0 to $d-1$ ($p_0 c_i = (c_i p_0)^* = (p_0 c_i p_0)^* = p_0 c_i p_0 = c_i p_0$), and furthermore we get

$$\mathcal{P}_{\mathcal{N}}(p_0) = \frac{1}{d}\sum_{i=0}^{d-1} c_i p_0 c_i = \frac{1}{d}\sum_{i=0}^{d-1} c_i^2\, p_0 = \mathcal{P}_{\mathcal{N}}(\mathrm{I}_d)\, p_0 = p_0.$$

Since p_0 belongs to $\mathcal{N}$, so does the matrix $a_1 = a - \lambda_1(p_0 - \mathrm{I}_d)$. Moreover, a_1 is still positive and the projection onto the kernel of a_1 is p_1. By the same argumentation as before, p_1 commutes with all generators c_i and is an element of $\mathcal{N}$. One proves by induction ($a_m = a - \lambda_m(\sum_{i=0}^{m-1} p_i - \mathrm{I}_d)$) that all spectral projections of a commute with $c_0, \ldots, c_{d-1}$, so that the same applies for the matrix a itself. □

Proof of Theorem 4.1.2, implication "⇒" (page 117)

We recall that a unitary representation $\pi : H \to M_d(\mathbb{C})$ is called irreducible if the only subspaces of $\mathbb{C}^d$ which are invariant under all unitaries $\pi(g), g \in G$ are $\mathbb{C}^d$ and $\{0\}$. With a unitary representation π, one associates a character $\chi : H \to \mathbb{T}$ via the formula $\chi(g) = \tau(\pi(g))$ and calls d the degree of χ. Such a character is called irreducible if and only if π is irreducible. Irreducible representations are isomorphic if and only if they induce the same character, so that conversely each irreducible character of degree d determines an irreducible representation in $\mathcal{U}_d$ up to an isomorphism.

By these facts, it is clear how to find a character of the proposed type for an abstract error group H. By assumption, H is isomorphic to a concrete error group H' of $\mathcal{U}_d$. The respective isomorphism π is an irreducible faithful representation of H (since the members of H' span $M_d(\mathbb{C})$, there is no non-trivial invariant subspace), hence the map $\chi : H \to \mathbb{T}$, defined by $\chi(h) = \tau(\pi(h)), h \in H$, is an irreducible character with trivial kernel. By definition of an error group, the centre of H' consists precisely of the contained multiples of I_d and coincides with the support of τ in H'.

For the converse implication of Theorem 4.1.2, we refer the reader to [61]. □

Proof of Observation 4.3.3 (page 135)

Recall that the mapping $\rho : G \to \mathcal{PU}_d$, $g \mapsto [u_g]$, defines an injective projective representation of G (cf. Observation 4.1.9).

Fix an index $0 \leq k \leq n$. Since $u_e \sim \mathrm{I}_d$ belongs to E_k, the unit element $e \in G$ lies in H_k. For any $g \in H_k$, the masa $\mathcal{M}_k$ generated by E_k does not only contain u_g, but clearly also u_g^*. As we have already seen earlier, the identity $[u_g][u_g^*] = [u_g^*][u_g] = [u_e]$ implies $u_g^* \sim_{\mathbb{T}} u_{g^{-1}}$, so $u_{g^{-1}}$ belongs to $\mathcal{M}_k$ as well. We thus get $g^{-1} \in H_k$, so H_k is closed under taking inverses.

Given two elements $g, h \in H_k$, the respective unitaries u_g, u_h belong to the masa $\mathcal{M}_k$. Consequently, the same applies for the product $u_g u_h$, hence also for $u_{gh} \sim_{\mathbb{T}} u_g u_h$. This yields $u_{gh} \in E_K$ and thus $gh \in H_k$, so H_k is closed under the group operation of G.

The unitaries u_g, u_h commute as elements of the same masa $\mathcal{M}_k$. This carries over to their cosets in $\mathcal{PU}_d$, and since ρ is a group homomorphism, we have

$$\rho(gh) = \rho(g)\rho(h) = [u_g][u_h] = [u_h][u_g] = \rho(hg).$$

The injectivity of ρ thereby implies $gh = hg$, hence H_k is commutative. The rest of the proof is straightforward.

An alternative verification of Observation 4.3.3 can be found in [3, lemma 4]. □

Proof of Lemma 5.3.6 (page 194)

We have already seen that for $p = 2$, there is exactly one complete smid family (cf. Example 5.1.3 (ii)), so there is nothing to show in this case. We therefore assume $p > 2$ in the sequel.

(i) First recall that according to Observation 5.3.4, there is a set $I \in \mathbb{F}_p^2$, and injective mappings $\phi_y : I_y \to \mathbb{F}_p$ for all non-empty sets $I_y = \{x \in \mathbb{F}_p \mid (x, y) \in I\}$ so that we can write

$$\mathcal{S} = \left\{ \begin{pmatrix} x & y \\ y & \phi_y(x) \end{pmatrix} \middle| \, (x, y) \in I \right\}.$$

For pairs $(x, y) \in I$, we set

$$K(x, y) = \begin{pmatrix} x & y \\ y & \phi_y(x) \end{pmatrix}$$

for convenience, we further denote the set $J = \mathbb{F}_p^2 \setminus I = \{(x_0, y_0), \ldots, (x_{n-1}, y_{n-1})\}$, where $n = p^2 - m \leq p$. By assumption, there is a set $\mathcal{C}$ of symmetric matrices completing the smid family $\mathcal{S}$. The invertibility of all differences $A - B$, where $A \in \mathcal{S}$ and $B \in \mathcal{C}$, ensures that $\mathcal{C}$ can only contain elements of the form

$$C_j = \begin{pmatrix} x_j & y_j \\ y_j & \gamma_j \end{pmatrix},$$

where $j \in \{0, \ldots, n-1\}$ and $\gamma_j \in \mathbb{F}_p$. We are done if we can prove that there is a *unique* choice of elements $\gamma_0, \ldots, \gamma_{n-1}$ (i.e. of matrices $C_0, \ldots, C_{n-1}$). Obviously, it suffices to prove uniqueness for γ_0.

To this end, we need the following simple fact. There are exactly $p + 1$ different (affine) lines through any given point $(x, y) \in \mathbb{F}_p^2$, namely

$$g^{(x,y)} = \{(x, y) + l(0, 1) \mid l \in \mathbb{F}_p\} \quad \text{and} \quad h_k^{(x,y)} = \{(x, y) + l(1, k) \mid l \in \mathbb{F}_p\} \;\; (k \in \mathbb{F}_p).$$

(Note that these lines pairwise intersect only in (x, y), since $\mathbb{F}_p$ is a field.)

As $|J| = n \leq p$, at least one of the p lines $h_0^{(x_0,y_0)}, \ldots, h_{p-1}^{(x_0,y_0)}$, say h_k, does *not* contain any other point of J besides (x_0, y_0). This means a matrix $K((x_0, y_0) + l(1, k)) \in \mathcal{S}$ corresponds to every point $(x_0, y_0) + l(1, k) \in h_k$, $l \neq 0$, whence all the differences $K((x_0, y_0) + l(1, k)) - C_1$ are invertible. For this reason, the determinant

$$\det\left(K\left((x_0, y_0) + l\,(1, k)\right) - C_1\right) = l\left(\phi_{y_0+lk}\left(x_0 + l\right) - \gamma_1\right) - l^2k^2$$

is non-zero for all $l \neq 0$. We end up with

$$\gamma_0 \notin M_0 = \left\{\phi_{y_0+lk}(x_0 + l) - lk^2 \;\middle|\; l \in \mathbb{F}_p^\times\right\}.$$

The clue to see the uniqueness of the element γ_0 (and hence of the matrix C_0) lies in the fact that, according to Observation 5.3.5, the mapping

$$\Psi_{(x_0,y_0,k)} : \mathbb{F}_p^\times \to \mathbb{F}_p, \quad l \mapsto \phi_{y_0+lk}(x_0 + l) - lk^2$$

is *injective*, so that $M_0 \subset \mathbb{F}_p$ contains exactly $p - 1$ elements. Hence γ_0 is the "missing" element of $\mathbb{F}_p$ and thereby uniquely determined. As the same argumentation applies as well for the remaining matrices $C_1, \ldots, C_{n-1}$, this proves the uniqueness of the completing set $\mathcal{C}$.

(ii) If the family $\mathcal{S}$ is included in a plane $\mathcal{T}$, then there are matrices

$$A = \begin{pmatrix} x & 0 \\ 0 & qx \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & y \\ y & ry \end{pmatrix}$$

generating this plane for appropriate $q, r \in \mathbb{F}_p$, so $\mathcal{S} \subset \langle A, B \rangle = \mathcal{T}$. A priori, q, r could take any values in $\mathbb{F}_p$. We show that the containment of $\mathcal{S}$ in $\langle A, B \rangle$ limits the possible values for q and r.

For any $k \in \mathbb{F}_p$, at least one of the parallel lines

$$h_k^{(x,0)} = \left\{l(1, k) \mid l \in \mathbb{F}_p\right\} \ (x \in \mathbb{F}_p)$$

through $\mathbb{F}_p^2$ contains two different points $l_0(1, k), l_1(1, k) \in I$ (defined as above), i.e. we have $K(l_0(1, k)), K(l_1(1, k)) \in \mathcal{S}$. Otherwise $\mathcal{S}$ would at most contain p points in $\mathcal{T}$, but we have $p^2 - p > p$ for all $p > 2$. The regularity of $K(l_0(1, k)) - K(l_1(1, k))$ yields the following equivalences.

$$\begin{aligned} & \det\left(K((x, 0) + l_0(1, k)) - K((x, 0) + l_1(1, k))\right) \neq 0 \\ \Leftrightarrow \quad & (l_0 - l_1)(q(l_0 - l_1) + rk(l_0 - l_1)) - k^2(l_0 - l_1)^2 \neq 0 \\ \underset{(l_0 \neq l_1)}{\Leftrightarrow} \quad & q + rk - k^2 \neq 0 \end{aligned}$$

This holds for all $k \in \mathbb{F}_p$, whence we deduce $q \in \mathbb{F}_p^\times$ and

$$r \notin N_q = \left\{ k - k^{-1}q \;\middle|\; k \in \mathbb{F}_p^\times \right\}.$$

By Theorem 5.2.2, the plane $\mathcal{T}$ is therefore a smid family. It is obviously a completion of $\mathcal{S}$, and thus unique by the first part of the proof.

(iii) Suppose there is a matrix $C \in \mathcal{C}$ which does not belong to $\langle \mathcal{S} \rangle$. Then the latter span is of dimension two—it does not fill the space of all symmetric matrices in $M_2(\mathbb{F}_p)$, and has too many generators to be one-dimensional. On that account, $\mathcal{S}$ is included in a plane. According to assertion (ii), the unique completion of $\mathcal{S}$ coincides with that plane, which thus also contains the matrix C. This contradicts our assumption, and so we end up with $\langle \mathcal{S} \rangle \supset \mathcal{S} \cup \mathcal{C}$. □

Proof of Corollary 5.3.7 (page 194)

Let $D \in M_2(\mathbb{F}_p)$ be a symmetric matrix which does not belong to the smid family $\mathcal{S}$. Then by completeness of the latter, there are matrices $A \in \mathcal{S}$ such that $A - D$ is not invertible. Let $\{A_0, \dots, A_m\} \subset \mathcal{S}$ denote the set of all such matrices ($0 \leq m < p^2$).

By construction, the set $\mathcal{S}' = \mathcal{S} \setminus \{A_0, \dots, A_m\}$ is completable, moreover it can be enlarged by D to a smid family $\mathcal{S}' \cup \{D\}$. Supposing $m < p$, any matrix enlarging the smid family $\mathcal{S}'$ would be a member of its *unique* completion $\{A_0, \dots, A_m\}$ by Lemma 5.3.6. This again would mean $D \in \{A_0, \dots, A_m\}$, which of course contradicts the choice of the matrix D.

To show that m cannot exceed p, we take a look at the kernels K_i of the matrices $B_i = A_i - D$, where $0 \leq i \leq m$. We clearly have $0 \leq \dim K_i \leq 2$. Given that B_i is neither invertible nor zero by definition, it only remains $\dim K_i = 1$ for all $0 \leq i \leq m$. The existence of a vector $0 \neq v \in K_i \cap K_j$ for $i \neq j$ $(i, j \in \{0, \dots, m\})$ would imply $(B_i - B_j)v = 0$, and thus contradict the fact that the difference $B_i - B_j = A_i - A_j$ is invertible.

So we see that the kernels $K_0, \dots, K_m$ are pairwise disjoint one-dimensional subspaces of $\mathbb{F}_p^2$. It is straightforward to check that there are exactly $p + 1$ such subspaces, namely

$$\left\langle \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\rangle, \dots, \left\langle \begin{pmatrix} 1 \\ p-1 \end{pmatrix} \right\rangle,$$

whence we get the inequality $m \leq p$, and therefore, by what we have shown before, the identity $m = p$. □

Proof of Corollary 5.3.8 (page 194)

Pick a matrix $0 \neq A \in \mathcal{S}$. Simply by the cardinality of $\mathcal{S}$, there are two matrices $B_0, B_1 \in \mathcal{S}$ such that each of the pairs $(A, B_0), (A, B_1)$ and (B_0, B_1) spans a plane. If A belongs to $\langle B_0, B_1 \rangle$, we are done. Let us presume the contrary.

By Lemma 5.3.6, we know

$$A \in \mathcal{S} \subset \langle \mathcal{S} \setminus \{A, 2A, \ldots, (p-1)A\} \rangle .$$

Since A does not belong to the plane $\langle B_0, B_1 \rangle$ by assumption, there must be another matrix $B_2 \in \mathcal{S} \setminus \{A, 2A, \ldots, (p-1)A\}$ such that $A \in \langle B_0, B_1, B_2 \rangle$. By construction, B_2 is neither a multiple of A nor an element of $\langle B_0, B_1 \rangle$ as demanded. (Note that the second case of the proof occurs for instance whenever $\mathcal{S}$ is an affine plane not containing the zero matrix.) □

Proof of Technical Lemma 5.3.9 (page 195)

We will need the so-called Newton Identities for our proof, which we will state at the beginning.

Fix a positive integer $n \in \mathbb{N}$. The *kth power sum* of the indeterminates $X_1, \ldots, X_n$ is given by

$$s_k(X_1, \ldots, X_n) = \sum_{j=1}^{n} X_j^k$$

for all $k \in \mathbb{N}$. The *kth elementary symmetric polynomial* in the same indeterminates is defined as

$$e_k(X_1, \ldots, X_n) = \sum_{1 \le j_1 < \ldots < j_k \le n} X_{j_1} \cdots X_{j_k}$$

for all $1 \le k \le n$. Furthermore, one sets $e_0(X_1, \ldots, X_n) = 1$ and $e_k(X_1, \ldots, X_n) = 0$ for $k > n$. Then (one version of) the Newton Identities can be stated as follows.

$$ke_k(X_1, \ldots, X_n) = \sum_{j=0}^{k-1} (-1)^{k-j-1} e_j(X_1, \ldots, X_n) s_{k-j}(X_1, \ldots, X_n) \text{ for all } k \ge 1$$

A proof and some other versions of the Newton Identities can for example be found in [65].

Let $\phi : \mathbb{F}_p \to \mathbb{F}_p$ and $\psi_c : \mathbb{F}_p \to \mathbb{F}_p$ denote maps as in our assertion for $c \in \mathbb{F}_p$. For all $a, c \in \mathbb{F}_p$, we define constants

$$x_a^{(c)} = \psi_c(a) = \phi(a) + ca \in \mathbb{F}_p$$

and polynomials

$$p_c(Z) = \prod_{a \in \mathbb{F}_p} \left(Z - x_a^{(c)} \right) \in \mathbb{F}_p[Z].$$

Our aim is to prove that we either have $p_c(Z) = Z^p - Z$ or $p_c(Z) = Z^p$, depending on the parameter $c \in \mathbb{F}_p$. Once this is achieved, we conclude as follows.

If $p_c(Z)$ equals $Z^p - Z$, then it clearly follows $p_c(b) = \prod_{a \in \mathbb{F}_p} (b - \psi_c(a)) = 0$ for all $b \in \mathbb{F}_p$, hence ψ_c is a permutation. This cannot hold for all $c \in \mathbb{F}_p$ at the same time: in this case, one clearly finds two elements $a_0, c_0 \in \mathbb{F}_p$, $a_0 \neq 0$ satisfying the identity $\phi(a_0) = -c_0 a_0$ and hence $\psi_{c_0}(a_0) = 0 = \psi_{c_0}(0)$.

So there is an element $c_0 \in \mathbb{F}_p$ (and it will immediately become obvious that there must be exactly *one* such element) obeying the equation $p_{c_0}(Z) = Z^p$, and hence

$$p_{c_0}(b) = \prod_{a \in \mathbb{F}_p} (b - \psi_{c_0}(a)) = b^p = b$$

for all $b \in \mathbb{F}_p$. This expression being only zero if b is zero, it follows $\psi_{c_0}(a) = 0$ and thereby $\phi(a) = -c_0 a$ for all $a \in \mathbb{F}_p$.

For a start, you easily convince yourself of the identity

$$p_c(Z) = \sum_{j=0}^{p} (-1)^j e_j(x_0^{(c)}, \ldots, x_{p-1}^{(c)}) Z^{p-j}.$$

Note that all the terms $(-1)^j e_j(x_0^{(c)}, \ldots, x_{p-1}^{(c)})$ in the sum above can be understood as polynomial expressions in the variable c. Setting

$$q_j(c) = (-1)^j e_j(x_0^{(c)}, \ldots, x_{p-1}^{(c)})$$

for all $c \in \mathbb{F}_p$, we therefore define polynomials $q_j \in \mathbb{F}_p[Y]$ for all $j \leq 0$ in the obvious sense. Especially, we have the identities $q_0 = 1$ and

$$q_p(c) = \prod_{a \in \mathbb{F}_p} \left(-x_a^{(c)} \right) = \prod_{a \in \mathbb{F}_p} (-\phi(a) - ac) \underset{\phi(0)=0}{=} 0$$

for all $c \in \mathbb{F}_p$.

By construction, each of the polynomials q_j has degree at most j for $0 \leq j < p$. For all $j \in \{1, \ldots, p-2\}$, we can even show $\deg q_j \leq j - 1$. To see this, we consider the polynomial expressions $p_c(Z)$ as polynomials in two indeterminates for a moment, substituting the variable $c \in \mathbb{F}_p$ by an indeterminant Y:

$$\tilde{p}(Y, Z) = \prod_{a \in \mathbb{F}_p} (Z - \phi(a) - aY) = \sum_{j=0}^{p-1} q_j(Y) Z^{p-j}$$

Now focus on the expression in the centre and ask for the coefficient of $Y^j Z^{p-j}$ in $\tilde{p}(Y, Z)$. As it stems from products only containing factors Z and aY, it must be the same coefficient as the one of $Y^j Z^{p-j}$ in the product

$$\prod_{a \in \mathbb{F}_p} (Z - aY) = Z^p - Y^{p-1} Z,$$

which is zero for $1 \leq j \leq p-2$. Looking at the right-hand expression for $\tilde{p}(Y,Z)$, we see that the coefficients of Y^j in q_j are zero for $1 \leq j \leq p-2$.

Suppose that the mapping $\psi_{c_0} : a \mapsto \phi(a) + c_0 a$ is a permutation of $\mathbb{F}_p$ for a fixed element $c_0 \in \mathbb{F}_p$. This implies

$$p_{c_0}(Z) = \prod_{a \in \mathbb{F}_p} \left(Z - x_a^{(c_0)} \right) = \prod_{a \in \mathbb{F}_p} (Z - a) = Z^p - Z,$$

thus in particular $q_j(c_0) = 0$ for all $j \in \{1, \ldots, p-1\}$. By assumption, there are at least $(p-1)/2$ elements $c \in \mathbb{F}_p$ such that ψ_c defined as above is a permutation. Thus, each of the polynomials $q_1, \ldots, q_{p-1}$ has at least $(p-1)/2$ zeros, so that by their degree, we get

$$q_j = 0 \text{ for } 1 \leq j \leq \frac{p-1}{2}. \tag{A.12}$$

Consider the jth power sums

$$s_j(c) := s_j(x_0^{(c)}, \ldots, x_{p-1}^{(c)}) = \sum_{a \in \mathbb{F}_p} (\phi(a) + ca)^j.$$

For $1 \leq j < p-1$, notice that

- if $\psi_{c_0} : a \mapsto \phi(a) + c_0 a$ is a permutation for $c_0 \in \mathbb{F}_p$, then we have
$$s_j(c_0) = \sum_{a \in \mathbb{F}_p} (\phi(a) + c_0 a)^j = \sum_{a \in \mathbb{F}_p} a^j = 0;$$
- the degree of each polynomial s_j is $j-1$, as the coefficient of c^j in the expression $s_j(c)$ is given by
$$\sum_{a \in \mathbb{F}_p} a^j = 0.$$

Thus, the same argumentation as applied for the polynomials q_j before leads to the equations

$$s_j(c) = 0 \text{ for } 1 \leq j \leq \frac{p-1}{2}. \tag{A.13}$$

At this point, the Newton Identities come into play. For all $c \in \mathbb{F}_p$, they yield

$$\begin{aligned}
\sum_{j=0}^{k-1} q_j(c) s_{k-j}(c) &= \sum_{j=0}^{k-1} (-1)^j e_j(x_0^{(c)}, \ldots, x_{p-1}^{(c)}) s_{k-j}(c) \\
&= (-1)^{k-1} \sum_{j=0}^{k-1} (-1)^{k-j-1} e_j(x_0^{(c)}, \ldots, x_{p-1}^{(c)}) s_{k-j}(c) \\
&\underset{\text{(N. I.)}}{=} (-1)^{k-1} k e_k(x_0^{(c)}, \ldots, x_{p-1}^{(c)}) \\
&= -k q_k(c)
\end{aligned}$$

and thereby

$$\begin{aligned}-kq_k(c) = \sum_{j=0}^{k-1} q_j(c)s_{k-j}(c) &\underset{(A.12)}{=} s_k(c) + \sum_{j=\frac{p+1}{2}}^{k-1} q_j(c)s_{k-j}(c)\\ &\underset{(A.13)}{=} s_k(c) + \sum_{j=\frac{p+1}{2}}^{k-\frac{p+1}{2}} q_j(c)s_{k-j}(c)\end{aligned}$$

for all $k \in \{1, \dots, p\}$. Since the last sum is empty, we end up with the identities

$$-kq_k(c) = s_k(c) \text{ for } 1 \leq k \leq p. \tag{A.14}$$

Applying the fact that $q_j(c) = (-1)^j e_j(x_0^{(c)}, \dots, x_{p-1}^{(c)}) = 0$ for all $j \geq p$ (for $j > p$, this holds by definition of the jth elementary symmetric polynomials), the first of the relations above asserts

$$\sum_{j=0}^{p-1} q_j(c)s_{p+l-j}(c) = \sum_{j=0}^{p+l-1} q_j(c)s_{p+l-j}(c) = -(p+l)q_{p+l} = 0$$

for all integers $l \geq 1$ and all $c \in \mathbb{F}_p$. Using equation (A.12), it follows

$$s_{p+l}(c) + \sum_{j=\frac{p+1}{2}}^{p-1} q_j(c)s_{p+l-j}(c) = 0. \tag{A.15}$$

We will use the collected information (i.e. equations (A.12), (A.13), (A.14), and (A.15)) to show that all of the polynomials $q_1, \dots, q_{p-2}$ are constantly zero when evaluated on the field $\mathbb{F}_p$. To this end, suppose that on the contrary $q_j(c)$ does *not* equal zero for a fixed element $c \in \mathbb{F}_p$ and an index $j \in \{1, \dots, p-2\}$. This imposes $j > {}^{(p-1)}/_2$ by equation (A.12). Let ${}^{(p-1)}/_2 < m < p-2$ be the minimal index such that $q_m(c) \neq 0$. Then equation (A.13) implies $s_j(c) = 0$ for all $1 \leq j \leq p-m$, because $p - m \leq {}^{(p-1)}/_2$. Let $n \geq p-m$ denote an index satisfying $s_j(c) = 0$ for all $1 \leq j \leq n$. We deduce the following equation from (A.15), where we set $l = n+m+1-p$, and from the minimality of m.

$$-s_{n+m+1}(c) = \sum_{j=m}^{p-1} q_j(c)s_{n+m+1-j}(c) = q_m(c)s_{n+1}(c)$$

Knowing that $n + m \geq p$ and $n + m + 2 - p < n$, one easily establishes the identity $s_{n+m+1}(c) = s_{n+m+1-(p-1)}(c) = s_{n+m+2-p}(c) = 0$. Thus the equation above leads to $s_{n+1}(c) = 0$. By induction, we therefore get $s_j(c) = 0$ for *all* $j \geq 1$, but then equation (A.14) especially implies $q_m(c) = -m^{-1}s_m(c) = 0$, which contradicts our assumption.

At this stage, we have shown that the polynomials $p_c(Z)$ are of the form

$$p_c(Z) = \sum_{j=0}^{p-1} q_j(c)Z^{p-j} = Z^p + q_{p-1}(c)Z$$

for all $c \in \mathbb{F}_p$. In regard to our considerations quite at the beginning of this proof, we are thus done if we can show that $q_{p-1}(c)$ lies in $\{0, -1\}$ for all $c \in \mathbb{F}_p$. To this aim, fix an element $c \in \mathbb{F}_p$. Since we have $q_j(c) = 0$ for $1 \leq j \leq p-2$, equation (A.15) implies, setting $l = p-2$,

$$\underbrace{s_{p-1}(c)}_{s_{2p-2}(c)} + \sum_{j=\frac{p+1}{2}}^{p-1} q_j(c) s_{2p-2-j}(c) = s_{p-1}(c) + q_{p-1}(c) s_{p-1}(c) = 0$$

and thus $q_{p-1}(c) = -1$ or $s_{p-1}(c) = 0$. Combined with equation (A.14), this means $q_{p-1}(c) \in \{0, -1\}$. Our proof is complete. □

The SmidDetect programs

In order to explore the equivalence classes of smid families of arbitrary length in some smaller dimensions, we have written a couple of computer programs. It turns out that even in fairly small dimensions ($p^n < 32$), some computational power is needed to determine the numbers of equivalence classes of smid families of all possible lengths in the matrices $M_n(\mathbb{F}_p)$.

While our programs examine the smid families in the matrix algebras $M_2(\mathbb{F}_2)$, $M_3(\mathbb{F}_2)$, and $M_2(\mathbb{F}_3)$ within a few seconds on a standard personal computer, already the cases $M_2(\mathbb{F}_5)$, $M_3(\mathbb{F}_3)$, $M_1(\mathbb{F}_{29})$, and $M_1(\mathbb{F}_{31})$ cannot reasonably be solved without *parallel computing.* Fortunately, we have access to the *HPC parallel cluster* of the university of Münster, which is a parallel computer cluster comprising 160 CPUs in 20 compute nodes. We have used up to 64 of these processors in parallel to compute the cases $M_2(\mathbb{F}_5)$ and $M_3(\mathbb{F}_3)$, which required more than a fortnight.

Concretely, we have written the following progam modules, which allow to implement a parallel computation on a non-specific number of processors. A small example of a (semi-)parallel search algorithm based on these modules is depicted in the diagram on page 232 (however, we have applied more elaborate algorithms to explore the dimensions greater than $p^n = 16$).

SDN *(SmidDetectNano).* This program receives the parameters p, n, and L. For each length $2 \leq l \leq L$, it creates a list of smid families of length l in $M_n(\mathbb{F}_p)$. Due to a filter algorithm, each entry added to one of these lists is *inequivalent* to all preceding entries. This ensures that the smid families in the lists which are finally written to file are pairwise inequivalent.

On the one hand, SmidDetectNano performs the initial step for a parallel computation; the length L is supposed to be relatively small in this case, say $L \leq 4$. The found smid families of length L are written to a file which is readable by all other SmidDetect modules.

On the other hand, SmidDetectNano can be used to compute the smallest cases in one single step. It is furthermore able to produce an output file which is "human readable", i.e. contains the found representatives of inequivalent smid families in matrix representation (the same holds true for all other SmidDetect programs). The smid families in $M_2(\mathbb{F}_2)$, $M_3(\mathbb{F}_2)$, and $M_2(\mathbb{F}_3)$, and in all trivial matrix algebras $M_1(\mathbb{F}_p)$ for $p \leq 23$, can be computed by SmidDetectNano. As an example, you can find the ("human readable") output file of a full search for smid families in the matrix algebra $M_2(\mathbb{F}_3)$ on page 233.

SDS *(SmidDetectStep).* This and each of the following program modules are meant to be used for parallel computing (see the scheme on page 232).

The command line arguments of SmidDetectStep are p, n, L, and $part$. SmidDetectStep loads a file containing a list of (pairwise inequivalent) smid families of length $L-1$ in $M_n(\mathbb{F}_p)$ into memory. It first divides this list into N parts and reads only the entries of fraction no. $1 \leq part \leq N$. Next, it searches for all possible extensions of the respective smid families of length $L-1$ to smid families of length L. Applying the filter algorithm of SmidDetectNano, it only adds such smid families to its output file which are inequivalent to all previously found representatives.

The output file is tagged with the parameter $part$. The number N of parts is implemented in the source code and specifies the number of involved CPUs. In the example depicted on the next page, four CPUs are used.

SDF *(SmidDetectFuse).* The module SmidDetectFuse reads two lists of smid families produced by SmidDetectStep, and "fuses" them to a new list containing all members of the first list, but only such smid families of the second input file which are inequivalent to all smid families of the first one.

SDR *(SmidDetectReduce).* This program works nearly as SmidDetectFuse, but does not keep the smid families from the first input file, that is to say, it creates an output file containing precisely all smid families of the second input file which are inequivalent to every smid family listed in the first file.

SDC *(SmidDetectCombine).* This is a simple tool to recombine two lists created by any SmidDetect module to one single list. It performs no equivalence check or anything of that kind.

SDP *(SmidDetectPlanes).* Unlike the other programs, this module only searches for such Smid families which are (part of) n-dimensional linear subspaces of the space of all symmetric matrices inside $M_n(\mathbb{F}_p)$.

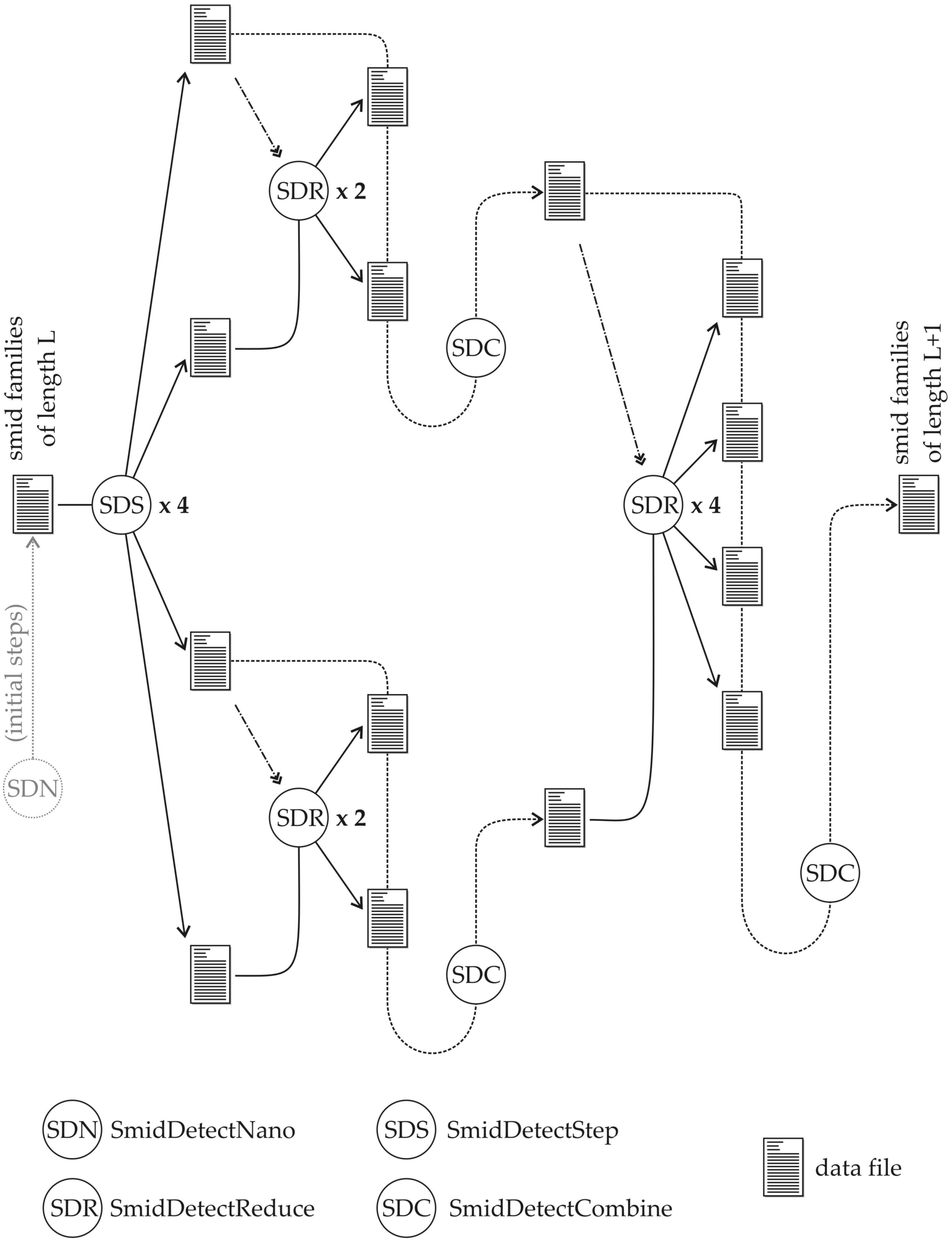


Figure A.1: *A SmidDetect algorithm on four CPUs*

```
--------- Output file of SmidDetectNano v5.2 ---------
---------  (c) 04/2014 Sebastian Krusekamp   ---------

[p = 3, n = 2, L = 9]

Process started at Wed May 14 12:59:42 2014

There are 48 invertible matrices in M_2(F_3),
among them 18 *symmetric* invertible matrices.

Found 2 conj. classes of smid families of length 2.
[0 h, 0 min, 3 s]
Found 5 conj. classes of smid families of length 3.
[0 h, 0 min, 3 s]
Found 6 conj. classes of smid families of length 4.
[0 h, 0 min, 3 s]
Found 4 conj. classes of smid families of length 5.
[0 h, 0 min, 3 s]
Found 3 conj. classes of smid families of length 6.
[0 h, 0 min, 3 s]
Found 2 conj. classes of smid families of length 7.
[0 h, 0 min, 3 s]
Found 1 conj. classes of smid families of length 8.
[0 h, 0 min, 4 s]
Found 1 conj. classes of smid families of length 9.
[0 h, 0 min, 4 s]

Combination process ended at Wed May 14 12:59:46 2014
Time needed for this process: 0 h, 0 min, 4 s

Representatives (zero matrix omitted):
[START]

0 1   0 2   1 0   1 1   1 2   2 0   2 1   2 2
1 0   2 0   0 2   1 2   2 2   0 1   1 1   2 1
(linear)

[END]

There are 1 linear subspaces among the representatives.
```

Bibliography

[1] W. O. Alltop. Complex sequences with low periodic correlations. *IEEE Trans. Inform. Theory*, 26(3):350–354, 1980.

[2] 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.

[3] M. Aschbacher, A. M. Childs, and P. Wocjan. The limitations of nice mutually unbiased bases. *Journal of Algebraic Combinatorics*, 25:111–123, 2007.

[4] L. Auslander and R. Tolimieri. Is computing with the finite Fourier transform pure or applied mathematics? *Bull. Amer. Math. Soc. (N.S.)*, 1(6):847–897, 1979.

[5] A. Azarchs. Entropic uncertainty relations for incomplete sets of mutually unbiased observables. *eprint arXiv:quant-ph/0412083*, December 2004.

[6] L. Bader, W. M. Kantor, and G. Lunardon. Symplectic spreads from twisted fields. *Boll. Un. Mat. Ital. A (7)*, 8(3):383–389, 1994.

[7] S. Ball, P. Govaerts, and L. Storme. On Ovoids of Parabolic Quadrics. *Designs, Codes and Cryptography*, 38(1):131–145, 2006.

[8] M. A. Ballester and S. Wehner. Entropic uncertainty relations and locking: Tight bounds for mutually unbiased bases. *Physical Review A*, 75(2):022319, February 2007.

[9] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and F. Vatan. A New Proof for the Existence of Mutually Unbiased Bases. *Algorithmica*, 34:512–528, 2002.

[10] K. Beauchamp and R. Nicoara. Orthogonal maximal abelian *-subalgebras of the 6x6 matrices. *ArXiv Mathematics e-prints*, September 2006.

[11] A. Belovs and J. Smotrovs. A Criterion for Attaining the Welch Bounds with Applications for Mutually Unbiased Bases. *ArXiv e-prints*, February 2008.

[12] I. Bengtsson. Three ways to look at mutually unbiased bases. October 2006.

[13] I. Bengtsson, W. Bruzda, Å. Ericsson, J.-Å. Larsson, W. Tadej, and Ka. Życzkowski. Mutually unbiased bases and Hadamard matrices of order six. *Journal of Mathematical Physics*, 48(5):052106, 2007.

[14] R. A. Bertlmann and P. Krammer. Bloch vectors for qudits. *Journal of Physics A Mathematical General*, 41(23):235303, June 2008.

[15] B. Blackadar. *Operator Algebras: Theory of C*-Algebras and von Neumann Algebras*. Encyclopaedia of Mathematical Sciences. Springer, 2006.

[16] P. O. Boykin, M. Sitharam, P. H. Tiep, and P. Wocjan. Mutually unbiased bases and orthogonal decompositions of Lie algebras. *Quantum Info. Comput.*, 7(4):371–382, May 2007.

[17] R. Brauer and H. C. H. Weyl. Spinors in n Dimensions. *Amer. J. Math.*, 57(2):425–449, 1935.

[18] R. P. Brent. Finding D-optimal designs by randomised decomposition and switching. *Australas. J. Combin.*, 55:15–30, 2013.

[19] S. Brierley and S. Weigert. Constructing mutually unbiased bases in dimension six. *Phys. Rev. A*, 79:052316, May 2009.

[20] T. Bröcker and T. Dieck. *Representations of Compact Lie Groups*. Graduate Texts in Mathematics. Springer, 1985.

[21] T. Bröcker and K. Jänich. *Introduction to Differential Topology*. Cambridge University Press, 1982.

[22] W. Bruzda, W. Tadej, and K. Życzkowski. Web page: Complex Hadamard matrices, last checked April 2014. `http://chaos.if.uj.edu.pl/~karol/hadamard/`.

[23] A. R. Calderbank, P. J. Cameron, W. M. Kantor, and J. J. Seidel. $\mathbb{Z}/4$-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets. *Proceedings of the London Mathematical Society*, 75(2):436–480, 1997.

[24] S. Chaturvedi. Aspects of mutually unbiased bases in odd-prime-power dimensions. *Phys. Rev. A*, 65:044301, Mar 2002.

[25] M. Choda. Relative entropy for maximal abelian subalgebras of matrices and the entropy of unistochastic matrices. *ArXiv e-prints*, March 2008.

[26] C. J. Colbourn and J. H. Dinitz. *Handbook of Combinatorial Designs, Second Edition*. Discrete mathematics and its applications. Taylor & Francis, 2010.

[27] M. Combescure. The Mutually Unbiased Bases Revisited. *eprint arXiv:quant-ph/0605090*, May 2006.

[28] M. Combescure. Block-circulant matrices with circulant blocks, Weil sums, and mutually unbiased bases. II. The prime power case. *Journal of Mathematical Physics*, 50(3):032104, March 2009.

[29] C. W. Curtis and I. Reiner. *Representation Theory of Finite Groups and Associative Algebras*. AMS Chelsea Publishing Series. AMS Chelsea Pub., 1962.

[30] K. R. Davidson. *C*-algebras by Example*. Fields Institute for Research in Mathematical Sciences Toronto: Fields Institute monographs. American Mathematical Society, 1996.

[31] P. de La Harpe and V. Jones. Paires de sous-algèbres semi-simples et graphes fortement réguliers. Technical Report IHES-M-90-29, Inst. Hautes Etud. Sci., Bures-sur-Yvette, Apr 1990.

[32] P. Delsarte, J. Goethals, and J. Seidel. Bounds for systems of lines and Jacobi polynomials. *Philips research reports*, 30:95–105, 1975.

[33] J. Dixmier. *Les Algèbres d'opérateurs dans l'espace hilbertien: (algèbres de Von Neumann)*. Les Grands classiques Gauthier-Villars. Éditions Jacques Gabay, 1996.

[34] T. Durt. A new expression for mutually unbiased bases in prime power dimensions. *eprint arXiv:quant-ph/0409090*, September 2004.

[35] T. Durt, B.-G. Englert, I. Bengtsson, and K. Życzkowski. On mutually unbiased bases. *ArXiv e-prints*, April 2010.

[36] R. J. Evans, J. Greene, and H. Niederreiter. Linearized polynomials and permutation polynomials of finite fields. *Mich. Math. J.*, 39(3):405–413, 1992.

[37] D. J. H. Garling. *Clifford Algebras: An Introduction*. London Mathematical Society Student Texts. Cambridge University Press, 2011.

[38] K. S. Gibbons, M. J. Hoffman, and W. K. Wootters. Discrete phase space based on finite fields. *Phys. Rev. A*, 70:062101, Dec 2004.

[39] J. E. Gilbert. *Clifford Algebras and Dirac Operators in Harmonic Analysis*. Cambridge Greek and Latin Classics. Cambridge University Press, 1991.

[40] C. Godsil and A. Roy. Equiangular lines, mutually unbiased bases, and spin models. *eprint arXiv:quant-ph/0511004*, November 2005.

[41] J.-M. Goethals and J. J. Seidel. Spherical designs. In *Relations between combinatorics and other parts of mathematics (Proc. Sympos. Pure Math., Ohio State Univ., Columbus, Ohio, 1978)*, Proc. Sympos. Pure Math., XXXIV, pages 255–272. Amer. Math. Soc., Providence, R.I., 1979.

[42] R. Gow. Generation of mutually unbiased bases as powers of a unitary matrix in 2-power dimensions. *ArXiv Mathematics e-prints*, March 2007.

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

[44] U. Haagerup. Orthogonal Maximal Abelian *-Subalgebras of the $n \times n$ Matrices and Cyclic N-Roots. *Institut for Matematik, U. of Southern Denmark*, 29:296–322, 1996.

[45] J. Hadamard. Résolution d'une question relative aux déterminants. *Bull. Sci. Math.*, 2:240–246, 1893.

[46] S. G. Hoggar. t-designs in projective spaces. *European J. Combin.*, 3(3):233–254, 1982.

[47] K. J. Horadam. *Hadamard matrices and their applications*. Princeton, N.J. Princeton University Press, 2007.

[48] R. A. Horn and C. R. Johnson. *Matrix Analysis*. Cambridge University Press, 2nd ed. edition, 2012.

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

[50] W. M. Kantor. Private communication (2014). Homepage: `http://pages.uoregon.edu/kantor/`.

[51] W. M. Kantor. On the inequivalence of generalized Preparata codes. *Information Theory, IEEE Transactions on*, 29(3):345–348, May 1983.

[52] W. M. Kantor. Note on Lie algebras, finite groups and finite geometries. In *Groups, difference sets, and the Monster (Columbus, OH, 1993)*, volume 4 of *Ohio State Univ. Math. Res. Inst. Publ.*, pages 73–81. de Gruyter, Berlin, 1996.

[53] W. M. Kantor. MUBs inequivalence and affine planes. *Journal of Mathematical Physics*, 53(3):–, 2012.

[54] B. R. Karlsson. Three-parameter complex Hadamard matrices of order 6. *Linear Algebra and its Applications*, 434(1):247–258, 2011.

[55] O. Kern, K. S. Ranade, and U. Seyfarth. Complete sets of cyclic mutually unbiased bases in even prime-power dimensions. *Journal of Physics A: Mathematical and Theoretical*, 43(27):275305, 2010.

[56] A. Klappenecker and M. Rötteler. Beyond stabilizer codes I: Nice error bases. *Information Theory, IEEE Transactions on*, 48(8):2392–2395, aug 2002.

[57] A. Klappenecker and M. Rötteler. Unitary Error Bases: Constructions, Equivalence, and Applications. In M. Fossorier, T. Høholdt, and A. Poli, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 2643 of *Lecture Notes in Computer Science*, pages 602–602. Springer Berlin / Heidelberg, 2003.

[58] A. Klappenecker and M. Rötteler. Mutually Unbiased Bases are Complex Projective 2-Designs. *eprint arXiv:quant-ph/0502031*, February 2005.

[59] A. Klappenecker and M. Rötteler. On the monomiality of nice error bases. *IEEE Trans. Inform. Theory*, 51(3):1084–1089, 2005.

[60] Andreas Klappenecker and Martin Rötteler. Constructions of Mutually Unbiased Bases. In G. L. Mullen, A. Poli, and H. Stichtenoth, editors, *Finite Fields and Applications*, volume 2948 of *Lecture Notes in Computer Science*, pages 137–144. Springer Berlin Heidelberg, 2004.

[61] E. Knill. Group Representations, Error Bases and Quantum Codes. *eprint arXiv:quant-ph/9608049*, August 1996.

[62] E. Knill. Non-binary Unitary Error Bases and Quantum Codes. Technical Report LANL report LAUR-96-2717, October 1996.

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

[64] R. Lidl and H. Niederreiter. *Introduction to Finite Fields and Their Applications*. Cambridge University Press, 1994.

[65] R. Lidl and H. Niederreiter. *Finite Fields*. Encyclopedia of mathematics and its applications ; 20. Cambridge University Press, Cambridge [u.a.], 2. ed., repr. edition, 2000.

[66] F. Lorenz. *Lineare Algebra I*. Number Bd. 1. Spektrum Akademischer Verlag, 2008.

[67] E. Lubkin. Entropy of an n-system from its correlation with a k-reservoir. *Journal of Mathematical Physics*, 19(5):1028–1031, 1978.

[68] M. Matolcsi. A Fourier analytic approach to the problem of mutually unbiased bases. September 2010.

[69] M. Matolcsi, I. Z. Ruzsa, and M. Weiner. Real and complex unbiased Hadamard matrices. *ArXiv e-prints*, January 2012.

[70] D. P. May. *Mutually Unbiased Bases: The Standard Construction and Automorphisms*. BiblioBazaar, 2011.

[71] D. McNulty and S. Weigert. All mutually unbiased product bases in dimension 6. *J. Phys. A*, 45(13):135307, 22, 2012.

[72] D. McNulty and S. Weigert. On the impossibility to extend triples of mutually unbiased product bases in dimension six. *Int. J. Quantum Inf.*, 10(5):1250056, 11, 2012.

[73] D. McNulty and S. Weigert. The limited role of mutually unbiased product bases in dimension 6. *J. Phys. A*, 45(10):102001, 5, 2012.

[74] A. O. Morris. On a generalized Clifford algebra. *The Quarterly Journal of Mathematics*, 18(1):7–12, 1967.

[75] A. O. Morris. On a generalized Clifford algebra (II). *The Quarterly Journal of Mathematics*, 19(1):289–299, 1968.

[76] A. Munemasa and Y. Watatani. Paires orthogonales de sous-algebres involutives. *Comptes Rendus de l'Academie des Sciences, Série I, Mathématiques*, 314(5):329–331, 1992.

[77] G. J. Murphy. *C*-Algebras and Operator Theory*. Academic PressInc, 1990.

[78] P. M. Neumann. An enumeration theorem for finite groups. *The Quarterly Journal of Mathematics*, 20(1):395–401, 1969.

[79] T. Paterek, B. Dakić, and Č. Brukner. Mutually unbiased bases, orthogonal Latin squares, and hidden-variable models. *Physical Review A*, 79(1):012109, January 2009.

[80] T. Paterek, M. Pawłowski, M. Grassl, and Č. Brukner. On the connection between mutually unbiased bases and orthogonal Latin squares. *Physica Scripta Volume T*, 140(1):014031, September 2010.

[81] A. O. Pittenger and M. H. Rubin. Mutually Unbiased Bases, Generalized Spin Matrices and Separability. *Linear Alg. Appl.*, 390:255, 2004.

[82] M. Planat, H. C. Rosu, and S. Perrine. A Survey of Finite Algebraic Geometrical Structures Underlying Mutually Unbiased Quantum Measurements. *Foundations of Physics*, 36:1662–1680, November 2006.

[83] S. Popa. *J. Oper. Theory*.

[84] A. Ramakrishnan, N. R. Ranganathan, T. S. Santhanam, P. S. Chandrasekaran, and R. Vasudevan. The generalized Clifford algebra and the unitary group. *Journal of Mathematical Analysis and Applications*, 27(1):164–170, 1969.

[85] A. E. Rastegin. Uncertainty relations for MUBs and SIC-POVMs in terms of generalized entropies. *European Physical Journal D*, 67:269, December 2013.

[86] P. Raynal, X. Lü, and B.-G. Englert. Mutually unbiased bases in six dimensions: The four most distant bases. *Phys. Rev. A*, 83:062303, Jun 2011.

[87] K. H. Rosen. *Handbook of Discrete and Combinatorial Mathematics, Second Edition*. Discrete mathematics and its applications. Taylor & Francis, 1999.

[88] A. Roy and A. J. Scott. Weighted complex projective 2-designs from bases: Optimal state determination by orthogonal measurements. *Journal of Mathematical Physics*, 48(7):072110, July 2007.

[89] M. Saniga and M. Planat. Viewing sets of mutually unbiased bases as arcs in finite projective planes. *Chaos, Solitons & Fractals*, 26(5):1267–1270, 2005.

[90] M. Saniga, M. Planat, and H. Rosu. Mutually unbiased bases and finite projective planes. *Journal of Optics B: Quantum and Semiclassical Optics*, 6(9):L19, 2004.

[91] J. Schwinger. UNITARY OPERATOR BASES. *Proceedings of the National Academy of Sciences*, 46(4):570–579, 1960.

[92] M. R. Sepanski. *Algebra*. Pure and applied undergraduate texts. American Mathematical Society, 2010.

[93] G. Seroussi and A. Lempel. On Symmetric Representations of Finite Fields. *SIAM Journal on Algebraic Discrete Methods*, 4(1):14–21, 1983.

[94] J. P. Serre. *Linear Representations of Finite Groups*. Graduate texts in mathematics. Springer-Verlag, 1996.

[95] U. Seyfarth and K. S. Ranade. Construction of mutually unbiased bases with cyclic symmetry for qubit systems. *Physical Review A*, 84(4):042327, October 2011.

[96] U. Seyfarth and K. S. Ranade. Cyclic mutually unbiased bases, Fibonacci polynomials and Wiedemann's conjecture. *J. Math. Phys.*, 53(6):062201, 10, 2012.

[97] P. W. Shor. Fault-tolerant quantum computation. In *Foundations of Computer Science, 1996. Proceedings., 37th Annual Symposium on*, pages 56–65, 1996.

[98] W. A. Sutherland. *Introduction to Metric and Topological Spaces*. Oxford science publications. Clarendon Press, 1975.

[99] J. J. Sylvester. Thoughts on inverse orthogonal matrices, simultaneous sign-successions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers. *Philos. Mag.*, (34):461, 1867.

[100] J. J. Sylvester. A word on nonions. *Johns Hopkins University Circulars*, I:241, 1882.

[101] J. J. Sylvester. On quaternions, nonions, sedenions, etc. *Johns Hopkins University Circulars*, III:7–9, 1884.

[102] F. Szöllősi. Complex Hadamard matrices of order 6: A four-parameter family. *Journal of the London Mathematical Society*, 85(3):616–632, 2012.

[103] S. Weigert, S. Brierley, and I. Bengtsson. All Mutually Unbiased Bases in Dimensions Two to Five. *Quantum Information and Computation*, 10(9–10):803–820, optional 2010.

[104] M. Weiner. A gap for the maximum number of mutually unbiased bases. *ArXiv e-prints*, February 2009.

[105] L. Welch. Lower bounds on the maximum cross correlation of signals (Corresp.). *Information Theory, IEEE Transactions on*, 20(3):397–399, May 1974.

[106] R. F. Werner. All teleportation and dense coding schemes. *Journal of Physics A Mathematical General*, 34:7081–7094, September 2001.

[107] H. C. H. Weyl. *Gruppentheorie und Quantenmechanik*. S. Hirzel, 1928.

[108] H. C. H. Weyl. *The Theory of Groups and Quantum Mechanics*. Dover books on advanced mathematics. Dover Publications, 1950.

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

[110] Wikipedia. Web page: Wikipedia – Bias (statistics), last checked April 2014. `http://en.wikipedia.org/wiki/Bias (statistics)`.

[111] D. P. Williams. *Crossed Products of C*-algebras*. Mathematical surveys and monographs. American Mathematical Society, 2007.

[112] P. Wocjan and T. Beth. New Construction of Mutually Unbiased Bases in Square Dimensions. *Quantum Information and Computation*, 5(2):93–101, optional 2005.

[113] M. W. Wong. *Discrete Fourier Analysis*. Pseudo-differential operators. Springer, 2011.

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

[115] K. Yamazaki. On projective representations and ring extensions of finite groups. *J. Fac. Sci. Univ. Tokyo Sect. I*, 10:147–195 (1964), 1964.

[116] N. Y. Yu. Reed-Muller Codes for Peak Power Control in Multicarrier CDMA. *CoRR*, abs/1010.0189, 2010.

[117] G. Zauner. *Quantendesigns. Grundzüge einer nichtkommutativen Designtheorie*. PhD thesis, University of Wien, 1999.

List of figures

List of symbols

Symbols that appear only in a very restricted context are not listed.

$\lvert z\rvert$	the absolute value of $z \in \mathbb{C}$
$\mathcal{A} \rtimes G$	the crossed product of a C*-algebra $\mathcal{A}$ by a group G, see Section 2.5
$\mathcal{A}(M)$	the (sub)algebra generated by the set M
$\operatorname{Aut} \mathcal{A}$	the automorphism group of some algebraic structure $\mathcal{A}$
$\mathbb{C}$	the field of complex numbers
$\mathcal{C}(X)$	the commutative C*-algebra of complex-valued continuous functions on a locally compact Hausdorff space X (which is always discrete and finite in the present work)
$\mathcal{C}(X, \mathcal{A})$	the commutative C*-algebra of continuous functions on a locally compact Hausdorff space X (which is always discrete and finite in the present work) with values in a C*-algebra $\mathcal{A}$
$\mathbb{C}l^c_m$	the generalised Clifford algebra, see Proposition/Definition 4.4.5
$\mathbb{C}l_m$	the Clifford algebra, see page 142
$\mathbb{C}^d$	the complex Hilbert space of dimension d
$\mathbb{C}^d_1$	the set of unit vectors in the complex Hilbert space of dimension d
$\mathcal{D}_d$	the group of diagonal complex $d{\times}d$-matrices
I_d	the unit matrix in the $d{\times}d$-matrices (the ground field depends on the context)
$\mathbb{F}_{p^n}$	the Galois field of order p^n, see page 88
$\mathbb{F}^{\times}_{p^n}$	the multiplicative group of invertibles inside the Galois field $\mathbb{F}_{p^n}$

X_d	the shift matrix, see page 30
Z_d	the clock matrix, see Example 1.4.2
$\lVert\cdot\rVert_{\mathrm{HS}}$	the Hilbert-Schmidt norm on the matrix algebra $M_d(\mathbb{C})$
$(\cdot\mid\cdot)_{\mathrm{HS}}$	the Hilbert-Schmidt scalar product for the complex $d\times d$-matrices
$\mathrm{Im}\ z$	the imaginary part of $z \in \mathbb{C}$
$\langle M\rangle$	see $\mathrm{span}(M)$
$\mathcal{L}(\mathbb{C}^d)$	the *-algebra of linear operators on the Hilbert space $\mathbb{C}^d$, identified with the set $M_d(\mathbb{C})$ of complex $d\times d$-matrices
$\mathfrak{m}_d$	the set of all masas in the complex $d\times d$-matrices
$M_d(\mathbb{C})$	see $\mathcal{L}(\mathbb{C}^d)$
$\mathbb{N}$	the set of natural numbers $\{1,2,\ldots\}$
$\mathbb{N}_0$	the union $\mathbb{N}\cup\{0\}$
$\lVert\cdot\rVert$	the standard norm on the Hilbert space $\mathbb{C}^d$
$\tau(a)$	the normalised trace of a matrix $a \in M_d(\mathbb{C})$
S_d	the symmetric group of order d; permutations of the set $\{0,\ldots,n-1\}$
$\perp_q$	quasi-orthogonal, see Definition 2.2.1
$\mathcal{W}_d$	the group of monomial unitary $d\times d$-matrices, see Definition 1.2.3
$\mathcal{PU}_d$	the projective unitary group of order d, see Definition 4.1.8
$\mathbb{R}$	the field of real numbers
$\mathbb{R}^+$	the set of positive real numbers
$\mathbb{R}_0^+$	the set of non-negative real numbers
$\mathrm{Re}\ z$	the real part of $z \in \mathbb{C}$
$\mathcal{A}^*\left(E,R\right)$	the universal *-algebra with generators E and relations R, see Definition 4.4.1
$\mathcal{A}^*(M)$	the *-algebra or *-subalgebra generated by the set M
σ_x	one of the Pauli matrices, see page 30

σ_z	one of the Pauli matrices, see Example 1.4.2
$(\cdot \mid \cdot)$	the standard scalar product for the Hilbert space $\mathbb{C}^d$
$\operatorname{span}(M)$	the linear span of the set of vectors M (with coefficients from the field determined by the context or notated as subscript, mostly $\mathbb{C}$)
$\mathbb{T}$	the unit circle inside the field of complex numbers
a^T	the transpose of a matrix $a \in M_d(\mathbb{C})$
$\operatorname{Tr}(a)$	the non-normalised trace of a matrix $a \in M_d(\mathbb{C})$; in some contexts the absolute trace of an element a of a Galois field, see Definition/Proposition 3.3.1
$\mathcal{U}_d$	the group of unitary $d \times d$-matrices
$\mathbb{Z}$	the ring of integers
$\mathbb{Z}/d$	the ring of integers modulo d
$a \sim_M b$	vectors a, b of a vector space over a field F coincide up to a factor $\lambda \in M \subset F$, that is $a = \lambda b$.
$C^*(E, R)$	the universal C*-algebra with generators E and relations R, see Definition 4.4.3
$C^*(G)$	the group C*-algebra of the group G, see Section 2.5
$F[X_0, \dots, X_{n-1}]$	the polynomial ring in n indeterminates $X_0, \dots, X_{n-1}$, with coefficients from a field F
$L^1(G)$	the Banach algebra of functions with bounded L^1-norm on a locally compact Hausdorff group G (which is always discrete and finite in the present work), see Section 2.5
S^{d-1}	the unit sphere inside the Hilbert space $\mathbb{C}^d$
Z_d	the group of dth roots of unity on the unit circle

Index