Mutually unbiased bases and related structures

A thesis submitted in fulfillment of the requirements for the degree of Doctor of Philosophy

Joanne Hall

BSc(Hons), MPhil

School of Mathematical and Geospatial Sciences

Science, Engineering, and Health Portfolio,

RMIT University

Melbourne, Victoria, Australia

May 2011

Declaration

The candidate hereby declares that in this thesis, presented for the award of the Doctor of Philosophy in Mathematics and submitted in the School of Mathematical and Geospatial Sciences, RMIT University:

- except where due acknowledgement has been made, the work is that of the candidate alone;
- the work has not been submitted previously, in whole or in part, to qualify for any other academic award;
- the content of the thesis is the result of work which has been carried out since the official commencement date of the approved research program;
- any editorial work, paid or unpaid, carried out by a third party is acknowledged;
- ethics procedures and guidelines have been followed;
- has been carried out under the supervision of Dr. Asha Rao and Prof. Kathy Horadam.

.....

Joanne Hall

Acknowledgements

Thanks are due to my supervisor Dr. Asha Rao who has guided, encouraged and supported me through the PhD process. I will always fondly recall our moments of shared excitement at new results, and the wise words of calm when things were becoming difficult.

To Assoc. Prof. Diane Donovan who has visited RMIT several times during my candidature. I have enjoyed our time around the whiteboard.

To my associate supervisor Prof. Kathy Horadam, always there for a conversation, an idea, and an almost inexhaustible bookshelf. To Assoc. Prof. Serdar Botzas, who has helped my understanding of the physical motivation behind this project.

To my husband Peter who has been supportive of all that I do. I am grateful for your professional level consulting on programming algorithms, your patient listening when I bound with excitement, and your willingness accompanying me to conferences so that our child may continue to breastfeed.

To the City Campus Children's Centre, who have made combining parenting and study possible. To everybody who has cared for my child, particularly my mother and my mother and father in law; thank-you for giving me time to write this thesis.

Proof reading has been done by Peter Hall, who has expertise in software engineering.

This research was funded by the Australian Postgraduate Awards scheme.

Contents

List of Figures

Summary

The mathematical structure of a complex vector space, $\mathbb{C}^d$, is used in quantum physics as a means of expressing physical properties.

Two orthonormal bases B_1 and B_2 of $\mathbb{C}^d$ are *unbiased* if $|\langle\vec{x}|\vec{y}\rangle| = \frac{1}{\sqrt{d}}$ for all $\vec{x} \in B_1$ and $\vec{y} \in B_2$. The term unbiased refers to when a quantum system is prepared in basis state B_1, all possible outcomes of a measurement with respect to B_2 will occur with equal probabilities [99].

A set of bases, each pair of which is unbiased, is a set of mutually unbiased bases (MUBs). MUBs have applications in quantum physics and quantum information theory. Although the motivation to study MUBs comes from physical properties, MUBs are a mathematical structure. This is a mathematical investigation.

Fifty years have passed since the initial description of MUBs. There are still many open problems, some of which have conjectured solutions.

Open Problem 0.1. *What is the maximum number of MUBs in $\mathbb{C}^d$?*

There is a maximum of $d + 1$ MUBs in $\mathbb{C}^d$ [112]. This upper bound is attained for all prime power dimensions, shown by explicit construction [112]. It is unknown if this upper bound is attained for any non prime power, even for the smallest non prime power of 6. Sets of $d+1$ MUBs in $\mathbb{C}^d$ are called *complete*. Some of the applications of MUBs rely on complete sets.

Open Problem 0.2. *Do complete sets of MUBs exist in all dimensions?*

It has been noted that mutually orthogonal Latin squares (MOLS) are 'similar in spirit' to MUBs [111].

Conjecture 0.3 (SPR Conjecture)**.** *[96] A complete set of MUBs exists in $\mathbb{C}^d$ if and only if a complete set of MOLS of order d exists.*

MOLS are much more thoroughly studied than MUBs. There are still many open questions about MOLS, however there are key results such as the Bruck-Ryser-Chowla Theorem which shows that complete sets of MOLS of specific orders cannot exist. If the SPR conjecture is proven, then results such as this can be used to show the non-existence of complete sets of MUBs in specific dimensions.

The aim of this research is to find evidence for or against the SPR conjecture. We will approach this conjecture directly as well as by investigating structures which are related to MOLS.

Research Question 0.4. *Are mutually unbiased bases intimately linked with mutually orthogonal Latin squares?*

Most known constructions of complete sets of MUBs rely on algebraic structures and functions, which are known to also construct complete sets of MOLS.

Research Question 0.5. *Do all complete sets of mutually unbiased bases have an algebraic structure?*

It has been 7 years since the publication of the SPR conjecture [96], and even longer since a connection between finite geometries and MUBs was foreshadowed [112]. It has been 30 years since an algebraic structure (Galois field) was first used to construct a set of MUBs [59].

There many research groups taking various approaches to these questions, and yet they are still open. In this thesis some significant progress has been made, which could be built upon to answer these questions in the future.

- Inspired by constructions of MUBs which use sets of MOLS [85, 110], complete sets of MOLS were constructed from two complete sets of MUBs. Of note is that the MOLS structure emerges not from the vectors, but from the inner products of the vectors. This has been published [47, 90].

- Analogous properties of Hjelmslev planes and MUBs, and gaps in knowledge motivated investigation of Hjelmslev planes. The substructures of a Hjelmslev plane over a Galois ring, and a combinatorial algorithm for generating Hjelmslev planes were developed. It is shown that the analogous properties of Hjelmslev planes and MUBs occur only for odd prime powers, making a strong connection between MUBs and Hjelmslev planes unlikely.

- A construction of MUBs that uses planar functions [93] was generalised by using an automorphism on the additive group of a Galois field. It is unclear if this generalisation is equivalent to the original construction.

- Relation algebras have been constructed using the structure of a complete set of MOLS [82]. Relation algebras were constructed from the structure of MUBs which do not share any similarities with algebras constructed from MOLS. This has been published [46].

- A set of WF type MUBs, when represented as elements of a group ring, forms a commutative monoid. A set of Alltop type MUBs when similarly represented does not form a closed algebraic structure. It is known that WF and Alltop MUBs are equivalent [42], thus the lack of a closed structure in the Alltop MUBs suggests that the monoid is not a property of MUBs in general.

Complete sets of MOLS and complete sets of MUBs are 'similar in spirit', but perhaps this is not an inherent feature of MUBs and MOLS. All the known constructions of MUBs rely on algebraic structures which exist only in prime power dimensions. The connection may not be with MOLS, but with algebraic structures which generate both MOLS and MUBs.

Chapter 1

Introduction

1.1 Motivation

1.1.1 Inspiration

Quantum physics uses the mathematical structure of a complex vector space, $\mathbb{C}^d$, as a means of expressing physical properties.

Two orthonormal bases B_1 and B_2 of $\mathbb{C}^d$ are *unbiased* if $|\langle\vec{x}|\vec{y}\rangle| = \frac{1}{\sqrt{d}}$ for all $\vec{x} \in B_1$ and $\vec{y} \in B_2$. These bases are unbiased in the following sense: if a quantum system is prepared in basis state B_1, then all possible outcomes of a measurement with respect to B_2 will occur with equal probabilities. If a system is prepared in basis state B_1, then a measurement in basis B_2 'destroys all prior knowledge' of the system with respect to basis B_1 [99].

A set of bases, each pair of which is unbiased, is a set of mutually unbiased bases, hereafter referred to as MUBs. MUBs have several applications in quantum physics and quantum information theory.

Although the inspiration comes from physical properties, MUBs are a mathematical structure, and will be treated as such. The physical interpretation will be mentioned for interest, but in no way influences the mathematics.

1.1.2 Historical note on MUBs

In 1960 Schwinger realised that a quantum system prepared in one basis state would reveal no information if measured with respect to another unbiased basis state [99]. In 1981 Ivanovic

considered the applications of MUBs in the problem of quantum state determination [59] and provided a construction of MUBs in odd prime power dimensions. A year earlier Alltop published a construction for sequences with low periodic correlation for use in communication systems [1]. Alltop's sequences are the first published constructions of complete sets of MUBs, though this was not known for some time. Alltop's work was used in sequence design for many years before the contribution to quantum physics was noticed. In 1989 Wootters and Fields extended the Ivanovic construction to all odd prime powers, and provided a construction for even prime powers [112]. In 2003 Klappenecker and Rötteler [64] published a summary of known constructions which included the sets of MUBs described by Alltop, Wootters and Fields and Ivanovic.

Mutually unbiased bases are a mathematical structure, however the original inspiration to study them came from a physical problem. That the applications of MUBs have been driving research is most evident in that the bulk of publications on MUBs appear in physics and communications journals.

1.1.3 Applications of MUBs

Quantum state tomography

In a quantum system, experimental measurement outcomes are only accessible as probabilities. The state of a quantum system can be written as a density matrix (Definition 2.14), where the entries of the matrix represent the probabilities of physical outcomes.

Tomography is the process of reconstructing the density matrix from a set of measurements. A measurement of a d-dimensional quantum ensemble yields $d-1$ real values, which are the probabilities of all but one of the d possible outcomes. The requirement that all probabilities sum to 1 forces the d^{th} value. Thus at least $(d^2-1)/(d-1) = d+1$ measurements are required to uniquely determine the state of the quantum ensemble [112].

It is possible to determine the state using measurements which are not mutually unbiased. However Wootters and Fields show that $d+1$ mutually unbiased bases provide the optimal set of measurements [112]. The unbiased measurements have minimal interaction with each other, so less errors are introduced.

MUBs are thus important for measuring quantum states and subsequent applications.

Quantum cryptography

MUBs are used in some cryptographic key distribution protocols. Cryptography is the process of writing a message so that it can only be read by specific authorised people; a problem almost as old as written communication.

For example: Alice wants to send a message to Bob, but must keep the message secret from Eve. Alice encrypts the message, which Bob can decrypt using a secret key. However if Eve also has the key, then Eve can decrypt the message. The secure distribution of a cryptographic key is one of the more difficult problems in cryptography.

An important innovation was public key cryptography in which the encryption key is publicly announced, and different from the decryption key, which is known only to the receiver. Current public key cryptography is based on the RSA protocol which uses the fact that multiplication is easy, but factoring large numbers is difficult [92]. However, given a sufficiently powerful computer and enough time, Eve can find the key.

The use of unbiased measurements of quantum systems can provide provably secure key distribution using optical signals. The BB84 key distribution protocol uses two MUBs [9]. The BB84 protocol has been extended to three MUBs [17], and later generalised to any set of $d+1$ MUBs in $\mathbb{C}^d$ [21].

The BB84 protocol may be described as follows: Alice and Bob both have a set of photon polarisers which have the angles of the vectors from a complete set of MUBs. Alice and Bob agree on which directions of polarisation represent each symbol of the key alphabet. Alice and Bob independently select a sequence of polarisations. Alice sends a sequence of photons polarised according to her sequence. Bob detects the photons using his sequence of polarisations. Alice and Bob can then communicate in public, to determine which parts of their polarisation sequences were the same. They then retain the corresponding symbol sequence as their raw key. A diagram of this process using two bases is given in Figure 1.1.

If photons behaved in a classical manner, Eve could set up intermediate detectors in the hope of matching some of Alice's polarisation sequence. However one of the fundamental properties of quantum physics is that any observation makes a small change to a quantum system. This is a highly un-intuitive notion, (think of Schrödinger's cat [105]), but it is backed up by a large body of experimental data [87].

Alice and Bob choose a subset of the raw key, and publicly check if they have the same

Alice's sequence	0	1	1	1	0	0	1	0	1	1
Alice's polarisers	⤫	✛	✛	⤫	✛	⤫	⤫	✛	⤫	✛
transmitted photons	↗	↕	↕	↘	↔	↗	↘	↔	↘	↕
Bob's polarisers	⤫	✛	⤫	⤫	✛	✛	✛	⤫	✛	✛
Bob's measurements	0	1	0	1	0	1	1	1	0	1
raw key	0	1		1	0					1

Figure 1.1: Transmission of polarised photons between Alice and Bob using 2 unbiased bases [6, Figure 2.7].

values. If the checked subset agrees, then another subset of the raw key may be used as the cryptographic key. If they don't agree, then changes have been introduced, which may mean that Eve intercepted the message. They can discard the raw key and begin again.

This is a provably secure system. There are various strategies that Eve can use to get limited information however these rely on the physical implementation of the protocol [97, 78]. If a set of MUBs is used, it is then an engineering challenge to successfully implement quantum key distribution.

1.2 Aim

1.2.1 Conjectures about MUBs

Fifty years have passed since the initial description of MUBs. There are still many open problems, some of which have conjectured solutions.

Open Problem 1.1. *What is the maximum number of MUBs in $\mathbb{C}^d$?*

There is a maximum of $d+1$ MUBs in $\mathbb{C}^d$ [112]. This upper bound is attained for all prime power dimensions. It is unknown if this upper bound is attainable for any non prime power. A lower bound on the maximum number of MUBs in $\mathbb{C}^d$ is based on the prime decomposition of d. These bounds are expounded in section 2.3.2. Sets of $d+1$ MUBs in $\mathbb{C}^d$ are called *complete*. Some of the applications of MUBs, such as tomography, rely on complete sets.

Open Problem 1.2. *Do complete sets of MUBs exist in all dimensions?*

This has been partially answered with constructions given for all dimensions that are a power of a prime [112]. However the question is open, even for 6, the smallest non prime power.

Conjecture 1.3 (Zauner's Conjecture)**.** *[116] A complete set of MUBs exists in $\mathbb{C}^d$ if and only if d is a power of a prime.*

This conjecture was originally published in the language of complex projective designs. However, it has been shown that MUBs are equivalent to specific types of complex projective designs. Thus it may be expressed as a conjecture about MUBs [65, §VI]. The only known constructions of complete sets of MUBs use algebraic structures which only exist in prime power order.

It has been noted that finite affine planes are 'similar in spirit' to MUBs [111]. This similarity has been elevated to a conjecture:

Conjecture 1.4 (SPR Conjecture)**.** *[96] A complete set of MUBs exists in $\mathbb{C}^d$ if and only if a finite affine plane of order d exists.*

A finite affine plane is combinatorially equivalent to a complete set of mutually orthogonal Latin squares (MOLS). Thus this conjecture may be rewritten for MOLS.

Conjecture 1.5 (SPR Conjecture)**.** *[96] A complete set of MUBs exists in $\mathbb{C}^d$ if and only if a complete set of MOLS of order d exists.*

It is known that complete sets of MOLS exist when the order is a power of a prime. One of the most famous and celebrated open problems in discrete mathematics regards the existence of complete sets of MOLS.

Open Problem 1.6. *[23, Rem III.3.21] Does a complete set of MOLS exist of order that is not a power of a prime?*

There are results such as the Bruck-Ryser-Chowla Theorem which exclude the existence of a complete set of MOLS for various non prime power orders [16], however there are an infinite number of orders for which the existence of a complete set of MOLS is an open problem. The SPR and Zauner's conjectures may in fact be equivalent if complete sets of MOLS only exist of prime prime order.

A weaker, though related idea connects MUBs with projective Hjelmslev planes.

Analogy 1.7 (SP Analogy)**.** *[95] A conic in a projective Hjelmslev plane over a Galois ring $GR(p^2, r)$ has analogous structure to a complete set of MUBs in $\mathbb{C}^{p^r}$.*

The evidence for this analogy is much weaker than that for the SPR conjecture. A Hjelmslev plane is a generalisation of a projective plane, which exists if and only if an affine plane also exists. Again this may effectively be the same as Zauner's conjecture.

1.2.2 Research Questions

We aim to find evidence for or against the SPR conjecture. We will approach this conjecture directly as well as by investigating structures which are related to MOLS.

Research Question 1.8. *Are mutually unbiased bases intimately linked with mutually orthogonal Latin squares?*

The only known constructions of complete sets of MUBs rely on algebraic structures and functions which exist only for prime power order. Most of the functions and algebraic structures which are known to construct MUBs can also be used to construct MOLS.

Research Question 1.9. *Do all complete sets of mutually unbiased bases have an algebraic structure?*

Perhaps the noticed connection with MOLS is actually a connection with algebraic structures which can generate both MOLS and MUBs.

1.3 Structure of this document

Chapter 2 provides an overview of current knowledge about MUBs. Each subsequent chapter takes a different perspective on the two underlying research questions.

Chapter 3 approaches research question 1.8 directly by constructing mutually orthogonal Latin squares from MUBs. This is shown to work for two constructions of MUBs.

Chapter 4 investigates Hjelmslev planes, which are a generalisation of projective planes. Hjelmslev planes are a largely unexplored topic. The outcome of this chapter is new knowledge about Hjelmslev planes.

Chapter 5 looks at planar functions which are known to construct specific sets of MUBs and specific sets of MOLS. A more general construction of MUBs is described, though it is not shown if this constructs MUBs which are non-equivalent to those already known.

Chapter 6 constructs relation algebras from MUBs, and compares them to relation algebras which have been constructed from projective planes.

Chapter 7 represents the vectors of sets of MUBs as elements of a group ring. An algebraic structure is then found for some sets of MUBs.

Chapter 8 summarises the findings and suggests directions for future research.

1.4 Original Contribution

Most of the original work in this document is the work of the author, with the usual amount of supervisory input. However some work was done in collaboration with Dr Asha Rao and Assoc. Prof. Diane Donovan, into which the author, Dr Rao and Assoc. Prof. Donovan each provided significant contribution. Sections 3.4 and 4.3 were the result of such collaboration.

Chapter 2

Literature review

2.1 Overview

The applications detailed in section 1.1.3 provide the motivation for this study, but not the substance. This is a mathematical investigation. There is a lot of mathematical background required of the reader. Section 2.2 gives some of the algebraic definitions and concepts used throughout. Each chapter also begins with a section of background on the structures of interest in that chapter.

Section 2.3 expounds some of the background results on MUBs. Section 2.4 shows some known constructions of MUBs. Section 2.5 presents some known and conjectured correlations with various algebraic and geometric structures. Section 2.6 shows the algebraic structures of some known constructions of MUBs. Section 2.7 expands upon the research questions stated in section 1.2.2.

2.2 Definitions and preliminary theorems

There are many algebraic and combinatorial concepts used in the discussion of MUBs. We define them along with the notation used. All other definitions will be introduced in the relevant chapters. Results cited from standard texts are stated without proof throughout this thesis.

2.2.1 Linear Algebra

General Linear Algebra

Definition 2.1. [104, §1,2] Let A be a matrix. $(A)_{ij}$ is the element in the cell which is in the i^{th} row and j^{th} column of A. For a matrix A, A^* is the *Hermitian transpose* of A. I_d is the $d \times d$ *identity* matrix. [0] is the matrix containing 0 in every entry.

Vectors are denoted $\vec{v}$. $\vec{v}_a$ is the a^{th} vector in a set. v_{a_b} is the b^{th} entry of $\vec{v}_a$. v_{a_b} is a scalar, and thus is not printed with $\vec{}$. All vectors are assumed to be column vectors. Entries in vectors and matrices will be labelled beginning with 0.

$\vec{x}$ is a column vector, $\vec{x}^T$ is a row vector. If $\vec{x} \in \mathbb{C}^d$ then $\vec{x}^*$ is a row vector with entries that are the complex conjugates of the entries in $\vec{x}$.

$\mathbb{C}$ is the field of complex numbers, $\mathbb{R}$ is the field of real numbers. $\mathbb{C}^d$ is the vector space of dimension d with entries from $\mathbb{C}$. MUBs are sets of bases for $\mathbb{C}^d$.

Definition 2.2. [104, §2] The *inner product* of two vectors $\vec{x}$ and $\vec{y}$ may be denoted as

$$\vec{x}^*\vec{y} \qquad \text{or} \qquad \langle\vec{x}|\vec{y}\rangle. \tag{2.1}$$

The Dirac notation (Bra, ket) favoured in physics literature will only be used in the sense of the inner product.

Definition 2.3. [104, §1,2] A *basis* B for a vector space is a set of vectors such that any element in the space can be given as a linear combination of the elements of B. A basis is *orthonormal* if all vectors are mutually orthogonal and of unit length.

The vectors of a basis may be represented as the columns of a matrix. Where context is clear we equate a basis with a matrix containing the basis vectors as its columns. This is not strictly correct as the order of columns within a matrix is fixed, but the order of the vectors in a set is not.

We have now introduced enough notation to define MUBs, however many more concepts are needed to construct and describe properties of MUBs.

Definition 2.4. [75, §2 Ex 5] The *standard basis* E_d, of $\mathbb{C}^d$ is $E_d = \{\vec{e}_0, \vec{e}_1, \ldots, \vec{e}_{d-1}\}$ where $e_{k_k} = 1$ and $e_{k_a} = 0$ for $k \neq a$, $0 \leq k$, $a \leq d-1$.

The matrix of E_d is a permutation of the columns of I_d.

Definition 2.5. [104, §2] $\mathbb{M}_d(\mathbb{C})$ is the space of all $d \times d$ matrices with entries from $\mathbb{C}$. A matrix $A \in \mathbb{M}_d(\mathbb{C})$ is *unitary* if $A^*A = I_d$. A is *Hermitian* if $A = A^*$. M is *diagonal* if $(A)_{ij} = 0$ for all $i \neq j$.

The matrix of an orthonormal basis is unitary.

Definition 2.6. [104, §2] Let $A \in \mathbb{M}_d(\mathbb{C})$ be a matrix, λ a scalar and $\vec{x}$ a vector such that

$$A\vec{x} = \lambda\vec{x} \tag{2.2}$$

then $\vec{x}$ is an *eigenvector* and λ is the corresponding *eigenvalue* of A. If the set of eigenvectors form a basis for $\mathbb{C}^d$ then this is called the *eigenbasis*

The eigenvalues are solutions to the *characteristic equation*

$$\det(\lambda I_d - A) = 0. \tag{2.3}$$

Theorem 2.7. *[104, §24] Let A be a matrix such that $A^*A = AA^*$, and Λ a diagonal matrix with the eigenvalues of A along the diagonal, then there exists a unitary matrix U, such that*

$$A = U\Lambda U^*. \tag{2.4}$$

This is the diagonalisation *of A, and the columns of U are the eigenvectors of A. Let $\vec{u}_i$ be the i^{th} column of U, and λ_i the eigenvalue, $(\Lambda)_{ii}$, then*

$$A = \sum_{i=0}^{d-1} \lambda_i \vec{u}_i \vec{u}_i^*. \tag{2.5}$$

This is the spectral decomposition *of A.*

Unitary and Hermitian matrices are diagonalisable. The eigenvectors of a matrix A form an orthogonal basis if and only if A is diagonalisable. An eigenvalue λ of a matrix A may appear more than once in the diagonal matrix Λ of equation (2.4).

Definition 2.8. The *algebraic multiplicity* of an eigenvalue of a matrix $A \in \mathbb{M}_d(\mathbb{F})$ is its multiplicity in the solution to the characteristic equation.

Definition 2.9. [104, §3] The *trace* of a square matrix is the sum of the entries on the main diagonal.

$$Tr(A) = \sum_i (A)_{ii} \tag{2.6}$$

Not to be confused with trace of a field element (Definition 2.30). For square matrices A and B, $\mathrm{Tr}(A^*B)$ forms an inner product. Matrices are *orthogonal* if $\mathrm{Tr}(A^*B) = 0$.

Lemma 2.10. *[104, Thm 24.6] The trace of a matrix is equal to the sum of its eigenvalues counted with algebraic multiplicity*

For vectors $\vec{x}, \vec{y} \in \mathbb{C}^d$

$$\mathrm{Tr}(\vec{x}\vec{y}^*) = \vec{x}^*\vec{y} = \langle \vec{x} | \vec{y} \rangle. \tag{2.7}$$

Definition 2.11. [102, §2.6] Let A be an $m \times n$ matrix and B an $m' \times n'$ matrix. The *Kronecker product* $A \otimes B$ is the $mm' \times nn'$ matrix defined by

$$(A \otimes B)_{ij} = (A)_{vw} (B)_{xy} \quad \text{where } i = vm + x, \quad j = wn + y. \tag{2.8}$$

Each entry of A has been replaced by a scaled copy of B.

Definition 2.12. [104, §2] The *Kronecker delta* is a function

$$\delta_{x,y} = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{if } x \neq y. \end{cases} \tag{2.9}$$

The standard basis vectors and the identity matrix may be defined using the Kronecker delta:

$$E_d = \{\vec{e}_k : e_{k_a} = \delta_{k,a}\} \tag{2.10}$$

$$(I_d)_{ij} = \delta_{i,j}. \tag{2.11}$$

Quantum physics

Quantum physics is a mathematical formalism for describing and representing the behaviour of objects such as photons and electrons. We give some definitions that are commonly used in quantum physics and in particular in quantum information theory, the subdiscipline of physics that the applications of MUBs belong to.

Definition 2.13. An *operator* is a mapping between vector spaces.

Quantum information theory uses operators $U : \mathbb{C}^d \mapsto \mathbb{C}^d$ in which case the *operator* may be represented as a matrix from $\mathbb{M}_d(\mathbb{C})$. An operator which is Hermitian is called an *observable* [6].

Definition 2.14. [6, §4.6.2] A *density matrix* is a Hermitian matrix, $A \in \mathbb{M}_d(\mathbb{C})$, such that $\mathrm{Tr}(A) = 1$ and $\vec{x}^* A \vec{x} \geq 0$ for all $\vec{x} \in \mathbb{C}^d$.

The state of a quantum system is represented as a density matrix.

Definition 2.15. [104, §6] A *projection* matrix is a matrix P which satisfies

$$P = P^2. \tag{2.12}$$

The name projection arises from the idea that $P\vec{v}$ is the 'shadow projected' by $\vec{v}$ onto space spanned by P. The matrix $P_i = \vec{u}_i \vec{u}_i^*$ with $\vec{u}_i$ as in equation (2.5) is a projection matrix, when $|u_i| = 1$:

$$P_i^2 = \vec{u}_i \vec{u}_i^* \vec{u}_i \vec{u}_i^* = \langle \vec{u}_i | \vec{u}_i \rangle \vec{u}_i \vec{u}_i^* = \vec{u}_i \vec{u}_i^*. \tag{2.13}$$

Definition 2.16. [6, §3.1] The *Pauli matrices* are

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.14}$$

The Pauli matrices provide a basis for the space of 2×2 Hermitian matrices, which are used to describe the properties of quantum objects in $\mathbb{C}^2$. Any Hermitian matrix A in $\mathbb{M}_2(\mathbb{C})$ may be written as

$$A = \lambda_0 I_2 + \lambda_x \sigma_x + \lambda_y \sigma_y + \lambda_z \sigma_z \tag{2.15}$$

where all the coefficients λ_i are real. The Pauli matrices have been generalised for larger dimensions.

Definition 2.17. [5] The *generalised Pauli matrices* are defined as:

$$X_d\vec{e}_i = \vec{e}_{i+1} \qquad Z_d\vec{e}_i = \omega_d^i\vec{e}_i \tag{2.16}$$

where $\vec{e}_i$ is the i^{th} standard basis vector of $\mathbb{C}^d$ and ω_d is a d^{th} root of unity.

The generalised Pauli matrices have a physical interpretation. X_d is the *position* operator and Z_d is the *momentum* operator [99].

For example

$$X_3 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad Z_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega_3 & 0 \\ 0 & 0 & \omega_3^2 \end{pmatrix} \tag{2.17}$$

The generalised Pauli matrices have the following properties [5, 41, 25]

$$Z_dX_d = \omega_dX_dZ_d \tag{2.18}$$

$$(X_d)^j(Z_d)^k\vec{e}_i = \omega^{ki}\vec{e}_{i+j} \tag{2.19}$$

$$X_d^d = Z_d^d = I_d \tag{2.20}$$

$$\mathrm{Tr}(X_d^jZ_d^k) = 0 \qquad \text{for } j,k \text{ not both equal to } d. \tag{2.21}$$

2.2.2 Abstract Algebra

All known constructions of MUBs use Galois fields and Galois rings. We give some definitions and basic results.

Groups, Rings and Fields

A group is one of the more basic structures in algebra. Fields and rings have a group as a substructure. All results on groups apply to fields and rings.

Definition 2.18. [40, Def 1.3.1] A *group* $\langle G, \star\rangle$ is a set G closed under a binary operation $\star$, such that the following axioms are satisfied:

- *Associativity*: $(a \star b) \star c = a \star (b \star c)$ for all $a, b, c \in G$.

- *Identity*: There exists an element of G, denoted 1_G, such that $1_G \star a = a \star 1_G = a$ for all $a \in G$.
- *Inverse*: For each $a \in G$ there is a corresponding a' such that $a \star a' = a' \star a = 1_G$.

If in addition $\langle G, \star \rangle$ satisfies the following then it is an *Abelian* group.

- *Commutativity*: $a \star b = b \star a$ for all $a, b \in G$.

For notational convenience, when the operation is obvious $\langle G, \star \rangle$ will be denoted as G.

Definition 2.19. [40, Defi 1.4.4, 2.3.2, 3.1.19] Let G be a group. A *subgroup*, H, of G is a subset of G that is also a group. For $a \in G$, the subset aH is a left *coset* and Ha is a right *coset* of H with

$$aH = \{ah : h \in H\} \qquad Ha = \{ha : h \in H\}. \tag{2.22}$$

A subgroup is *normal* if its left and right cosets coincide.

$$aH = Ha \qquad \forall a \in G. \tag{2.23}$$

In an Abelian group, the left and right cosets always coincide.

Definition 2.20. [40, Defi 5.1.1] A *ring* $\langle R, +, \cdot \rangle$ is a set R closed under two binary operations such that the following axioms are satisfied.

- $\langle R, + \rangle$ is an Abelian group.
- $\cdot$ is associative.
- For all $a, b, c \in R$ the *left distribution* law, $a(b + c) = (ab) + (ac)$, and *right distribution* law, $(a + b)d = (ad) + (bd)$ hold.

Let 0 be the identity element of $\langle R, + \rangle$, and $R^* = R \setminus \{0\}$. Then $\langle R, +, \cdot \rangle$ is a *field* if $\langle R^*, \cdot \rangle$ is an Abelian group.

As with groups, where the operations are implied, the ring $\langle R, +, \cdot \rangle$ will be denoted R. $\mathbb{F}$ is the usual notation for a field.

Definition 2.21. [40, Defi 6.1.10] A subring N of a ring R is an ideal if it satisfies

$$aN \subseteq N \qquad \text{and} \qquad Na \subseteq N \qquad \forall a \in R. \tag{2.24}$$

Definition 2.22. [40, Defi 5.2.13] The *characteristic* of a ring R is the least positive integer n such that $\sum_{i=1}^{n} x = 0$ for all $x \in R$. If no such n exists then R has characteristic 0.

$\mathbb{C}$ and $\mathbb{R}$ are fields of characteristic 0.

Definition 2.23. ω_d is a d^{th} root of unity.

$$\omega_d = e^{2i\pi/d}. \tag{2.25}$$

Where context is clear ω will be used without subscript.

The following result is obvious but important.

Lemma 2.24.

$$\sum_{k=1}^{np} \omega_p^k = 0, \tag{2.26}$$

where n is any positive integer, p is a prime.

Definition 2.25. [76, §5] A *character* is a homomorphism from a finite Abelian group to the unit circle in $\mathbb{C}$.

We make extensive use of characters of the additive group of a Galois field to construct MUBs. There are some general properties which apply to all characters on all groups.

Lemma 2.26. *[76, §5.1] The set of characters of a group is a group, denoted $G^\wedge$.*

χ_0 is the *trivial* character where $\chi_0(x) = 1$ for all $x \in G$.

Lemma 2.27. *[11, Thm 3.4] Let $G^\wedge$ be the group of characters of a group G then*

$$\sum_{\chi \in G^\wedge} \chi(x) = \begin{cases} |G| & \text{for } x = 1_G \\ 0 & \text{otherwise,} \end{cases} \tag{2.27}$$

$$\sum_{x \in G} \chi(x) = \begin{cases} |G| & \text{for } \chi = \chi_0 \\ 0 & \text{otherwise.} \end{cases} \tag{2.28}$$

For some characters, equation (2.28) is equivalent to Lemma 2.24.

Galois Fields

Definition 2.28. [40, 8.5.10] Let p be a prime and $h(x)$ a primitive polynomial of degree r over $\mathbb{Z}_p$. If $q = p^r$ then the *Galois field* $\mathbb{F}_q$ of characteristic p is defined to be the quotient field $\mathbb{Z}_p[x]/(h(x))$.

$\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ is a cyclic group under multiplication.

Theorem 2.29. *[40, Thm 8.5.10] A Galois field of order q exists if and only if q is a power of a prime.*

Definition 2.30. [40, Ex 9.17] Let $\alpha \in F = \mathbb{F}_{q^n}$ and $K = \mathbb{F}_q$. Then the *trace* of F over K is given by

$$\mathrm{tr}_{F/K}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}}. \tag{2.29}$$

If q is a prime, then this is referred to as the *absolute trace*.

We will always use the absolute trace and refer to it as the trace.

Theorem 2.31. *[107, Thm 7.12] Let $\mathbb{F}_q$ be a Galois field of characteristic p. For $x, y \in \mathbb{F}_q$ and $a \in \mathbb{F}_p$:*

$$\mathrm{tr}(x) \in \mathbb{F}_p \tag{2.30}$$

$$\mathrm{tr}(x+y) = \mathrm{tr}(x) + \mathrm{tr}(y) \tag{2.31}$$

$$\mathrm{tr}(ax) = a\mathrm{tr}(x) \tag{2.32}$$

$$\mathrm{tr}(x^p) = \mathrm{tr}(x). \tag{2.33}$$

Let $q = p^r$ and ω_p be a primitive p^{th} root of unity. We use two characters of $\mathbb{F}_q$. All additive characters, χ, over $\mathbb{F}_q$ are of the form [76, eqn 5.6]

$$\chi_a(x) = \omega_p^{\mathrm{tr}(ax)} \tag{2.34}$$

χ_1 is denoted as χ. This character is used to construct MUBs in odd prime power dimensions. Another character we make use of is the quadratic character η over $\mathbb{F}_q^*$:

$$\eta(x) = \begin{cases} 1 & \text{if } x \text{ is the square of an element in } \mathbb{F}_q \\ -1 & \text{otherwise.} \end{cases} \tag{2.35}$$

In general, sums of characters are difficult to evaluate, and only known explicitly in a few cases. Lemma 2.27 and Theorem 2.33 are a few of the known cases.

Definition 2.32. [76, §5.2] Let η be the quadratic character and χ an additive character of $\mathbb{F}_q$. Then the Gaussian sum is defined by

$$G(\eta, \chi) = \sum_{c \in \mathbb{F}_q^*} \eta(c)\chi(c). \tag{2.36}$$

Theorem 2.33. *[76, Thm 5.33] Let χ be a non-trivial additive character of $\mathbb{F}_q$ with q odd and let $f(x) = a_2x^2 + a_1x + a_0 \in \mathbb{F}_q[x]$ and $a_2 \neq 0$. Then*

$$\sum_{x \in \mathbb{F}_q} \chi(f(x)) = \chi\left(a_0 - \frac{a_1^2}{4a_2}\right)\eta(a_2)G(\eta, \chi), \tag{2.37}$$

where η is the quadratic character of $\mathbb{F}_q$ and G is the Gaussian Sum.

This character sum is required to prove the accuracy of some constructions of MUBs.

Just as a vector space has a basis, a field may also have a basis.

Definition 2.34. [76, Defi 2.30] Let $q = p^r$. If all elements $x \in \mathbb{F}_q$ can be written as

$$x = c_1a_1 + c_2a_2 + \cdots + c_ra_r \qquad c_i \in \mathbb{F}_p \tag{2.38}$$

then $\{a_1, \ldots, a_r\}$ is a *basis* for $\mathbb{F}_q$. Two bases $\{a_1, \ldots, a_r\}$ and $\{b_1, \ldots, b_r\}$ of $\mathbb{F}_q$ are *dual* if

$$\mathrm{tr}(a_ib_j) = \delta_{i,j}. \tag{2.39}$$

Every basis has a unique dual basis. Some bases are self dual.

Functions

The functions described below also apply to more general structures, including multidimensional functions. However they will only be used in the context of a single dimension function, and thus will be quoted for this restricted setting.

Definition 2.35. [76, §7.1] A *permutation* function h on a group G is a function that induces a permutation on G.

Definition 2.36. [57, §3.5.2] For groups G and H and a function $f : G \mapsto H$, for each $a \in G$ we define the *difference operator* by:

$$\Delta_{f,a}(x) = f(x + a) - f(x). \tag{2.40}$$

f is *perfect non-linear* if $\Delta_{f,a}$ is uniformly distributed. If $|G| = |H|$ and f is a perfect non-linear function, then $\Delta_{f,a}$ is a permutation function for each $a \in G \setminus \{1_G\}$, and f is called *planar*.

Planar functions are so called because they can be used to construct projective planes (see Theorem 3.22). It is known that for a planar function to exist, $|G|$ must be odd [30, Thm 5.13]. If G is Abelian, then $|G|$ must be an odd prime power [12, Cor 1.3].

Conjecture 2.37. *Planar functions only exist in groups of odd prime power order.*

This is a sub conjecture of the wider question on the existence of projective planes (Question 1.6).

Definition 2.38. [57, Defi 9.17] Let G be a finite Abelian group of order d. A function $f : G \mapsto \mathbb{C}$ is *bent* if

$$\left| \sum_{x \in G} f(x)\chi(x) \right| = \sqrt{q} \qquad \forall \chi \in G^{\wedge}. \tag{2.41}$$

A narrower version of the above definition is more useful in our case. Let G and H be finite Abelian groups and $g : G \mapsto H$. Then g is *bent* if for some character $\eta \in H^{\wedge}$,

$$\left| \sum_{x \in G} \eta(g(x))\chi(x) \right| = \sqrt{|G|} \qquad \forall \chi \in G^{\wedge}. \tag{2.42}$$

Definition 2.39. [57, Defi 9.51] Let G and H be groups. A function $f : G \mapsto H$ is *differentially* 1*-uniform* if for every $(a, b) \neq (0, 0) \in G \times H$, there is at most one $x \in G$ such that

$$\Delta_{f,a}(x) \quad = b. \tag{2.43}$$

If $|G| = |H|$ then a differentially 1- uniform function is planar [57, §9.2.2]. The names bent, perfect non-linear and planar come from some of the applications where these polynomials were first studied. The name perfect non-linear is also used for multidimensional planar functions. A good summary is provided in [20].

Theorem 2.40. *[57, Thm 9.19] Let G and H be finite Abelian groups such that $|G| = |H|$. A function $g : G \mapsto H$ is bent if and only if it is perfect non-linear.*

Bent and planar functions will be used to describe and construct MUBs in prime power dimensions.

Galois Rings

Galois rings do not find as many applications as Galois fields, thus not all books on algebra include a thorough treatment of Galois rings. An excellent reference on Galois rings is [107]. Galois rings are used to construct MUBs in even prime power dimensions.

Definition 2.41. [107, §14] Let p be a prime. Let $h(x)$ be a monic irreducible polynomial of degree r in $\mathbb{Z}_{p^s}$. The *Galois ring*, $GR(p^s, r)$, of characteristic p^s, is the residue classes of

$$\mathbb{Z}_{p^s}[x]/(h(x)). \tag{2.44}$$

The trace and additive characters are defined analogously as for Galois fields (Definition 2.30, equation (2.34)). The properties of the trace as described in Theorem 2.31 also apply to Galois rings [107, Thm 14.34].

There exists a non-zero element $\zeta \in GR(p^s, r)$ which is a root of $h(x)$. Elements of $GR(p^s, r)$ have a p-adic representation

$$g = a_0 + pa_1 + \cdots + p^{s-1}a_{s-1}, \tag{2.45}$$

where each a_i belongs to the *Teichmüller set*

$$\mathcal{T}_r = \{0, 1, \zeta, \zeta^2, \ldots, \zeta^{p^r-2}\}. \tag{2.46}$$

All elements g with $a_0 = 0$ are zero or zero divisors, all elements with $a_0 \neq 0$ are units. The set of zero divisors an 0 forms a group, denoted H. For $GR(p^2, r)$, $H = p\mathcal{T}_r$, $\mathcal{T}_r \cong \mathbb{F}_{p^r}$ [107, Thm 13.2].

Definition 2.42. [107, Thm 13.1] We define the ring homomorphism $^-$: $GR(p^s, r) \mapsto \mathbb{F}_{p^r}$ by

$$\overline{g} = \overline{a_0 + pa_1 + \cdots + p^{s-1}a_{s-1}} = a_0. \tag{2.47}$$

So far Galois rings and Galois fields are the only two algebraic structures which have been used to construct MUBs. There are many other algebraic structures which have not as yet been applied to the constructions of MUBs.

2.3 Mutually Unbiased Bases

2.3.1 Definitions of MUBs

The object of study in this thesis is mutually unbiased bases. We give several equivalent definitions and preliminary results to acquaint the reader with the 'star' of this study.

MUBs may be defined as a set of vectors or a set of matrices. Depending on the situation it may be more convenient to work with one or the other.

Definition 2.43. [112, Eqn 1] Two orthonormal bases B_0 and B_1 in $\mathbb{C}^d$ are called *mutually unbiased* if and only if

$$|\langle \vec{x}|\vec{y}\rangle|^2 = \frac{1}{d} \qquad \forall \vec{x} \in B_0 \text{ and } \vec{y} \in B_1. \tag{2.48}$$

A set of MUBs may be characterised as a set of $d \times d$ matrices. We need each column of each matrix B to have modulus 1 and each pair of columns to be orthogonal. A unitary matrix satisfies this. The inner product of a column from B_0 with any column from B_1 must have modulus $\frac{1}{\sqrt{d}}$ which is satisfied by the following:

Definition 2.44. [15] A set $\{B_0, \ldots, B_n\}$ is a set of $n+1$ MUBs provided that each B_i is unitary, and

$$B_x^* B_y = M \qquad \text{where} \quad |(M)_{ij}|^2 = \frac{1}{d} \qquad \forall\ 0 \leq i, j \leq n,\ \forall x \neq y. \tag{2.49}$$

This characterisation of MUBs will be further developed in section 2.4.3. The following is a set of objects, from which a set of MUBs can always be constructed. This is not a definition of MUBs, but a criteria that may be used to search for MUBs.

Theorem 2.45. *[5, Thm 3.2] Let $\mathcal{B}$ be a basis for $\mathbb{M}_d(\mathbb{C})$ consisting of unitary matrices which are orthogonal under the trace inner product and can be partitioned as*

$$\mathcal{B} = \{I_d\} \cup \mathcal{C}_0 \cup \cdots \cup \mathcal{C}_d \tag{2.50}$$

where each class $\mathcal{C}_j$ contains $d-1$ commuting matrices. Then the eigenbases for each class form a set of $d+1$ MUBs in $\mathbb{C}^d$.

Proof. Let $\mathcal{C}_j = \{U_{j,1}, \ldots, U_{j,d-1}\}$ and $U_{j,0} = I_d$, for any $0 \leq j \leq d$. Then

$$\mathcal{C}_j \cup \{I_d\} = \{U_{j,0}, U_{j,1}, \ldots, U_{j,d-1}\} \tag{2.51}$$

is a maximal set of commuting orthogonal unitary matrices. For each $1 \leq j \leq d+1$ there exists an orthonormal basis P_j such that

$$U_{j,t} = P_j D_{j,t} P_j^{-1} \tag{2.52}$$

where $D_{j,t}$ is a diagonal matrix. Let

$$\lambda_{j,t,i} := (D_{j,t})_{ii}, \qquad (M_j)_{ti} := \lambda_{j,t,i} \tag{2.53}$$

Then M_j is a unitary $d \times d$ matrix. Note that, since $U_{j,0} = I_d$, $(M_j)_{0i} = 1$, for all $0 \leq i \leq d-1$.

Consider $\mathcal{C}_1$ and $\mathcal{C}_2$. Then for $0 \leq s, t \leq d-1$ the orthogonality condition requires that

$$\mathrm{Tr}(U_{1,s}^* U_{2,t}) = d\delta_{s,0}\delta_{t,0}. \tag{2.54}$$

Let $\vec{p}_{j,k}$ be the vector which is the k^{th} column of P_j. Since $\mathrm{Tr}(\vec{p}_{1,k}\vec{p}_{2,l}^*) = \langle \vec{p}_{1,k} | \vec{p}_{2,l} \rangle$,

$$\begin{aligned}
\mathrm{Tr}(U_{1,s}^* U_{2,t}) &= \mathrm{Tr}\left(\sum_{k=1}^{d} \sum_{l=1}^{d} \lambda_{1,s,k}^* \lambda_{2,t,l} \vec{p}_{1,k} \vec{p}_{1,k}^* \vec{p}_{2,l} \vec{p}_{2,l}^* \right) && (2.55)\\
&= \sum_{k=0}^{d-1} \sum_{l=0}^{d-1} \lambda_{1,s,k}^* \lambda_{2,t,l} \vec{p}_{1,k}^* \vec{p}_{2,l} \mathrm{Tr}(\vec{p}_{1,k} \vec{p}_{2,l}^*) && (2.56)\\
&= \sum_{k=0}^{d-1} \sum_{l=0}^{d-1} \lambda_{1,s,k}^* \lambda_{2,t,l} |\langle \vec{p}_{1,k} | \vec{p}_{2,l} \rangle|^2. && (2.57)
\end{aligned}$$

Then combine equations (2.54) and (2.57) to get :

$$\sum_{k=1}^{d} \sum_{l=1}^{d} \lambda_{1,s,k}^* \lambda_{2,t,l} |\langle \vec{p}_{1,k} | \vec{p}_{2,l} \rangle|^2 = d\delta_{s,0}\delta_{t,0}. \tag{2.58}$$

Which can be written in matrix form as $A\vec{x} = \vec{b}$ where

$$A = M_1^* \otimes M_2 \tag{2.59}$$

$$\vec{x} = (|\langle \vec{p}_{1,0}|\vec{p}_{2,0}\rangle|^2, |\langle \vec{p}_{1,0}|\vec{p}_{2,1}\rangle|^2, |\langle \vec{p}_{1,0}|\vec{p}_{2,2}\rangle|^2, \ldots, |\langle \vec{p}_{1,d-1}|\vec{p}_{2,d-1}\rangle|^2)^T \tag{2.60}$$

$$\vec{b} = d\vec{e}_0. \tag{2.61}$$

Note that A is unitary, thus $\vec{x} = A^*\vec{b}$; from which it follows that

$$|\langle p_{1,s}|p_{2,t}\rangle|^2 = \frac{1}{d} \quad 0 \leq s, t \leq d-1. \tag{2.62}$$

Hence P_1 and P_2 are unbiased bases. Repeating for each of the classes we conclude that $\{P_0, P_1, \ldots, P_d\}$ are a set of $d+1$ MUBs in $\mathbb{C}^d$. □

Constructing sets of matrices which obey the conditions of Theorem 2.45 is an indirect method for constructing MUBs. This fact is exploited in the Pauli matrix construction (Theorem 2.56), and in computational searches [44].

2.3.2 Bounds on the number of MUBs

In this section we give some bounds on the size of a set of MUBs.

Definition 2.46. [64, §4] Let $N(d)$ be the maximum number of MUBs in $\mathbb{C}^d$.

Theorem 2.47. *[112, Eq 9]* $N(d) \leq d+1$.

Proof. A d dimensional quantum state is represented as a $d \times d$ density matrix, D. Let

$$T_D = D - \frac{1}{d} I_d \tag{2.63}$$

then T_D is a Hermitian matrix of trace zero. Let $\mathcal{T} \subset \mathbb{M}_d(\mathbb{C})$ be the space of all Hermitian matrices of trace 0. There are d^2 entries in $T \in \mathcal{T}$. The d diagonal entries of T must be chosen such that $\mathrm{Tr}(T) = 0$, hence one entry is forced and the dimension of $\mathcal{T}$ is $d^2 - 1$.

Let $\{B_0, B_1, \ldots, B_n\}$ be a set of MUBs in $\mathbb{C}^d$ represented as $d \times d$ matrices. Let $\vec{b}_{ij}$ be the j^{th} column of B_i.

Let $\mathcal{T}_i$ be the $d-1$ dimensional subspace spanned by the matrices $\vec{b}_{ij}\vec{b}_{ij}^* - \frac{1}{d}I_d$ with $0 \leq j \leq d-1$. To see that $\mathcal{T}_i$ is $d-1$ dimensional, note that $\sum_{i=0}^{d-1} \vec{e}_i\vec{e}_i^* - \frac{1}{d}I_d = [0]$.

$$\begin{aligned} \mathrm{Tr}\left[(\vec{b}_{ij}\vec{b}_{ij}^* - \frac{1}{d}I_d)(\vec{b}_{kl}\vec{b}_{kl}^* - \frac{1}{d}I_d)\right] &= \mathrm{Tr}(\vec{b}_{ij}\vec{b}_{ij}^*\vec{b}_{kl}\vec{b}_{kl}^*) - \frac{1}{d} && (2.64)\\ &= \langle\vec{b}_{ij}|\vec{b}_{kl}\rangle^2 - \frac{2}{d} + \frac{1}{d} && (2.65)\\ &= 0. && (2.66)\end{aligned}$$

Thus any element of $\mathcal{T}_i$ is orthogonal to any element of $\mathcal{T}_k$ for $i \neq k$.

There is then a maximum of $\frac{d^2-1}{d-1} = d+1$ subspaces $\mathcal{T}_i$ and hence a maximum of $d+1$ mutually unbiased bases. □

Definition 2.48. [112] A set of $d+1$ MUBs in $\mathbb{C}^d$ is a *complete* set of MUBs.

The applications of MUBs described in section 1.1.3 rely on complete sets, thus much of the interest in MUBs is aimed at finding complete sets. Constructions will be given in section 2.4 of complete sets of MUBs in all prime power dimensions.

Theorem 2.49. *[112] Complete sets of MUBs exist in $\mathbb{C}^d$ when d is a power of a prime.*

It is also of interest to find the maximum size of a set of MUBs, even if complete sets do not exist. The following theorem gives a lower bound.

Theorem 2.50. *[64, Lem 3] Let $d = p_1^{a_1}p_2^{a_2}\dots p_r^{a_r}$ be the prime power decomposition of d. Then*

$$N(d) \geq \min\{N(p_1^{a_1}), N(p_2^{a_2}), \dots, N(p_r^{a_r})\}. \tag{2.67}$$

Proof. Let $m = \min\{N(p_1^{a_1}), N(p_2^{a_2}), \dots, N(p_r^{a_r})\}$ and $q = p_i^{a_i}$ such that $m = N(p_i^{a_i})$, then we have m MUBs $B_1, \dots, B_m$ of $\mathbb{C}^q$. Let $s = \frac{d}{q}$. Then

$$\left\{\bigotimes^{s} B_k : k = 1, \dots, m\right\} \tag{2.68}$$

is a set of m mutually unbiased bases in $\mathbb{C}^d$. □

This is referred to as the 'reduce to prime powers' construction and is a lower bound on the maximum number of MUBs. It is known that this lower bound is not sharp since more MUBs can be constructed in certain square dimensions [110] (see section 3.2.6). Combining Theorems 2.49 and 2.50 we find that

Corollary 2.51. *[64] At least three MUBs exist in all dimensions.*

2.4 Constructions of complete sets of MUBs

Complete sets of MUBs are known in prime power dimensions. This knowledge comes from constructions using Galois fields and Galois rings. There are two different construction methods which use Galois fields, one uses planar functions and the other generalised Pauli matrices. We expound several constructions which appear in the literature and then show that some of them are equivalent. A construction which gives incomplete sets of MUBs, but more than the lower bound of Theorem 2.50 will be presented in section 3.2.6.

2.4.1 Galois Fields

Planar functions

We begin with the most general construction. This uses planar functions over a Galois field. There is an ongoing search to find new planar functions, which will then result in new sets of MUBs. The following is a narrowing of a result which used differentially 1-uniform functions.

Theorem 2.52 (Planar function construction)**.** *[93, Thm 4.1] Let $\mathbb{F}_q$ be a field of odd characteristic p. Let $\Pi(x)$ be a planar function on $\mathbb{F}_q$. Let $V_a := \{v_{ab} : b \in \mathbb{F}_q\}$ be the set of vectors*

$$\vec{v}_{ab} = \frac{1}{\sqrt{q}} \left(\omega_p^{\mathrm{tr}(a\Pi(x)+bx)}\right)_{x\in\mathbb{F}_q} = \frac{1}{\sqrt{q}} \Big(\chi\left(a\Pi(x) + bx\right)\Big)_{x\in\mathbb{F}_q} \qquad \textit{with } a, b \in \mathbb{F}_q. \tag{2.69}$$

The standard basis E along with the sets V_a, $a \in \mathbb{F}_q$, form a complete set of $q+1$ MUBs in $\mathbb{C}^q$.

Proof. Let $\vec{v}_{ab}$ be as given in equation (2.69). We must show that

$$|\langle \vec{v}_{ab} | \vec{v}_{cd} \rangle| = \begin{cases} 1 & \text{for } a = c, b = d \\ 0 & \text{for } a = c, b \neq d \\ \frac{1}{\sqrt{q}} & \text{otherwise} \end{cases} \tag{2.70}$$

$$\begin{aligned} \langle \vec{v}_{ab} | \vec{v}_{ab} \rangle &= \frac{1}{q} \sum_{x\in\mathbb{F}_q} \omega_p^{\mathrm{tr}[(a-a)\Pi(x)+(b-b)x]} && (2.71)\\ &= \frac{1}{q} \sum_{x\in\mathbb{F}_q} 1 && (2.72)\\ &= 1 && (2.73) \end{aligned}$$

Let $b \neq d$,

$$\langle \vec{v}_{ab} | \vec{v}_{ad} \rangle = \frac{1}{q} \sum_{x \in \mathbb{F}_q} \omega_p^{\mathrm{tr}[(a-a)\Pi(x)+(b-d)x]} \tag{2.74}$$

$$= \frac{1}{q} \omega_p^{\mathrm{tr}(b-d)} \sum_{x \in \mathbb{F}_q} \omega_p^{\mathrm{tr}(x)}. \tag{2.75}$$

Apply Lemma 2.27 to find that $\sum_{x \in \mathbb{F}_q} \omega_p^{\mathrm{tr}(x)} = 0$ and hence $\langle \vec{v}_{ab} | \vec{v}_{ad} \rangle = 0$. Each V_a is an orthonormal basis. Next we show that V_a and V_c are unbiased:

$$\langle \vec{v}_{ab} | \vec{v}_{cd} \rangle = \frac{1}{q} \sum_{x \in \mathbb{F}_q} \omega_p^{\mathrm{tr}[(a-c)\Pi(x)+(b-d)x]}. \tag{2.76}$$

Applying Theorem 2.40 we see that

$$\left| \sum_{x \in \mathbb{F}_q} \omega_p^{\mathrm{tr}[(a-c)\Pi(x)+(b-d)x]} \right| = \sqrt{q} \tag{2.77}$$

and hence

$$|\langle \vec{v}_{ab} | \vec{v}_{cd} \rangle| = \frac{1}{q}\sqrt{q} = \frac{1}{\sqrt{q}}. \tag{2.78}$$

Each pair V_a and V_c are unbiased when $a \neq c$. Each entry of each vector has magnitude $\frac{1}{\sqrt{q}}$, therefore each V_a is unbiased to the standard basis. □

Since x^2 is a planar function for all Galois fields (see Lemma 3.24), the next construction is a special case of the planar function construction. We write it explicitly as it is used later. This construction was first shown for prime dimensions by Ivanovic [59], generalised to prime powers by Wootters and Fields [112], then given in the simplified form below by Klappenecker and Rötteler [64].

Theorem 2.53 (WF Construction)**.** *[64, Thm 2] Let $\mathbb{F}_q$ be a finite field of odd characteristic p and $\omega := e^{2i\pi/p}$. Let $V_a := \{\vec{v}_{ab} : b \in \mathbb{F}_q\}$ be the set of vectors*

$$\vec{v}_{ab} := \frac{1}{\sqrt{q}} \left(\omega^{\mathrm{tr}(ax^2+bx)} \right)_{x \in \mathbb{F}_q} = \frac{1}{\sqrt{q}} \Big(\chi \left(ax^2 + bx \right) \Big)_{x \in \mathbb{F}_q} \quad \text{with } a, b \in \mathbb{F}_q. \tag{2.79}$$

The standard basis E along with the sets V_a, $a \in \mathbb{F}_q$, form a complete set of $q+1$ MUBs in $\mathbb{C}^q$.

Proof.

$$|\langle \vec{v}_{ab} | \vec{v}_{cd} \rangle| = \left| \frac{1}{q} \sum_{x \in \mathbb{F}_p} \chi\left((c-a)x^2 + (d-b)x\right) \right|. \tag{2.80}$$

Using Theorem 2.27, if $a = c$, then equation (2.80) evaluates to 1 if $b = d$ and 0 if $b \neq d$. This shows the vectors in V_a are orthonormal. Using Theorem 2.33 we see that if $a \neq c$ then $|\langle \vec{v}_{ab} | \vec{v}_{cd} \rangle| = \frac{1}{\sqrt{q}}$. Each entry of each vector has magnitude $\frac{1}{\sqrt{q}}$, therefore each V_a is unbiased to the standard basis. □

The next construction was the first published construction of a complete set of MUBs in 1980 [1]. The construction has been generalised to all prime powers by Klappenecker and Rötteler in 2003 [64].

Theorem 2.54 (Alltop Construction)**.** *[64, Thm 1] Let $\mathbb{F}_q$ be a finite field of odd characteristic $p \geq 5$ and $\omega := e^{2i\pi/p}$. Let $V_a := \{\vec{v}_{ab} : b \in \mathbb{F}_q\}$ be the set of vectors*

$$\vec{v}_{ab} := \frac{1}{\sqrt{q}} \left(\omega^{\mathrm{tr}((x+b)^3 + a(x+b))} \right)_{x \in \mathbb{F}_q} = \frac{1}{\sqrt{q}} \left(\chi\left((x+b)^3 + a(x+b)\right) \right)_{x \in \mathbb{F}_q} \quad \text{with } a, b \in \mathbb{F}_q. \tag{2.81}$$

The standard basis E along with the sets V_a, $a \in \mathbb{F}_q$, form a complete set of $q+1$ MUBs in $\mathbb{C}^q$.

Proof.

$$|\langle \vec{v}_{ab} | \vec{v}_{cd} \rangle| = \left| \frac{1}{q} \sum_{x \in \mathbb{F}_p} \chi\big(3(a-c)x^2 + (3a^2 - 3c^2 + b - d)x + (a^3 - c^3 + ba - dc)\big) \right| \tag{2.82}$$

which is a quadratic in x. Then use the same logic as Theorem 2.53 to show this is a complete set of MUBs. □

Notice that both of the polynomials in the inner products of the WF and Alltop constructions are quadratic. Godsil and Roy [42, §6] have shown that the sets of MUBs constructed by the Alltop and WF constructions are equivalent (see Theorem 2.65).

Generalised Pauli matrices

The following construction is equivalent to the WF construction when d is an odd prime (see Corollary 2.66). Also note that this construction works for both odd and even prime powers in contrast to the planar function construction which only works for odd prime powers.

Theorem 2.55. *[5, Thm 2.3] Let X_d and Z_d be the generalised Pauli matrices in $\mathbb{M}_d(\mathbb{C})$ (Definition 2.17). For any prime, d, the eigenbases of*

$$Z_d, X_d, X_dZ_d, X_d(Z_d)^2, \ldots, X_d(Z_d)^{d-1} \tag{2.83}$$

are a complete set of MUBs.

Proof. The set of eigenvectors of Z_d are the standard basis vectors. The eigenvectors of $X_d(Z_d)^k$ are

$$\vec{v}_{kt} = \left(\frac{1}{\sqrt{d}}\chi(-tj - k\sigma_j)\right)_{j\in\mathbb{F}_d} \tag{2.84}$$

where $\sigma_j = j + (j+1) + \cdots + (d-1)$. Summing the arithmetic progression:

$$\sigma_j = \frac{1}{2}(d-j)(j+d-1) = \frac{1}{2}(d^2 - j^2 - d + j). \tag{2.85}$$

$$\begin{aligned}
\langle \vec{v}_{kt} | \vec{v}_{lu} \rangle &= \frac{1}{d}\sum_{j=0}^{d-1} \chi\big((t-u)(-j) - (k-l)s_j\big) && (2.86)\\
&= \frac{1}{d}\chi\left(\frac{1}{2}(l-k)(d^2-d)\right)\sum_{j=0}^{d-1}\chi\left((u-t)j + \frac{1}{2}(l-k)(j-j^2)\right) && (2.87)\\
&= \frac{1}{d}\chi\left(\frac{1}{2}(l-k)(d^2-d)\right)\sum_{j=0}^{d-1}\chi\left(\frac{1}{2}(k-l)j^2 + (u-t+\frac{1}{2}l-\frac{1}{2}k)j\right). && (2.88)
\end{aligned}$$

Thus we have a quadratic equation inside the character sum. Following the proof of Theorem 2.53 we conclude that a complete set of MUBs has been constructed. □

This has been extended to all prime powers.

Theorem 2.56 (Pauli matrix construction)**.** *[41] Let $\mathbb{F}_q$ be a field of characteristic p. Let X_p and Z_p be the generalised Pauli matrices in $\mathbb{M}_p(\mathbb{C})$. Let $q = p^r$ and let $E = \{e_1, \ldots, e_r\}$ and $\bar{E} = \{\bar{e}_1, \ldots, \bar{e}_r\}$ be dual bases for $\mathbb{F}_q$. Let $f_i = k\bar{e}_i$ so that $F = k\bar{E}$ for some $k \in \mathbb{F}_{p^r}^*$. Let*

$$T_{ab} = X_p^{a_1}Z_p^{b_1} \otimes X_p^{a_2}Z_p^{b_2} \cdots \otimes X_p^{a_r}Z_p^{b_r} \qquad a, b \in \mathbb{F}_q \tag{2.89}$$

where $a_i = \mathrm{tr}(ak^{-1}f_i) = \mathrm{tr}(a\bar{e_i})$ *and* $b_i = \mathrm{tr}(bke_i)$. *The eigenbases of* $\{T_{ab} : a, b \in \mathbb{F}_q\}$ *are a complete set of MUBs.*

Proof. From equation (2.18)

$$X_p^a Z_p^b X_p^{a'} Z_p^{b'} = \omega_p^{ba'} X_p^{a+a'} Z_p^{b+b'} \tag{2.90}$$

$$X_p^{a'} Z_p^{b'} X_p^a Z_p^b = \omega_d^{ab'} X_p^{a'+a} Z_p^{b'+b}. \tag{2.91}$$

Thus when q is a prime T_{ab} and $T_{a'b'}$ commute if and only if $ab' - ba' = 0$. Since

$$(X_p^{a_1} Z_p^{b_1} \otimes X_p^{a_2} Z_p^{b_2})(X_p^{a_1'} Z_p^{b_1'} \otimes X_p^{a_2'} Z_p^{b_2'}) = X_p^{a_1} Z_p^{b_1} X_p^{a_1'} Z_p^{b_1'} \otimes X_p^{a_2} Z_p^{b_2} X_p^{a_2'} Z_p^{b_2'} \tag{2.92}$$

we find that when q is a power of a prime T_{ab} and $T_{a'b'}$ commute if and only if $a_i b_i' - b_i a_i' = 0$ for each $1 \leq i \leq r$, which can be summarised as

$$\sum_{i=1}^{r} a_i b_i' - b_i a_i' = 0. \tag{2.93}$$

Using equation (2.38) we find that

$$\sum_{i=1}^{r} a_i b_i = \mathrm{tr}(ab) \tag{2.94}$$

and hence equation (2.93) becomes: T_{ab} and $T_{a'b'}$ commute if and only if

$$\mathrm{tr}(ab') - \mathrm{tr}(ba') = 0. \tag{2.95}$$

Let the line $l_{\alpha,\beta,\gamma}$ be a subset of the space $\mathbb{F}_q^2$ such that

$$l_{\alpha,\beta,\gamma} = \{(a, b) : \alpha a + \beta b = \gamma \text{ with } a, b, \in \mathbb{F}_q\}. \tag{2.96}$$

Choose (a, b) and (a', b') so that there exist $\alpha, \beta \in \mathbb{F}_q$

$$\alpha a + \beta b = 0 \quad \text{and} \quad \alpha a' + \beta b' = 0, \tag{2.97}$$

that is (a, b) and (a', b') are on the line $l_{\alpha,\beta,0}$. Then

$$\mathrm{tr}(ab') - \mathrm{tr}(ba') = \mathrm{tr}\left(\frac{-\beta b}{\alpha} b'\right) - \mathrm{tr}\left(b\frac{-\beta b'}{\alpha}\right) = 0, \tag{2.98}$$

which means that T_{ab} and $T_{a'b'}$ commute when (a, b) and (a', b') are both in $l_{\alpha,\beta,0}$. There are q points on each line, and $q + 1$ lines through $(0, 0)$. Thus we have a set which may be

partitioned into $q+1$ subsets of q commuting matrices. Next we need to show orthogonality. From equations (2.21) and (2.90)

$$\mathrm{Tr}(X_p^a Z_p^b X_p^{a'} Z_p^{b'}) = \omega_d^{ba'} \mathrm{Tr}(X_p^{a+a'} Z_p^{b+b'}) = 0, \tag{2.99}$$

thus T_{ab} and $T_{a'b'}$ are orthogonal. This result also applies when d is a power of a prime.

Hence we have a set of orthogonal unitary matrices which can be partitioned into $q+1$ subsets of q commuting matrices. Theorem 2.45 shows that the eigenbases of these matrices are a complete set of MUBs in $\mathbb{C}^d$. □

The eigenbases of the T_{ab} have a physical interpretation. They are *rotation* operators [67].

A version of this construction, has appeared in two independent publications in 2009 [85, 25], five years after the construction was first published [41].

The construction of Paterek, Dakič and Brukner [85] is a special case when $k=1$. It is acknowledged that their construction is 'related to' [41]. The mathematical presentation in [85] is easier to follow. This comment has been published as [48].

Combescure [25] generates sets of matrices $C_\theta = \{T_{ab} : b = \theta a,\ a,b \in \mathbb{F}_q\}$ then constructs operators R_θ, which diagonalise the matrices of C_θ. From Theorem 2.7 we know that the columns of R_θ form the eigenbasis of T_{ab} where $b = \theta a$. The eigenbases of the operators T_{ab} are the MUBs constructed in [41]. Hence this is the same construction of MUBs. [25] does not cite [41]. A group like structure of these MUBs is shown in [25] which will be expounded in section 2.6.

2.4.2 Galois Rings

The planar function construction only constructs MUBs in odd prime powers. The generalised Pauli matrix construction however can construct MUBs in even and odd prime power dimensions. Galois rings may also be used to construct MUBs in even prime power dimensions. Arithmetic modulo 4 and block diagonal matrices were used in the first construction of MUBs in even prime powers [112]. Klappenecker and Rötteler simplified this construction using the ring $GR(4,r)$ [64, Thm 3]. $GR(4,r)$ has applications in coding theory [50], hence $GR(4,r)$ is the most widely studied family of Galois rings.

Lemma 2.57. *[19, Lem 3][114, Lem 3,Lem 4] Let $GR(4,r)$ be a Galois ring of characteristic*

4 *with Teichmüller set* $\mathcal{T}_r$. *Let* $i = \omega_4 = \sqrt{-1}$. *For* $a \in GR(4, r)$

$$\left| \sum_{x \in \mathcal{T}_r} i^{\mathrm{tr}(ax)} \right| = \begin{cases} 0 & \text{if } a \in 2\mathcal{T}_r,\ a \neq 0 \\ 2^r & \text{if } a = 0 \\ \sqrt{2^r} & \text{otherwise.} \end{cases} \tag{2.100}$$

Proof. $\mathcal{T}_r$ is a group of order 2^r, thus we can use Lemma 2.24 when $a \in 2\mathcal{T}_r, a \neq 0$. If $a = 0$ then

$$\begin{aligned} \sum_{x \in \mathcal{T}_r} i^{\mathrm{tr}(ax)} &= \sum_{x \in \mathcal{T}_r} 1 && (2.101) \\ &= |\mathcal{T}_r| && (2.102) \\ &= 2^r. && (2.103) \end{aligned}$$

Let $a = \gamma + 2\delta$ with $\gamma, \delta \in \mathcal{T}_r$ and $\gamma \neq 0$. Note that $x + \beta + 2\sqrt{x\beta} \in \mathcal{T}_r$ for $x, \beta \in \mathcal{T}_r$, and that $x + \beta + 2\sqrt{x\beta}$ runs through $\mathcal{T}_r$ as x runs through $\mathcal{T}_r$.

$$\begin{aligned} \sum_{x \in \mathcal{T}_r} i^{\mathrm{tr}(ax)} &= \sum_{x \in \mathcal{T}_r} i^{\mathrm{tr}[a(x+\beta+2\sqrt{x\beta})]} && (2.104) \\ &= i^{\mathrm{tr}(a\beta)} \sum_{x \in \mathcal{T}_r} i^{\mathrm{tr}[a(x+2\sqrt{x\beta})]}. && (2.105) \end{aligned}$$

Set $a = 1$, and note that $\mathrm{tr}(2\sqrt{x\beta}) = \mathrm{tr}(2x\beta)$, then

$$\sum_{x \in \mathcal{T}_r} i^{\mathrm{tr}(x)} = i^{\mathrm{tr}(\beta)} \sum_{x \in \mathcal{T}_r} i^{\mathrm{tr}[(1+2\beta)x]}. \tag{2.106}$$

Substituting $a = \gamma + 2\delta$ into equation (2.104), then using equation (2.106),

$$\begin{aligned} \sum_{x \in \mathcal{T}_r} i^{\mathrm{tr}[\gamma(1+2\delta/\gamma)x]} &= \sum_{x \in \mathcal{T}_r} i^{\mathrm{tr}[(1+2\delta/\gamma)(\gamma x)]} && (2.107) \\ &= i^{-\mathrm{tr}(\delta/\gamma)} \sum_{x \in \mathcal{T}_r} i^{\mathrm{tr}(\gamma x)}. && (2.108) \end{aligned}$$

Then using the fact that γx is a permutation of $\mathcal{T}_r$ and the properties of the trace map (Theorem 2.31 and Definition 2.41),

$$\sum_{x \in \mathcal{T}_r} i^{\mathrm{tr}[\gamma(1+2\delta/\gamma)x]} = i^{\mathrm{tr}(-\delta/\gamma)} \sum_{x \in \mathcal{T}_r} i^{\mathrm{tr}(x)}. \tag{2.109}$$

From [114, Lem 4] we get that

$$\left| \sum_{x \in \mathcal{T}_r} i^{\mathrm{tr}(x)} \right| = \sqrt{2^r}. \tag{2.110}$$

and therefore $|\sum_{x \in \mathcal{T}_r} i^{\mathrm{tr}(ax)}| = \sqrt{2^r}$. □

If p is odd, then not every element of $\mathcal{T}_r$ has a square root, and thus $x+\beta+2\sqrt{x\beta}$ is not a permutation of $\mathcal{T}_r$. Thus Lemma 2.57 does not hold in $GR(p^2,r)$ when p is odd, and the following construction, which relies upon it is not valid in odd dimensions.

Theorem 2.58 (Galois ring construction)**.** *[64, Thm 3] Let $GR(4,r)$ be the Galois ring of characteristic 4 and Teichmüller set $\mathcal{T}_r$. Let $i=\omega_4=\sqrt{-1}$. Let $V_a:=\{\vec{v}_{ab}:b\in\mathcal{T}_r\}$ be the set of vectors*

$$\vec{v}_{ab}:=\frac{1}{\sqrt{2^r}}\left(i^{\mathrm{tr}[(a+2b)x]}\right)_{x\in\mathcal{T}_r}. \tag{2.111}$$

The standard basis E along with the sets V_a, $a\in\mathcal{T}_r$ form a complete set of 2^r+1 MUBs in $\mathbb{C}^{2^r}$.

Proof. By definition

$$|\langle\vec{v}_{ab}|\vec{v}_{cd}\rangle|=\frac{1}{2^r}\left|\sum_{x\in\mathcal{T}_r}i^{\mathrm{tr}[(c-a)+2(d-b)]}\right|. \tag{2.112}$$

If $c=a$ then Lemma 2.57 shows that equation (2.112) evaluates to 0 when $d\neq b$ and 1 when $d=b$. Hence each V_a is an orthonormal basis for $\mathbb{C}^d$.

If $c\neq a$ then from Lemma 2.57 the sum in equation (2.112) evaluates to $\frac{1}{\sqrt{2^r}}$ showing that $\vec{v}_{ab}$ and $\vec{v}_{cd}$ are unbiased vectors. The entries in the vectors have magnitude $\frac{1}{\sqrt{2^r}}$, and so each V_a is unbiased to the standard basis. □

This construction of MUBs may also be generated using the planar function construction, but modified to a differentially 1-uniform function [93]. It is known that if differentially 1-uniform functions do exist for groups of even order, then the groups must be of different size [93]. Let $\mathcal{T}_r=\{0,1,\zeta,\zeta^2,\ldots,\zeta^{2^r-2}\}$ be the Teichmüller set of $GR(4,r)$ and let $\mathbb{F}_{2^r}$ be represented cyclicly: $\mathbb{F}_{2^r}=\{0,1,\alpha,\alpha^2,\ldots,\alpha^{2^r-2}\}$. Let $f:\mathbb{F}_{2^r}\mapsto GR(4,r)$ be defined by

$$f(x)=\begin{cases}0 & \text{for } x=0\\ 2\zeta^y & \text{for } x=\alpha^y\end{cases}. \tag{2.113}$$

Equation (2.111) may be rewritten as [93, Eqn 4.6]

$$\vec{v}_{ab}:=\frac{1}{\sqrt{2^r}}\Big(\chi_a(x)\psi_b(f(x))\Big)_{x\in\mathbb{F}_{2^r}} \tag{2.114}$$

where $\chi_a(x) = i^{\mathrm{tr}(ax)}$, tr over $\mathbb{F}_{2^r}$, and $\psi_b = i^{\mathrm{tr}(bf(x))}$, tr over $GR(4,r)$. From equation (2.32) there are 2^r elements $a, c \in GR(4,r)$ such that $\mathrm{tr}(a) = \mathrm{tr}(c)$, meaning that $\vec{v}_{ab} = \vec{v}_{cb}$. Thus each vector is constructed multiple times.

It is known that the planar function and Alltop constructions do not generalise to rings in arbitrary dimension [3]. Thus to construct complete sets of MUBs in arbitrary dimension, a new type of construction is needed.

2.4.3 Equivalences of MUBs

Definition of Equivalence

Some of the constructions mentioned in sections 2.4.1 and 2.4.2 are equivalent. We begin by defining what is meant by equivalence of MUBs.

Definition 2.59. [15, App A] Two sets of MUBs, $\mathcal{B} = \{B_0, B_1, \ldots, B_d\}$ and $\mathcal{B}' = \{B'_0, B'_1, \ldots, B'_d\}$, written as matrices, are *equivalent* if $\mathcal{B}$ can be transformed into $\mathcal{B}'$ by application of the following four transformations.

- A *unitary* matrix U applied to the entire set of bases:

$$\mathcal{B} \to U\{B_0, B_1, \ldots, B_d\} = \{UB_0, UB_1, \ldots UB_d\}. \tag{2.115}$$

- Unitary diagonal matrices D_i which apply *phase changes* to the vectors within each basis:

$$\mathcal{B} \to \{B_0D_0, B_1D_1, \ldots, B_dD_d\}. \tag{2.116}$$

- Permutation matrices P_i which *permute columns* and therefore permute vectors within bases:

$$\mathcal{B} \to \{B_0P_0, B_1P_1, \ldots, B_dP_d\}. \tag{2.117}$$

- *Complex conjugation* of the entire set of bases:

$$\mathcal{B} \to \{B_0^*, B_1^*, \ldots, B_d^*\}. \tag{2.118}$$

Each matrix of an orthonormal basis is unitary, meaning that $B_xB_x^* = I_d$ for any matrix in a set of MUBs. This property and the definition of equivalence gives the following important fact.

Lemma 2.60. *[42] Every set of MUBs is equivalent to a set of MUBs which contains the standard basis.*

Definition 2.61. [57, Eqn 2.1, §4.1,4.2] A *Hadamard* matrix is a $d \times d$ matrix, H, with entries from $\{\pm 1\}$ such that

$$HH^* = dI_d. \tag{2.119}$$

A *complex Hadamard* matrix is a $d \times d$ matrix with entries from $\mathbb{C}$ of modulus 1 satisfying equation (2.119). A *Butson Hadamard* matrix $BH(q, d)$ is a $d \times d$ complex Hadamard matrix with entries that are complex q^{th} roots of unity.

In the literature on MUBs the term *generalised Hadamard* matrix is sometimes used instead of complex Hadamard matrix [110]. In some publications a complex Hadamard matrix refers to a $BH(4, d)$.

It is known that Hadamard matrices must be of order 1, 2, or a multiple of 4. However it is unknown if a Hadamard matrix exists for all permissible sizes. The discrete Fourier transform constructs a $BH(d, d)$, thus there is at least one Butson Hadamard matrix of every size.

Definition 2.62. [15, §1] A set of $n + 1$ MUBs in $\mathbb{C}^d$ is *dephased* if it can be written as

$$\{I_d, \frac{1}{\sqrt{d}}H_1, \frac{1}{\sqrt{d}}H_2, \ldots, \frac{1}{\sqrt{d}}H_n\}, \tag{2.120}$$

where each H_i is a complex Hadamard matrix, with the first row and the first column having 1 in every entry.

From Definitions 2.59 and 2.62 we get:

Lemma 2.63. *[15] All sets of MUBs may be dephased.*

The search for a set of MUBs, may then be replaced by the search for sets of complex Hadamard matrices. A complete classification of complex Hadamard matrices up to order 5 has allowed for a complete classification of MUBs up to dimension 5 [15].

Theorem 2.64. *[15] There is a unique set of MUBs in $\mathbb{C}^d$ for $d \leq 5$.*

The relationship with Hadamard matrices has also been used in searches for MUBs in $\mathbb{C}^6$ [8, 60, 10].

Equivalence of constructions

Theorem 2.65. *[42, §6] A complete set of Alltop type MUBs in $\mathbb{C}^q$ is equivalent to a complete set of WF type MUBs in $\mathbb{C}^q$.*

For $q = 3^r$, WF type MUBs exist, but Alltop MUBs do not. Thus not all WF type MUBs are equivalent to Alltop type MUBs.

Proof. Let $\{W_a : a \in \mathbb{F}_q\}$ be a set of WF type MUBs generated using equation (2.79), and $\{A_a : a \in \mathbb{F}_q\}$ be a set of Alltop type MUBs generated using equation (2.81) in $\mathbb{C}^q$. We show that a permutation of A_0^* is the unitary transform required to show equivalence according to Definition 2.59.

$$A_0^* A_0 = I_q \tag{2.121}$$

$$A_0^* I_q = A_0^* \tag{2.122}$$

which after applying a phase change of $\chi(-x^3)$ to each column is W_0.

$$\begin{aligned}(A_0^* A_a)_{xy} &= \sum_{z\in\mathbb{F}_q} (A_0^*)_{xz} (A_a)_{zy} && (2.123)\\ &= \frac{1}{q}\sum_{z\in\mathbb{F}_q} \chi\left(-z^3 - xz\right)\chi\left((z-a)^3 + y(z+a)\right) && (2.124)\\ &= \frac{1}{q}\sum_{z\in\mathbb{F}_q} \chi\left(3az^2 + (3a^2 + y - x)z + (a^3 + ya)\right). && (2.125)\end{aligned}$$

The polynomial inside the sum is a quadratic, thus we can apply Theorem 2.33:

$$(A_0^* A_a)_{xy} = \frac{1}{q}\chi\left(\frac{12a^4 + 12ya^2 - (3a^2 + y - x)^2}{12a}\right)\eta(3a)G(\eta,\chi). \tag{2.126}$$

Divide each column by the entry in the row $x = 0$. Most of the terms cancel, including $\eta(3a)$ and $G(\eta, \chi)$.

$$\begin{aligned}\frac{(A_0^* A_a)_{xy}}{(A_0^* A_a)_{0,y}} &= \chi\left(\frac{-x^2 + 2x(3a^2 + y)}{12a}\right) && (2.127)\\ &= \left(W_{\frac{-1}{12a}}\right)_{x,\frac{3a^2+y}{6a}}. && (2.128)\end{aligned}$$

We conclude that A_0^* is the unitary transform and $y \mapsto \frac{3a^2+y}{6a}$ the permutation required by Definition 2.59 to show equivalence. □

Some of the other constructions are equivalent, but are only known for specific cases. The following are not published results, but are simple observations.

Corollary 2.66. *[42, Lem 6.2] The MUBs generated in $\mathbb{C}^d$ using the WF construction and the Pauli matrix construction are the same when d is an odd prime.*

Proof. In prime dimensions the proof of Theorem 2.55 shows the equivalence of the two constructions. □

Explicit calculation of the eigenvectors of the Pauli matrix MUBs would determine the equivalence (or not) in prime power dimensions.

Conjecture 2.67. *The MUBs generated in $\mathbb{C}^d$ using the WF construction and the Pauli matrix construction are the same when d is odd.*

Corollary 2.68. *The MUBs generated in $\mathbb{C}^d$ using the Galois ring construction and the Pauli matrix construction are the same for $d = 2$ and $d = 4$.*

Proof. This can be shown by calculating the set of MUBs using each method. For $d = 2$ both obtain [112, Eq 3]:

$$\left\{\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix}\right\},\quad \left\{\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix},\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}\right\},\quad \left\{\frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix},\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix}\right\}. \quad (2.129)$$

In the case $d = 4$ the bases are explicitly calculated in [41, Fig 3] and [64, Ex 2], and are the same. Note that [64] contains a misprint, which is corrected in [65, Ex 2]. □

This result may also be obtained from Theorem 2.64 [15]. Further calculations are required to show equivalence (or not) in larger dimensions.

2.5 Structures related to MUBs

2.5.1 Equivalent objects

There are some objects which have been shown to be equivalent to sets of MUBs, such as sets of commuting matrices (Theorem 2.45) and sets of complex Hadamard matrices (Lemma 2.62). We present two further objects which are equivalent to MUBs. Information about any of these equivalent objects will lead to information about MUBs.

Complex projective t-designs

We describe complex projective t-designs, then show that specific designs are equivalent to complete sets of MUBs. The notion of a t-design on a projective space is an extension of t-designs on a discrete set which we will make use of in subsequent chapters (see definition 3.16).

Definition 2.69. [65, §III] Let $\mathcal{S}^{d-1}$ denote the *sphere* of unit vectors in $\mathbb{C}^d$. Two unit vectors $\vec{u}, \vec{v}$ are equivalent, denoted $\vec{u} \equiv \vec{v}$, if there exists some $\theta \in \mathbb{R}$ such that $\vec{u} = e^{i\theta}\vec{v}$. Let the *complex projective sphere* be the quotient space

$$\mathbb{C}\mathcal{S}^{d-1} := \mathcal{S}^{d-1}/\equiv . \tag{2.130}$$

$\mathbb{C}\mathcal{S}^{d-1}$ is isomorphic to complex projective space, denoted $\mathbb{C}\mathcal{P}^{d-1}$, but using vectors of unit length is common in quantum physics. We write the elements of $\mathbb{C}\mathcal{S}^{d-1}$ using vectors, where $\langle\vec{x}\rangle \in \mathbb{C}\mathcal{S}^{d-1}$ represents all vectors of the form $e^{i\theta}\vec{x} \in \mathbb{C}^d$.

Definition 2.70. [65, Thm 1] Suppose that X is a nonempty finite subset of $\mathbb{C}\mathcal{S}^{d-1}$. X is a t-design in $\mathbb{C}\mathcal{S}^{d-1}$ if for all k in the range $0 \leq k \leq t$

$$\frac{1}{|X|^2} \sum_{\langle\vec{x}\rangle, \langle\vec{y}\rangle \in X} |\langle\vec{x}|\vec{y}\rangle|^{2k} = \frac{1}{\binom{d+k-1}{k}}. \tag{2.131}$$

There is also a definition of complex projective t-design which uses cubature formula and measure theory, material which is well beyond the scope of this thesis [23, §VI 54.6][65, Def 2]. If $\geq$ replaces $=$ in equation (2.131), then we have the Welch bound [109].

We denote the elements of a complex projective t-design as vectors, where $\vec{v}$ represents all vectors in $\mathbb{C}^d$ of the form $e^{i\theta}\vec{v}$. The representation of a vector as a point in $\mathbb{C}S^{d-1}$ is analogous to the idea of dephasing MUBs.

Definition 2.71. [23, Defi VI 54.6, 54.23] The *angle set*, A, of a t-design X is the set

$$A := \{|\langle\vec{x}|\vec{y}\rangle|^2 : \langle\vec{x}\rangle, \langle\vec{y}\rangle \in X, \langle\vec{x}\rangle \neq \langle\vec{y}\rangle\}. \tag{2.132}$$

The *subdegree* of $d_\theta(\vec{x})$ of a point $\langle\vec{x}\rangle \in X$ is the size of the set

$$d_\theta(x) := |\{\langle\vec{y}\rangle \in X : |\langle\vec{x}|\vec{y}\rangle|^2 = \theta\}|. \tag{2.133}$$

MUBs are defined by the angles between vectors. Specifying the angle set is remarkably prescriptive of other properties.

Lemma 2.72. *[23, Thm VI 54.25, 54.35] Let X be a t-design on $\mathbb{C}\mathcal{S}^{d-1}$ with angle set $\{0, \alpha\}$. Then for every $\langle\vec{x}\rangle, \langle\vec{y}\rangle \in X$, $d_\alpha(\vec{x}) = d_\alpha(\vec{y})$.*

Theorem 2.73. *[65, Thm 3] A set of $d+1$ MUBs in $\mathbb{C}^d$ is a 2-design in $\mathbb{C}S^{d-1}$ with angle set $\{0, \frac{1}{d}\}$ and $d(d+1)$ elements.*

Proof. Let X be a set of $d+1$ MUBs in $\mathbb{C}^d$. For $k=0$ equation (2.131) is trivially satisfied. Evaluating the left side of equation (2.131) for $k=1$ we get

$$\frac{1}{d^2(d+1)^2}\sum_{\langle\vec{x}\rangle,\langle\vec{y}\rangle\in X}|\langle\vec{x}|\vec{y}\rangle|^2 = \frac{1}{d^2(d+1)^2}d(d+1)\left(1+(d-1)0+d^2\frac{1}{d}\right) \tag{2.134}$$

$$= \frac{1}{d}. \tag{2.135}$$

$\binom{d}{1} = d$, thus equation (2.131) is satisfied. Similarly for $k=2$:

$$\frac{1}{d^2(d+1)^2}\sum_{\langle\vec{x}\rangle,\langle\vec{y}\rangle\in X}|\langle\vec{x}|\vec{y}\rangle|^4 = \frac{1}{d^2(d+1)^2}d(d+1)\left(1+(d-1)0+d^2\frac{1}{d^2}\right) \tag{2.136}$$

$$= \frac{2}{d(d+1)}. \tag{2.137}$$

$\binom{d+1}{2} = \frac{d(d+1)}{2}$, thus equation (2.131) is satisfied. X is a 2-design in $\mathbb{C}S^{d-1}$. □

Theorem 2.74. *[65, Thm 4] A 2-design $X \subseteq \mathbb{C}S^{d-1}$ with $d(d+1)$ elements and angle set $\{0, \frac{1}{d}\}$ is a complete set of MUBs in $\mathbb{C}^d$.*

Proof. Rearranging equation (2.131) to count subdegrees

$$\frac{1}{|X|^2}\left(\sum_{\langle\vec{x}\rangle\in X}1+\sum_{\langle\vec{x}\rangle\in X}\sum_{\theta\in\{0,\frac{1}{d}\}}d_\theta(\vec{x})\theta^k\right) = \frac{1}{\binom{d+k-1}{k}}. \tag{2.138}$$

We know $|X| = d(d+1)$. For $k=1$ equation (2.138) becomes

$$\frac{1}{d^2(d+1)^2}\left(d(d+1)+\sum_{\langle\vec{x}\rangle\in X}d_{\frac{1}{d}}(\vec{x})\frac{1}{d}\right) = \frac{1}{d} \tag{2.139}$$

$$d(d+1)+\frac{1}{d}\sum_{\langle\vec{x}\rangle\in X}d_{\frac{1}{d}}(\vec{x}) = d(d+1)^2 \tag{2.140}$$

$$\sum_{\langle\vec{x}\rangle\in X}d_{\frac{1}{d}}(\vec{x}) = d^3(d+1). \tag{2.141}$$

Using the calculations for $k = 2$ yields the same solution. From Lemma 2.72 and equation (2.141) we find that $d_{\frac{1}{d}}(\vec{x}) = d^2$ and $d_0(\vec{x}) = d - 1$ for every $\vec{x} \in X$.

Let

$$B_x = \{\langle\vec{x}\rangle\} \cup \{\langle\vec{y}\rangle \in X : \langle\vec{x}|\vec{y}\rangle = 0\}. \tag{2.142}$$

We must show that $B_x = B_y$ for each $\vec{y} \in B_x$. If $\vec{y} \in B_x$ then $\vec{x} \in B_y$. Thus we need that the intersection set

$$I(x, y) = \{\vec{z} \in X : \langle\vec{x}|\vec{z}\rangle = 0 \wedge \langle\vec{y}|\vec{z}\rangle = 0\} = B_x \cup B_y \setminus \{x, y\} \tag{2.143}$$

contains $d - 2$ elements. Specialising [54, Thm 5.2] to the case at hand shows that

$$|I(x, y)| = d^2 \sum_{i,j=0}^{1} \sigma^0_{1-i}\sigma^0_{1-j}(d(d + 1)g_{ij}(0) - 0^i - 0^i). \tag{2.144}$$

Evaluating $g_{ij}(0)$ using [54, Thm 5.3] we obtain that $|I(x, y)| = d - 2$ as required. □

Equation (2.144) is a 'fairly complicated summation' [54], involving objects which would require significant space to define and explain. As no further use is made of this result we omit a detailed exposition.

Theorems 2.52 and 2.73 provide a link between planar functions and complex projective t-designs.

Corollary 2.75. *Let $\mathbb{F}_q$ be a field of odd characteristic, and Π a planar function on $\mathbb{F}_q$, then the set of vectors defined by equation (2.69) along with the vectors of the standard basis is a 2-design on $\mathbb{C}\mathcal{S}^{d-1}$.*

This has been further generalised with a link between differentially 1-uniform functions and weighted complex projective t-designs [93, Thm 4.1]. However the only known differentially 1-uniform functions which produce unweighted t-designs, and therefore MUBS, are planar functions (Theorem 2.52) and equation (2.113) [93]. New discoveries of differentially 1-uniform functions may result in new sets of MUBs.

There is extensive literature investigating properties of complex projective t-designs, and in particular sets which attain the Welch bound for use in communication systems [62, 113]. Constructions of such sets are found only in specific cases, and so this connection does not immediately add to our knowledge of MUBs.

Relative difference sets

Relative difference sets are algebraic structures, which have been shown to be equivalent to specific sets of MUBs. This is not as strong as the connections with projective t-designs or Hadamard matrices, as it only applies to specific sets of MUBs. However it is still important.

Definition 2.76. [11, Defi 10.1] Let G be a group with identity element 1_G, and N a normal subgroup. A subset D of G is an (m, n, d, λ)-*relative difference set* if

$$\{ab^{-1} : a, b \in D\} = \{1_G\} \cup G \setminus N. \tag{2.145}$$

$|N| = n$, $|G| = mn$, $|D| = d$. For each $x \in G \setminus N$, there are exactly λ pairs $a, b \in D$ such that $ab^{-1} = x$.

Several of the constructions of MUBs use character sums. Difference sets are another of the few cases where explicit calculations of character sums is known.

Lemma 2.77. *[11, § VI Thm 10.9] Let G be an Abelian group with normal subgroup N. The characters of G form a group, $G^\wedge$, as do the characters of G/N. Every character of G/N induces a character of G which is constant on the cosets of N, and these characters form a subgroup $H^\wedge$ of $G^\wedge$.*

D is a (d, n, d, λ)-relative difference set of G relative to N, if and only if for every character χ of G

$$\left| \sum_{x \in D} \chi(x) \right| = \begin{cases} d & \text{for } \chi = \chi_0 \\ 0 & \text{for } \chi \in H^\wedge \setminus \{\chi_0\} \\ \sqrt{d} & \text{for } \chi \in G^\wedge \setminus H^\wedge. \end{cases} \tag{2.146}$$

Theorem 2.78. *[42, Thm 4.1] The existence of a (d, n, d, λ)-relative difference set in an Abelian group implies the existence of a set of $n + 1$ MUBs in $\mathbb{C}^d$.*

Proof. Let D be a (d, n, d, λ)-relative difference set and

$$\chi\downarrow_D = (\chi(x))_{x \in D} \tag{2.147}$$

be a vector in $\mathbb{C}^d$. Define a basis B_i for $\mathbb{C}^d$ using the i^{th} coset of $H^\wedge$

$$B_i = \{ \frac{1}{\sqrt{d}} \chi_{ij}\downarrow_D : \chi_{ij} \in H^\wedge + i \}. \tag{2.148}$$

The inner product of two such vectors is

$$\langle \chi_a\lfloor_D \mid \chi_b\lfloor_D \rangle = \sum_{x\in D} \chi_a(x)\overline{\chi_b(x)} \tag{2.149}$$

$$= \sum_{x\in D} \chi_{ab^{-1}}(x). \tag{2.150}$$

From Lemma 2.77, when the vectors are normalised each base is orthonormal and mutually unbiased. Since every entry of each vector has magnitude $\frac{1}{\sqrt{d}}$, each B_i is also unbiased to the standard basis. □

This theorem has a weaker converse.

Theorem 2.79. *[42, Cor 4.2] Let $\mathcal{B} = \{E_d, B_1, \ldots, B_n\}$ be a set of MUBs in $\mathbb{C}^d$. If the vectors of $\{B_1 \cup B_2 \cup \cdots \cup B_n\}$ form a group with respect to component-wise multiplication, then there exits a $(d, n, d, \lambda)-$relative difference set.*

Proof. Let $\vec{u}, \vec{v}$ be vectors of $\mathcal{B} \setminus E_d$.

$$|\langle\sqrt{d}\vec{u}|\sqrt{d}\vec{v}\rangle| = \begin{cases} d & \text{for } \vec{u} = \vec{v} \\ 0 & \text{for } \vec{u} \neq \vec{v}, \quad \vec{u}, \vec{v} \in B_i \\ \sqrt{d} & \text{otherwise} \end{cases} \tag{2.151}$$

A relative difference set is then inferred from Theorem 2.77. □

This does not show that relative difference sets are equivalent to MUBs. In section 2.6 we see that the odd dimensional Pauli matrix MUBs and the WF MUBs form a group using component-wise multiplication, but the Alltop MUBs do not.

It is known that (p^a, p^b, p^a, p^{a-b})-relative difference sets exist for all primes p [89, §4]. However MUBs constructed using these relative difference sets are equivalent to the WF type MUBs [42].

2.5.2 SIC-POVM

MUBs use sets of orthogonal measurements to determine the state of a quantum system. There are many other sets of measurements which may be used. *Positive operator valued measures* (POVM) are one such type of measurements. POVM share some of the applications of MUBs such as quantum state tomography, but as yet have not found use in cryptography [111, §3]. A POVM is *informationally complete* if its statistics completely determine the

state which was measured as is required for quantum state tomography. An IC-POVM is *symmetric* if all the pair-wise inner products are equal. From a mathematical perspective a SIC-POVM is a set of d^2 equiangular lines.

Definition 2.80. [91] A SIC-POVM is a set of d^2 vectors $\vec{x}, \vec{y} \in \mathbb{C}^d$ of unit length satisfying

$$|\langle \vec{x}|\vec{y}\rangle|^2 = \frac{1}{d+1}, \quad \vec{x} \neq \vec{y}. \tag{2.152}$$

It is conjectured that MUBs are intimately connected with finite affine planes (see Conjecture 3.28). It has also been suggested that SIC-POVMs show analogous structure, but with the role of points and lines swapped [111, 96]. Another geometric interpretation notes that when using the Bloch representation of density matrices [84, §4.2], the Bloch vectors of a SIC-POVM are maximally distant from the subspaces representing MUBs [2, §2].

Analytic solutions are known for SIC-POVMs in $\mathbb{C}^d$ where $d = 2, 3, 4, 5, 6, 8$ [116, 91](2004), and more recently $d = 9, 10, 11, 12, 13, 14, 15, 19, 24, 35, 48$ (2010)[100]. Of particular note is $d = 6, 10, 14$, where it is known that no finite affine planes of these orders can exist [16, 73]. Thus a strong connection between affine planes and SIC-POVMs is unlikely.

Conjecture 2.81. *[91] SIC-POVMs exist in all dimensions.*

Along with the aforementioned analytic solutions, there is numerical evidence that SIC-POVMs exist in all dimensions. SIC-POVMs have been calculated up to machine precision for $d = 67$ [91, 100]. However there are no known infinite families of constructions, suggesting that if general constructions are found, they will not use well studied algebraic objects such as Galois fields.

A commonality with MUBs is that SIC-POVMs may also be represented as complex projective 2-designs.

Theorem 2.82. *[91, Thm 2][65, Thm 5] A SIC-POVM in $\mathbb{C}^d$ forms a 2-design on $\mathbb{C}\mathcal{S}^{d-1}$ with angle set $\{\frac{1}{d+1}\}$ and d^2 elements.*

Proof. As with Theorem 2.73 we must show that the vectors in a SIC-POVM satisfy the Welch bound (equation (2.131)) for $k = 0, 1, 2$. This is obvious for $k = 0$. For $k = 1$ we evaluate the lefthand side of equation (2.131):

$$\frac{1}{d^4} \sum_{\langle \vec{x}\rangle, \langle \vec{y}\rangle \in X} |\langle \vec{x}|\vec{y}\rangle|^2 = \frac{1}{d^4}\left(d^2 + (d^4 - d^2)\frac{1}{d+1}\right) \tag{2.153}$$

$$= \frac{1}{d}. \tag{2.154}$$

$\binom{d}{1} = d$, thus equation (2.131) is satisfied. Similarly for $k = 2$:

$$\frac{1}{d^4} \sum_{\langle\vec{x}\rangle,\langle\vec{y}\rangle \in X} |\langle\vec{x}|\vec{y}\rangle|^4 = \frac{1}{d^4}\left(d^2 + (d^4 - d^2)\frac{1}{(d+1)^2}\right) \tag{2.155}$$

$$= \frac{2}{d(d+1)}. \tag{2.156}$$

$\binom{d+1}{2} = \frac{d(d+1)}{2}$, thus equation (2.131) is satisfied. □

It has been noted that this result may also be obtained from [116, Thms 2.29, 2.30].

Theorem 2.83. *[91, Thm 2] A 2-design $X \subseteq \mathbb{C}\mathcal{S}^{d-1}$ with d^2 elements is a SIC-POVM.*

Proof. Let A be the angle set of X. Using equation (2.138) for $k = 1$

$$\frac{1}{d^4}\left(\sum_{\langle\vec{x}\rangle\in X} 1 + \sum_{\langle\vec{x}\rangle\in X}\sum_{\theta\in A} d_\theta(\vec{x})\theta\right) = \frac{1}{d} \tag{2.157}$$

$$\sum_{\langle\vec{x}\rangle\in X}\sum_{\theta\in A} d_\theta(\vec{x})\theta = d^3 - d^2 = d^2(d^2-1)\frac{1}{d+1} \tag{2.158}$$

and for $k = 2$

$$\frac{1}{d^4}\left(\sum_{\langle\vec{x}\rangle\in X} 1 + \sum_{\langle\vec{x}\rangle\in X}\sum_{\theta\in A} d_\theta(\vec{x})\theta^2\right) = \frac{2}{d(d+1)} \tag{2.159}$$

$$\sum_{\langle\vec{x}\rangle\in X}\sum_{\theta\in A} d_\theta(\vec{x})\theta = \frac{2d^3}{d+1} - d^2 = d^2(d^2-1)\frac{1}{(d+1)^2} \tag{2.160}$$

To satisfy equations (2.158) and (2.160), we require that $\theta = \frac{1}{d+1}$ and $d_\theta(\vec{x}) = d^2 - 1$ for all $\langle\vec{x}\rangle \in X$. □

It is also shown that d^2 is the minimum number of elements in a 2-design. Thus a SIC-POVM is a minimal 2-design on $\mathbb{C}\mathcal{S}^{d-1}$.

There are some similarities between MUBs and SIC-POVM, both in their physical interpretation and mathematical properties. However there are distinctions that suggest that information about SIC-POVMs may have little bearing on knowledge of MUBs.

2.5.3 Computer search

There are several groups searching for sets of MUBs using computational methods. Searches have focused on MUBs in $\mathbb{C}^6$, the smallest unresolved case.

The constructions of MUBs behave quite differently in odd and even prime power dimensions. 6 has both odd and even prime factors, thus it may not be the best place to search for MUBs [7]. There are conjectures surrounding MUBs and affine planes; it is known that a finite affine plane cannot exist of order 6, 10 or 14. It may be more fruitful to search in $\mathbb{C}^{15}$, however each increase in size greatly increases the amount of computation required [7].

The techniques that have been employed generate sets of 3 MUBs, known to exist in any dimension (by Theorem 2.50), and attempt to find a fourth base unbiased to the original three.

Grassl takes advantage of Theorem 2.55 to generate the initial 3 MUBs using generalised Pauli matrices [44], then goes on to conclude that if more than 3 MUBs exist in $\mathbb{C}^6$, they cannot be constructed in this way.

Butterly and Hall use optimisation techniques on various functions to search for MUBs [18]. They find many complete sets of MUBs for $d = 2, 3, 4$ and 5, no complete sets for $d = 6$, and few complete sets when $d = 7$. Thus the methods do not scale well[18], and are not strong evidence for the absence of complete sets of MUBs in $\mathbb{C}^6$

Several groups have searched for Hadamard matrices with appropriate properties. Jamming, Matolcsi and Móra describe a strategy for discretising the possible sets of unbiased Hadamard matrices [60]. Their preliminary results find an infinite family of sets of 3 MUBs in $\mathbb{C}^6$, and show that no sets in this family can be extended to a set of four MUBs in $\mathbb{C}^6$ [61]. Bengston et.al. find subspaces for which it is possible to find sets of 3 MUBs in $\mathbb{C}^6$. They use this 'landscape' to conjecture that there exist 4 MUBs in $\mathbb{C}^6$ [8, §VIII].

The amount of computing power that has been allocated to finding MUBs in $\mathbb{C}^6$, and the lack of success is strong evidence that complete sets of MUBs do not exist in $\mathbb{C}^6$.

2.6 Algebraic Structure of MUBs

Theorem 2.79 shows that a set of MUBs which forms a group under component-wise multiplication is equivalent to a specific type of relative difference set. We give a simple proof to show that planar function MUBs meet this criteria, and expound a more complicated proof that shows that this is also the case for the Pauli matrix MUBs.

2.6.1 Group structure of planar function MUBs

The following results on planar and Alltop MUBs are not published, but are simple calculations.

Let $\odot$ denote component-wise multiplication.

Lemma 2.84. *Let $\mathcal{B} := \{E_q, B_0, B_1, \ldots, B_{q-1}\}$ be a complete set of MUBs in $\mathbb{C}^q$ as constructed using the planar function construction. The vectors in $\mathcal{B} \setminus E_q$ form an Abelian group under component-wise multiplication.*

Proof. Let $\vec{v}_{ab}$ and $\vec{v}_{cd}$ be vectors constructed using equation (2.69).

$$\vec{v}_{ab} \odot \vec{v}_{cd} = \frac{1}{\sqrt{q}}\Big(\chi((a+c)\Pi(x) + (b+d)x)\Big)_{x\in\mathbb{F}_q} \quad \text{with } a,b,c,d \in \mathbb{F}_q \tag{2.161}$$

$$= \vec{v}_{(a+c)(b+d)}. \tag{2.162}$$

□

Lemma 2.85. *Let $\mathcal{B} := \{E_q, B_0, B_1, \ldots, B_{q-1}\}$ be a complete set of MUBs in $\mathbb{C}^q$ as constructed using the Alltop construction. The vectors in $\mathcal{B} \setminus E_q$ do not form a closed algebraic structure under component-wise multiplication.*

Proof. Let $\vec{v}_{ab}$ and $\vec{v}_{cd}$ be vectors constructed using equation (2.81).

$$\vec{v}_{ab} \odot \vec{v}_{cd} = \frac{1}{\sqrt{q}}\Big(\chi((x+b)^3 + a(x+b) + (x+d)^3 + c(x+d))\Big)_{x\in\mathbb{F}_q} \tag{2.163}$$

with $a,b,c,d \in \mathbb{F}_q$. The cubic polynomial inside the character cannot be factored into the form $(x+y)^3 + z(x+y)$. □

The WF MUBs, which are a special case of the planar function MUBs, form a group. However the Alltop MUBs, which, by Theorem 2.65 are equivalent, do not. Thus the group structure is not an inherent property of MUBs.

2.6.2 Group structure of Pauli matrix MUBs

The Pauli matrix type MUBs have been shown to have a group structure. This is a much more complicated proof, but with essentially the same results. It is not yet known if the Pauli matrix MUBs are equivalent to the WF MUBs in all dimensions.

Theorem 2.86. *[25, Thm 2.14][67, §3.3] Let $\mathcal{B} := \{I_d, B_0, B_1, \ldots, B_{d-1}\}$ be a set of matrices representing a complete set of MUBs in $\mathbb{C}^d$ as constructed using the Pauli matrix construction. For d, an odd prime power, $\mathcal{B} \setminus I_d$ forms a group using component-wise multiplication:*

$$B_{j+k} = B_j \odot B_k, \qquad i, j \in \mathbb{F}_q. \tag{2.164}$$

Proof. Let two bases $E = \{e_1, \ldots, e_r\}$ and $F = \{f_1, \ldots, f_r\}$ be chosen for $\mathbb{F}_{p^r}$ such that F is a multiple of the dual basis of E, $f_i = k\bar{e_i}$, $k \in \mathbb{F}_{p^r}$. Let X_p and Z_p be the generalised Pauli matrices and let

$$U_a = X_p^{a_1} \otimes X_p^{a_2} \otimes \cdots \otimes X_p^{a_r} \tag{2.165}$$

$$V_b = Z_p^{b_1} \otimes Z_p^{b_2} \otimes \cdots \otimes Z_p^{b_r} \tag{2.166}$$

where $a_i = \mathrm{tr}(ak^{-1}f_i) = \mathrm{tr}(a\bar{e_i})$ and $b_i = \mathrm{tr}(be_i)$. Then from equation (2.89), $T_{ab} = U_aV_b$. By construction B_j diagonalises $T_{(ja)a}$, with diagonal matrix D,

$$T_{(ja)a} = B_jDB_j^*. \tag{2.167}$$

Using equation (2.21), $\mathrm{Tr}(T_{(ja)a}) = 0$,

$$\mathrm{Tr}(T_{(ja)a}) = \mathrm{Tr}(B_jDB_j^*) = \mathrm{Tr}(DB_j^*B_j) = \mathrm{Tr}(DI_d) = \mathrm{Tr}(D). \tag{2.168}$$

Thus $\mathrm{Tr}(D) = 0$, and hence the rows and columns of B_j and D may be permuted so that $D := \mu_{ja}V_a$ where $\mu_{ja} := \chi(m)$ for some $0 \leq m \leq p$. From equation (2.167)

$$T_{(ja)a} = \mu_{ja}B_jV_aB_j^*. \tag{2.169}$$

Let $\vec{u}_x$ be an x^{th} eigenvector of U_a, then

$$U_a\vec{u}_x = \chi(-ax)\vec{u}_x, \qquad U_a = \sum_{x\in\mathbb{F}_q} \chi(-ax)\vec{u}_x\vec{u}_x^*. \tag{2.170}$$

$\vec{u}_x$ may also be obtained using the discrete Fourier transform [67, Eq 8]. The set of eigenvectors of U_a form an orthonormal basis for $\mathbb{F}_q$.

$$V_a\vec{u}_x = \vec{u}_{x+a}, \qquad \vec{u}_x^*V_a = \vec{u}_{x-a}^*. \tag{2.171}$$

From equations (2.171) and (2.169)

$$B_j = \sum_{x\in\mathbb{F}_q} \lambda_{xj}\vec{u}_x\vec{u}_x^* \tag{2.172}$$

for some scalars $\lambda_{x,j}$, with $\lambda_{0,j} = 1$. Then

$$B_j V_a B_j^* = \sum_{x \in \mathbb{F}_q} \lambda_{x,j} \lambda^*_{x-a,j} \vec{u}_x \vec{u}^*_{x-a}. \tag{2.173}$$

Note that from equation (2.169)

$$T_{(ja)a} = U_{ja} V_a = \sum_{x \in \mathbb{F}_q} \chi(-jax) \vec{u}_x \vec{u}^*_{x-a} \tag{2.174}$$

which shows that

$$\lambda_{x,j} \lambda^*_{x-a,j} = \mu_{aj} \chi(-jax). \tag{2.175}$$

Let $x = 0$,

$$\lambda_{0,j} \lambda^*_{-a,j} = \mu_{aj} \tag{2.176}$$

hence $\mu_{aj} = \lambda^*_{-a,j}$. Rewriting equation (2.175),

$$\lambda_{x,j} \lambda^*_{x-a,j} = \lambda^*_{-a,j} \chi(-jax). \tag{2.177}$$

Let $a = 0$, we find that $|\lambda_{x,j}|^2 = 1$. Let $\lambda_{x,j} = \chi(-\frac{1}{2}x^2 j)$, this is a solution to equation (2.175)

$$\chi\left(-\frac{1}{2}x^2 j\right) \chi\left(-\frac{1}{2}j(x^2 - 2ax + a^2)\right) = \chi\left(-\frac{1}{2}a^2 j\right) \chi(-jax) \tag{2.178}$$

$$\chi\left(-jax + \frac{1}{2}a\right) = \chi\left(-jax + \frac{1}{2}a\right). \tag{2.179}$$

We also find that

$$\lambda^*_{x,j} = \lambda_{x,-j} \tag{2.180}$$

and

$$\lambda_{x,j} \lambda_{x,k} = \lambda_{x,j+k}. \tag{2.181}$$

Thus the set of scalars $\{\lambda_{x,j} : x, j \in \mathbb{F}_q\}$ form a group with $\lambda_{0,0}$ as the identity element.

$$B_j \odot B_k = \sum_{x \in \mathbb{F}_q} \lambda_{x,j} \lambda_{x,k} \vec{u}_x \vec{u}^*_x = \sum_{x \in \mathbb{F}_q} \lambda_{x,j+k} \vec{u}_x \vec{u}^*_x = B_{j+k} \tag{2.182}$$

which shows that $\{B_j : j \in \mathbb{F}_q\}$ forms a group, which has the structure of $\langle \mathbb{F}_q, + \rangle$. □

A group is not formed under component-wise multiplication when q is even; equation (2.177) does not have a unique solution [67, §3.3.2].

Theorem 2.87. *[67, §3.3.2][25, Rem 2.15] Let $q = 2^r$, then the set $X = \{B_j : j \in \mathbb{F}_q\} \cup \{U_j : j \in \mathbb{F}_q\}$ forms an algebraic structure using component-wise multiplication. $\langle X, \odot \rangle$ obeys the following 'group like laws':*

$$B_j \odot B_j = U_{\sqrt{j}} \tag{2.183}$$

$$U_j \odot U_{j+1} = U_1. \tag{2.184}$$

Proof. We are using a field of characteristic 2, hence $-x = x$. From equation (2.177), let $a = x$,

$$\lambda_{x,j}\lambda^*_{2x,j} = \lambda^*_{x,j}\chi(jx^2) \tag{2.185}$$

$$\lambda^2_{x,j} = \chi(jx^2). \tag{2.186}$$

Then

$$B_j \odot B_j = \sum_{x\in\mathbb{F}_q} \lambda^2_{x,j}\vec{u}_x\vec{u}^*_x = \sum_{x\in\mathbb{F}_q} \chi(jx^2)\vec{u}_x\vec{u}^*_x \tag{2.187}$$

Using the identity $jx^2 = (\sqrt{j}x)^2$, equation (2.170) and Theorem 2.31,

$$B_j \odot B_j = \sum_{x\in\mathbb{F}_q} \chi(\sqrt{j}x)\vec{u}_x\vec{u}^*_x = U_{\sqrt{j}}. \tag{2.188}$$

This shows equation (2.183).

$$U_j \odot U_{j+1} = \sum_{x\in\mathbb{F}_q} \chi(jx^2 + (j+1)x^2)\vec{u}_x\vec{u}^*_x \tag{2.189}$$

$$= \sum_{x\in\mathbb{F}_q} \chi(x^2)\vec{u}_x\vec{u}^*_x \tag{2.190}$$

showing equation (2.184). □

The group structure is not an underlying property of MUBs since the Alltop MUBs and even dimensional Pauli matrix MUBs do not form a group. There may be a weaker structure that all MUBs conform to using different binary operations. This idea will be explored in chapter 7.

2.7 Research Aim

Despite this large body of research the big question still remains unanswered.

Open Problem 2.88. *Do complete sets of MUBs exist in non-prime power dimensions?*

There has been much discussion of the similarities between complete sets of MUBs and geometric and combinatorial structures. In this study we focus on mutually orthogonal Latin squares. We know specific sets of MOLS are linked to specific sets of MUBs through the planar function construction. There are also similarities in the cardinalities of various sub-structures within MOLS and MUBs. Are these similarities a deep connection, or coincidences?

Research Question 2.89. *Are mutually unbiased bases intimately linked with mutually orthogonal Latin squares?*

The only known constructions of complete sets of MUBs rely on algebraic structures such as Galois fields and Galois rings. Galois fields are known to construct complete sets of MOLS. However there are many complete sets of MOLS which do not have known algebraic constructions. Perhaps the same will be true for MUBs.

Research Question 2.90. *Do all complete sets of mutually unbiased bases have an algebraic structure?*

Perhaps the similarities with MOLS come from underlying algebraic structures, which also underpin MUBs. As shown in section 2.6 some properties of MUBs are quite different in odd and even prime power dimensions, with weaker properties appearing in even dimensions. The same is true of projective planes. Will MUBs in non prime power dimensions (if they exist) have any algebraic structure?

Chapter 3

MUBs and MOLS

3.1 Introduction

3.1.1 Motivation

Similarities between MUBs and mutually orthogonal Latin squares (MOLS) have been noted by several authors [96, 111]. This noted similarity has been expressed as a conjecture.

Conjecture 3.1 (SPR Conjecture)**.** *[96] A complete set of MUBs exists in $\mathbb{C}^d$ if and only if a complete set of MOLS of order d exists.*

The evidence for this is based on cardinalities of various substructures, and similarities of upper and lower bounds. Specific complete sets of MUBs can be constructed using specific complete sets of MOLS [85]. A construction that uses general sets of MOLS constructs incomplete sets of MUBs, but more than the lower bound of Theorem 2.50.

3.1.2 Historical note on MOLS

The name 'Latin' square rose out of the writings of Leonard Euler who used Latin characters as the symbols in the squares. Euler essentially began the study of mutually orthogonal Latin squares (MOLS) with his famous '36 officers problem' which asks for the construction on a pair of orthogonal Latin squares of order 6 [23, Rem III 3.22]. This sparked interest in a range of combinatorial designs. Combinatorial design theory expanded in the 1850s with Kirkman and Steiner making significant contributions [102, §2]. There are many combinatorial structures which are equivalent to sets of MOLS, thus a lot research has been done in different guises.

3.1.3 Applications of MOLS

Latin squares have been used in experimental design for centuries. In 1788 an experiment involving diets for sheep farming is the first evidence of use of a Latin square in experimental design [102, §2]. In 1926 Ronald Fisher noted that Latin squares and families of mutually orthogonal Latin squares could be used systematically for experimental design [102, §2]. A variety of combinatorial designs are now used to design experiments across all scientific disciplines.

MOLS also have applications in error correcting codes. Linear error correcting codes rely on the assumption that noise in the communication channel is uniform, that is each symbol of each message being sent has equal probability of being changed to any other symbol by errors in the system. However some systems do not adhere to this assumption. A recent example is the use of powerlines to transmit internet data [24]. A complete set of MOLS can be used as a more robust code in this instance.

In recent years Latin squares in the form of Sudoku problems have appeared in newspapers and magazines worldwide [29].

3.1.4 Aim

In this chapter we approach the question of a link between MUBs and MOLS directly. We look within the structure of some complete sets of MUBs to find MOLS. We aim to find what part of the structure of MUBs is most closely linked with MOLS.

Section 3.2 provides definitions of MOLS and equivalent objects, some preliminary results including the SPR conjecture, and constructions of MUBs that use MOLS. Section 3.3 details a method for constructing MOLS from MUBs, and shows that this works for two constructions in prime dimensions. Section 3.4 extends this construction to prime power dimensions. Section 3.5 provides a summary of findings and some further directions for this research.

3.2 Definitions and preliminary results

Definitions can be found in any standard work on combinatorial designs eg [23, 11, 102]. Many of the geometric definitions apply to infinite and higher dimensional geometries, however only finite planar geometries are considered in relation to MUBs. Thus all geometric definitions

and theorems will be stated for finite planar geometries only.

3.2.1 Latin squares

Definition 3.2. [102, §5.1] A *Latin square* of order n is an n by n array, with each of n symbols appearing exactly once in each row and each column.

A Latin square may also be represented as a set of ordered triples.

$$\mathcal{L} := \{(i, j, k) : \text{symbol } k \text{ occurs in cell } (i, j) \text{ of the Latin square}\}. \tag{3.1}$$

A cell of the Latin square may be called a *point*. A set of cells which are in the same row, a set of cells which are in the same column, or a set of cells which contain the same symbol may be called a *line*. There are three types of lines in a Latin square. A *row* line

$$L_i^r := \{(i, j, k) : 0 \leq j, k \leq d-1 \text{ and } (i, j, k) \in \mathcal{L}\}, \tag{3.2}$$

a *column* line

$$L_j^c := \{(i, j, k) : 0 \leq i, k \leq d-1 \text{ and } (i, j, k) \in \mathcal{L}\}, \tag{3.3}$$

and a *Latin* line

$$L_k^l := \{(i, j, k) : 0 \leq i, j \leq d-1 \text{ and } (i, j, k) \in \mathcal{L}\}. \tag{3.4}$$

Definition 3.3. [11, §I, Def 5.4] A parallel class, ∥-class, A, is a partition of a set of points into lines which are parallel. Two ∥-classes A and B are *unbiased* if each line of A contains exactly one element in common with each line of B.

A *row* ∥*-class* is the collection $\{L_i^r \mid 0 \leq i \leq d-1\}$, and $L = \cup_{0 \leq i \leq d-1} L_i^r$. A *column* ∥*-class* is the collection $\{L_j^c \mid 0 \leq j \leq d-1\}$, and $L = \cup_{0 \leq j \leq d-1} L_j^c$. A *Latin* ∥*-class* is the collection $\{L_k^l \mid 0 \leq k \leq d-1\}$, and $L = \cup_{0 \leq k \leq d-1} L_k^l$. A Latin square represents 3 *mutually unbiased* ∥*-classes*, the row ∥-class, the column ∥-class, and the Latin ∥-class.

0	1	2	3
2	3	0	1
1	0	3	2
3	2	1	0

0	1	2	3
3	2	1	0
2	3	0	1
1	0	3	2

0	1	2	3
1	0	3	2
3	2	1	0
2	3	0	1

Figure 3.1: A complete set of MOLS of order 4 [23, §III.3 Ex 3.4].

00	11	22	33
23	32	01	10
12	03	30	21
31	20	13	02

Figure 3.2: The first and second Latin squares from figure 3.1 are superimposed. Every pair appears exactly once, showing orthogonality.

3.2.2 Mutually orthogonal Latin squares

Definition 3.4. [102, §6.1] Two Latin squares A and B of the same order are *orthogonal* if their Latin $\|$-classes are unbiased. A set of Latin squares which are pairwise orthogonal are *mutually orthogonal Latin squares* (MOLS).

Figure 3.2 shows a method of checking if two Latin squares are orthogonal: superimpose the two Latin squares and check that every ordered pair of symbols appears exactly once.

A set of n MOLS is equivalent to $n + 2$ mutually unbiased $\|$-classes; the row $\|$-class, column $\|$-class and n Latin $\|$-classes. Each Latin square represents the same row and column $\|$-classes, as they have the same arrangement of cells. Each of the n MOLS have a different arrangement of symbols within the cells, and hence represent different Latin $\|$-classes.

We give an example of three MOLS of order 4 in Figure 3.1. A Latin square is in *standard form* if the symbols in the first row appear in lexicographic order. The Latin squares in Figure 3.1 are in standard form.

Many of the counting theorems for MOLS are similar to those for MUBs. Let $M(d)$ be the maximum number of MOLS of side length d.

Theorem 3.5. *[102, Thm 6.2] For $d > 1$, $M(d) \leq d - 1$.*

Proof. Suppose that L_1, L_2, ..., L_d are d MOLS of order d, each in standard form. Let $(1, 2, a_i)$ be an element of L_i. Since all the Latin squares are in standard form $(1, 1, 1) \in L_i$ for each $1 \leq i \leq d$, and hence $a_i \neq 1$. Because L_1, L_2, ..., L_d are mutually orthogonal we know that a_1, a_2, ..., a_d are distinct. Hence we must choose d distinct elements from the set $\{2, 3, \ldots, d\}$, clearly an impossibility. Hence there can be at most $d-1$ MOLS of order d. □

Thus counting ‖-classes, Theorem 3.5 is analogous to the upper bound on the number of MUBs (Theorem 2.47). This bound is attainable; a set of $d-1$ MOLS of order d is called *complete*.

Theorem 3.6. *[102, §6.2] For $d = p^n$, a complete set of MOLS of order d exists.*

Proof. A construction is given in Theorem 3.22, which from Lemma 3.24 can be used with any Galois field. Galois fields exist for all prime powers (see for example [40, Thm 8.5.10]). □

As with MUBs it is unknown if complete sets of MOLS exist in non prime power dimensions.

Open Problem 3.7. *Do complete sets of MOLS of order d exist when d is not a power of a prime?*

The following is analogous to the reduce to prime powers construction of MUBs (Theorem 2.50).

Theorem 3.8. *(MacNeish Bound) [80] $M(xy) \geq \min\{M(x), M(y)\}$*

Proof. [102, Thm 6.5] Let $m = \min\{M(x), M(y)\}$, and $n \geq m$. Let $\{K_1, K_2, \ldots, K_m\}$ be a set of m MOLS of order x with symbol set $\{0, 1, \ldots, x-1\} \subset \mathbb{Z}_{xy}$. Let $\{N_1, N_2, \ldots, N_n\}$ be a set of n MOLS of order y with symbol set $\{0, 1, \ldots, y-1\} \subset \mathbb{Z}_{xy}$. The proof is by construction. We show that a set of m MOLS of order xy can be constructed.

For $1 \leq a \leq n$ let N_a^r be the array obtained from N_a by:

$$(N_a^r)_{ij} = (N_a)_{ij} + ry \qquad \text{for } 0 \leq r \leq x-1. \tag{3.5}$$

Now construct the $xy \times xy$ array L_a by taking the cells of M_a that contain symbol r and inserting the matrix N_a^r. This is similar, but not the same as the Kronecker product. The symbol set of L_a is $\{0, 1, \ldots, xy-1\} = \mathbb{Z}_{xy}$.

For each symbol $k \in \mathbb{Z}_{xy}$ there are unique numbers $r_k \in \{0, 1, \ldots, m-1\}$ and $s_k \in \{0, 1, \ldots, n-1\}$ such that

$$k = r_k y + s_k. \tag{3.6}$$

Then $(L_a)_{ij}$ contains symbol k if and only if

$$i = r_i y + s_i, \qquad j = r_j y + s_j, \qquad (N_a)_{s_i s_j} = s_k, \qquad \text{and} \quad (K_a)_{r_i r_j} = r_k. \tag{3.7}$$

We now check that L_a and L_b are orthogonal for $a \neq b$. As K_a and K_b are orthogonal, each pair $(N_a^r, N_b^{r'})$, where $0 \leq r, r' \leq (k-1)$, is superimposed exactly once when L_a and L_b are superimposed. Since N_a and N_b are orthogonal, every pair (k, k'), where $0 \leq k, k' \leq xy - 1$, will appear exactly once when L_a and L_b are superimposed. □

The MacNeish bound was originally conjectured as an equality when d is not a prime power [80]. However there are examples for which there are more MOLS than this bound shows. E.g. $M(12) \geq 5$, $M(14) \geq 3$ [23, §III 3.4].

The combinatorial similarities between complete sets of MOLS and complete sets of MUBs are expressed most strongly in the SPR conjecture. Further evidence for and against this conjecture will be given in section 3.2.5.

3.2.3 Objects equivalent to MOLS

The SPR conjecture was originally published referring to finite projective planes.

Lemma 3.9. *[23, §III Thm 3.20] A projective plane of order d exists if and only if a complete set of MOLS of order d also exists.*

A complete set of MOLS is equivalent to a range of combinatorial structures. The following is a non-exhaustive list.

Theorem 3.10. *[23, §III Thm 3.18] A complete set of MOLS of sidelength d is combinatorially equivalent to*

- *an affine plane of order d.*
- *a $(d+1, d)$-net.*
- *an orthogonal array $OA(d^2, d+1, d, 2)$.*

- *a* $2-(d^2+d+2, d+1, 1)$ *design.*

We give definitions of each of these, as all have appeared somewhere in the literature on MUBs. We choose to always refer to MOLS or affine planes where possible, as these are the objects that the author is most familiar with.

Affine planes are a geometric structure, thus most of the published literature uses geometric definitions. MOLS are a combinatorial structure described using combinatorial definitions.

Definition 3.11. [102, §1.2] Let X be a set of points and $\mathcal{B}$ be a set of subsets of X. The subsets are called blocks and $(X, \mathcal{B})$ is a *block design.*

Definition 3.12. [30, §1.1] An *incidence structure*$(\mathcal{P}, \mathcal{L}, \mathcal{I})$ is a set of points $\mathcal{P}$, a set of lines $\mathcal{L}$ and a set of flags $\mathcal{I} \subset \mathcal{P} \times \mathcal{L}$. A point P is incident with a line l if $(P, l) \in \mathcal{I}$.

Block design is a definition from combinatorial mathematics that is equivalent to an *incidence structure* from geometry.

Definition 3.13. [30, §3.1] A *finite affine plane* is an incidence structure $\mathcal{A} = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ such that

1. any two distinct points are incident with exactly one line.
2. for any point P not incident with l, there is exactly one line incident with P which has no point in common with l.
3. there exist three points not incident with a common line.

Definition 3.14. [23, III.3.15] A $(k, v)-net$ is a block design, (X, C), where X is a set of v^2 points, and C is set of kv blocks. Each block contains v points such that the intersection of two distinct blocks contains at most one element.

Let $\{\mathcal{L}_l | 1 \leq l \leq k-2\}$ be a set of $k-2$ MOLS of order v. We construct a (k, v)-net (X, C). Let the set of points, X, be ordered pairs (i, j) where $0 \leq i, j \leq v-1$. Block b_{nl} contains point (i, j) if n appears in cell (i, j) of Latin square l. Block $b_{n(k-1)}$ is the n^{th} row of the row $\|$-class, and b_{nk} is the n^{th} column of the column $\|$-class.

Definition 3.15. [102, §9.7] An *orthogonal array*, $OA(N, k, v, t)$ is a $k \times N$ matrix, A, with entries from a symbol set of size v, such that in any $t \times N$ submatrix of A, each t-tuple appears exactly N/v^t times.

Definition 3.16. [23, II.4.1] A $t-(v,k,\lambda)$ *design* is a block design (X,C) where X is a set of v points, C is a set of $\lambda\binom{v}{t}/\binom{k}{t}$ blocks. Each block contains k points. For any subset $Q \subset X$ such that $|Q| = t$, there are exactly λ blocks which contain Q.

The notation $S_\lambda(t,k;v)$, which is related to Steiner systems, is often used [11, Defi3.1]. A $2-(v,k,\lambda)$ design may also be called a *balanced incomplete block design.*

Theorem 3.17. *(Bruck-Ryser-Chowla)[16][102, §12 Thm 1] Let v, k and λ be integers with $\lambda(v-1) = k(k-1)$ for which there exists a $2-(v,k,\lambda)$ design.*

- *If v is even then $n = k-\lambda$ is a square*
- *If v is odd, then the equation $z^2 = (k-\lambda)x^2 + (-1)^{(v-1)/2}\lambda y^2$ has a solution in integers x, y, z not all zero.*

The Bruck-Ryser-Chowla theorem is the best general condition for the existence of a complete set of MOLS. It is written in terms of a t-design, however using Theorem 3.10 we find that if n is to be the order of a complete set of MOLS then

$$z^2 = nx^2 + (-1)^{(n^2+n)/2}y^2 \tag{3.8}$$

must have a solution in integers.

This means that in particular n cannot take the values of 6, 14 or 21. In fact no pair of orthogonal Latin squares of side length 6 exits [23, Theorem 3.39]. It has been shown through exhaustive computation that there is no complete set of MOLS of side length 10 [73]. However there are an infinite number of values for which neither the Bruck-Ryser-Chowla theorem, nor any other result, excludes the existence of a complete set of MOLS. The existence of a complete set of MOLS of non-prime-power order is thus an open problem.

3.2.4 Constructions of MOLS

One of the most important classes of MOLS is those that are equivalent to the Desarguesian planes. Desargues was a French architect and mathematician, who proved an important theorem on triangles in real Euclidean geometry [39]. Any geometry that obeys the Theorem of Desargues is called *Desarguesian.*

Definition 3.18. [30, 1.4.1] Let V be a 2 dimensional vector space over a finite field $\mathbb{F}$. A coset of V is a subset $S + a = \{x + a \mid x \in S\}$, where S is a subspace of V and $a \in V$. Let the cosets of a subspace of dimension 0 be points, and cosets of subspaces of dimension 1 be lines. Then the geometry formed is a *Desarguesian* affine plane.

Definition 3.19. Let $AG(2, q)$ denote the affine plane which is constructed from $\mathbb{F}_q$ as in Definition 3.18. Points of $AG(2, q)$ are ordered pairs (a, b) with $a, b \in \mathbb{F}_q$. A line is the set of points (a, b) such that

$$\alpha a + \beta b = \gamma \tag{3.9}$$

for $\alpha, \beta, \gamma \in \mathbb{F}_q$ with α, β, γ fixed and α, β not both zero.

Lemma 3.20. *[30, 1.4.5] The only finite Desarguesian affine planes are $AG(2, q)$, for all prime powers q.*

A set of MOLS which is equivalent to $AG(2, q)$ may be called the Desarguesian MOLS.

Planar functions are so called because they can be used to construct finite affine planes, though not all affine planes have a planar function construction [30]. Hence planar functions can be used to construct complete sets of MOLS. The definition given for a planar function (Definition 2.36) does not mention planes. We give an alternate definition which shows where the name planar originated.

Definition 3.21. Let G, H be finite groups of order n. Let f be a function from G into H. Define points to be elements of $G \times H$, and lines to be the sets

$$L_{lj} = \{(i, f(i - l) + j) : i \in G\}, \quad l \in G, j \in H, \tag{3.10}$$

$$L_c = \{(c, y) : y \in H\}, \quad c \in G. \tag{3.11}$$

If the structure defined is an affine plane then f is a *planar* function.

Definitions 3.21 and 2.36 are equivalent [26]. The set of lines $\{L_{lj} : l \in G, j \in H\}$ are the row $\|$-class and the Latin $\|$-class. The set of lines $\{L_c : c \in G\}$ are the column $\|$-class.

The planar function construction of MUBs (Thm 2.52) uses planar functions to construct the vectors of the set of MUBs. Planar functions can be used to construct complete sets of MOLS, however there are MOLS that cannot be constructed via a planar function [30, §5].

Theorem 3.22. *[27, Thm 5.3] Let f be a planar function on the group G of order n, and let $i, j, k, l \in G \setminus \{0\}$. Let*

$$k := f(i) - f(i-l) + j, \quad l \in G \setminus \{0\}. \tag{3.12}$$

Then the sets

$$\mathcal{L}_l := \{(i, j, k) : i, j \in G\}, \quad l \in G \setminus \{0\} \tag{3.13}$$

are Latin squares, and $\cup_{l \in G\setminus\{0\}} \mathcal{L}_l$ form a complete set of mutually orthogonal Latin squares.

Proof. Note that given (k, l), for each i there is at least one j that will solve equation (3.12).

Let (i, j) and (i, j') solve equation (3.12) for a given k:

$$f(i) - f(i-l) + j = f(i) - f(i-l) + j' \tag{3.14}$$

$$j = j'. \tag{3.15}$$

Let (i, j) and (i', j) solve equation (3.12) for a given k:

$$f(i) - f(i-l) + j = f(i') - f(i'-l) + j \tag{3.16}$$

$$f(i) - f(i-l) = f(i') - f(i'-l) \tag{3.17}$$

$$\Delta_{f,l}(i) = \Delta_{f,l}(i'). \tag{3.18}$$

since $\Delta_{f,l}$ is a permutation polynomial, $i = i'$. Thus each symbol (value for k) appears in each row and each column exactly once and $\mathcal{L}_l$ is a Latin square.

For $\mathcal{L}_l$ and $\mathcal{L}_{l'}$ to be orthogonal we need that given l and l', for any k and k' there is exactly one pair (i, j) that solves equation (3.12) for l and l'. Let $k = f(i) - f(i-l) + j$ and $k' = f(i) - f(i-l') + j$:

$$k - k' = f(i-l) - f(i-l'). \tag{3.19}$$

Let $l' = l + x$ and $i - l = y$ then

$$k - k' = f(y) - f(y-x) = \Delta_{f,x}(y). \tag{3.20}$$

Since $\Delta_{f,x}$ is a permutation function, for any choice of k, k' there is exactly one solution for y, and hence exactly one value of i which solves equation (3.19). There are $n-1$ values for l and each pair $\mathcal{L}_l$ and $\mathcal{L}_{l'}$ is orthogonal for $l \neq l'$, thus a complete set of MOLS has been constructed.

□

Theorem 3.23. *All known planar functions on $\mathbb{F}_{p^r}$ are equivalent to one of the following [115]:*

- $\Pi(x) = x^{p^\alpha+1}$, *where* $\alpha \geq 0$ *is an integer and* $\frac{r}{gcd(r,\alpha)}$ *is an odd integer [31]. This includes* $\Pi(x) = x^2$ *as the simplest case.*
- $\Pi(x) = x^{(3^k+1)/2}$, *where* $p = 3$, k *is odd and* $gcd(r, k) = 1$ *[27].*
- $\Pi(x) = x^{10} - ux^6 - u^2x^2$, *where* $p = 3$, r *is odd, and* $u \in \mathbb{F}_{p^r}^*$ *[32].*

There are planar functions over other groups [51], but since Galois fields are used in many applications, the greater focus has been on planar functions over Galois fields.

Lemma 3.24. *[31, Cor 3] The planar function $f \in \mathbb{F}_q[X]$ with $f(i) = i^2$ generates the Desarguesian MOLS.*

Proof.

$$k = i^2 - (i-l)^2 + j \tag{3.21}$$
$$= 2il - l^2 + j \tag{3.22}$$

This is now a linear finction in i, j, k, which mirrors the structure of equation (3.9) which is linear in a, b, γ. □

Therefore any MOLS generated from any quadratic equations are equivalent.

Theorem 3.25. *[27, Thm 5.1, 5.2] Let f be a planar function, h an additive function, and g an additive permutation function on a group G. The MOLS generated from $f(i)$ and $f(g(i)) + h(i)$ using Theorem 3.22 are equivalent.*

Proof. First we show that $f(i)$ and $f(i) + h(i)$ generate equivalent MOLS. Let k be as in equation (3.12) and let

$$k' = f(i) + h(i) - f(i-l) - h(i-l) + j. \tag{3.23}$$

Since h is additive $h(i-l) = h(i) - h(l)$. Therefore

$$k' = f(i) - f(i-l) - h(l) + j \tag{3.24}$$
$$= k - h(l). \tag{3.25}$$

Thus h is just a permutation of the symbols in each Latin square.

We now show that $f(i)$ and $f(g(i))$ generate equivalent MOLS. k may be thought of as a solution to a function:

$$k = \phi_f(i, j, l) = f(i) - f(i - l) + j. \tag{3.26}$$

g is a permutation and thus has an inverse. Then

$$\begin{aligned}
\phi_{f\circ g}(g^{-1}(i), j, l) &= f(g(g^{-1}(i) - g^{-1}(l))) + j && (3.27)\\
&= f(g(g^{-1}(i))) - f(g(g^{-1}(i) - l)) + j && (3.28)\\
&= f(i) - f(i - g(l)) + j && (3.29)\\
&= \phi_f(i, j, g(l)) + j. && (3.30)
\end{aligned}$$

g is thus a permutation of the Latin squares. □

Corollary 3.26. *[31] All quadratic functions on $\mathbb{F}_q$ generate equivalent sets of MOLS.*

Proof. Let f be a quadratic function in $\mathbb{F}_q[x]$ given by $f(x) = ax^2 + bx + c$. Let $h(x) = \alpha x + \beta$ and $g(x) = \gamma x + \delta$ be linear functions in $\mathbb{F}_q[x]$.

$$\begin{aligned}
f(g(x)) + h(x) &= a(\gamma x + \delta)^2 + b(\gamma x + \delta) + c + \alpha x + \beta && (3.31)\\
&= a\gamma^2 x^2 + (2a\gamma\delta + b\gamma + \alpha)x + a\delta^2 + b\delta + c + \beta && (3.32)
\end{aligned}$$

which is quadratic in $\mathbb{F}_q$. □

It is known that if a complete set of MOLS exists in a non prime power dimension, then it cannot be Desarguesian [30, §1.4 Thm 5]. Necessary and sufficient conditions are known for a complete set of MOLS to be constructed from a planar function [30, §5.1 Thm 13]. However it is not known if these conditions can be met with MOLS of non prime power order.

Conjecture 3.27. *If a complete set of MOLS exists in a non prime power dimension, then it cannot be described using a planar function.*

3.2.5 SPR Conjecture

SPR Conjecture

Similarities between MUBs and (MOLS) were first noted by Wootters and Fields in 1989 [112]. Wootters further noted in 2004[1] that the problem of finding mutually unbiased measurements is 'similar in spirit' to finding mutually unbiased ‖-classes [111]. These similarities were put formally in the following conjecture.

Conjecture 3.28 (SPR Conjecture)**.** *[96] A complete set of MUBs exists in $\mathbb{C}^d$ if and only if a complete set of MOLS of sidelength d exists.*

If there is a concrete connection between MOLS and MUBs, then results on the non-existence of complete sets of MOLS (Thm 3.17) could be used to show non-existence of complete sets of MUBs.

If MUBs and MOLS are indeed equivalent then there should be mathematical aspects of MUBs that correspond to points and lines of mutually unbiased ‖-classes.

Evidence for the SPR conjecture

Some counting theorems for MOLS are analogous to the counting theorems for MUBs. The upper bound of $d+1$ MUBs (Theorem 2.47) is analogous to upper bound of $d+1$ mutually unbiased ‖-classes (Theorem 3.5). The reduce to prime powers lower bound on the number of MUBs (Theorem 2.50) is analogous to the MacNeish bound for MOLS (Theorem 3.8). This evidence is at the level of cardinalities only, and may be coincidental.

There are also structural similarities. The following is a suggestion of Wootters [111]. Let M be a complete set of MOLS of order d. Assign to each point α of M a d dimensional Hermitian operator A_α, and to each line l of M a one dimensional projection operator P_l such that

$$\mathrm{Tr}(\frac{1}{d}A_\alpha) = \frac{1}{d} \tag{3.33}$$

$$\mathrm{Tr}(\frac{1}{d}A_\alpha)(\frac{1}{d}A_\beta) = \frac{1}{d}\delta_{\alpha\beta} \tag{3.34}$$

$$\sum_{\alpha\in l}\frac{1}{d}A_\alpha = P_l. \tag{3.35}$$

[1] published in 2006, but preprint available in 2004.

It follows from the geometry that $\mathrm{Tr}(P_l P_m) = 0$ if l, m are parallel and $\mathrm{Tr}(P_l P_m) = \frac{1}{d}$ if l, m are not parallel. Since a complete set of MOLS has $d+1$ sets of d parallel lines, the projection operators define a complete set of MUBs. It is however unknown how to construct the operators A_α.

It has been noted that if affine planes exist in no prime power dimensions they must be non-Desarguesian (Lemma 3.20). The MUBs constructed using the planar function construction are non-Desarguesian when the planar function used is not x^2 (Lemma 3.24). Much of the evidence given above for the SPR conjecture relies on the properties of Galois fields. However if the SPR conjecture is true, then we would expect sets of MUBs that do not rely on Galois fields to exist. The Galois ring MUBs are such an example.

Evidence against the SPR conjecture

Definition 3.29. A *mutually unbiased constellation* is a set of vectors that can be partitioned into $d+1$ subsets of orthonormal vectors such that for any two vectors ϕ and ψ that are in different subsets of the partition, $|\langle\phi|\psi\rangle|^2 = \frac{1}{d}$.

Any subset of a set of MUBs is a mutually unbiased constellation. Thus if for some $c \leq d(d+1)$ there exists no MU constellations with c vectors in $\mathbb{C}^d$, then a complete set of MUBs cannot exist in $\mathbb{C}^d$.

Definition 3.30. [108] An *affine constellation* of order d consists of $d+1$ sets of parallel lines, each line having d points, and any two lines from different sets having exactly one point in common.

If at least two of the sets contain d lines then a MU constellation is a set of mutually orthogonal partial Latin squares [23, §III, Def 1.21].

There are affine constellations of dimension 6, [108] with no corresponding mutually unbiased constellations. Whilst this does not disprove the SPR conjecture, it does hint that perhaps there is no deep connection between MUBs and MOLS.

3.2.6 Constructions of MUBs using MOLS

Construction using Desarguesian MOLS

This section has been published as [48].

The Pauli matrix construction of MUBs as published in [85] uses the Desarguesian MOLS which have been generated using a Galois field. The MOLS are then used to generate a net, which is further used to construct a set of matrices with eigenbases that form a complete set of MUBs. The conversion from MOLS to a net is slightly different to that given in definition 3.14.

Theorem 3.31. *[85, § V] Let p be a prime and $i, j, k, x \in \mathbb{F}_p$, then*

$$\mathcal{L}_x := \{(i, j, k) : k = ix + j\}. \tag{3.36}$$

is a Latin square, $\mathcal{M} = \{\mathcal{L}_x : x \in \mathbb{F}_p\}$ is a complete set of MOLS.

A $(p+1, p)$-net is constructed with point set $\mathbb{F}_q \times \mathbb{F}_q$, and blocks

$$b_{row,j} = \{(y, k) : y \in \mathbb{F}_p\}, \tag{3.37}$$

$$b_{j,col} = \{(k, y) : y \in \mathbb{F}_p\}, \tag{3.38}$$

$$b_{i,j} = \{(x, k) : k = ix + j\} \qquad \text{for } x \in \mathbb{F}_p^*. \tag{3.39}$$

Let

$$X = \{b_{row,0}, b_{0,col}\} \cup \{b_{i,0} : i \in \mathbb{F}_p^*\}. \tag{3.40}$$

Let $q = p^r$ and let $E = \{e_1, \ldots, e_r\}$ and $\bar{E} = \{\bar{e}_1, \ldots, \bar{e}_r\}$ be dual bases for $\mathbb{F}_q$. For each block in X choose a point (a, b). Let

$$T_{ab} = X_p^{a_1} Z_p^{b_1} \otimes X_p^{a_2} Z_p^{b_2} \cdots \otimes X_p^{a_r} Z_p^{b_r} \qquad a, b \in \mathbb{F}_q \tag{3.41}$$

where $a_i = \mathrm{tr}(a\bar{e}_i)$ and $b_i = \mathrm{tr}(be_i)$ and X_p, Z_p are the generalised Pauli matrices. The eigenbases of $\{T_{ab} : a, b \in \mathbb{F}_q\}$ are a complete set of MUBs.

In the Pauli matrix construction the two bases E, F chosen for $\mathbb{F}_q$ are required to have the relationship $F = k\bar{E}$. Thus the construction given in Theorem 3.31 is a special case of the Pauli matrix construction with $F = \bar{E}$. The equation which is used to construct the orthogonal Latin squares (equation (3.36)) is the same equation that is used to define lines in the proof of the Pauli matrix construction (equation (2.96)).

The fact that complete sets of MOLS are constructed is an unused intermediate step, as the construction and proof rely on the equation $k = ix + j$ over a Galois field.

0	1	2	3	4	5	6	7	8	9
1	2	6	5	8	0	9	3	4	7
2	9	4	0	5	7	3	8	6	1
3	4	9	7	6	8	5	1	0	2
4	3	7	8	1	6	0	2	9	5
5	8	3	6	2	9	7	0	1	4
6	5	1	9	7	3	8	4	2	0
7	0	5	2	9	1	4	6	3	8
8	7	0	4	3	2	1	9	5	6
9	6	8	1	0	4	2	5	7	3

0	2	4	9	1	8	7	5	3	6
1	7	3	4	5	9	2	6	0	8
2	3	8	7	6	4	1	9	5	0
3	9	5	2	4	7	0	8	6	1
4	5	6	1	9	2	8	0	7	3
5	6	2	0	8	1	9	3	4	7
6	1	7	8	3	0	4	2	9	5
7	4	9	3	0	5	6	1	8	2
8	0	1	5	7	6	3	4	2	9
9	8	0	6	2	3	5	7	1	4

Figure 3.3: A pair of orthogonal Latin squares of order 10

00	01	02	03	04	05	06	07	08	09
00	10	20	30	40	50	60	70	80	90
00	11	22	33	44	55	66	77	88	99
00	12	24	39	41	58	67	74	83	96

Figure 3.4: A set of blocks of the $(4, 1)$*-net corresponding to the OLS of Figure 3.3.*

In [85, §1] Paterek, Dakić and Brukner state that they 'link every OLS of order being a power of a prime with a MUB'. The MOLS constructed using equation (3.36) are the Desarguesian MOLS. There are many sets of non-Desarguesian MOLS, for example there are several planar functions on some Galois fields which construct non-equivalent MOLS (Theorem 3.23).

It may be possible that this method constructs MUBs from MOLS which have been constructed differently, but Theorem 3.31 only shows MUBs from the Desarguesian MOLS.

In subsequent work by Paterek, Pawlowski, Grassl and Brukner an attempt is made to use a pair of orthogonal Latin squares of order 10 to create a set of MUBs in $\mathbb{C}^d$[86].

The pair of orthogonal Latin squares is given in Figure 3.3. The first set of blocks of the corresponding net is given in Figure 3.4.

The operators X^2Z^4 and X^3Z^9 do not commute, thus this pair of MOLS cannot be used

to construct a set of 4 MUBs in dimension 10 using the algorithm of Theorem 3.31. This is not surprising as the proof of Theorem 3.31 (given as the Pauli matrix construction) relies on properties of Galois fields. There is no Galois field of order 10, hence the calculation in [86] is evidence that the Pauli matrix product construction only works in the presence of a Galois field.

Incomplete sets of MUBs using MOLS

The following construction uses a set of MOLS. Unlike the construction detailed in Theorem 3.31, any set of MOLS may be used, not just those generated using a Galois field. However this construction cannot generate complete sets of MUBs.

Definition 3.32. [23, Def 1.7] The *Hamming weight* of a vector is the number of non-zero entries. The *support* of a vector is the set of positions where a vector has non-zero entry.

The Hamming weight of a vector is the size of its support.

Definition 3.33. [110, Eqn 6] Let $\vec{m} \in \{0,1\}^d$ with Hamming weight s and support $\{r_0, r_1, \ldots, r_{s-1}\}$, and let $\vec{h} \in \mathbb{C}^s$. The *embedding of $\vec{h}$ into $\mathbb{C}^d$ controlled by $\vec{m}$*, denoted $h \uparrow m$ is given by:

$$\vec{h} \uparrow \vec{m} := \sum_{i=0}^{s-1} \vec{h}_i \vec{e}_{r_i} \tag{3.42}$$

where h_i is the i^{th} entry in $\vec{h}$ and $\vec{e}_{r_i}$ is the r_i^{th} standard basis vector.

For example:

$$\vec{m} := \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \qquad \vec{h} := \begin{pmatrix} \omega \\ 1 \end{pmatrix} \qquad \vec{h} \uparrow \vec{m} := \begin{pmatrix} \omega \\ 0 \\ 0 \\ 1 \end{pmatrix}. \tag{3.43}$$

Theorem 3.34 (WB construction)**.** *[110, Thm 3] Given a set of $k-2$ mutually orthogonal Latin squares of order s and a complex Hadamard matrix of order s, a set of k mutually unbiased bases in $\mathbb{C}^{s^2}$ can be constructed.*

Proof. Using the construction given below Definition 3.14 we construct a (k, s)-net. Let $\vec{m}_{ab}$ be the incidence vector of block c_{ab} of the net. Let $\vec{h}_i$ be the i^{th} column of the complex Hadamard matrix. Let

$$\vec{v}_{abj} := \frac{1}{\sqrt{s}}(\vec{h}_j \uparrow \vec{m}_{ba}) \tag{3.44}$$

and let

$$B_a := \{\vec{v}_{abj} : 1 \leq j, b \leq s\}. \tag{3.45}$$

We show that $\cup_{a=1}^{k} B_a$ is a set of k MUBs in $\mathbb{C}^d$.

All vectors $\vec{h}_j \uparrow \vec{m}_{ba}$ have magnitude $\sqrt{s}$ because all incidence vectors $\vec{m}_{ab}$ have Hamming weight s. Thus vectors constructed from equation (3.44) are normalized.

The vectors $\vec{m}_{ba}$ and $\vec{m}_{ba'}$ have disjoint supports and are therefore orthogonal. The vectors $\vec{h}_j$ and $\vec{h}_{j'}$ are orthogonal from the properties of Hadamard matrices. Hence the vectors $\vec{h}_j \uparrow \vec{m}_{ba}$ and $\vec{h}_{j'} \uparrow \vec{m}_{ba'}$ are orthogonal for $(j, a) \neq (j'a')$. This shows that each B_a is an orthonormal basis for $\mathbb{C}^d$.

For $a \neq a'$, there is exactly one i such that $\vec{m}_{ba_i} = \vec{m}_{b'a'_i} = 1$. Thus

$$\langle \vec{h}_j \uparrow \vec{m}_{ba} | \vec{h}_{j'} \uparrow \vec{m}_{b'a'} \rangle = (\vec{h}_j \uparrow \vec{m}_{ba})_i \cdot (\vec{h}_{j'} \uparrow \vec{m}_{b'a'})_i = x, \tag{3.46}$$

where x is a complex number of modulus 1. Then

$$\langle \vec{v}_{abj} | \vec{v}_{a'b'j'} \rangle = \frac{1}{\sqrt{s}} x. \tag{3.47}$$

Thus vectors from B_a and $B_{a'}$ are unbiased. □

This constructs more MUBs than the lower bound of Theorem 2.50 in $\mathbb{C}^{s^2}$, if the number of MOLS of order s exceeds the MacNeish bound for MOLS of order s^2, eg. $s = 26, 30, 34, 42, 46, 50, 54, 62$ [23, §III 3.4].

The WB construction relies entirely on the properties of the MOLS, and complex Hadamard matrices, and is thus independent of any particular algebraic structure. It is dependent on constructions of MOLS, which is an ongoing topic of research.

3.3 Constructing MOLS from MUBs in prime dimensions

This section has been published as [47].

We have a construction which, when given a complete set of MUBs, constructs complete sets of MOLS. This construction will be shown to work for 2 known constructions of MUBs: the WF and Alltop (Thm 2.53, Thm 2.54). This is different to other constructions which have focused on constructing MUBs from MOLS (see section 2.4). The construction exploits properties of the polynomials which generate the MUBs.

The WF and Alltop MUBs are equivalent (Theorem 2.65). However the vectors of the Alltop MUBs are not constructed from planar functions. Any structural properties that are from both WF and Alltop MUBs may be underlying properties of MUBs.

3.3.1 Inner product vectors

Definition 3.35. The *inner product vector*, $IPV[u, w]$, of two vectors u, w can be generated by $IPV[\vec{u}, \vec{w}]_i = u_i\overline{w_i} = v_i$ where $\vec{v} = (v_1, v_2, \ldots, v_n)^T$, $\vec{u} = (u_1, u_2, \ldots, u_n)^T$ and $\vec{w} = (w_1, w_2, \ldots, w_n)^T$.

In both the WF and Alltop MUBs, a vector $\vec{u}$ is constructed from a function f_u by

$$\vec{u} = \left(\omega_p^{\mathrm{tr}(f_u(x))}\right)_{x\in\mathbb{F}_p}. \tag{3.48}$$

Thus we may call f_u the function of $\vec{u}$. The inner product between $\vec{u}$ and $\vec{w}$ is given by

$$\langle\vec{u}|\vec{w}\rangle = \sum_{x\in\mathbb{F}_p} \omega^{\mathrm{tr}(f_u(x)-f_w(x))}. \tag{3.49}$$

Thus the inner product vector is constructed from the function $f_v(x) = f_u(x) - f_w(x)$ by

$$IPV[\vec{u}, \vec{w}] = \left(\omega_p^{\mathrm{tr}(f_u(x)-f_w(x))}\right)_{x\in\mathbb{F}_p} = \left(\omega_p^{\mathrm{tr}(f_v(x))}\right)_{x\in\mathbb{F}_p}. \tag{3.50}$$

The inner product is easily recovered from the inner product vector by summing the entries in the inner product vector:

$$\langle\vec{u}|\vec{w}\rangle = \sum_{x\in\mathbb{F}_p} IPV[\vec{u}, \vec{w}]_x. \tag{3.51}$$

In prime dimensions, trace is an identity function. In both the WF and Alltop MUBs the polynomials of the inner product vectors are quadratic and therefore planar functions.

3.3.2 WF type MUBs

The construction of MOLS using MUBs will be illustrated using WF MUBs before a more general construction is given.

Let $\vec{v}_{ab}$ be as in equation (2.79), and $B_a = \{\vec{v}_{ab} : b \in \mathbb{F}_q\}$. Since each B_a is a basis, each vector $\vec{e}_k$, $0 \leq k \leq q-1$, can be expressed as a linear combination of the vectors of B_a, for fixed $a \in \mathbb{F}_q$. First consider $\sum_{b\in\mathbb{F}_q} \vec{v}_{ab}$ for $\vec{v}_{ab} \in B_a$. The i^{th} component of this sum is given by

$$\begin{aligned} \frac{1}{\sqrt{q}} \sum_{b\in\mathbb{F}_q} \omega_p^{\text{tr}(ax_i^2+bx_i)} &= \frac{1}{\sqrt{q}}\ \omega_p^{\text{tr}(ax_i^2)} \sum_{b\in\mathbb{F}_q} \omega_p^{\text{tr}(bx_i)} \\ &= \begin{cases} \sqrt{q} & \text{if } i = 0 \\ 0 & \text{if } i \neq 0 \end{cases}, \end{aligned} \tag{3.52}$$

x_i is fixed and bx_i ranges over all the elements of $\mathbb{F}_q$ as b ranges over $\mathbb{F}_q$. In addition, the trace map is equiv-distributed and the result follows from Lemma 2.24. Therefore

$$\vec{e}_0 = \sum_{b\in\mathbb{F}_q} \vec{v}_{ab}. \tag{3.53}$$

To get $\vec{e}_k$ for $k \neq 0$, each vector needs to be multiplied by an appropriate weight. From equation (3.52), by multiplying each vector of B_a by

$$\text{w}_{(k,a,b)} := \frac{1}{\sqrt{q}}\ \omega_p^{\text{tr}(-ax_k^2-bx_k)} \tag{3.54}$$

for fixed k, the i^{th} component of $\sum_{b\in\mathbb{F}_q} \text{w}_{(k,a,b)}\vec{v}_{ab}$ for $\vec{v}_{ab} \in B_a$, (for fixed $a \in \mathbb{F}_q$), is given by

$$\begin{aligned} \sum_{b\in\mathbb{F}_q} (\text{w}_{(k,a,b)}\vec{v}_{ab})_i &= \frac{1}{\sqrt{q}} \sum_{b\in\mathbb{F}_q} \frac{1}{\sqrt{q}}\ \omega_p^{\text{tr}(ax_i^2+bx_i)} \omega_p^{\text{tr}(-ax_k^2-bx_k)} \\ &= \frac{1}{q}\ \omega_p^{\text{tr}[a(x_i^2-x_k^2)]} \sum_{b\in\mathbb{F}_q} \omega_p^{\text{tr}[b(x_i-x_k)]} \\ &= \begin{cases} 1 & \text{if } i = k \\ 0 & \text{if } i \neq k. \end{cases} \end{aligned} \tag{3.55}$$

Thus each vector of the standard basis is obtained as a linear combination of the vectors of each basis, i.e.,

$$\vec{e}_k = \text{w}_{(k,a,b_0)}\vec{v}_{ab_0} + \text{w}_{(k,a,b_1)}\vec{v}_{ab_1} + \cdots + \text{w}_{(k,a,b_{q-1})}\vec{v}_{ab_{q-1}} \tag{3.56}$$

where $\{b_0, b_1, \ldots, b_{q-1}\}$ is an ordering of the elements of $\mathbb{F}_q$, with $b_0 = 0$ and $0 \leq k \leq q-1$.

We now turn our attention to the simpler case when q is a prime. The benefit of this simplification is $\text{tr}(x) = x$ for $x \in \mathbb{F}_p$.

S	B_0	B_1	B_2
$\vec{e}_0=\begin{pmatrix}1\\0\\0\end{pmatrix}$	$\vec{v}_{00}=\frac{1}{\sqrt{3}}\begin{pmatrix}1\\1\\1\end{pmatrix}$	$\vec{v}_{10}=\frac{1}{\sqrt{3}}\begin{pmatrix}1\\\omega\\\omega\end{pmatrix}$	$\vec{v}_{20}=\frac{1}{\sqrt{3}}\begin{pmatrix}1\\\omega^2\\\omega^2\end{pmatrix}$
$\vec{e}_1=\begin{pmatrix}0\\1\\0\end{pmatrix}$	$\vec{v}_{01}=\frac{1}{\sqrt{3}}\begin{pmatrix}1\\\omega\\\omega^2\end{pmatrix}$	$\vec{v}_{11}=\frac{1}{\sqrt{3}}\begin{pmatrix}1\\\omega^2\\1\end{pmatrix}$	$\vec{v}_{21}=\frac{1}{\sqrt{3}}\begin{pmatrix}1\\1\\\omega\end{pmatrix}$
$\vec{e}_2=\begin{pmatrix}0\\0\\1\end{pmatrix}$	$\vec{v}_{02}=\frac{1}{\sqrt{3}}\begin{pmatrix}1\\\omega^2\\\omega\end{pmatrix}$	$\vec{v}_{12}=\frac{1}{\sqrt{3}}\begin{pmatrix}1\\1\\\omega^2\end{pmatrix}$	$\vec{v}_{22}=\frac{1}{\sqrt{3}}\begin{pmatrix}1\\\omega\\1\end{pmatrix}$

Figure 3.5: The complete set of WF MUBs in dimension 3.

3.3.3 WF type MUBs in a worked example for prime dimensions

We choose the smallest possible example to illustrate the construction. In the case $q = 3$ the complete set of MUBs is given in Figure 3.5.

We call E the standard basis, and B_0, B_1, B_2 the non-standard bases where $\omega = e^{2i\pi/3}$. Using Lemma 2.24, the first standard basis vector may be written as

$$\vec{e}_0 = \begin{pmatrix}1\\0\\0\end{pmatrix} = \frac{1}{3}\begin{pmatrix}1+1+1\\1+\omega+\omega^2\\1+\omega^2+\omega\end{pmatrix}. \tag{3.57}$$

This can be written as a linear combination of various non-standard bases vectors. e.g.

$$\begin{aligned}\vec{e}_0 &= \frac{1}{\sqrt{3}}\left(\frac{1}{\sqrt{3}}\begin{pmatrix}1\\1\\1\end{pmatrix}+\frac{1}{\sqrt{3}}\begin{pmatrix}1\\\omega\\\omega^2\end{pmatrix}+\frac{1}{\sqrt{3}}\begin{pmatrix}1\\\omega^2\\\omega\end{pmatrix}\right)\\ &= \frac{1}{\sqrt{3}}(\vec{v}_{00}+\vec{v}_{01}+\vec{v}_{02}).\end{aligned} \tag{3.58}$$

In all e_0 can be written as six different linear combinations of non-standard bases vectors.

$\vec{v}_{00}$	$\vec{v}_{01}$	$\vec{v}_{02}$
$\vec{v}_{10}$	$\vec{v}_{11}$	$\vec{v}_{12}$
$\vec{v}_{20}$	$\vec{v}_{21}$	$\vec{v}_{22}$

Figure 3.6: The structure of rows and columns to be used to build Latin squares

$$\begin{aligned}
\vec{e}_0 &= \frac{1}{\sqrt{3}}(\vec{v}_{00} + \vec{v}_{01} + \vec{v}_{02}) && (3.59)\\
&= \frac{1}{\sqrt{3}}(\vec{v}_{10} + \vec{v}_{11} + \vec{v}_{12}) && (3.60)\\
&= \frac{1}{\sqrt{3}}(\vec{v}_{20} + \vec{v}_{21} + \vec{v}_{22}) && (3.61)
\end{aligned}$$

$$\begin{aligned}
\vec{e}_0 &= \frac{1}{\sqrt{3}}(\vec{v}_{00} + \vec{v}_{10} + \vec{v}_{20}) && (3.62)\\
&= \frac{1}{\sqrt{3}}(\vec{v}_{01} + \vec{v}_{11} + \vec{v}_{21}) && (3.63)\\
&= \frac{1}{\sqrt{3}}(\vec{v}_{02} + \vec{v}_{12} + \vec{v}_{22}) && (3.64)
\end{aligned}$$

Then ignoring the scalar, $\frac{1}{\sqrt{3}}$, the vectors may be arranged in an array (Figure 3.6), with the row $\|$-class representing the vectors which appear in linear combinations of equations (3.59-3.61), and the column $\|$-class representing the vectors which appear in the linear combinations of equations (3.62-3.64).

This array (Figure 3.6) is the structure we will use to build Latin squares. We have the row and column $\|$-classes, we now require a further $\|$-class to give the symbols for the Latin square. Finding 3 representations of $\vec{e}_1$ requires using weights.

$$\begin{aligned}
\vec{e}_1 &= \frac{1}{3}(\vec{v}_{00} + \omega^2\vec{v}_{01} + \omega\vec{v}_{02}) && (3.65)\\
&= \frac{1}{3}(\omega^2\vec{v}_{10} + \omega\vec{v}_{11} + \vec{v}_{12}) && (3.66)\\
&= \frac{1}{3}(\omega\vec{v}_{20} + \vec{v}_{21} + \omega^2\vec{v}_{22}) && (3.67)
\end{aligned}$$

Here the same vectors are found as in equations (3.59-3.61), which represents the rows $\|$-class. This is unsurprising as any vector may be written as a linear combination of the vectors in a base. The weights, which when arranged according the array of Figure 3.6, gives an interesting

1	ω^2	ω
ω^2	ω	1
ω	1	ω^2

Figure 3.7: The Latin square formed from the weights in equations (3.65-3.67)

Vectors

♡	♢	♣
♣	♡	♢
♢	♣	♡

Figure 3.8: The Latin square formed from the vectors in equations (3.68-3.70)

pattern, in this case a Latin square (Figure 3.7). The next three representations of $\vec{e}_1$ give us another mutually unbiased ‖-class.

$$\vec{e}_1 = \frac{1}{3}(\vec{v}_{00} + \omega\vec{v}_{11} + \omega^2\vec{v}_{22}) \tag{3.68}$$

$$= \frac{1}{3}(\omega^2\vec{v}_{01} + \vec{v}_{12} + \omega\vec{v}_{20}) \tag{3.69}$$

$$= \frac{1}{3}(\omega\vec{v}_{02} + \omega^2\vec{v}_{10} + \vec{v}_{21}). \tag{3.70}$$

The groupings according to equations (3.68-3.70) can be organized into a Latin square (Figure 3.8). The vectors used in equation (3.68) are represented by ♡, the vectors used in equation (3.69) are represented by ♢ and the vectors used in equation (3.70) are represented by ♣. This gives us a Latin square in the vectors. The weights form the same arrangement as when using equations (3.65-3.67), which can be seen in Figure 3.7. The weights Latin square and vectors Latin square are orthogonal to each other.

Repeating this for a further standard basis vector we get another 3 equations which form the row ‖-classes and 3 equations which form a Latin ‖-class in the vectors and in the weights (Figure 3.9). The pair of vector Latin ‖-classes are orthogonal, as are the pair of weights Latin squares. By using the linear combinations of the vectors of the WF MUBs we have constructed a complete set of MOLS. This construction also yields a complete set of MOLS in the weights.

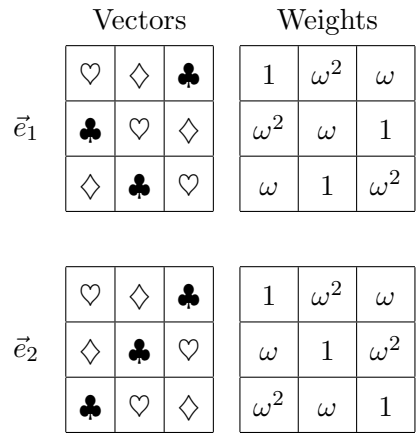

Figure 3.9: Latin squares formed from the collections of vectors and weights used in linear combinations that equal $\vec{e}_1$ and $\vec{e}_2$.

3.3.4 Alltop type MUBs in a worked example for prime dimensions

When using the Alltop MUBs (Thm 2.54), a complete set of MOLS is constructed in the vectors of the linear combinations, but the weights form Butson Hadamard Matrices. For example for $q = 5$, we get the set of MOLS and Butson Hadamard Matrices in Figure 3.10. Again we have exploited the linear combinations of the vectors in a complete set of MUBs to produce a complete set of MOLS. Note that the matrices generated from the scalars are Butson Hadamard matrices. This may have connections with the WB construction (Theorem 3.34).

In the next section we prove that the complete set of MOLS will always be generated for the WF and Alltop MUBs in prime dimensions.

3.3.5 Algebraic proof in prime dimensions

There are p vectors in the standard basis, hence for each $k \in \mathbb{F}_p$ there is a standard basis vector s_k. Any vector may be written as a linear combination of vectors from any basis. Thus

$$\vec{e}_k = \sum_{i \in P} \mathrm{w}_{(k,i)} \vec{v}_i \tag{3.71}$$

where P is some set of vector labels, $\vec{v}_i$ is the vector and $\mathrm{w}_{(k,i)}$ is the weight assigned to that vector in linear combinations which sum to $\vec{e}_k$.

The outline of the construction and proof: for each $k \in \mathbb{F}_p$, choose the weight that will

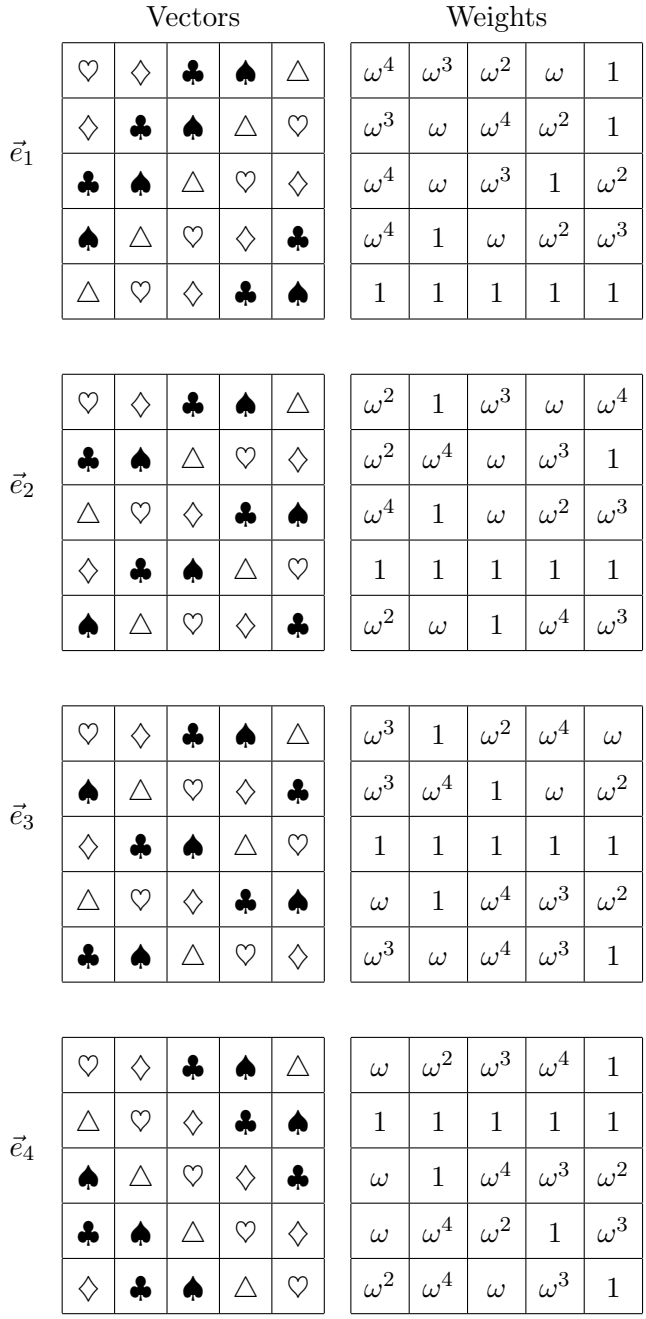

Figure 3.10: The mutually orthogonal Latin squares generated from the collections of vectors in linear combinations. The collections of weights form Butson Hadamard matrices.

be assigned to each vector, then choose the vectors that will (with their weights) form a linear combination that represents $\vec{e}_k$. Then show that for each k the same row ‖-class is constructed, for $k = 0$ a column ‖-class is also constructed and that for each $k \neq 0$ a Latin ‖-class is also constructed. Each of the Latin ‖-classes from each of the values of k are mutually orthogonal giving $p - 1$ MOLS.

Let

$$\vec{v}_{ab} = \frac{1}{\sqrt{q}} \left(\omega^{\mathrm{tr}(f_{ab}(x))} \right)_{x \in \mathbb{F}_q}. \tag{3.72}$$

Any vector can be expressed as a linear combination of the vectors of a base. This grouping of vectors into bases gives the row ‖-class. For each $k \in \mathbb{F}_p$, the weight $\mathrm{w}_{(k,a,b)}$ is assigned to $\vec{v}_{ab}$. A representation of $\vec{e}_k$ as a linear combination is required, where all summands have the same magnitude. Thus the phase of the summands is of interest. The k^{th} component of $\mathrm{w}_{(k,a,b)}\vec{v}_{ab}$ must be $\frac{1}{q}$, and hence

$$\mathrm{w}_{(k,a,b)} = \frac{1}{\sqrt{q}} \omega^{-\mathrm{tr}(f_{ab}(k))}. \tag{3.73}$$

Thus the elements in the linear combinations representing $\vec{e}_k$ are:

$$\mathrm{w}_{(k,a,b)}\vec{v}_{ab} = \frac{1}{q} \left(\omega^{\mathrm{tr}[f_{ab}(x) - f_{ab}(k)]} \right)_{x \in \mathbb{F}_q}. \tag{3.74}$$

Choosing the vectors to be all from the same base fixes a. For each choice of a and each choice of k

$$\sum_{b \in \mathbb{F}_p} \mathrm{w}_{(k,a,b)}\vec{v}_{ab} = \vec{e}_k. \tag{3.75}$$

This gives p copies of the row ‖-class. E.g. equations (3.59-3.61) and (3.65-3.67) show two copies of the row ‖-class, a third copy has been omitted as a repetitious calculation.

In the WF MUBs, f_{ab} is a planar function, so it is no surprise that the arrays of weights, as generated by equation (3.73) are Latin squares (e.g. Figure 3.7). In the Alltop MUBs f_{ab} is not a planar function, and so the arrays of weights are not Latin squares (e.g. Figure 3.10).

Next, create the equations for the non-row ‖-classes using the same weights assigned to each vector, but different groups of vectors. Note that in equations (3.65-3.67) and (3.68-3.70) each vector has the same weight. In order to create a linear combination involving $\mathrm{w}_{(k,a,b)}\vec{v}_{ab}$ which contains vectors not in the same base, first choose one vector e.g. $\vec{v}_{0c}$, and

see which elements can form the appropriate summation. To sum to $\vec{e}_k$, it is required that $(\mathrm{w}_{(k,a,b)}\vec{v}_{ab})_k = 1$ and $(\mathrm{w}_{(k,a,b)}\vec{v}_{ab})_x \neq (\mathrm{w}_{(k,0,c)}\vec{v}_{0c})_x$ for all $x \neq k$. Hence

$$\omega^{\mathrm{tr}[f_{ab}(x)-f_{ab}(z)]} \neq \omega^{\mathrm{tr}[f_{0c}(x)-f_{0c}(z)]} \quad \forall k \neq x, a \neq 0. \tag{3.76}$$

Thus if equation (3.76) is satisfied for $k = 0$ then this grouping forms the column $\|$-class and from which an array may be prepared (Figure 3.6). If equation (3.76) is satisfied for $k \neq 0$ then the cell in the prepared array corresponding to $\vec{v}_{ab}$ shall contain the c^{th} symbol. In Figure 3.8, $\heartsuit$ is the 0^{th} symbol, $\diamondsuit$ is the 1^{st} symbol and $\clubsuit$ is the 2^{nd} symbol.

In the simplified situation of prime fields, the trace function is equivalent to the identity function. Thus without loss of generality equation (3.76) may also be simplified to

$$[f_{ab}(x) - f_{0c}(x)] - [f_{ab}(k) - f_{0c}(k)] \neq 0 \quad \forall k \neq x, a \neq 0. \tag{3.77}$$

In equation (3.77), $[f_{ab}(x) - f_{0c}(x)]$ is the function of the inner product vector $IPV[\vec{v}_{ab}, \vec{v}_{0c}]$. $[f_{ab}(k) - f_{0c}(k)]$ represents the k^{th} position of the inner product vector. It is the functions of the inner products that create the MOLS, not the functions of the vectors themselves.

Theorem 3.36. *Let $\vec{v}_{ab}$ be as in equation (2.79)(WF MUBs) or (2.81)(Alltop MUBs) with $a, b \in \mathbb{F}_p$, p a prime. Let f_{ab} be defined as*

$$\vec{v}_{ab} = \frac{1}{\sqrt{p}}\omega_p^{f_{ab}}. \tag{3.78}$$

Let

$$\mathcal{L}_k := \{(a, \sigma(b), c) : \textit{equation (3.77) is satisfied}\}, \tag{3.79}$$

then there is a permutation σ such that $\{\mathcal{L}_k : k \in \mathbb{F}_p^*\}$ is a complete set of MOLS.

Proof. Let $f_{ab} = ax^2 + bx$ be the function for WF MUBs, as in equation (2.79). Let $g_{ab} = (x + a)^3 + b(x + a)$ be the function for Alltop MUBs, as in equation (2.81) then

$$\begin{aligned} [f_{ab}(x) - f_{0c}(x)] - [f_{ab}(k) - f_{0c}(k)] &= a(x^2 - k^2) + (b - c)(x - k) && (3.80)\\ &= (x - k)[a(x + k) + b - c], && (3.81) \end{aligned}$$

and

$$\begin{aligned} [g_{ab}(x) - g_{0c}(x)] - [g_{ab}(k) - g_{ab}(k)] &= 3a(x^2 - k^2) + (3a^2 + b - c)(x - k) && (3.82)\\ &= (x - k)[3a(x + k) + 3a^2 + b - c]. && (3.83) \end{aligned}$$

For the WF MUBs, the identity permutation is used: $\sigma(b) = b$. For the Alltop MUBs $\sigma(b) = b + 3a^2$.

The proof is in three parts.

1. For each $(\sigma(b), k)$ there are exactly p valid pairs (a, c) that satisfy inequality (3.77). No two of the valid (a, c) contain the same a or the same c. This ensures that each column of each square contains every symbol exactly once.

2. For each (a, k) there are exactly p valid pairs $(\sigma(b), c)$ that satisfy inequation (3.77). No two of the valid pairs $(\sigma(b), c)$ contain the same $\sigma(b)$ nor the same c. This ensures that each row of each square contains every symbol exactly once.

3. For each $(a, \sigma(b))$, $a \neq 0$ there are exactly p valid pairs (c, k) that satisfy inequation (3.77). No two of the valid pairs (c, k) contain the same c, nor the same k. Moreover for any c, c',k and k' with $c \neq c'$ and $k \neq k'$, there is exactly one pair $(a, \sigma(b))$ for which (c, k) and (c', k') are both valid pairs. This ensures that all of the squares are mutually orthogonal.

Properties 1, 2 and 3 combine to show that each $\mathcal{L}_k$ is a Latin square, and for $k \neq k'$, $\mathcal{L}_k$ is orthogonal to $\mathcal{L}_{k'}$. With $d-1$ possible values for k a complete set of MOLS is constructed.

Proof of 1. For the WF MUBs the identity permutation $\sigma(b) = b$ is used. For equation (3.81), fix b and k, and set $x = k$, then

$$a(2k) + b - c = 0. \tag{3.84}$$

Inequality (3.77) requires inequality, thus solving the statement for equality shows the values which will not give inequality. For each a there is a unique c that solves this equation and hence there are p pairs (a, c). If $x \neq k$ then none of those pairs (a, c) will be solutions to equation (3.84), and hence satisfy inequality (3.77).

For the Alltop MUBs the permutation $\sigma(b) = b + 3a^2$ is required. For equation (3.83), fix b and k and set $x = k$ then,

$$3a(2k) + 3a^2 + b - c = 3a(2k) + \sigma(b) - c = 0. \tag{3.85}$$

For each a there is a unique c that solves this equation and hence there are p pairs (a, c). If $x \neq k$ then none of these pairs (a, c) will be solutions to equation (3.85), and hence satisfy inequality (3.77).

Note that for inequality (3.77) $a \neq 0$ is required, as this yields the solution $b = c$ giving one of the pairs that solve equations (3.81) and (3.83). This shows that the first row of every

Latin square is in standard form.

Proof of 2. For equations (3.84, 3.85), fix a and k and set $x = k$ then solve. In the WF MUBs $c = 2ak + \sigma(b)$, and in the Alltop MUBs $c = 6ak + \sigma(b)$. Thus for each $\sigma(b)$ there is a unique c. There are p values of $\sigma(b)$ and hence p valid pairs $(\sigma(b), c)$ for each (a, k).

Proof of 3. For the WF MUBs, from equation (3.81) a solution is required for

$$(x - k)[a(x + k) + b - c] = 0. \tag{3.86}$$

Assuming the $x \neq k$ and fix $c \neq b$. Then for each x there is a unique k that solves equation (3.86). There are p combinations of x and k that solve equation (3.86). One of these combinations will be of the form $x = k$. Select this k and set $(a, \sigma(b), c) \in L_k$, then equation (3.77) is satisfied. Allow $c = b$, then either $a = 0$, which represents the symbol in the $\sigma(b)^{th}$ column, 0^{th} row of each square; or $k = 0$, which creates a column $\|$-class. Hence there are p pairs (c, k). From equation (3.86), setting $x \neq k$ and $x \neq k'$:

$$a(x + k) - c = b \tag{3.87}$$

$$a(x + k') - c' = b. \tag{3.88}$$

Hence $a = (c - c')(k - k')^{-1}$. Parts 1 and 2 show that $\mathcal{L}_k$ is a Latin square, thus for fixed a, c and k there is a unique b which satisfies equation (3.77). Thus for each $k \neq k'$, $\mathcal{L}_k$ and $\mathcal{L}_{k'}$ are orthogonal.

For the Alltop MUBs a solution is required for

$$(x - k)[3a(x + k) + \sigma(b) - c] = 0. \tag{3.89}$$

Then follow the argument for the WF MUBs. □

3.4 Constructing MOLS from MUBs in prime-power dimensions

This section has been published as [90].

3.4.1 Setting up the parallel classes

We now generalise the results of the previous section to apply to odd prime powers.

Let $AG(2, q)$ be as in Definition 3.19

Lemma 3.37. *Let $B_a := \{\vec{v}_{ab} : a, b \in \mathbb{F}_q\}$ be an orthonormal basis and $\cup_{a\in\mathbb{F}} B_a$ be a complete set of MUBs. Define a function from the set of bases to the finite field*

$$\begin{aligned} f &: \cup_{a\in\mathbb{F}_q} B_a \to \mathbb{F}_q, \\ f(\vec{v}_{ab}) &= (a+b) \ mod \ h(x) \end{aligned} \tag{3.90}$$

where $h(x)$ is the primitive polynomial defining $\mathbb{F}_q$. Then the set of ordered triples

$$\mathcal{L}_1 = \{(a, b, f(\vec{v}_{ab})) : a, b \in \mathbb{F}_q\} \tag{3.91}$$

forms a Latin square of order q.

Proof. By contradiction. Assume that there exists row a_0 such that the same entry occurs in column b and b', then $f(\vec{v}_{a_0 b}) = f(\vec{v}_{a_0 b'})$, and so $a_0 + b \equiv a_0 + b' \bmod h(x)$ but this implies $b = b'$.

Alternatively, assume that there exists b_0 such that $f(\vec{v}_{ab_0}) = f(\vec{v}_{a'b_0})$, then $a + b_0 \equiv a' + b_0 \bmod h(x)$ but this implies $a = a'$. □

Note that defining the function f in this manner would only give us one Latin square whereas $q-1$ mutually orthogonal Latin squares are needed for a complete set. In what follows we will show that we may assign the vectors of complete sets of MUBs to cells in an array in $q-1$ ways and these $q-1$ arrays will give $q-1$ MOLS. These MOLS will correspond to $q+1$ $\|$-classes and it will be shown that each of these will partition the vectors of $\cup_{a\in\mathbb{F}} B_a$ into q subsets, such that the vectors in each subset can be used to generate a member of the standard basis.

3.4.2 WF type MOLS

Again we detail the construction using the WF MUBs.

Let $\mathrm{w}_{(k,a,b)}$ be as in equation (3.54). Let $\vec{v}_{ab}$ be as in equation (2.79). Let

$$\vec{v}^{\,k}_{ab} := \mathrm{w}_{(k,a,b)}\vec{v}_{ab} = \frac{1}{\sqrt{q}}\omega_p^{\mathrm{tr}(-ax_k^2 - bx_k)}\vec{v}_{ab} \quad 0 \le k \le q-1 \tag{3.92}$$

be the weighted vector for $\vec{v}_{ab}$. Let

$$B_a^k := \{\vec{v}^{\,k}_{ab} : b \in \mathbb{F}_q\} \quad 0 \le k \le q-1 \tag{3.93}$$

denote the weighted bases where $B_a^0 = B_a$, and $\vec{v}^{\,0}_{ab} = \vec{v}_{ab}$.

For each k, $0 \leq k \leq q-1$, equation (3.56) can be used to partition the set of vectors across a collection of ordered triples (called lines) for each $a \in \mathbb{F}_q$:

$$Q^r_{a,k} := \{(a, b, \vec{v}^k_{ab}) \mid b \in \mathbb{F}_q\} \tag{3.94}$$

with the property that the sum of the vectors in each partition gives $\vec{e}_k$. This partitioning can also be used to identify a row $\|$-class given by the q lines

$$L^r_{1a} := \{(a, b, f(\vec{v}^k_{ab})) \mid b \in \mathbb{F}_q\} \tag{3.95}$$

where $0 \leq a \leq q-1$. Here the function f is the same as that defined in equation (3.90), and equation (3.95) describes the rows of the Latin square $\mathcal{L}_1$ (equation (3.91)). Note that the same row $\|$-class is obtained for every k, $0 \leq k \leq q-1$.

Similarly, for fixed $b \in \mathbb{F}_q$, for each k, the vector $\vec{e}_k$ is the weighted sum of the b^{th} vectors of every basis (fixing b and taking the sum over a of $\vec{v}_{ab}$), since the i^{th} component of $\sum_{a\in\mathbb{F}_q} \vec{v}^k_{ab}$ for $\vec{v}_{ab} \in B_a$, is given by

$$\begin{aligned} \sum_{a\in\mathbb{F}_q} (\vec{v}^k_{ab})_i &= \frac{1}{\sqrt{q}} \sum_{a\in\mathbb{F}_q} \frac{1}{\sqrt{q}}\ \omega_p^{\text{tr}(ax_i^2+bx_i)} \omega_p^{\text{tr}(-ax_k^2-bx_k)} \\ &= \frac{1}{q}\ \omega_p^{tr[b(x_i-x_k)]} \sum_{a\in\mathbb{F}_q} \omega_p^{tr[a(x_i^2-x_k^2)]} \\ &= \begin{cases} 1 & \text{if } i = k \\ 0 & \text{if } i \neq k. \end{cases} \end{aligned} \tag{3.96}$$

Note that the weights in this case are the same as the ones in equation (3.55). Summarising, for all $b \in \mathbb{F}_q$

$$\vec{e}_k = \vec{v}^k_{a_0 b} + \vec{v}^k_{a_1 b} + \cdots + \vec{v}^k_{a_{(q-1)} b}. \tag{3.97}$$

As with equation (3.95), this equation can be used to partition the set of vectors into a collection of ordered triples, for each $b \in \mathbb{F}_q$:

$$Q^c_{b,k} := \{(a, b, \vec{v}^k_{ab}) \mid a \in \mathbb{F}_q\} \tag{3.98}$$

with the property that the sum of the vectors in each partition gives $\vec{e}_k$. This partitioning can also be used to identify a column $\|$-class given by the q lines

$$L^c_{1b} := \{(a, b, f(\vec{v}^k_{ab})) \mid a \in \mathbb{F}_q\} \tag{3.99}$$

where $0 \leq b \leq q-1$.

Equation (3.99) describes the columns of the Latin square $\mathcal{L}_1$ (equation (3.91)). The row $\|$-class (equation (3.95)) and column $\|$-class (equation (3.99)) are unbiased since a line in a row $\|$-class $L^r_{1a_0} = \{(a_0, b, f(\vec{v}^k_{ab_0})) \mid b \in \mathbb{F}_q\}$ has only one point in common with a line in the column $\|$-class $L^c_{1b_0} = \{(a, b_0, f(\vec{v}^k_{ab_0})) \mid a \in \mathbb{F}_q\}$ which is $(a_0, b_0, f(\vec{v}^k_{a_0b_0}))$. It may seem at this point that it would be enough to express $\vec{e}_0$ as the sum of the vectors $\vec{v}_{ab}$ and the weighting of the $\vec{v}_{ab}$ to get the remaining $\vec{e}_k$ are unnecessary. But this is untrue since $q-1$ mutually unbiased Latin $\|$-classes (and consequently the $q-1$ MOLS) are required. These $q-1$ Latin $\|$-classes are obtained by combining the weighted vectors $\vec{v}^k_{ab}$ of the q MUBs in $q-1$ uniquely different ways.

In section 3.3.3, the $\vec{e}_k, 1 \leq k \leq q-1$ are expressed as other combinations of the $\vec{v}_{ab}$ resulting in the Latin $\|$-classes. The construction follows on similar lines here.

The row and column $\|$-classes are obtained from the first two classes of parallel lines in the affine plane $AG(2,q)$ (Definition 3.19), given by $\alpha = 1$ and $\beta = 0$ (the row $\|$-class) and $\alpha = 0$ and $\beta = 1$ (the column $\|$-class). Since we need to choose vectors $\vec{v}^k_{ab}$, one from each B^k_a with fixed k, such that the sum of the vectors gives $\vec{e}_k$, and since MOLS are equivalent to affine planes, the obvious place to look for possible combinations is from the classes of parallel lines in an affine plane. Other than the first two classes of parallel lines, the rest of the classes are defined by $\alpha a + b = \gamma$, $(\beta = 1)$ with $\alpha \neq 0$ constant for each class of parallel lines, and γ constant for each line in a class. Thus within each class, if (a, b) and (c, d) are two points on a line, then $a \neq c$ and $b \neq d$.

Taking any q vectors, one from each B^k_a for fixed k, and summing them will give 1 in the k^{th} component of the sum of these vectors. We need to choose vectors such that we get zero in the remaining components.

Choosing the set of $(a, b) \in \mathbb{F}_q \times \mathbb{F}_q$: Let

$$S^\gamma_\alpha = \{(a, b) \in \mathbb{F}_q \times \mathbb{F}_q : \alpha a + b = \gamma\} \text{ for fixed } (\alpha, \gamma) \in \mathbb{F}^*_q \times \mathbb{F}_q, \tag{3.100}$$

and let

$$S_\alpha = \{(a, b) \in \mathbb{F}_q \times \mathbb{F}_q : \alpha a + b = \gamma, \gamma \in \mathbb{F}_q\} \text{ for } \alpha \in \mathbb{F}^*_q. \tag{3.101}$$

Then S^γ_α is a line in S_α, and S_α is the α class of parallel lines in $AG(2,q)$. Let $x_k = 2^{-1}\alpha$; this is always possible since q is odd. This implies that $k \neq 0$, hence giving a different partition for each $k, 1 \leq k \leq q-1$.

Lemma 3.38. *Let $\vec{v}_{ab}$ be a vector in a set of WF MUBs as in equation (2.79). The vector $\vec{e}_k$ is the sum of the vectors $\vec{v}^k_{ab}$ for $\alpha = 2x_k, (a,b) \in S^\gamma_\alpha$ and $1 \leq k \leq q-1$.*

Proof. The i^{th} component of $\sum_{(a,b)\in S^\gamma_\alpha, \alpha=2k} \vec{v}^k_{ab}$ is given by

$$\begin{aligned}
\sum_{(a,b)\in S^\gamma_\alpha,\alpha=2k} (\vec{v}^k_{ab})_i &= \frac{1}{\sqrt{q}} \sum_{(a,b)\in S^\gamma_\alpha} \frac{1}{\sqrt{q}}\ \omega_p^{\mathrm{tr}(ax_i^2+bx_i)} \omega_p^{\mathrm{tr}(-ax_k^2-bx_k)} \\
&= \frac{1}{q} \sum_{(a,b)\in S^\gamma_\alpha} \omega_p^{\mathrm{tr}\{(x_i-x_k)[a(x_i+x_k)+b]\}} \\
&= \frac{1}{q} \sum_{(a,b)\in S^\gamma_\alpha} \omega_p^{\mathrm{tr}\{(x_i-x_k)[(2x_ka+b)+a(x_i-x_k)]\}} \\
&= \frac{1}{q} \sum_{(a,b)\in S^\gamma_\alpha} \omega_p^{\mathrm{tr}\{(x_i-x_k)[\gamma+a(x_i-x_k)]\}} \\
&= \begin{cases} 1 & \text{if } i = k \\ 0 & \text{if } i \neq k \end{cases},
\end{aligned} \tag{3.102}$$

since γ is a constant for $(a,b) \in S^\gamma_\alpha$, $(x_i - x_k)[\gamma + a(x_i - x_k)]$ is a permutation polynomial in a, and the trace map is equiv-distributed. □

Summarising,

$$\vec{e}_k = \sum_{(a,b)\in S^\gamma_\alpha,\alpha=2k} \vec{v}^k_{ab} \text{ for } 1 \leq k \leq q-1. \tag{3.103}$$

This equation can be used to partition the set of vectors into a collection of ordered triples for each $\gamma \in \mathbb{F}_q$,

$$Q^l_{\gamma,\alpha} := \{(a,b,\vec{v}^k_{ab}) \mid (a,b) \in S^\gamma_\alpha\} \tag{3.104}$$

with the property that the sum of the vectors in each partition gives s_k for $1 \leq k \leq q-1$. This partition can be used to identify a Latin $\|$-class given by the q lines

$$L^l_{1,\gamma,\alpha} := \{(a,b,\gamma) \mid (a,b) \in S^\gamma_\alpha\} \tag{3.105}$$

where $0 \leq \gamma \leq q-1$.

Note that for each $\alpha \in \mathbb{F}^*_q$, a different Latin $\|$-class is obtained.

Theorem 3.39. *The Latin $\|$-classes $\cup_{\gamma\in\mathbb{F}_q} L^l_{1,\gamma,\alpha}$ where $\alpha \in \mathbb{F}^*_q$ together with a column $\|$-class $\cup_{b\in\mathbb{F}_q} L^c_{1b}$, and a row $\|$-class $\cup_{a\in\mathbb{F}_q} L^r_{1a}$ form a complete set of mutually orthogonal Latin squares.*

Proof. To obtain the corresponding Latin squares, for each $\alpha \in \mathbb{F}_q^*$, define an array L_α. Thus fix $\alpha \in \mathbb{F}_q^*$ and for each $\gamma \in \mathbb{F}_q$ place symbol γ in cell (a, b) of L_α if $(a, b) \in S_\alpha^\gamma$. Repeating this for each α, $q-1$ arrays are constructed.

To prove each of these arrays is a Latin square, we argue by contradiction. Assume that there exists $(a, b), (a, b') \in S_\alpha^\gamma$. That is, symbol γ will occur twice in row a of array L_α. Then $a\alpha + b = \gamma = a\alpha + b'$, but this implies $b = b'$. Alternatively assume $(a, b), (a', b) \in S_\alpha^\gamma$, and γ occurs twice in column b of array L_α. Implying $a\alpha + b = \gamma = a'\alpha + b$. But since $\alpha \neq 0$, this implies $a = a'$. So for each α a Latin square L_α is constructed.

Next to prove that these Latin squares are mutually orthogonal: assume this is not the case. Consequently there exists distinct α, α' and γ, γ' such that for some (a, b) and (c, d), $(a, b, \gamma), (c, d, \gamma) \in L_\alpha$ and $(a, b, \gamma'), (c, d, \gamma') \in L_{\alpha'}$. Thus $(a, b), (c, d) \in S_\alpha^\gamma$ and $(a, b), (c, d) \in S_{\alpha'}^{\gamma'}$, or equivalently

$$\begin{aligned} a\alpha + b = &\quad \gamma \quad &= c\alpha + d \\ a\alpha' + b = &\quad \gamma' \quad &= c\alpha' + d. \end{aligned}$$

Subtracting these equations gives

$$\begin{aligned} a(\alpha - \alpha') &= \gamma - \gamma' \\ c(\alpha - \alpha') &= \gamma - \gamma'. \end{aligned}$$

Hence $a = c$ and it follows that $b = d$.

The above calculations show that the $q+1$ $\|$-classes obtained from equations (3.95), (3.99) and (3.105) are mutually unbiased. Hence the Latin squares form a set of $q-1$ MOLS. □

3.4.3 Alltop type MUBs

Using the same method, complete sets of MOLS can be obtained from the Alltop MUBs. Let u_{ab} be as in equation (2.81). Let $C_a := \{u_{ab} : b \in \mathbb{F}_q\}$ and

$$\mathrm{w}'_{(k,a,b)} = \frac{1}{\sqrt{q}}\, \omega_p^{tr[-(a+x_k)^3 - b(a+x_k)]} \tag{3.106}$$

then the i^{th} component of $\sum_{b\in\mathbb{F}_q} \mathrm{w}'_{(k,a,b)}u_{ab}$ for $u_{ab}\in C_a$, is given by

$$\begin{aligned}\sum_{b\in\mathbb{F}_q}(\mathrm{w}'_{(k,a,b)}u_{ab})_i &= \frac{1}{q}\sum_{b\in\mathbb{F}_q}\omega_p^{\mathrm{tr}[(a+x_i)^3+b(a+x_i)]}\omega_p^{\mathrm{tr}[-(a+x_k)^3-b(a+x_k)]}\\ &= \frac{1}{q}\sum_{b\in\mathbb{F}_q}\omega_p^{\mathrm{tr}[x_i^3-x_k^3+3a(x_i^2-x_k^2)+(3a^2+b)(x_i-x_k)]}\\ &= \frac{1}{q}\,\omega_p^{\mathrm{tr}[x_i^3-x_k^3+3a(x_i^2-x_k^2)+3a^2(x_i-x_k)]}\sum_{b\in\mathbb{F}_q}\omega_p^{\mathrm{tr}[b(x_i-x_k)]}\\ &= \begin{cases}1 & \text{if } i=k\\ 0 & \text{if } i\neq k.\end{cases}\end{aligned} \tag{3.107}$$

Thus each vector of the standard basis is a linear combination of the vectors of each basis, giving the same row ‖-class as in equation (3.95).

Next, use a permutation $\sigma(b)=b-3a^2$ and let $u^k_{a\sigma(b)}=\mathrm{w}'_{(k,a,\sigma(b))}u_{a\sigma(b)}$. Keeping $\sigma(b)$ (and hence b) fixed and summing over a, the i^{th} component of $\sum_{a\in\mathbb{F}_q}u^k_{a\sigma(b)}$ for $u_{a\sigma(b)}\in C_a$, is given by

$$\begin{aligned}\sum_{a\in\mathbb{F}_q}(u^k_{a\sigma(b)})_i &= \frac{1}{q}\sum_{a\in\mathbb{F}_q}\omega_p^{\mathrm{tr}\{[(a+x_i)^3+(b-3a^2)(a+x_i)]-[(a+x_k)^3+(b-3a^2)(a+x_k)]\}}\\ &= \frac{1}{q}\,\omega_p^{\mathrm{tr}[x_i^3-x_k^3+b(x_i-x_k)]}\sum_{a\in\mathbb{F}_q}\omega_p^{\mathrm{tr}[3a(x_i^2-x_k^2)]}\\ &= \begin{cases}1 & \text{if } i=k\\ 0 & \text{if } i\neq k\end{cases}\end{aligned} \tag{3.108}$$

and the column ‖-classes are obtained the same way as in equation (3.99). Now for the Latin ‖-classes. Since replacing b by $\sigma(b)$ amounts to a permutation of the vectors in C_a for each $a\in\mathbb{F}_q$, the set $(a,b)\in\mathbb{F}_q\times\mathbb{F}_q$ is chosen. Let $S^\gamma_\alpha=\{(a,b)\in\mathbb{F}_q\times\mathbb{F}_q : \alpha a+b=\gamma\}$ for fixed $(\alpha,\gamma)\in\mathbb{F}_q\times\mathbb{F}_q^*$, and let $S_\alpha=\{(a,b)\in\mathbb{F}_q\times\mathbb{F}_q : \alpha a+b=\gamma,\gamma\in\mathbb{F}_q\}$ for $\alpha\in\mathbb{F}_q$. Then S^γ_α is a line in S_α, and S_α is the α class of parallel lines in $AG(2,q)$. Let $x_k=2^{-1}3^{-1}\alpha$; this is always possible since q is odd, and greater than 3.

Lemma 3.40. *The vector $\vec{e}_k$ is the sum of the vectors $u^k_{a\sigma(b)}$ for $\alpha=6x_k$, $(a,b)\in S^\gamma_\alpha$ and $1\leq k\leq q-1$.*

Proof. The i^{th} component of $\sum_{(a,b)\in S_\alpha^\gamma} u^k_{a\sigma(b)}$ is given by

$$\begin{aligned}\sum_{(a,b)\in S_\alpha^\gamma,\alpha=6x_k}(u^k_{a\sigma(b)})_i &= \frac{1}{q}\sum_{(a,b)\in S_\alpha^\gamma}\omega_p^{\text{tr}\{x_i^3-x_k^3+3a(x_i^2-x_k^2)+b(x_i-x_k)\}} \\ &= \frac{1}{q}\sum_{(a,b)\in S_\alpha^\gamma}\omega_p^{\text{tr}\{(x_i-x_k)[x_i^2+x_ix_k+x_k^2+(6x_ka+b)+3a(x_i-x_k)]\}} \\ &= \frac{1}{q}\sum_{(a,b)\in S_\alpha^\gamma}\omega_p^{\text{tr}\{(x_i-x_k)[x_i^2+x_ix_k+x_k^2+\gamma+3a(x_i-x_k)]\}} \\ &= \begin{cases}1 & \text{if } i=k\\ 0 & \text{if } i\neq k\end{cases}.\end{aligned} \tag{3.109}$$

Since γ is a constant for $(a,b)\in S_\alpha^\gamma$, the function $(x_i-x_k)[x_i^2+x_ix_k+x_k^2+\gamma+3a(x_i-x_k)]$ is a permutation polynomial in a and the trace map is equiv-distributed, the result follows from Lemma 2.24. □

The same arguments as section 3.4.2 are used to show that the Latin squares are mutually orthogonal.

3.5 Conclusion

3.5.1 Findings

The correlation between WF MUBs and MOLS has been noted in [85]. However the method presented also yields MOLS from the Alltop type construction, which is not covered by previously published results. The fact the inner product vectors of the Alltop construction are planar has been noted in [64].

A planar function is not necessary in constructing the vectors, as in the WF construction, but is sufficient in the angles between the vectors, as in both the Alltop and WF constructions.

The MUBs tested here are generated by a Galois field. The MOLS are also generated using a Galois field. This may have nothing to do with the MUBs structure, but from the common properties of Galois fields as in section 3.2.6.

3.5.2 Further directions

Question 3.41. *Are there sets of vectors which cannot be described by planar functions, but the angles between the vectors are described by planar functions?*

The Alltop construction may be unique in this respect. The different properties of the function which generates the vectors, and the function which describes the inner product vectors, points to the possibility of other functions which construct the inner product vectors, but not the vectors of sets of MUBs.

Chapter 4

MUBs and Hjelmslev planes

4.1 Introduction

4.1.1 Motivation

Connections between MUBs and finite projective planes have been noted in the SPR conjecture [96]. A similar idea is that MUBs may be related to projective Hjelmslev planes, which are a generalisation of projective planes. The structure of Hjelmslev planes has some analogous properties with the structure of a complete set of MUBs [95]. A non-degenerate conic of the Hjelmslev plane $PH(2, q)$, with q odd, has $q(q+1)$ points, of which q points are in each of $q+1$ neighbourhoods. This is analogous to the $q(q+1)$ vectors of a complete set of MUBs, of which q vectors are in each of $q+1$ bases.

This structural analogy is at the level of cardinalities only. This is not a strong enough link to be called a conjecture.

Analogy 4.1 (SP Analogy)**.** *[95] A conic in a projective Hjelmslev plane over a Galois ring $GR(p^2, r)$ has analogous structure to a complete set of MUBs in $\mathbb{C}^{p^r}$.*

This analogy will be detailed in section 4.2.4, after definitions and notation have been expounded.

4.1.2 Historical note on Hjelmslev planes

In 1916 Johanes Hjelmslev, a Danish geometer proposed a 'Geometry of reality' [53]. The crux of the idea was that discrete geometries do not capture some of the intuitive notions of

real geometry. In ordinary discrete geometry there is no notion of distance between points or angles between lines. Points may be classified as identical or non-identical; lines may be classified as identical, intersecting or parallel.

Hjelmslev realised that a great deal of geometry could be done without the axiom that any two points are on a unique line [13]. In 1954 (4 years after the death of Hjelmslev) Wilhelm Klingenberg defined an incidence geometry inspired by the ideas of Hjelmslev [68]. Klingenberg showed that the incidence geometry could be constructed from a specific type of ring [68, 69]. In 1959 Erwin Kleinfeld first used the name 'Hjelmslev plane' [66] for the geometry as defined by Klingenberg.

In a Hjelmslev geometry points (or lines) may be identical, neighbour, or non-neighbour. This is a discrete notion that captures some of the properties of points and lines being either close or remote in a real geometry.

Substantial investigations of Hjelmslev planes were carried out by Drake in the 1970s [33, 36, 34, 37]. These investigations seem to have been motivated by personal interest, rather than applications. Thus, there are many aspects of Hjelmslev geometries that are entirely untouched.

4.1.3 Applications of Hjelmslev planes

Linear codes are easily encoded and decoded using a Galois field. For more background on coding theory see for example [81]. There exists families of codes which have useful properties, better than any known linear code, but that are not linear over a Galois field. It has been shown that the Kerdock and Preparata codes while non-linear over a Galois field, are linear over a Galois ring [50]. Since this discovery linear codes over rings have received a great deal of attention. For a background on codes over rings see [56].

A code that is linear over $\mathbb{F}_q$ corresponds to a multiset in $PG(k-1,q)$. Analogously, a code that is linear over $GR(p^2,2)$ corresponds to a multiset in $PH(2,p^2)$ [56]. Research into the structure of Hjelmslev planes generated by rings is of importance in this emerging area of coding theory.

4.1.4 Aim

The aim of this research is to establish a concrete connection between MUBs and Hjelmslev planes. The best possible result would be a construction of MUBs that uses only the combinatorial and geometric properties of Hjelmslev planes i.e. non algebraic properties. Section 4.5 gives some preliminary results in this direction.

Hjelmslev geometries are not well studied, and thus there is not the wealth of knowledge on which to build connections with MUBs. As in all research we are 'standing on the shoulders of giants'. However with Hjelmslev geometry, there are not so many 'giants' to stand on. Hjelmslev planes are mentioned in some books on finite geometry [30, §7.2][106], but not in the more standard works on design theory e.g. [11, 23].

Given the obscurity, there is much unknown about Hjelmslev planes[1]. It is with some serendipity that the results of section 4.4 were developed. Examples of Hjelmslev planes are required to test hypotheses, thus a method for generating Hjelmslev planes was developed. Some intuition as to the properties of certain Hjelmslev planes lead to the results of section 4.3. The main results of this chapter may appear to have little to do with the aim of the overall investigation, but future work may prove otherwise.

4.2 Definitions and preliminary results

4.2.1 Hjelmslev planes

Hjelmslev planes are generalisations of affine planes (Defi 3.13) and projective planes.

Definition 4.2. [11, I Defi 2.1] A *projective plane* is an incidence structure such that

1. any two distinct points are incident with exactly one line.
2. any two distinct lines are incident with exactly one point.
3. there exist four points, no three of which are on a common line.

[1]Much of the early work on Hjelmslev planes is published in German. I have endeavoured to understand the original German language publications, and have also cited an English language version that I have fully understood.

A projective plane of order m has $m+1$ points on each line, $m+1$ lines through each point, m^2+m+1 points and m^2+m+1 lines. The dual incidence structure (swapping points for lines) of a projective plane is also a projective plane.

Affine and projective planes are trivial examples of Hjelmslev planes. We use the geometric notation: $P \in h$, to show that the point P is incident with line h; PR is a line incident with points P and R; $f \cap h$ is a point of intersection of lines f and h. For Hjelmslev geometry there is also the property of neighbours which is denoted $\sim$.

Definition 4.3. [36, Defi 1.3] A *projective Hjelmslev plane*, $\mathcal{H}$, is an incidence structure such that:

1. any two points are incident with at least one line.
2. any two lines intersect in at least one point.
3. any two points P and Q that are incident with more than one line are neighbours.
4. any two lines g, h that intersect at more than one point are neighbours.
5. there exists an epimorphism ϕ from $\mathcal{H}$ to an ordinary projective plane $\mathcal{P}$ such that:
   (a) $\phi(P) = \phi(Q) \iff P \sim Q$.
   (b) $\phi(g) = \phi(h) \iff g \sim h$.

Axioms 1 and 2 are dual, axioms 3 and 4 are dual, and axioms 5a and 5b are dual. Thus just as in projective planes, points and lines are dual in a projective Hjelmslev plane.

Lemma 4.4. *[30, Thm 7.2.1] The neighbour property of projective Hjelmslev planes is an equivalence relation.*

Proof. $\sim$ is obviously symmetric and reflexive. Let $P \sim Q$ and $Q \sim R$. From Definition 4.3,5a we get that $\phi(P) = \phi(Q)$ and $\phi(Q) = \phi(R)$. Thus $\phi(P) = \phi(R)$ and we get $P \sim R$. A similar argument applies to lines. □

The set of points and the set of lines of a Hjelmslev plane may be partitioned into *line-neighbourhoods* and *point-neighbourhoods*. Let the point-neighbourhood containing P be denoted $\tilde{P}$, and the line neighbourhood containing l be denoted $\tilde{l}$.

Inspired by Fraleigh, 'Never underestimate a theorem that counts something' [40, p 125], we proceed by counting points, lines and neighbourhoods of projective Hjelmslev planes.

Lemma 4.5. *[66, Thm 1] Let $\mathcal{H}$ be a finite projective Hjelmslev plane. For any line g and point $P \in g$ let s be the number of non-neighbour points of P incident with g and let t be the number of neighbour points of P incident with g.*

1. *s and t are independent of the choice of P and g.*
2. *each line-neighbourhood has t^2 lines and each point-neighbourhood has t^2 points.*
3. *t divides s; Let $r = \frac{s}{t}$.*
4. *r is the order of the projective plane associated with $\mathcal{H}$ by the epimorphism ϕ.*

Proof. 1. From Lemma 4.4, neighbour is an equivalence relation. Hence for $P, Q \in g$ with $P \sim Q$, s and t have the same values for the pair P, g and the pair Q, g. Similarly for g, h incident with P with $g \sim h$, s and t have the same values for the pairs P, g and P, h. We have: For any pair Q, h such that $P \sim Q$ and $g \sim h$, the values s and t are the same as for the pair P, g.

Let j be a line incident with P, but non-neighbour to g. Let t' be the number of points on j neighbour to P. Since $g \not\sim j$, from axioms 2 and 4 of Definition 4.3, j must intersect each line of $\tilde{g}$ in exactly one point. Thus $|\tilde{P}| = tt'$. Let k be a line incident with P, but non-neighbour to g and j. Let $t^\dagger$ be the number of points on k neighbour to P. k must intersect each line of $\tilde{g}$ in exactly one point. Thus $|\tilde{P}| = tt^\dagger$ and $|\tilde{P}| = t't^\dagger$. Hence $t^\dagger = t' = t$ and $|\tilde{P}| = t^2$. Now we have: For any pair Q, h such that $P \sim Q$ and $g \not\sim h$, the value of t is the same as for the pair P, g.

Let T be a point incident with g but non-neighbour to P. From axioms 1 and 3 of Definition 4.3, each member of $\tilde{P}$ is incident with exactly one line which is also incident with T. Thus there are $t^2/t = t$ lines neighbour to g and incident with T. Choose a line l incident with T and non-neighbour to g. Following the same argument as for lines j, k above we find that: for any pair Q, h such that $P \not\sim Q$ and $g \sim h$, the value of t is the same as for the pair P, g; Every point-neighbourhood has t^2 points.

Each neighbourhood of points is collapsed to a single point in a projective plane by the epimorphism ϕ. Thus the number of distinct point neighbourhoods which have points incident

with a line is the same for all lines, and hence all lines contain the same number of points. In conclusion s and t are the same for all lines and all points.

2. The size of a point neighbourhood is shown in part 1.

For $P \not\sim T$ there is a unique line incident with each point of $\tilde{P}$ and each point of $\tilde{T}$. Each line contains t points from $\tilde{T}$ and t points from $\tilde{P}$. Thus there are $(t^2t^2)/(t.t) = t^2$ lines which are neighbour to g. As all point-neighbourhoods contain t^2 points, this result holds for all line-neighbourhoods.

3. A consequence of dividing the $s+t$ points on a line into equivalence classes of neighbour points. Each class has t points, so t divides $s + t$.

4. Each neighbourhood of points is collapsed to a single point in a projective plane by the epimorphism ϕ. Thus there are $(s + t)/t = r + 1$ points on a line of $\phi(\mathcal{H})$. Hence $\phi(\mathcal{H})$ is a projective plane of order $r = (s/t)$. □

Definition 4.6. A $(t, r)PH$-plane is a projective Hjelmslev plane, with t and r as in Lemma 4.5.

A $(1, r)PH$-plane is a projective plane of order r, and may be called a *trivial* projective Hjelmslev plane. This notation should not be confused with $PH(R)$, the projective Hjelmslev plane over the ring R, or $PH(n, p^r)$ the projective Hjelmslev plane over the ring $GR(p^n, r)$ [95, 55] (defined in section 4.2.3).

We now define an affine Hjelmslev plane, for which we need the concept of parallelism.

Definition 4.7. [11, Defi 5.4] A *parallelism*, denoted $\|$, is a partition of the lines of an incidence structure into $\|$-classes.

Definition 4.8. [36, Defi 1.1] An *affine Hjelmslev plane* $\mathcal{H}$ is an incidence structure such that

1. any two points are incident with at least one line.
2. any two points P, Q, that are incident with more than one line are neighbours.
3. any two lines g, h, that meet at more than one point are neighbours.
4. There exists an epimorphism, ϕ, from $\mathcal{H}$ to an ordinary affine plane, $\mathcal{A}$, such that
   (a) $\phi(P) = \phi(Q) \iff P \sim Q$.

(b) $\phi(g) = \phi(h) \iff g \sim h$.

(c) $|g \cap h| = 0 \Rightarrow \phi(g) \parallel \phi(h)$.

As with affine planes, points and lines are not dual in an affine Hjelmslev plane. An affine Hjelmslev plane may have parallel lines which are neighbours as axiom 4*c* of Definition 4.8 is a one way implication. The following is analogous to Lemmas 4.4 and 4.5.

Lemma 4.9. *[33][77, Satz 2.11] Let $\mathcal{H}$ be a finite affine Hjelmslev plane. Neighbour is an equivalence relation. For any line g and point $P \in g$ let s be the number of non-neighbour points of P incident with g and let t be the number of neighbour points of P incident with g.*

1. *s and t are independent of the choice of P and g.*
2. *each line-neighbourhood has t^2 lines and each point-neighbourhood has t^2 points.*
3. *t divides s; $r = \frac{s}{t}$.*
4. *r is the order of the affine plane associated with $\mathcal{H}$ by the epimorphism ϕ.*

Proof. Similar arguments to the proof of Lemmas 4.4 and 4.5. □

An affine Hjelmslev plane may be denoted $(t, r)AH$-plane, with t, r as in Lemma 4.9. A $(1, r)AH$-plane is an ordinary affine plane and may be called a *trivial* affine Hjelmslev plane.

There are also definitions of *near affine* Hjelmslev planes and *fairly near affine* Hjelmslev planes [34], as well as higher dimensional Hjelmslev geometries [71] but they have no bearing on this study so are omitted.

4.2.2 Uniform Hjelmslev planes

The Hjelmslev planes in the SP analogy are uniform (Analogy 4.1, 4.39). In order to define uniform we need a function which describes the structure of neighbourhoods.

Definition 4.10. [33, Defi 2.3] Let P be a point of a Hjelmslev plane $\mathcal{H}$. The *point-neighbourhood restriction*, $\tilde{P}$, is defined as follows:

1. the points of $\tilde{P}$ are the points that are neighbour to P.

2. the lines of $\tilde{P}$ are the restrictions of lines g of $\mathcal{H}$ to the points $\tilde{P}$: $g_P = g \cap \tilde{P}$.

Strictly speaking $\tilde{P}$ is an incidence structure. Where context is clear $\tilde{P}$ refers to the set of points.

Definition 4.11. [33, Defi 2.4] A 1-uniform projective (affine) Hjelmslev plane $\mathcal{H}$ is an ordinary projective (affine) plane. A projective (affine) Hjelmslev plane is n-uniform if

1. for every point $P \in \mathcal{H}$, $\tilde{P}$ is an $(n-1)$ uniform affine Hjelmslev plane.
2. for each point P of $\mathcal{H}$, every line of $\tilde{P}$ is the restriction of the same number of lines of $\mathcal{H}$.

In a 2-uniform projective Hjelmslev plane every point-neighbourhood restriction is an ordinary affine plane. Note than a point-neighbourhood restriction never resembles a projective plane as it has exactly t^2 points, whereas a projective plane has (t^2+t+1) points. Earlier definitions of uniform Hjelmslev planes [66, 30] are equivalent to 2-uniform Hjelmslev planes in Definition 4.11.

Theorem 4.12. *[33, Prop 2.2] Let $\mathcal{H}$ be an n-uniform $(t,r)PH$-plane or $(t,r)AH$-plane. Then for invariants t, r, s as given in Lemmas 4.5 and 4.9,*

$$s = r^n, \qquad t = r^{n-1}. \tag{4.1}$$

Proof. We use induction. Clearly the statement is true if $\mathcal{H}$ is 1-uniform. Let $n \geq 2$. Let P be a point of $\mathcal{H}$ and let s', t' be the invariants for $\tilde{P}$, which is an $(n-1)$-uniform AH-plane. The inductive assumption implies that there exists r' such that

$$s' = (r')^{n-1}, \qquad t' = (r')^{n-2}. \tag{4.2}$$

From Lemmas 4.5 and 4.9 we know that $s/t = r$, thus we need only prove the value of t. The number of points on each line of $\tilde{P}$ is $t = r't'$, therefore

$$t = r't' = \frac{s'}{t'}t' = s' = (r')^{n-1}. \tag{4.3}$$

Hence $r = r'$ and $t = r^{n-1}$. □

Lemma 4.13. *[66, Thm 2] A projective Hjelmslev plane, $\mathcal{H}$, is 2-uniform if and only if it is a (t,t)-PH plane.*

Proof. From Theorem 4.12 it is clear that a 2-uniform PH-plane must have invariants (t,t). We need to show that a $(t,t)PH$-plane is 2-uniform. Since the smallest projective plane has order 2 (the Fano plane), we may assume that $t \geq 2$.

We count the number of intersections between a particular line, h, and all lines of $\mathcal{H}$ in two ways.

There are $s+t$ points on h and each point is incident with $s+t$ distinct lines, hence there are $(s+t)(s+t)$ total intersections.

Let λ_h be the average number of points of intersection between h and lines neighbour to, but distinct from, h. Each point of h is incident with h; each point of h is incident with on average $\lambda_h(t^2-1)$ lines that are neighbour to h; h intersects each non-neighbour line exactly once. We obtain

$$s+t+\lambda_h(t^2-1)+s(s+t)=(s+t)(s+t). \tag{4.4}$$

From Lemma 4.5 part 3 we know that $s=t^2$.

$$\lambda_h=(t^2+t)(t+1)=t. \tag{4.5}$$

From Theorem 4.5 part 1 we know that λ_h is the same for all lines. Since t is the number of neighbouring points on a line, t is the maximum possible value for λ_h; and so every pair of neighbouring lines must meet in exactly t points. As points and lines are dual, every pair of neighbouring points is incident with exactly t lines. This satisfies axiom 2 of Definition 4.11.

Thus $\tilde{P}$ contains t copies of $t+1$ $\|$-classes, each $\|$-class contains t lines, each line incident with t points. Each line from each $\|$-class meets each line from every other $\|$-class in exactly one point. This satisfies axioms 1 and 2 of Definition 3.13. Setting $t>1$ satisfies axiom 3 and we have that $\tilde{P}$ is an affine plane. This shows that $\mathcal{H}$ is uniform. □

Definition 4.14. [30, §1.3] Let $(\mathcal{P},\mathcal{L},I)$ be an incidence structure with $|\mathcal{P}|=m$ points and $|\mathcal{L}|=n$ lines. Let the points and lines be given a fixed order. The *incidence matrix* is an $m\times n$ matrix C such that $(C)_{ij}=1$ if point p_i is incident with line l_j, and $(C_{ij})=0$ if point p_i is not incident with line l_j.

The entries in the incidence matrix can be treated as elements of $\mathbb{C}$, and normal matrix properties apply. Finding properties of the incidence matrix is a standard technique in discrete mathematics.

Theorem 4.15. *[63, Lem 1] Let C be the incidence matrix of a 2-uniform (t,t)-PH plane with $t \neq 1$. Then the points and lines can be ordered such that C^2 has eigenvalues t^2, t^3 and $t^2(t+1)^2$ with algebraic multiplicities $(t^2-1)(t^2+t+1)$, t^2+t and 1.*

Proof. Order the points and lines so that neighbourhoods are together, then the incidence matrix splits into sub matrices

$$C = \begin{bmatrix} C_{00} & \dots & C_{0(n-1)} \\ \vdots & & \vdots \\ C_{(n-1)0} & \dots & C_{(n-1)(n-1)} \end{bmatrix}. \tag{4.6}$$

Consider $CC^T = C^2$, then $(C^2)_{ii}$ is the number of lines incident with the point x_i, and $(C^2)_{ij}$ is the number of lines incident with x_i and x_j. There are $s+t = t^2+t$ lines incident with a point, t lines incident with two neighbouring points and exactly one line incident with two non-neighbouring points. Thus

$$CC^T = C^2 = \begin{bmatrix} N & J & J & \dots & J \\ J & N & J & \dots & J \\ J & J & N & & \\ \vdots & \vdots & & \ddots & J \\ J & J & & J & N \end{bmatrix} \tag{4.7}$$

where J is the matrix with every entry 1, and N is the $t^2 \times t^2$ matrix with every entry on the main diagonal equal to $s+t = t^2+t$ and all other entries equal to t.

Via a tedious calculation we find the characteristic equation.

$$\det\left(C^2 - \lambda I_{(t^4+t^3+t^2)}\right) = (t^2-\lambda)^{(t^2-1)(t^2+t+1)}(t^3-\lambda)^{t^2+t}\left(t^2(t+1)^2-\lambda\right) \tag{4.8}$$

from which the eigenvalues are found. □

This method is readily adapted to find the eigenvalues of incidence matrices of other projective Hjelmslev planes.

Uniform Hjelmslev planes have a rich structure which may be useful in applications where ordinary affine or projective geometry is insufficient.

4.2.3 Constructions of Hjelmslev planes

Applications of Hjelmslev planes require explicit constructions. Affine and projective geometries can be generated using Galois fields. Hjelmslev planes may be generated using Galois rings. We detail a construction of a projective Hjelmslev plane using a Galois ring and give some examples of other rings which also construct Hjelmslev planes. We also show a purely combinatorial construction which uses semi-nets.

Hjelmslev planes constructed from Galois Rings

We first show a construction for an ordinary projective plane using a Galois field.

Definition 4.16. [30, 1.4.2] Let V be a 3 dimensional vector space over a field $\mathbb{F}$. Let the subspaces of dimension 1 be points, and subspaces of dimension 2 be lines. Then the geometry formed is a *Desarguesian* projective plane.

Definition 4.17. Let $PG(2,q)$ denote the projective plane which is constructed from $\mathbb{F}_q$ as in Definition 4.16. $\langle \vec{x} \rangle$ is a point of $PG(2,q)$ and represents all column vectors $\rho\vec{x}$ in $\mathbb{F}_q^3$ such that $\rho \in \mathbb{F}_q^*$ and at least one of the entries in $\vec{x}$ is nonzero.

Definition 4.18. [58, §1] For any subspace W of a vector space V, we define the annihilator $a_V(W)$ to be the set

$$a_V(W) = \{\vec{x}^T : \vec{x}^T\vec{w} = 0, \forall\ \vec{w} \in W\}. \tag{4.9}$$

$a_V(W)$ is a subspace of the dual vector space V^T. When W is a set of column vectors, $a_V(W)$ is a set of row vectors. The annihilator uniquely defines a subspace.

The annihilator of a two dimensional subspace is a one dimensional subspace written as a row vector.

Definition 4.19. [30, §7.2] A two dimensional subspace is called a line denoted $\langle \vec{l}^T \rangle$, which represents all row vectors $\sigma\vec{l}^T$ such that $\sigma \in \mathbb{F}_q^*$, and at least one of the entries in $\vec{l}^T$ is nonzero.

The point $\langle \vec{x} \rangle$ is incident with the line $\langle \vec{l}^T \rangle$ if

$$\vec{l}^T\vec{x} = 0. \tag{4.10}$$

We check that $PG(2,q)$ satisfies the properties of a projective plane as defined in Definition 4.2. Let $\langle\vec{x}\rangle, \langle\vec{y}\rangle$ be two points in $PG(2,q)$. We want to find any lines $\langle\vec{l}^T\rangle$ that are incident with both $\langle\vec{x}\rangle$ and $\langle\vec{y}\rangle$. Find $\langle\vec{l}^T\rangle$ such that

$$\vec{l}^T\vec{x} = 0 \qquad \text{and} \qquad \vec{l}^T\vec{y} = 0. \tag{4.11}$$

Expanded out this becomes

$$x_0l_0 + x_1l_1 + x_2l_2 = 0 \quad \text{and} \quad y_0l_0 + y_1l_1 + y_2l_2 = 0. \tag{4.12}$$

Without loss of generality we choose scalars ρ, ρ' and σ such that $x_0 = y_0 = l_0 = 1$ for the representative vectors $\vec{x}, \vec{y}$ and $\vec{l}^T$.

$$1 + x_1l_1 + x_2l_2 = 0 \quad \text{and} \quad 1 + y_1l_1 + y_2l_2 = 0 \tag{4.13}$$

which has a unique solution. This satisfies axiom 1 of Definition 4.2. The duality of points and lines is evident from equation (4.10), and satisfies axiom 2. The points $\langle(1,0,0)^T\rangle$, $\langle(0,1,0)^T\rangle$, $\langle(0,0,1)^T\rangle$, $\langle(1,1,1)^T\rangle$ form the quadrangle required of axiom 3. We conclude that $PG(2,q)$ is a projective plane.

The construction of Hjelmslev planes using Galois rings is similar to the construction of projective planes using Galois fields [30][69]. We follow the construction of [95].

Definition 4.20. Let $PH(2,q)$, with $q = p^r$, denote the Projective Hjelmslev plane constructed from $GR(p^2,r)$ as follows: $\langle\vec{x}\rangle$ is a point of $PG(2,q)$ and represents all column vectors $\rho\vec{x}$ in $(GR(p^2,r))^3$ such that ρ is a unit of $GR(p^2,r)$ and at least one of the entries of $\vec{x}$ is a unit of $GR(p^2,r)$.

A subspace of dimension two is called a line. As with projective planes we represent a line by its annihilator, denoted $\langle\vec{l}^T\rangle$, which represents all row vectors $\sigma\vec{l}^T$ such that σ is a unit of $GR(p^2,r)$ and at least one of the entries in $\vec{l}^T$ is a unit.

The point $\langle\vec{x}\rangle$ is incident with the line $\langle\vec{l}^T\rangle$ if

$$\vec{l}^T\vec{x} = 0. \tag{4.14}$$

A similar argument as for $PG(2,q)$ will satisfy axioms 1, 2, 3 and 4 of Definition 4.3. The ring homomorphism, $^-$ (Definition 2.42), applied to the entries of the representative vector, induces the the required epimorphism, ϕ, on points and lines as given in axioms 5a and 5b of Definition 4.3. The duality of points and lines is evident from equation (4.14). These properties will be explicitly shown in section 4.3.

Hjelmslev planes constructed from other rings

Hjelmslev planes may be constructed using any ring which may be classified as a Hjelmslev ring (Definition 4.22). A Galois ring is an example of a Hjelmslev ring. For an introduction to geometry over rings see for example [106]. The construction of the Hjelmslev plane is the same as when using a Galois ring (Definition 4.20).

Definition 4.21. [106, Defi 8.3] A ring is called a left (right) *chain ring* if for every pair of left (right) ideals, N_1, N_2, either $N_1 \subseteq N_2$ or $N_1 \supseteq N_2$. This is called the *chain* condition.

Definition 4.22. [106, Defi 9.2] A ring R is a *Hjelmslev ring* if it is a left and right chain ring and every non-unit is 0 or a zero divisor.

Lemma 4.23. *[106, Lem 8.4] Let R be a left (right) chain ring. Then R has a unique maximal ideal and is commutative.*

Definition 4.24. [74, §II.4] A ring is *local* if it has a unique maximal ideal M, and the residue ring R/M is a division ring.

All finite division rings are fields. Thus if R is a finite local ring then R/M is a field. The unique maximal ideal consists of 0 and all the zero divisors of R.

Axioms 1 and 2 of Definition 4.3 correspond to the chain condition. The requirement that every non-unit is 0 or a zero divisor corresponds to axioms 3 and 4 of Definition 4.3. The neighbour property being an equivalence relation corresponds to the local property of a Hjelmslev ring, where finding the residue field, R/M, corresponds to the epimorphism ϕ of axioms 5a and 5b of Definition 4.3.

Lemma 4.25. *[28] Let σ be an automorphism of $\mathbb{F}_q$, then $R_\sigma = \langle \mathbb{F}_q \times \mathbb{F}_q, +, \cdot \rangle$ with $+$ defined component-wise and multiplication defined as*

$$(x_0, x_1)(y_0, y_1) = (x_0 y_0, x_0 y_1 + x_1 \sigma(y_0)) \tag{4.15}$$

is a Hjelmslev ring.

Proof. The zero divisors of R_σ are elements of the form $(0, x_1)$, $x_1 \in \mathbb{F}_q^*$:

$$(0, x_1)(0, y_1) = (0, 0 + 0y_1 + x_1\sigma(0)) = (0, 0). \tag{4.16}$$

For $x_0 \neq 0$, let $y_1 = x_0^{-1}(1 - x_1\sigma(x_0^{-1}))$ then

$$(x_0, x_1)(x_0^{-1}, y_1) = (1, 1 - x_1\sigma(x_0^{-1}) + x_1\sigma(x_0^{-1}) = (1, 1). \tag{4.17}$$

Thus every element is either a unit, 0, or a zero divisor.

There is a unique proper ideal of R_α, being the subring of zero divisors. This fulfils the left and right chain conditions. □

All Hjelmslev rings that generate 2-uniform Hjelmslev planes have been catalogued. If $q = p^r$ then there are exactly $r+1$ isomorphism classes of such rings: the Galois ring $GR(p^2, r)$, and R_σ for each of the r automorphisms, σ, of $\mathbb{F}_q$. For more on this topic see [55, 56].

Hjelmslev planes constructed from a semi net with Zings

A purely combinatorial construction of Hjelmslev planes uses a semi net.

Definition 4.26. [38] A (k, t)-*semi net* with *zings* is an incidence structure with t^2 points and kt^2 lines. The set of lines $\mathcal{L}$ is the disjoint union of *zings*, $\mathcal{L} = \mathcal{L}_1 \cup \cdots \cup \mathcal{L}_k$ such that

1. each zing contains t^2 lines.
2. lines g and h intersect in exactly one point if and only if they belong to distinct zings.
3. if two points are incident with a common line, then they are incident with more than one common line.

A semi net is *full* if every pair of points is joined by at least one line.

If each zing is replaced by a single parallel class, then the resulting structure is equivalent to a net (Definition 3.14). A net is therefore a trivial semi net, and a ∥-class is a trivial zing.

Theorem 4.27. *[38, Prop 2.4] Let P be the incidence matrix of a projective plane of order r. Let $m = r^2 + r + 1$. Let A_{ij} with $1 \leq i, j \leq m$ be a $t^2 \times t^2$ matrix with entries from $\{0, 1\}$. Let M be the $mt^2 \times mt^2$ matrix constructed by replacing the entry in cell i, j of P with the matrix A_{ij}. Then M is the incidence matrix of a $(t, r)PH$-plane if*

1. *For fixed i, the concatenation of the non-zero A_{ix} is an incidence matrix for a full $(r + 1, t)$-semi net. Each nonzero A_{ij} corresponds to a zing.*

2. *For fixed j, the concatenation of the non-zero A_{xj} is an incidence matrix for a dual full $(r+1,t)$-semi net . Each nonzero A_{ij} corresponds to a zing.*

Conversely all $(t,r)PH$-planes can be represented in this way.

Proof. Each zing is the intersection of a line-neighbourhood with a point-neighbourhood restriction. Each semi net is a point-neighbourhood restriction. □

Theorem 4.27 gives an alternate representation of a Hjelmslev plane and may be viewed as an equivalent definition of a Hjelmslev plane. Theorem 4.27 changes the problem of constructing a Hjelmslev plane to that of constructing a semi net with zings.

Equivalent definitions can be useful as shown by the wealth of literature on objects equivalent to MOLS. Given that a net is equivalent to a range of other combinatorial objects (Theorem 3.10), nets are well studied. However there is little known about semi nets.

4.2.4 MUBs and conics of Hjelmslev planes

Conics in projective planes

In 2005 it was noted by Saniga and Planat that $q+1$ is the number of points in a non-degenerate conic of a $PG(2,q)$, which is the same number as the maximum number of MUBs in $\mathbb{C}^q$ [94].

Analogy 4.28. *[94] A conic in a $PG(2,q)$ has the same number of points as the number of bases in a complete set of MUBs in $\mathbb{C}^q$.*

In 2006 this analogy was developed into the SP Analogy concerning conics in projective Hjelmslev planes [95]. We define conics in projective planes before moving on to the richer setting of a projective Hjelmslev plane.

Definition 4.29. [58, §II.7] Let A be a symmetric matrix with at least one entry that is a unit, $A \in \mathbb{M}_3(\mathbb{F}_q)$. A *conic* of $PG(2,q)$ is

$$\mathcal{C} := \{\langle \vec{x} \rangle \in PG(2,q) : \vec{x}^T A \vec{x} = 0\}. \tag{4.18}$$

The matrix A represents a linear transformation which, combined with the transpose, maps a point $\langle \vec{x} \rangle$ to a line $\langle \vec{x}^T A \rangle$ in the dual plane. Let C be the incidence matrix of a

projective plane. Let the rows of C be in a fixed ordering of the points $\langle\vec{x}_0\rangle, \langle\vec{x}_1\rangle, \ldots, \langle\vec{x}_{n^2+n}\rangle$, and the columns of C be given the ordering $\langle\vec{x}_0^T A\rangle, \langle\vec{x}_1^T A\rangle, \ldots, \langle\vec{x}_{n^2+n} A\rangle$. Then $(C)_{ii} = 1$ if and only if $\vec{x}_i^T A\vec{x}_i = 0$, and hence the points in the conic are $\langle\vec{x}_i\rangle$ such that $(C)_{ii} = 1$.

Often the definition of a conic is given in the expanded form [58, Lem 2.30]:

Let $a_{00}, a_{01}, a_{02}, a_{11}, a_{12}, a_{22} \in \mathbb{F}_q$ with at least one a_{ij} nonzero. A conic in $PG(2,q)$ is the set of points of the form $\langle\vec{x}\rangle = \langle(x_0, x_1, x_2)^T\rangle$, with at least one of x_0, x_1, x_2 nonzero that satisfy

$$a_{00}x_0^2 + a_{11}x_1^2 + a_{22}x_2^2 + 2a_{01}x_0x_1 + 2a_{02}x_0x_2 + 2a_{12}x_1x_2 = 0. \tag{4.19}$$

If A is the matrix of the conic, then the coefficients in equation (4.19) are the entries of A.

Lemma 4.30. *[58, Lem 2.35] Let $\mathcal{C}$ be a conic with matrix A. A line $\langle\vec{l}^T\rangle$ meets the conic in exactly one point if and only if*

$$\vec{l}^T A\vec{l} = 0. \tag{4.20}$$

A line that meets a conic in exactly one point is called an *absolute line*.

Corollary 4.31. *[58, Lem 2.35, Cor 2, Lem 2.68, Cor 1] A conic in $PG(2,q)$ is either empty, a single point, or has $q+1$ points.*

A conic that does not contain $q+1$ points is called *degenerate*. If the matrix A from equation (4.18) is singular, then the conic is degenerate.

This corollary is the basis for Analogy 4.28. We give further results on projective planes over a field that are neccesary to understand Hjelmslev planes.

Theorem 4.32. *[58, Thm 2.36] Let $\mathcal{C}$ be a nonempty conic in $PG(2,q)$ with q odd. Then a basis for $\mathbb{F}_q^3$ can be chosen such that the matrix of $\mathcal{C}$ has the form*

$$\begin{pmatrix} 0 & 0 & -1 \\ 0 & 2 & 0 \\ -1 & 0 & 0 \end{pmatrix} \tag{4.21}$$

and the points of $\mathcal{C}$ are points $\langle\vec{y}\rangle$ such that $y_1^2 = y_0y_2$.

Note that this does not hold for a field of characteristic 2 since the matrix of equation (4.21) is singular in this case.

Theorem 4.33. *[58, Thm 2.69] Let $\mathcal{C}$ be a nonempty conic in $PG(2,q)$ with q even, then the points of $\mathcal{C}$ are the points of some line.*

Corollary 4.34. *[58, Cor 2.36] Any two nonempty conics in $PG(2,q)$ are isomorphic.*

The correspondence between MUBs and conics in $PG(2,q)$ noted in Analogy 4.28 is at the level of cardinalities only. Furthermore the points in the conic are analogous to bases; there is no structure which is analogous to a vector. Analogy 4.28 relies on properties of $PG(2,q)$. An arc is a purely geometric structure, which occurs in all projective planes. It can be shown that all arcs with $q+1$ points in projective planes of odd order are conics [76, 9.6.4]. Non-Desarguesian planes (not $PG(2,q)$) occur in prime powers ≥ 9, thus we could expect a correspondence between non-Desarguesian MUBs (e.g. those constructed without using the planar function x^2) and non-Desarguesian projective planes.

The lack of an analogous structure for vectors leads to interest in generalisations of projective planes.

Conics in Hjelmslev planes

The SP analogy (Analogy 4.1) notes some commonalities between the structure of a conic in $PH(2,q)$ and a complete set of MUBs. The neighbourhood relation of a Hjelmslev plane can be considered analogous to base membership of vectors in MUBs. A conic in $PH(2,q)$ is defined analogously to a conic in $PG(2,q)$.

Definition 4.35. [58, §II.7] Let A be a symmetric matrix with at least one entry that is a unit, $A \in \mathbb{M}_3(GR(p^2,r))$. A *conic* of $PH(2,q)$ is

$$\mathcal{C} := \{\langle \vec{x} \rangle \in PH(2,q) : \vec{x}^T A \vec{x} = 0\}. \tag{4.22}$$

The definition of a conic may also be given in expanded form (compare with equation (4.19)). A *conic* in $PH(2,q)$ is a set of points $\langle (x_0, x_1, x_2)^T \rangle$ which obeys

$$c_{00}x_0^2 + c_{11}x_1^2 + c_{22}x_2^2 + c_{01}x_0x_1 + c_{02}x_0x_2 + c_{12}x_1x_2 = 0 \tag{4.23}$$

where $c_{ij} \in GR(p^2,r)$ and at least one of the c_{ij}s is a unit.

Lemma 4.36. *[22, Thm 2.2] Let $\mathcal{C}$ be a nonempty conic of $PH(2,q)$ with q odd. Then $\mathcal{C}$ has $q(q+1)$ points, of which q points are in each of $q+1$ neighbourhoods.*

Proof. First we show that $\mathcal{C}$ has points from $q+1$ distinct point-neighbourhoods.

Let $\langle\vec{x}\rangle = \langle(x_0, x_1, x_2)^T\rangle$. Let the equation of the conic $\mathcal{C}$ be as in equation (4.23). Let $\bar{}$ be the ring homomorphism, and let $\phi(\langle\vec{x}\rangle) = \langle(\bar{x}_0, \bar{x}_1, \bar{x}_2)\rangle$ be the epimorphism $\phi(PH(2,q)) = PG(2,q)$. Then the conic $\phi(\mathcal{C})$ has the equation

$$\bar{c}_{00}\bar{x}_0^2 + \bar{c}_{11}\bar{x}_1^2 + \bar{c}_{22}\bar{x}_2^2 + 2\bar{c}_{01}\bar{x}_0\bar{x}_1 + 2\bar{c}_{02}\bar{x}_0\bar{x}_2 + 2\bar{c}_{12}\bar{x}_1\bar{x}_2 = 0. \tag{4.24}$$

Let A be the matrix of the conic of equation (4.23). Let $B \in \mathbb{M}_3(GR(p^2,r))$ such that $\bar{B} \in \mathbb{M}_3(\mathbb{F}_q)$ is the change of basis transformation required of Theorem 4.32, $\bar{B}\bar{\vec{x}} = \bar{\vec{y}}$ such that:

$$\bar{y_0}^2 - \bar{y}_1\bar{y}_2 = 0. \tag{4.25}$$

We apply the same transformation, $B\vec{x} = \vec{y}$ and $BA = D$ to equation (4.23). D is the matrix of the conic

$$d_{00}y_0^2 + d_{11}y_1^2 + d_{22}y_2^2 + 2d_{01}y_0y_1 + 2d_{02}y_0y_2 + 2d_{12}y_1y_2 = 0. \tag{4.26}$$

Comparing equations (4.25) and (4.26) we see that $\bar{d}_{00} = 1$, $2\bar{d}_{12} = -1$ and $d_{11}, d_{22}, d_{01}, d_{02} \in H$ where H is the group of zero divisors of $GR(p^2,r)$.

The point $\langle(0,1,0)^T\rangle$ is on the conic of equation (4.25), Let the point $\langle\vec{y}\rangle = \langle(0,1,k)^T\rangle$ be on the conic of equation (4.26), where $k \in H$. From equation (4.26):

$$d_{11} + d_{22}k^2 + 2d_{12}k = 0. \tag{4.27}$$

Define a mapping $\psi : H \mapsto H$

$$\psi(k) = d_{22}k^2 + 2d_{12}k + d_{11}. \tag{4.28}$$

Let $j \in H$. If $[\psi(k) - \psi(j) = 0 \iff k - j = 0]$ then equation (4.27) has a unique solution.

$$\psi(k) - \psi(j) = d_{22}k^2 + 2d_{12}k + d_{11} - d_{22}j^2 - 2d_{12}j - d_{11} \tag{4.29}$$

$$= (k-j)(d_{22}(k+j) + 2d_{12}) \tag{4.30}$$

$2d_{12} \notin H$ and $d_{22} \in H$, therefore $[d_{22}(k+j) + 2d_{12}] \notin H$. Thus if equation (4.30) evaluates to zero, $(k-j) = 0$ and equation (4.27) has a unique solution. Thus $\langle\vec{y}\rangle = \langle(0,1,k)^T\rangle$ is on the conic of equation (4.26), and its image in $\phi(PH(2,q))$ is $\langle\bar{\vec{y}}\rangle = \langle(0,1,0)^T\rangle$.

Then any point $\langle\vec{x}\rangle$ such that $B\vec{x} = \vec{y}$ is on the conic with equation (4.23). As there are $q+1$ points on a conic in $PG(2,q)$, $\mathcal{C}$ contains points from $q+1$ distinct point-neighbourhoods. We now show that the conic contains q points from each of the $q+1$ distinct point-neighbourhoods.

Let $\langle\bar{\vec{w}}\rangle = \langle(\bar{x}_0, 1, \bar{x}_0^2)^T\rangle$. Then from equation (4.25) for each $x_0 \in GR(p^2, r)$, the point $\vec{w}$ is on the conic $\mathcal{C}$, and satisfies $\phi(\langle\vec{w}\rangle) = \langle\bar{\vec{w}}\rangle$. Since each element of $GR(p^2, r)$ may be written as $x = a + 2b$, where $2b \in H$, there are exactly $|H| = p^r = q$ elements of $GR(p^2, r)$ such that $\bar{x} = \overline{a + 2b} = a$. Hence each point-neighbourhood that contains a point incident with $\mathcal{C}$, contains q points incident with $\mathcal{C}$.

There are $q+1$ point-neighbourhoods, with q points from each. $q(q+1)$ points altogether. □

It must be noted that Lemma 4.36 as originally published [22, Thm 2.2] states that q must be even. However this is clearly a misprint as Theorem 4.32 requires odd q.

q^2 of the points of a conic of $PH(2,q)$ with q odd are of the form [95]

$$\rho(1, \alpha, \alpha^2) \qquad \alpha \in GR(p^2, r). \tag{4.31}$$

The remaining q points are of the form

$$\rho(0, 1, \delta) \qquad \delta \in H. \tag{4.32}$$

As with constructions of MUBs, things are different in even dimensions.

Theorem 4.37. *[63, Prop 2,5] Let $\mathcal{C}$ be a conic in a 2-uniform $(q,q)PH$ plane with q even, then $|\mathcal{C}| \neq q(q+1)$.*

Proof. When considering the incidence matrix C of a projective Hjelmslev plane for which the rows and columns have been ordered into neighbourhoods as in Theorem 4.15, the rows and columns may be further ordered within neighbourhoods such that $(C)_{ii} = 1$ if and only if $\langle\vec{x_i}\rangle$ is a member of the conic (see comment after Definition 4.29). Hence the number of points on the conic is $\mathrm{Tr}(C)$. The trace of a matrix is the sum of its eigenvalues (Lemma 2.9). From Theorem 4.15 the eigenvalues of C^2 are q^2, q^3 and $q^2(q+1)^2$ with algebraic multiplicities $(q^2-1)(q^2+q+1)$, q^2+q and 1. Any eigenvalue of C is a square root of an eigenvalue of C^2.

C has constant row sum $q(q+1)$, hence $q(q+1)$ is an eigenvalue of C. $q^2(q+1)^2$ is an eigenvalue of C^2 with multiplicity 1, thus $-q(q+1)$ is not an eigenvalue of C and $q(q+1)$

has multiplicity 1. Let n_1, n_2, n_3 and n_4 be the respective multiplicities of the eigenvalues q, $-q$, $q^{3/2}$ and $-q^{3/2}$, which may be zero.

$$\mathrm{Tr}(C) = q(q+1) + (n_1 - n_2)q + (n_3 - n_4)q^{3/2} \tag{4.33}$$

with $n_1 + n_2 = (q^2-1)(q^2+q+1)$ and $n_3 + n_4 = q^2 + q$.

If q is even then $(q^2-1)(q^2+q+1)$ is odd and q^2+q is even, and therefore $n_1 - n_2 \neq 0$ and $n_1 - n_2 \neq -(n_3 - n_4)\sqrt{q}$. Hence

$$\mathrm{Tr}(C) \neq q(q+1) \tag{4.34}$$

which means that $|\mathcal{C}| \neq q(q+1)$. □

In Lemma 4.40 we find that $PH(2,q)$ is 2-uniform.

Corollary 4.38. *A conic in $PH(2,q)$ with q even cannot contain exactly $q(q+1)$ points.*

SP Analogy

Analogy 4.39 (SP Analogy)**.** *[95] A conic in a $PH(2,q)$ has the same number of points as the number of vectors in a complete set of MUBs in $\mathbb{C}^q$ for q odd.*

The $q(q+1)$ points in a conic for odd q, is analogous to the $q(q+1)$ vectors in a complete set of MUBs, of which q vectors are in each of $q+1$ bases. The q points of the form $\rho(0,\delta,1)^T$ are analogous to the vectors of the standard basis, with the remaining q^2 points analogous to the vectors in the non-standard bases. This analogy is at the level of cardinalities only.

Conics in Hjelmslev planes of even neighbourhood size cannot contain the $q(q+1)$ points required of the SP Analogy. Thus the SP Analogy does not hold in even dimensions.

For each $d = p^r$ there are at least $r+1$ non-isomorphic $(d,d)PH$-planes [28]. Thus if there is a connection between MUBs and Hjelmslev planes in odd dimensions we could expect at least $r+1$ sets of non-equivalent MUBs in $\mathbb{C}^d$. If MUBs in $\mathbb{C}^q$ and $PH(2,q)$ are intimately linked for q odd, then finding conics would be a method for finding MUBs.

The lack of correspondence between conics and MUBs in even dimensions makes the SP Analogy invalid as a general model for MUBs.

4.3 Structure of Hjelmslev planes over Galois rings

4.3.1 Motivation

The SP Analogy is based on properties of $PH(2,q)$. In order to investigate the SP Analogy the properties of $PH(2,q)$ were investigated. $PH(2,q)$ is also a candidate for use in applications such as coding theory due to the emerging use of Galois rings.

$PH(2,q)$ is shown to be 2-uniform, and the structure of the neighbourhoods of $PH(2,q)$ is determined to be $AG(2,q)$.

4.3.2 Uniformity

In this section some of the known properties of $PH(2,q)$ are expounded.

Lemma 4.40. *[69] $PH(2,q)$, the projective Hjelmslev plane generated by $GR(p^2,r)$ with $q=p^r$, is a (q,q)-PH plane, and is therefore 2-uniform.*

We do not follow the original proof.

Proof. $PH(2,q)$ contains $q^2(q^2+q+1)$ points and $q^2(q^2+q+1)$ lines. The number of points incident with a given line is $q(q+1)$, every point and every line has q^2 neighbours [95]. There are exactly q points on a line h neighbour to a point P, and exactly q^2 points on h non-neighbour to P.

Using Lemma 4.5, $t=q$ and $s=q^2$ and hence $PH(2,q)$ is a (q,q)-PH plane. Then using Lemma 4.13 we see that $PH(2,q)$ is a 2-uniform projective Hjelmslev plane. □

The following theorem shows how zero divisors create the neighbourhoods of a Hjelmslev plane.

Theorem 4.41. *[68, Satz 6.1] Let H be the additive subgroup of zero divisors of $GR(p^2,r)$. For lines $\langle \vec{l}^T\rangle = \langle (l_0,l_1,l_2)^T\rangle$, $\langle \vec{m}^T\rangle = \langle (m_0,m_1,m_2)^T\rangle \in PH(2,q)$, $\langle \vec{l}^T\rangle \sim \langle \vec{m}^T\rangle$ if and only if*

$$l_1m_2 - l_2m_1, \quad l_2m_0 - l_0m_2, \quad l_0m_1 - l_1m_0 \in H. \tag{4.35}$$

For points $\langle \vec{x}\rangle = \langle (x_0,x_1,x_2)^T\rangle$, $\langle \vec{y}\rangle = \langle (y_0,y_1,y_2)^T\rangle \in PH(2,q)$, $\langle \vec{x}\rangle \sim \langle \vec{y}\rangle$ if and only if

$$x_1y_2 - x_2y_1, \quad x_2y_0 - x_0y_2, \quad x_0y_1 - x_1y_0 \in H. \tag{4.36}$$

Proof. Points and lines are dual, thus we only need to prove the theorem for points. When equation (4.36) fails, there is a single line incident with both $\langle\vec{x}\rangle$ and $\langle\vec{y}\rangle$.

Assume equation (4.36) holds. We need to show that there exists 2 lines, $\langle\vec{g}^T\rangle$ and $\langle\vec{h}^T\rangle$, such that points $\langle\vec{x}\rangle$ and $\langle\vec{y}\rangle$ are both incident with both $\langle\vec{g}^T\rangle$ and $\langle\vec{h}^T\rangle$. Without loss of generality let $x_0 \notin H$. For some $a \in GR(p^2, r)$

$$a(x_0y_1 - y_0x_1) = (x_2y_0 - x_0y_2), \tag{4.37}$$

since H is an ideal. For the specific line $\langle\vec{g}^T\rangle = \langle(x_0^{-1}(-x_1a - x_2), a, 1)\rangle$ we find that

$$\vec{g}^T\vec{x} = x_0x_0^{-1}(-x_1a - x_2) + x_1a + x_2 = 0 \tag{4.38}$$

and $\langle\vec{g}^T\rangle$ is incident with $\langle\vec{x}\rangle$. From equation (4.37),

$$x_0^{-1}a(x_0y_1 - x_1y_0) = x_0^{-1}(x_2y_0 - x_0y_2) \tag{4.39}$$

$$ay_1 + y_2 = x_0^{-1}ax_1y_0 + x_0^{-1}x_2y_0. \tag{4.40}$$

Consider the point $\langle\vec{y}\rangle$.

$$\vec{g}^T\vec{y} = y_0x_0^{-1}(-x_1a - x_2) + y_1a + y_2 \tag{4.41}$$

which from equations (4.37) and (4.40),

$$\vec{g}^T\vec{y} = -x_0^{-1}ax_1y_0 - x_0^{-1}y_0x_2 + ay_1 + y_2 = 0 \tag{4.42}$$

and $\langle\vec{g}^T\rangle$ is incident with $\langle\vec{y}\rangle$.

Because $x_0y_1 - x_1y_0 \in H$ we know that there exists a' such that $a'(x_0y_1 - x_1y_0) = 0$. Let $\langle\vec{h}^T\rangle = \langle(x_0^{-1}(-x_1(a + a') - x_2), a + a', 1)\rangle$. Let $a' \neq 0$, then $\langle\vec{h}^T\rangle \neq \langle\vec{g}^T\rangle$.

$$\vec{h}^T\vec{x} = \vec{g}^T\vec{x} + a'x_1 - a'x_1 = 0 \tag{4.43}$$

$$\vec{h}^T\vec{y} = \vec{g}^T\vec{y} + a'(y_1 - y_0x_0^{-1}x_1) \tag{4.44}$$

$$x_0(\vec{h}^T\vec{y}) = a'(x_0y_1 - y_0x_1) = 0. \tag{4.45}$$

Since x_0 is a unit, $\vec{h}^T\vec{y} = 0$. Hence $\langle\vec{h}^T\rangle$ is incident with $\langle\vec{x}\rangle$ and $\langle\vec{y}\rangle$. Therefore $\langle\vec{x}\rangle \sim \langle\vec{y}\rangle$. □

Corollary 4.42. *[95] For points $\langle\vec{x}\rangle = \langle(x_0, x_1, x_2)^T\rangle$, $\langle\vec{y}\rangle = \langle(y_0, y_1, y_2)^T\rangle$ and lines $\langle\vec{l}^T\rangle = \langle(l_0, l_1, l_2)\rangle$, $\langle\vec{m}^T\rangle = \langle(m_0, m_1, m_2)\rangle \in PH(2, q)$, $\langle\vec{x}\rangle \sim \langle\vec{y}\rangle$ if and only if*

$$x_0 - y_0, \quad x_1 - y_1, \quad x_2 - y_2 \in H \tag{4.46}$$

and $\langle \vec{l}^T \rangle \sim \langle \vec{m}^T \rangle$ *if and only if*

$$l_0 - m_0, \quad l_1 - m_1, \quad l_2 - m_2 \in H. \tag{4.47}$$

This corollary shows that the zero divisors describe the structure of a neighbourhood, and a ring without zero divisors cannot construct a non-trivial Hjelmslev plane.

The following result is credited in [55, Def 1] to [70], however the proof is original.

Lemma 4.43. *Let* H *be the ideal containing all zero divisors of* $GR(p^2, r)$*. Let*

$$H^3 = \{(y_0, y_1, y_2)^T : y_i \in H\}, \tag{4.48}$$

be an ideal of $GR(p^2, r)^3$*. Each point-neighbourhood of* $PH(2, q)$ *is a coset of* H^3*.*

Proof. Let $\vec{x} = (x_0, x_1, x_2)^T \in GR(p^2, r)^3$ with at least one of x_0, x_1, x_2 a unit, and $P = \langle \vec{x} \rangle$ be a point in $PH(2, q)$. Then from Lemma 4.42, any point which is neighbour to P must be of the form

$$\langle \vec{x} + \vec{h} \rangle, \quad \vec{h} \in H^3. \tag{4.49}$$

Using coordinate wise addition,

$$\tilde{P} = \{\langle \vec{y} \rangle : (\vec{x} - \vec{y}) \in H^3\}. \tag{4.50}$$

Then

$$\tilde{P} \quad = \quad P + H^3 \tag{4.51}$$

and $\tilde{P}$ is a coset of H^3. Since $(0, 0, 0)^T \in H^3$, $P \in \tilde{P}$, and P is the coset leader. □

The following result stems from the relationship between a Galois field and a Galois ring.

Theorem 4.44. *[56, Thm 4.5] Let* ϕ *be the epimorphism given in Definition 4.3 part 5. Then* $\phi(PH(2, q))$ *is* $PG(2, q)$*.*

Proof. Let $\mathcal{T}_r$ be the Teichmüller set of $GR(p^2, r)$. Let $x_i \in GR(p^2, r)$ then $x_i = a_i + pb_i$ where $a_i, b_i \in \mathcal{T}_r$. The points of $PH(2, q)$ may be written as

$$\langle (x_0, x_1, x_2)^T \rangle = \langle (a_0, a_1, a_2)^T + p(b_0, b_1, b_2)^T \rangle \text{ with } a_i, b_i \in \mathcal{T}_r. \tag{4.52}$$

Recall the ring homomorphism $\overline{x}_i = \overline{a_i + pb_i} = \overline{a}_i$ (Definition 2.42). Let

$$\phi(\langle\vec{x}\rangle) = \langle(\overline{x}_0, \overline{x}_1, \overline{x}_2)^T\rangle \tag{4.53}$$

$$= \langle(\overline{a}_0, \overline{a}_1, \overline{a}_2)^T\rangle. \tag{4.54}$$

Given that for $GR(p^2, r)$, $\mathcal{T}_r \cong \mathbb{F}_{p^r}$, points in $\phi(PH(2, q))$ may be written as $\langle(\overline{a}_0, \overline{a}_1, \overline{a}_2)^T\rangle$ with $\overline{a}_0, \overline{a}_1, \overline{a}_2 \in \mathbb{F}_{p^r}$. Thus the points of $\phi(PH(2, q))$ are the points of $PG(2, q)$. A similar argument shows that the lines of $\phi(PH(2, q))$ are the lines of $PG(2, q)$, and thus $^-$ induces the required epimorphism, ϕ. □

4.3.3 Structure of the neighbourhoods

We explore neighbourhoods as substructures of $PH(2, q)$. Because $PH(2, q)$ is 2-uniform (Theorem 4.40), we know that the point-neighbourhood restrictions are affine planes. We now determine which affine plane. As seen in Corollary 4.42, it is the zero divisors of the Galois ring that determine the neighbourhood structure.

Theorem 4.45. *The point-neighbourhood restrictions of $PH(2, q)$ are $AG(2, q)$.*

Proof. From Lemma 4.40 the point-neighbourhood restrictions of $PH(2, q)$ are affine planes. We must show that the affine plane is $AG(2, q)$ which is generated by the equation

$$\alpha x + \beta y = \gamma, \quad \alpha, \beta, \gamma \in \mathbb{F}_q. \tag{4.55}$$

Let H be the ideal consisting of zero divisors of $GR(p^2, r)$. Let $\mathcal{C}_{\alpha\beta\gamma}$ be the set of ordered pairs $(h_1, h_2) \in H \times H$ such that

$$\alpha h_1 + \beta h_2 = \gamma. \tag{4.56}$$

The sets $\mathcal{C}_{\alpha\beta\gamma}$ partition the set $H \times H$. If α, β, γ and h_1 are fixed, then there is a unique value of h_2 such that equation (4.56) holds. Thus each $|\mathcal{C}_{\alpha\beta\gamma}| = q$.

Let $x_0, x_1, x_2 \in \mathcal{T}_r$ with at least one of x_0, x_1, x_2 nonzero. From Lemma 4.43 and without loss of generality, taking $x_0 \neq 0$,

$$\tilde{P} = \{\langle(x_0, x_1 + h_1, x_2 + h_2)^T\rangle : x_i \in \mathcal{T}_r, h_i \in H\}. \tag{4.57}$$

Choose $P = \langle\vec{p}\rangle = \langle(x_0, x_1 + u_1, x_2 + u_2)^T\rangle \in \tilde{P}$. Choose a line $\langle\vec{l}^T\rangle$ of $PH(2, q)$ through P, and without loss of generality let $\langle\vec{l}^T\rangle = \langle(0, l_1, l_2)\rangle$. Then from equation (4.14) we get

$$l_1(x_1 + u_1) + l_2(x_2 + u_2) = 0. \tag{4.58}$$

Note that we can choose $\alpha = l_1$ and $\beta = l_2$, so there exists a unique γ for which $\alpha u_1 + \beta u_2 = \gamma$. Thus $(u_1, u_2) \in \mathcal{C}_{\alpha\beta\gamma}$; there are $q-1$ other pairs (w_{1i}, w_{2i}) that satisfy $\alpha w_{1i} + \beta w_{2i} = \gamma$, $1 \leq i \leq q-1$.

Note that

$$\alpha u_1 + \beta u_2 = \alpha w_{1i} + \beta w_{2i}. \tag{4.59}$$

Let Q be a point which is neighbour to P.

$$Q = \langle \vec{q} \rangle = \langle (x_0, x_1 + w_{1i}, x_2 + w_{2i})^T \rangle. \tag{4.60}$$

Consider

$$\vec{l}^T \vec{q} = l_1 x_1 + l_2 x_2 + l_1 w_{1i} + l_2 w_{2i}. \tag{4.61}$$

We have chosen $\alpha = l_1$ and $\beta = l_2$, now use equation (4.59) to get

$$\vec{l}^T \vec{q} = l_1 x_1 + l_2 x_2 + l_1 u_1 + l_2 u_2 = 0. \tag{4.62}$$

Thus Q is incident with $\langle \vec{l}^T \rangle$. There are $q-1$ points generated by the pairs (w_{1i}, w_{2i}) which are also incident with $\langle \vec{l}^T \rangle$. Thus line $\langle \vec{l}^T \rangle$ is generated by equation (4.55) and is incident with q points from $\tilde{P}$.

In conclusion the point neighbourhood restriction $\tilde{P}$ has the structure of the affine plane $AG(2, q)$. □

Given the relationship between Galois rings and Galois fields it is unsurprising that a Galois field defines the structure of neighbourhoods. Points and lines are dual and generated by the same equation. Hence the following corollary.

Corollary 4.46. *The line neighbourhoods of $PH(2, q)$ are the dual structure of $AG(2, q)$.*

4.3.4 Discussion

These results show the strong connection between $PH(2, q)$ and $AG(2, q)$. Given that $AG(2, q)$ is the most elementary affine plane, this shows that $PH(2, q)$ is the most elementary projective Hjelmslev plane.

This is also important as many computer packages and various applications such as coding theory are familiar with Galois fields. The neighbourhood substructures of $PH(2, q)$ can all

be described by Galois fields, and thus may be constructed using Galois fields. An algorithm has been developed in the next section.

Of further interest is the neighbourhood structures of projective Hjelmslev planes constructed using other rings, but this is not explored here.

4.4 An algorithm to construct 2-uniform Hjelmslev planes

This section has been submitted as [45].

4.4.1 Motivation for algorithm

Explicit constructions and concrete examples are required for further investigation of applications of Hjelmslev planes. Hjelmslev planes can be constructed using Galois rings (Section 4.2.3). Common software packages such as Maple, Mathematica, Matlab, and Magma either do not have a Galois rings package, or do not currently have sufficient features to calculate Hjelmslev planes. Also just as there are affine planes which cannot be constructed via a Galois field, there are Hjelmslev planes which cannot be constructed using a Galois ring.

We show an algorithm for constructing 2-uniform projective Hjelmslev planes, some of which cannot be constructed using Galois rings. This algorithm is easily implemented in most programming languages so that a Hjelmslev plane may be generated for use in applications. The construction uses a projective plane, an affine plane and an orthogonal array as inputs for the algorithm. There are open online lookup tables (eg. [4, 101]) for these objects, or specific examples may be constructed using a Galois field [23, §VII.2].

Drake and Shult show that all Hjelmslev planes can be constructed from a projective plane and semi-nets with zings [38, Prop 2.4] (see section 4.2.3), however there is no library of semi-nets with zings.

We also show that all 2-uniform Hjelmslev planes may be constructed using this algorithm.

4.4.2 Ingredients for algorithm

The algorithm takes three different combinatorial structures and uses them to generate a 2-uniform projective Hjelmslev plane: an affine plane (Definition 3.13), a projective plane (Definition 4.2) and an orthogonal array (Defintion 3.15).

A projective plane of order m may be represented as a $2-(m^2+m+1, m+1, 1)$ block design [102, §8.4]. An affine plane of order m may be represented as a $2-(m^2, m, 1)$ block design [102, Thm 18]. An affine plane may be constructed from a projective plane by deleting a line, and the points incident with that line from every other line in the plane. In this way an affine plane is a sub-geometry of a projective plane.

An affine plane of order m has a parallelism: there are $m+1$ mutually unbiased $\|$-classes, each $\|$-class contains m lines, and each line is incident with m points.

Each symbol occurs in each column of the orthogonal array v times. An orthogonal array may be obtained from an affine plane by assigning each point of the affine plane to a row of the array, and each $\|$-class of the affine plane to a column of the array. The symbol, s, in position (i, j) of the array indicates that line s of $\|$-class j is incident with point i of the affine plane.

The three structures above may all be generated from a projective plane. However, for this algorithm it is not essential that the objects have any relationship other than size.

4.4.3 An algorithm for constructing $2-$uniform projective Hjelmslev planes

Algorithm 4.47. An algorithm for constructing a 2-uniform projective Hjelmslev plane is as follows:

Step 1 Let $\mathcal{P}$ be a projective plane of order m, $\mathcal{A}$ an affine plane of order m and $\mathcal{O}$ an orthogonal array $OA(m^2, m+1, m, 2)$. We now create a new structure $\mathcal{H}$.

Step 2 Replace each of the points of $\mathcal{P}$ with m^2 points which are a copy of $\mathcal{A}$. This gives $(m^2+m+1)m^2$ points in $\mathcal{H}$. Each affine plane will now be called a point-neighbourhood restriction.

Step 3 Choose a line l in $\mathcal{P}$ and for each point of l, choose a parallel class of $\mathcal{A}$ for the corresponding point-neighbourhood restriction (The parallel class may be the same or different for each point of l). Label each of the lines of the parallel class of each point-neighbourhood restriction with the symbols from $\mathcal{O}$. Since each point-neighbourhood restriction is in m lines of $\mathcal{P}$, each time a particular point-neighbourhood restriction is incident with a chosen line, a different parallel class of $\mathcal{A}$ must be used. Label each column of O with a point-neighbourhood restriction.

$$\mathcal{P} = \left\{ \begin{array}{l} \{0,1,2,9\}, \\ \{3,4,5,9\}, \\ \{6,7,8,9\}, \\ \{0,3,6,A\}, \\ \{1,4,7,A\}, \\ \{2,5,8,A\}, \\ \{0,4,8,B\}, \\ \{1,5,6,B\}, \\ \{2,3,7,B\}, \\ \{0,7,5,C\}, \\ \{1,3,8,C\}, \\ \{2,4,6,C\}, \\ \{9,A,B,C\}, \end{array} \right\} \quad \mathcal{A} = \left\{ \begin{array}{l} \{R,S,T\}, \\ \{U,V,W\}, \\ \{X,Y,Z\}, \\ \{R,U,X\}, \\ \{S,V,Y\}, \\ \{T,W,Z\}, \\ \{R,V,Z\}, \\ \{S,W,X\}, \\ \{T,U,Y\}, \\ \{R,W,Y\}, \\ \{S,U,Z\}, \\ \{T,V,X\} \end{array} \right\} \quad \mathcal{O} = \begin{array}{cccc} L & L & L & L \\ L & M & M & M \\ L & N & N & N \\ M & L & M & N \\ M & M & N & L \\ M & N & L & M \\ N & L & N & M \\ N & M & L & N \\ N & N & M & L \end{array}$$

Figure 4.1: Constructing a 2-uniform PH plane: Step 1. A projective plane of order 3, an affine plane of order 3 and an orthogonal array $OA(9,4,3,2)$.

$$\{0R, 0S, 0T, 0U, 0V, 0W, 0X, 0Y, 0Z, 1R, 1S, \ldots CX, CY, CZ\}.$$

Figure 4.2: Constructing a 2-uniform PH plane: Step 2. The points of $\mathcal{H}$ can be written with a double label to show membership of point-neighbourhoods.

Step 4 We now create lines in $\mathcal{H}$ by joining the lines of the parallel class of each point-neighbourhood restriction according to $\mathcal{O}$.

An example is given in Figures 4.1-4.4.

Theorem 4.48. *The structure generated by Algorithm 4.47 is a 2-uniform $(m,m)PH$-plane.*

Proof. Algorithm 4.47 generates an incidence structure $\mathcal{H}$ with $(m^2+m+1)m^2$ points, $(m^2+m+1)m^2$ lines, each line containing (m^2+m) points, and each point incident with (m^2+m) lines. We show that $\mathcal{H}$ satisfies all the axioms of Definition 4.3.

Axioms 1 and 3: Any pair of points P and Q which are in the same point-neighbourhood

In neighbourhood $\tilde{3}$; $L := \{R, S, T\}$, $M := \{U, V, W\}$, $N := \{X, Y, Z\}$.
In neighbourhood $\tilde{4}$; $L := \{R, S, T\}$, $M := \{U, V, W\}$, $N := \{X, Y, Z\}$.
In neighbourhood $\tilde{5}$; $L := \{R, S, T\}$, $M := \{U, V, W\}$, $N := \{X, Y, Z\}$.
In neighbourhood $\tilde{9}$; $L := \{R, U, X\}$, $M := \{S, V, Y\}$, $N := \{T, W, Z\}$.

3	4	5	9
L	L	L	L
L	M	M	M
L	N	N	N
M	L	M	N
M	M	N	L
M	N	L	M
N	L	N	M
N	M	L	N
N	N	M	L

Figure 4.3: Constructing a 2-uniform PH plane: Step 3. Choosing line $l = \{3, 4, 5, 9\}$ of $\mathcal{P}$, the chosen $\|$-classes of each point-neighbourhood of l, and the labels for the columns of $\mathcal{O}$.

$\{3R,\ 3S,\ 3T,\ 4R,\ 4S,\ 4T,\ 5R,\ 5S,\ 5T,\ 9R,\ 9U,\ 9X\}$
$\{3R,\ 3S,\ 3T,\ 4U,\ 4V,\ 4W,\ 5U,\ 5V,\ 5W,\ 9S,\ 9V,\ 9Y\}$
$\{3R,\ 3S,\ 3T,\ 4X,\ 4Y,\ 4Z,\ 5X,\ 5Y,\ 5Z,\ 9T,\ 9W,\ 9Z\}$
$\{3U,\ 3V,\ 3W,\ 4R,\ 4S,\ 4T,\ 5U,\ 5V,\ 5W,\ 9T,\ 9W,\ 9Z\}$
$\{3U,\ 3V,\ 3W,\ 4U,\ 4V,\ 4X,\ 5X,\ 5Y,\ 5Z,\ 9R,\ 9U,\ 9X\}$
$\{3U,\ 3V,\ 3W,\ 4X,\ 4Y,\ 4Z,\ 5R,\ 5S,\ 5T,\ 9S,\ 9V,\ 9Y\}$
$\{3X,\ 3Y,\ 3Z,\ 4R,\ 4S,\ 4T,\ 5X,\ 5Y,\ 5Z,\ 9S,\ 9V,\ 9Y\}$
$\{3X,\ 3Y,\ 3Z,\ 4U,\ 4V,\ 4X,\ 5R,\ 5S,\ 5T,\ 9T,\ 9W,\ 9Z\}$
$\{3X,\ 3Y,\ 3Z,\ 4X,\ 4Y,\ 4Z,\ 5U,\ 5V,\ 5W,\ 9R,\ 9U,\ 9X\}$
$\{6R,\ 6S,\ 6T,\ 7R,\ 7S,\ 7T,\ 8R,\ 8S,\ 8T,\ 9R,\ 9V,\ 9Z\}$
$\{6R,\ 6S,\ 6T,\ 7U,\ 7V,\ 7W,\ 8U,\ 8V,\ 8W,\ 9U,\ 9Y,\ 9T\}$
$\{6R,\ 6S,\ 6T,\ 7X,\ 7Y,\ 7Z,\ 8X,\ 8Y,\ 8Z,\ 9X,\ 9S,\ 9W\}$
$\{6U,\ 6V,\ 6W,\ 7R,\ 7S,\ 7T,\ 8U,\ 8V,\ 8W,\ 9X,\ 9S,\ 9W\}$
$\{6U,\ 6V,\ 6W,\ 7U,\ 7V,\ 7X,\ 8X,\ 8Y,\ 8Z,\ 9R,\ 9V,\ 9Z\}$
$\{6U,\ 6V,\ 6W,\ 7X,\ 7Y,\ 7Z,\ 8R,\ 8S,\ 8T,\ 9U,\ 9Y,\ 9T\}$
$\{6X,\ 6Y,\ 6Z,\ 7R,\ 7S,\ 7T,\ 8X,\ 8Y,\ 8Z,\ 9U,\ 9Y,\ 9T\}$
$\{6X,\ 6Y,\ 6Z,\ 7U,\ 7V,\ 7X,\ 8R,\ 8S,\ 8T,\ 9X,\ 9S,\ 9W\}$
$\{6X,\ 6Y,\ 6Z,\ 7X,\ 7Y,\ 7Z,\ 8U,\ 8V,\ 8W,\ 9R,\ 9V,\ 9Z\}$

Figure 4.4: Constructing a 2-uniform PH plane: Step 4. The lines of $\mathcal{H}$ in the line-neighbourhoods corresponding to the lines $\{3,4,5,9\}$ and $\{6,7,8,9\}$ of $\mathcal{P}$ are constructed according to $\mathcal{O}$. Note that every pair of lines from within a line-neighbourhood share exactly 3 points, and every pair of lines from different line-neighbourhoods share exactly one point. Note that different $\|$-classes of the point-neighbourhood restriction $\tilde{9}$ are used for each line neighbourhood.

are incident with exactly one line of the point neighbourhood restriction, which is an affine plane. Each line of the point-neighbourhood restriction is used in m lines of $\mathcal{H}$, as each symbol appears m times in each column of $\mathcal{O}$. For points P and R which are in different point-neighbourhoods, there is exactly one line of $\mathcal{P}$ which is incident with any pair of point-neighbourhoods. Given $\|$-classes $\tilde{P}_X$ and $\tilde{R}_Y$ of each point-neighbourhood, $\mathcal{O}$ ensures that each line of $\tilde{P}_X$ is in a line of $\mathcal{H}$ with each line of $\tilde{R}_Y$ exactly once.

Axioms 2 and 4: $\mathcal{O}$ ensures that lines in the same line-neighbourhood meet in exactly one line of a $\|$-class of a point-neighbourhood restriction, which is m points. For lines g and h which are in different line-neighbourhoods, their line-neighbourhoods may be labelled with lines from $\mathcal{P}$. Any pair of lines in $\mathcal{P}$ intersect in exactly one point, thus any line-neighbourhoods of $\mathcal{H}$ intersect in exactly one point neighbourhood $\tilde{Q}$. Each line-neighbourhood is allocated a different $\|$-class $\tilde{Q}_X$, $\tilde{Q}_Y$. Thus the line g in $\mathcal{H}$ must contain a line of $\tilde{Q}_X$ and h a line of $\tilde{Q}_Y$. As the $\|$-classes of each point neighbourhood restriction are unbiased, g and h meet in exactly one point.

Let ϕ collapse point-neighbourhoods and line-neighbourhoods. It is trivial to check that this is incidence preserving and surjective, and thus an epimorphism.

All axioms of Definition 4.3 are satisfied. Thus $\mathcal{H}$ is a projective Hjelmslev plane.

To see that $\mathcal{H}$ is 2-uniform, we see that the point-neighbourhood restrictions are constructed to be affine planes, and each line of each point-neighbourhood restriction is used in $m+1$ lines of $\mathcal{H}$. □

4.4.4 Properties of the algorithm

In the example the affine plane used is a sub-geometry of the projective plane. However this is not required. Any projective plane, any affine plane and any orthogonal array of the appropriate sizes may be used. In fact different affine planes may be used for each point-neighbourhood restriction.

Theorem 4.49. *All 2-uniform projective Hjelmslev planes can be generated using Algorithm 4.47.*

Proof. We already know that $\mathcal{H}$ is a 2-uniform projective Hjelmslev plane. Axiom 1 of Definition 4.11 requires that point-neighbourhood restrictions are affine planes; this is guaranteed by step 2. Requiring that every line of every $\tilde{P}$ is the restriction of the same number of

lines is equivalent to ensuring that each line of each parallel class of the point-neighbourhood restriction is included in the same number of lines at step 4. This is ensured as each symbol occurs in each column of an orthogonal array the same number of times. □

For orders where there are several possible projective planes, affine planes and orthogonal arrays, this algorithm generates many different Hjelmslev planes of the same size.

Cataloguing of projective planes, affine planes and orthogonal arrays is an ongoing project on which any catalogue of Hjelmslev planes is dependant. Further investigation into isomorphism classes of Hjelmslev planes is also required.

Algorithm 4.47 may be amended to construct 2-uniform affine Hjelmslev planes

Lemma 4.50. *[36]A $(t,r)PH$-plane can be truncated to a $(t,r)AH$ plane.*

Proof. Take $PH(t,r)$ and remove all the lines of one line-neighbourhood together with all incident points. Uniformity is maintained as the structure of the point-neighbourhood restriction remains unchanged. □

A 2-uniform affine Hjelmslev plane may be generated directly by using Algorithm 4.47: let $\mathcal{P}$ be an affine plane of size m, $\mathcal{A}$ an affine plane of size m and take the first m columns of an $OA(m^2, m+1, m, 2)$ orthogonal array.

Unlike an ordinary affine plane which may be extended to a projective plane, not all affine Hjelmslev planes may be extended to projective Hjelmslev planes [35]. The non-extendibility of affine Hjelmslev planes is shown by giving a specific example which is 3-uniform [35, Cor 6.2]. Thus it may be the case that all 2-uniform affine Hjelmslev planes are extendable to a projective Hjelmslev plane. If so all 2-uniform affine Hjelmslev planes may be generated using Algorithm 4.47.

4.5 Proposed algorithm for constructing MUBs from Hjelmslev planes

An algorithm to construct a complete set of MUBs using a projective Hjelmslev plane has been developed. This algorithm is shown to construct a complete set of MUBs in $\mathbb{C}^4$ when using $PH(2,2)$.

The algorithm is combinatorial, and may work on Hjelmlsev planes other than $PH(2,q)$. However no work has been done to asses the success of this algorithm on any plane other than $PH(2,2)$.

Algorithm 4.51. 1. Let $\mathcal{H}$ be $PH(2,q)$.

2. Choose $q+1$ points from $\mathcal{H}$ which are collinear, but from different line-neighbourhoods.

3. Remove all lines that contain these points.

4. Truncate all remaining lines by removing all points in the point-neighbourhoods of the chosen points. Call this sub-geometry $\mathcal{X}$.

5. Each point in $\mathcal{X}$ corresponds to a vector in the set of MUBs. Each of the lines of $\mathcal{X}$ represents vectors which have the same symbol in particular fixed a position. Label q^4 vectors of length q^2 with the points of $\mathcal{X}$.

6. Fill the first position in every vector with a 1.

7. Each set of disjoint line-neighbourhoods of $\mathcal{X}$ corresponds to an unfilled position in the set of vectors. Allocate a symbol to each of the lines such that each line from the same line neighbourhood has an opposing symbol, e.g. ω^α, $\omega^{-\alpha}$. For each line in $\mathcal{X}$ fill the allocated position of the vectors whose corresponding points appear in each line, with the symbol allocated to that line.

8. Apply an appropriate scalar multiplier to all vectors.

Algorithm 4.51 is illustrated by constructing the Galois ring MUBs in $\mathbb{C}^4$ using $PH(2,2)$; see Figures 4.5-4.9.

$PH(2,2)$ is generated from $GR(2^2,1)$. The MUBs in $\mathbb{C}^4$ constructed according to the Galois ring construction (Theorem 2.58) use $GR(2^2,2)$. Different, but related algebraic structures are used to generate the Hjelmslev plane and the MUBs. The construction established in Algorithm 4.51 may be an algebraic one, where the construction of the Hjelmslev plane is an unnecessary middle step (compare with section 3.2.6).

Conjecture 4.52. *The q^4 vectors generated using Algorithm 4.51 along with the standard basis form a complete set of MUBs in $\mathbb{C}^{q^2}$.*

line-neighbourhood	line of $\mathcal{H}$	line-neighbourhood	line of $\mathcal{H}$
026	$\{0A, 0B, 2A, 2B, 6A, 6B\}$	045	$\{0A, 0D, 4A, 4D, 5A, 5D\}$
	$\{0A, 0B, 2C, 2D, 6C, 6D\}$		$\{0A, 0D, 4B, 4C, 5B, 5C\}$
	$\{0C, 0D, 2A, 2B, 6C, 6D\}$		$\{0B, 0C, 4A, 4D, 5B, 5C\}$
	$\{0C, 0D, 2C, 2D, 6A, 6B\}$		$\{0B, 0C, 4B, 4C, 5A, 5D\}$
346	$\{3A, 3B, 4A, 4B, 6A, 6D\}$	235	$\{2A, 2D, 3A, 3D, 5A, 5C\}$
	$\{3A, 3B, 4C, 4D, 6B, 6C\}$		$\{2A, 2D, 3B, 3C, 5B, 5D\}$
	$\{3C, 3D, 4A, 4B, 6B, 6C\}$		$\{2B, 2C, 3A, 3D, 5B, 5D\}$
	$\{3C, 3D, 4C, 4D, 6A, 6D\}$		$\{2A, 2D, 3B, 3C, 5A, 5C\}$
031	$\{0A, 0C, 3A, 3C, 1A, 1C\}$	156	$\{1A, 1D, 5A, 5C, 6A, 6B\}$
	$\{0A, 0C, 3B, 3D, 1B, 1D\}$		$\{1A, 1D, 5B, 5D, 6C, 6D\}$
	$\{0B, 0D, 3A, 3C, 1B, 1D\}$		$\{1B, 1C, 5A, 5C, 6C, 6D\}$
	$\{0B, 0D, 3B, 3D, 1A, 1C\}$		$\{1B, 1C, 5B, 5D, 6A, 6B\}$
241	$\{2A, 2C, 4A, 4C, 1A, 1B\}$		
	$\{2A, 2C, 4B, 4D, 1C, 1D\}$		
	$\{2B, 2D, 4A, 4C, 1C, 1D\}$		
	$\{2B, 2D, 4B, 4D, 1A, 1B\}$		

Figure 4.5: Constructing MUBs: Step 1. The lines of $\mathcal{H}$. The points are labelled with a double label ij where i is the point-neighbourhood. The lines are listed according to their line-neighbourhood, which is shown in the left column.

line-neighbourhood	line of $\mathcal{H}$
026	$\{0A, 0B, 2C, 2D, 6C, 6D\}$
	$\{0C, 0D, 2A, 2B, 6C, 6D\}$
346	$\{3A, 3B, 4A, 4B, 6A, 6D\}$
	$\{3C, 3D, 4C, 4D, 6A, 6D\}$
031	$\{0A, 0C, 3B, 3D, 1B, 1D\}$
	$\{0B, 0D, 3A, 3C, 1B, 1D\}$
241	$\{2A, 2C, 4A, 4C, 1A, 1B\}$
	$\{2B, 2D, 4B, 4D, 1A, 1B\}$
045	$\{0A, 0D, 4B, 4C, 5B, 5C\}$
	$\{0B, 0C, 4A, 4D, 5B, 5C\}$
235	$\{2A, 2D, 3A, 3D, 5A, 5C\}$
	$\{2A, 2D, 3B, 3C, 5A, 5C\}$
156	

Figure 4.6: Constructing MUBs: Steps 2 and 3. We chose points $1C$*,* $5D$ *and* $6B$*, and remove all lines from* $\mathcal{H}$ *that contain any of these points.*

truncated line-neighbourhood	line of $\mathcal{X}$
02	$\{0A, 0B, 2C, 2D\}$
	$\{0C, 0D, 2A, 2B\}$
34	$\{3A, 3B, 4A, 4B\}$
	$\{3C, 3D, 4C, 4D\}$
03	$\{0A, 0C, 3B, 3D\}$
	$\{0B, 0D, 3A, 3C\}$
24	$\{2A, 2C, 4A, 4C\}$
	$\{2B, 2D, 4B, 4D\}$
04	$\{0A, 0D, 4B, 4C\}$
	$\{0B, 0C, 4A, 4D\}$
23	$\{2A, 2D, 3A, 3D\}$
	$\{2A, 2D, 3B, 3C\}$

Figure 4.7: Constructing MUBs: Step 4. The lines of $\mathcal{H}$ have been truncated by removing point-neighbourhoods 1, 5 *and* 6. *$\mathcal{X}$ is a sub-geometry of $\mathcal{H}$*

$$0A = \begin{pmatrix} 1 \\ 1 \\ * \\ * \end{pmatrix}, \quad 0B = \begin{pmatrix} 1 \\ 1 \\ * \\ * \end{pmatrix}, \quad 0C = \begin{pmatrix} 1 \\ -1 \\ * \\ * \end{pmatrix}, \quad 0D = \begin{pmatrix} 1 \\ -1 \\ * \\ * \end{pmatrix},$$

$$2A = \begin{pmatrix} 1 \\ -1 \\ * \\ * \end{pmatrix}, \quad 2B = \begin{pmatrix} 1 \\ -1 \\ * \\ * \end{pmatrix}, \quad 2C = \begin{pmatrix} 1 \\ 1 \\ * \\ * \end{pmatrix}, \quad 2D = \begin{pmatrix} 1 \\ 1 \\ * \\ * \end{pmatrix}.$$

Figure 4.8: Constructing MUBs: Steps 5, 6 and 7. Each vector is labelled with the points of $\mathcal{X}$. Let the truncated line-neighbourhoods 02 *and* 34 *correspond to the second position. We fill the second position of each of the vectors corresponding to the points of the truncated line $\{0A, 0B, 2C, 2D\}$ with* 1 *and fill the second position of each of those vectors corresponding to the points of the truncated line $\{0C, 0D, 2A, 2B\}$ with -1.*

4.6 Conclusion

4.6.1 Findings

The aim of this chapter was to establish connections between MUBs and Hjelmslev planes and to find evidence for or against the SP Analogy. Theorem 4.37 shows that conics in Hjelmslev planes with even neighbourhood size cannot contain exactly $q(q+1)$ points, making the SP Analogy invalid as a model for MUBs in even dimensions. Hjelmslev planes have a rich structure, thus other aspects of a Hjelmslev plane may have connections with MUBs. The results of section 4.5 are a small piece of evidence supporting this.

The investigation of Hjelmslev planes has been necessitated by the lack of available knowledge. Building connections between Hjelmslev planes and other structures will be assisted by knowing more about Hjelmslev planes.

The neighbourhood structure of a Hjelmslev plane over a Galois ring, $PH(2, q)$, has been shown to have the structure of an affine plane over a Galois field, $AG(2, q)$.

A combinatorial algorithm has been developed to construct 2-uniform Hjelmslev planes.

$$0A = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \quad 0B = \begin{pmatrix} 1 \\ 1 \\ -1 \\ -1 \end{pmatrix}, \quad 0C = \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix}, \quad 0D = \begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix},$$

$$2A = \begin{pmatrix} 1 \\ -1 \\ -i \\ -i \end{pmatrix}, \quad 2B = \begin{pmatrix} 1 \\ -1 \\ i \\ i \end{pmatrix}, \quad 2C = \begin{pmatrix} 1 \\ 1 \\ -i \\ i \end{pmatrix}, \quad 2D = \begin{pmatrix} 1 \\ 1 \\ i \\ -i \end{pmatrix},$$

$$3A = \begin{pmatrix} 1 \\ -i \\ -1 \\ -i \end{pmatrix}, \quad 3B = \begin{pmatrix} 1 \\ -i \\ 1 \\ i \end{pmatrix}, \quad 3C = \begin{pmatrix} 1 \\ i \\ -1 \\ i \end{pmatrix}, \quad 3D = \begin{pmatrix} 1 \\ i \\ 1 \\ -i \end{pmatrix},$$

$$4A = \begin{pmatrix} 1 \\ -i \\ -i \\ -1 \end{pmatrix}, \quad 4B = \begin{pmatrix} 1 \\ -i \\ i \\ 1 \end{pmatrix}, \quad 4C = \begin{pmatrix} 1 \\ i \\ -i \\ 1 \end{pmatrix}, \quad 4D = \begin{pmatrix} 1 \\ i \\ i \\ -1 \end{pmatrix}.$$

Figure 4.9: Constructing MUBs: Step 7. We continue with truncated line-neighbourhoods 03 *and* 24 *representing the third position and,* 04 *and* 23 *representing the fourth position. Pairs of lines from the same truncated line-neighbourhood are allocated opposing symbols.*

This algorithm uses well catalogued objects as seeds. The construction of explicit examples will be of use in applications.

4.6.2 Further directions

Each of the three sections of original work in this chapter could start an entirely new research project.

Section 4.3 investigates properties of $PH(2, q)$, the projective Hjelmslev plane generated by a Galois ring. The properties of Hjelmslev planes over other rings may be further investigated using similar techniques.

Question 4.53. *What are the permissible neighbourhood structures of a Hjelmslev plane?*

Section 4.4 develops an algorithm for constructing 2-uniform projective Hjelmslev planes. This algorithm could possibly be modified to construct other objects such as affine Hjelmslev planes, Hjelmslev planes of higher uniformity, and non-uniform Hjelmslev planes.

Question 4.54. *For what sizes do non-uniform Hjelmslev planes exist?*

We have shown that the analogous behaviour of conics in a Hjelmslev planes and MUBs does not hold for all sets of MUBs. There are other aspects of Hjelmslev planes which are as yet unexplored for connections with MUBs. Section 4.5 proposes a construction for a set of MUBs in $\mathbb{C}^d$.

Question 4.55. *Can a Hjelmslev plane be used to construct mutually unbiased bases?*

This construction is shown to work with $PH(2, 2)$. Further investigation is required to determine if this construction is valid for other Hjelmslev planes.

Chapter 5

MUBs and Planar Functions

5.1 Introduction

5.1.1 Motivation

The planar function construction of MUBs (Theorem 2.52) is the most general construction of MUBs. Planar functions can be used to construct both MUBs and MOLS. It may be that the connection between MUBs and MOLS is actually a connection between MUBs and planar functions. Further investigation of planar functions in relation to MUBs may yield this answer.

5.1.2 Aim

From the planar function construction we know that a planar function is sufficient to construct a set of MUBs. The planar function construction constructs a single set of MUBs for each planar function over each field. We aim to determine if non-equivalent MUBs may be constructed from the same planar function.

5.2 Definitions and preliminary results

Planar functions and characters over fields were introduced in Chapter 2. There are a few more results that will be used in this chapter.

5.2.1 Planar Functions

Planar functions (Definition 2.36) can be used to construct affine planes (Definition 3.21) and MUBs (Theorem 2.52). A list of known planar functions is given in Theorem 3.23. There are some related types of functions that we make use of.

Definition 5.1. [27, §2] An *additive* function h on $\mathbb{F}_q$ satisfies

$$h(x+y) = h(x) + h(y). \tag{5.1}$$

Algebra books would call this a *homomorphism* of the additive group of $\mathbb{F}_q$. We use the term additive function as it appears in the literature on planar functions.

Definition 5.2. A function f which is both additive and a permutation on a group, G, is an *automorphism* of G.

A Galois field $\mathbb{F}_q$ has two operations; an automorphism of a field is an automorphism in both operations. An automorphism of the additive group of $\mathbb{F}_q$ may not be an automorphism of the multiplicative group. Let $h(x) = ax$ where $a \in \mathbb{F}_q^*$, then h is a cyclic permutation of $\mathbb{F}_q$. The function h is also additive,

$$h(x+y) = a(x+y) = ax + ay = h(x) + h(y), \tag{5.2}$$

and so is an automorphism of the additive group of $\mathbb{F}_q$. However

$$h(xy) = axy \neq axay = h(x)h(y). \tag{5.3}$$

Thus h is not an automorphism of $\mathbb{F}_q^*$, the multiplicative group of $\mathbb{F}_q$.

There is extensive literature on automorphisms of Galois fields [40, §9].

5.2.2 Characters

The planar function construction of MUBs uses characters (Theorem 2.52). Some definitions and results on characters are given in section 2.2.2. Character sums of the form

$$\sum_{c \in \mathbb{F}_q} \chi(f(c)) \tag{5.4}$$

where f is a polynomial of positive degree may be called *Weil sums*. Evaluating the sum of characters is difficult. In many cases only the magnitude of the solution or a bound on the magnitude is known [76, §5.4]. Recent results improve some bounds, but do not add to the set of polynomials of which the character sum is explicitly known [43].

Theorem 5.3. *[76, Thm 5.11] Let $G(\eta, \chi)$ be the Gaussian sum of χ, an additive character, and η, the quadratic character, on $\mathbb{F}_q$. Then*

$$G(\eta, \chi) = 0 \quad \text{for } \chi = \chi_0 \tag{5.5}$$

$$|G(\eta, \chi)| = \sqrt{q} \quad \text{for } \chi \neq \chi_0 \tag{5.6}$$

where $\chi_0(c) = 1$ for all $c \in \mathbb{F}_q$.

Theorem 5.4. *[76, Cor 5.31] If χ is a non-trivial additive character of $\mathbb{F}_q$ then for all $a_0, a_1 \in \mathbb{F}_q$*

$$\sum_{x \in \mathbb{F}_q} \chi(a_1 x + a_0) = 0. \tag{5.7}$$

5.3 Generalised planar function construction of MUBs

The following result is a generalisation of [72, prop 5] for which $L(x) = x$. We only require the result in one variable, thus although this result is true for multi-variate functions, we state it in the single variable case.

Lemma 5.5. *Let Π be a planar polynomial and L an additive permutation polynomial over $\mathbb{F}_q$. Let χ be a non-trivial character of $\mathbb{F}_q$ then*

$$\left| \frac{1}{\sqrt{q^n}} \sum_{x \in \mathbb{F}_q} \chi\left(\Pi(x) - b.L(x)\right) \right| = 1 \quad \forall b \in \mathbb{F}_q. \tag{5.8}$$

Proof.

$$\left| \frac{1}{\sqrt{q}} \sum_{x \in \mathbb{F}_q} \chi(\Pi(x) - b.L(x)) \right|^2 = \frac{1}{q} \sum_{x \in \mathbb{F}_q} \chi(\Pi(x) - b.L(x)) \sum_{y \in \mathbb{F}_q} \chi(-\Pi(y) + b.L(y)) \tag{5.9}$$

$$= \frac{1}{q} \sum_{x \in \mathbb{F}_q} \chi\left(\Pi(x)\right) \sum_{y \in \mathbb{F}_q} \chi\left(-\Pi(y) - b.L(x - y)\right) \tag{5.10}$$

$$= \frac{1}{q} \sum_{x \in \mathbb{F}_q} \chi\left(\Pi(x)\right) \sum_{z \in \mathbb{F}_q} \chi\left(-\Pi(x - z) - b.L(z)\right) \tag{5.11}$$

$$= \frac{1}{q} \sum_{z \in \mathbb{F}_q} \chi\left(b.L(z)\right) \sum_{x \in \mathbb{F}_q} \chi\left(\Pi(x) - \Pi(x - z)\right). \tag{5.12}$$

A function which satisfies equation (2.38) is bent and by Theorem 2.40 it is also planar. Thus the inner sum of equation (5.12) is zero unless $z = 0$, in which case the inner sum has value q. Then

$$\left| \frac{1}{\sqrt{q}} \sum_{x \in \mathbb{F}_q} \chi(\Pi(x) - b.L(x)) \right|^2 = \frac{1}{q} \chi\left(b.L(0)\right) q. \tag{5.13}$$

Because L is additive $L(0) = 0$. Hence we have equation (5.9) equates to 1, and equation (5.8) is satisfied. □

All known planar functions over $\mathbb{F}_q$ require odd q [27]. We now generalize the planar function construction of MUBs.

Theorem 5.6 (Generalised Planar construction)**.** *Let $\Pi(x)$ be a planar function and $L(x)$ be an additive permutation function on $\mathbb{F}_q$. Then the set of vectors*

$$\vec{v}_{ab} = \frac{1}{\sqrt{q}} \left(\omega_p^{tr[a\Pi(x)+bL(x)]} \right)_{x \in \mathbb{F}_q} \tag{5.14}$$

$a, b \in \mathbb{F}_q$ and the standard basis forms a complete set of MUBs.

Proof.

$$\langle \vec{v}_{ab} | \vec{v}_{cd} \rangle = \frac{1}{q} \sum_{x \in \mathbb{F}_q} \omega_p^{\mathrm{tr}[(c-a)\Pi(x)+(d-b)L(x)]} \tag{5.15}$$

If $a = c$, then, because L is a permutation function,

$$\langle \vec{v}_{ab} | \vec{v}_{ad} \rangle = \frac{1}{q} \sum_{x \in \mathbb{F}_q} \omega_p^{\mathrm{tr}[(d-b)L(x)]} = \begin{cases} 1 & \text{if } d = b \\ 0 & \text{if } d \neq b. \end{cases} \tag{5.16}$$

This shows the bases are orthonormal.

If $a \neq c$ then, from Definition 2.38 and Lemma 5.5, equation (5.15) equals $\frac{1}{\sqrt{q}}$. This shows that bases B_a and B_c are unbiased. Each component of each vector has magnitude $\frac{1}{\sqrt{q}}$, so each base is unbiased to the standard basis. □

It is possible for L to be an automorphism of $\mathbb{F}_q$, but the extra conditions on the multiplicative operation are not required.

5.4 Equivalences of MUBs

Lemma 5.7. *Let $\mathcal{A} = \{I_d, A_0, \ldots, A_{n-1}\}$ and $\mathcal{B} = \{I_d, B_0, \ldots, B_{n-1}\}$ be complete sets of MUBs represented as matrices with columns that form the vectors of each base. Let $\mathcal{A}$ and $\mathcal{B}$ be equivalent with the unitary transform U such that $U\mathcal{A} = \mathcal{B}$. Then U is one of:*

- *a permutation matrix P,*
- *A_i^*, where A_i is an element of $\mathcal{A}$,*
- *PA_i^*P', permutations applied to A_i^* where A_i is an element of $\mathcal{A}$.*

Proof. If $U(\mathcal{A}) = \mathcal{B}$ then for some matrix A_i in $\mathcal{A}$

$$UA = I_d. \tag{5.17}$$

That is $U = A_i^{-1}$. Because each base is orthonormal, each A_i is unitary. We also allow a permutation matrix, as the order of the columns within the matrix is an arbitrary ordering of the vectors within the base, and the ordering of the rows within the whole set of matrices is an arbitrary ordering of the dimensions. □

In Theorem 2.65 a permutation of A_0^* was used to show equivalence of the WF and Alltop type MUBs. Lemma 5.7 is a formalisation of this idea.

5.4.1 Example

Unfortunately summing over characters is difficult. Thus we cannot algebraically determine if the generalised planar construction will construct MUBs that are not equivalent to those constructed using the planar function construction. We show an example of two equivalent sets of MUBs.

Let $\mathcal{A}$ be the set of MUBs generated by $\Pi(x) = x^2$ and $L(x) = x$, and $\mathcal{B}$ be the set of MUBs generated by $\Pi(x)$ and $L'(x) = x^3$ according to equation (5.14) over $\mathbb{F}_9$. This is the *Frobenius automorphism* of $\mathbb{F}_9$ [40, Thm 9.1.19].

The column permutation $(3,7)(5,6)(4,8)$ transforms $\mathcal{A}$ into $\mathcal{B}$, and hence they are equivalent sets of MUBs.

We are yet to find an explicit example of a planar function and two additive permutation functions which produce non-equivalent sets of MUBs.

5.5 Conclusion

5.5.1 Findings

We have generalised the planar function construction of MUBs by using an automorphism on the additive group of a Galois field. However it is unclear if this generalisation will lead to new sets of MUBs.

5.5.2 Further directions

Question 5.8. *Can non-equivalent sets of MUBs be constructed from the same planar function?*

More knowledge about character sums would enable an algebraic test for equivalence. Explicit computation of examples may show that there are non-equivalent MUBs which are based on the same planar function.

Chapter 6

MUBs and Relation Algebras

This chapter has been published as a section of [46].

6.1 Introduction

6.1.1 Motivation

Relation algebras have been constructed from the set of points and the set of lines of projective planes [52, 82]. A projective plane exists if and only if a complete set of MOLS also exists. Given the SPR conjecture connecting MOLS and MUBs, these relation algebras are investigated for connections with MUBs.

6.1.2 Historical note on relation algebras

In 1860 De Morgan [83] published the first discussion of binary relations as a branch of formal logic. Until that time studies of logic had remained essentially unchanged since Aristotle [52, §1.1]; however Aristotle's system did not consider relations between objects.

In the second half of the nineteenth century several authors [88, 98] studied the properties of relations and operations [82, §1.1]. Boole [14] had formalized an algebra of unary relations in 1851 (Boolean algebra), and this structure was built upon to define relation algebras.

6.1.3 Aim

We construct algebras of relational type using the structure of MUBs. These algebras are compared with two known relation algebras which use the structure of a projective plane.

Constructing a relation algebra from a set of MUBs that is equivalent to a relation algebra from a projective plane would be evidence for the SPR conjecture.

6.2 Definitions and preliminary results

Definitions can be found in comprehensive works on logic such as [49, 103]. For a more comprehensive study of relation algebras see for example [52, 82]. We follow the notation of [82].

6.2.1 Axioms of relation algebras

Relation algebras are algebraic structures which can be generated by a set of relations on some underlying set, and using set theoretic operations on those relations.

Definition 6.1. Let X be a set of objects. A *binary relation*, R, on X is a subset of $X \times X$.

Let R be a relation, then for notational convenience $(x, y) \in R$ may be written as Rxy, and $(x, y) \notin R$ may be written as $\neg Rxy$.

Let $\mathcal{S}b(X)$ be the *powerset* of a set X. Then a set of binary relations $\mathcal{M}$ is a subset of $\mathcal{S}b(X \times X)$.

Definition 6.2. An algebra, $\mathfrak{M}$, on a set, $\mathcal{M}$, that has 2 unary operations, $^-$, $^\smile$, 2 binary operations, $+$, $;$, and an identity element, I, is an algebra of *relational type*. Denoted $\mathfrak{M} = \langle \mathcal{M}, +, ^-, ;, ^\smile, I \rangle$.

There are 10 axioms that describe the structure of an algebra of relational type [82, §6.01].

$$\begin{array}{lrcll}
\forall A, B, C \in \mathfrak{M}: & & & & \\
R_1 & A + B & = & B + A & + \text{ commutativity} \\
R_2 & A + (B + C) & = & (A + B) + C & + \text{ associativity} \\
R_3 & \overline{\bar{A} + \bar{B}} + \overline{\bar{A} + B} & = & A & \text{Huntington} \\
R_4 & A;(B;C) & = & (A;B);C & ; \text{ associativity} \\
R_5 & (A + B);C & = & A;C + B;C & ; + \text{ distributivity} \\
R_6 & A;I & = & A & \text{identity} \\
R_7 & \breve{\breve{A}} & = & A & \breve{} \text{ involution} \\
R_8 & (A + B)\breve{} & = & \breve{A} + \breve{B} & \breve{} + \text{ distributivity} \\
R_9 & (A;B)\breve{} & = & \breve{A};\breve{B} & ;\breve{} \text{ distributivity} \\
R_{10} & \breve{A};\overline{A;B} + \bar{B} & = & \bar{B} & \text{Tarski/DeMorgan.}
\end{array} \tag{6.1}$$

Definition 6.3. [82, §6.01] An algebra of relational type that meets axioms R_1-R_{10} is a *relation algebra.*

There are algebras which meet some, but not all of these axioms. For example the class of non-associative relation algebras meets axioms $R_1 - R_3$ and $R_5 - R_{10}$ [82, §6.3].

Lemma 6.4. *[82, §1] Let P and Q be relations on a set X. Define operations on relations as:*

$$P \cup Q := \{(x, y) : (x, y) \in P \vee (x, y) \in Q\} \quad \text{Union,} \tag{6.2}$$

$$\overline{P} := \{(x, y) : (x, y) \notin P\} \quad \text{Complement,} \tag{6.3}$$

$$P|Q := \{(x, z) : \exists y, (x, y) \in P \wedge (y, z) \in Q\} \quad \text{Composition,} \tag{6.4}$$

$$\breve{P} := \{(x, y) : (y, x) \in P\} \quad \text{Converse.} \tag{6.5}$$

Any set of relations which is closed under the operations $\cup, \bar{}, |, \breve{}$ obeys axioms $R_1 - R_{10}$ and is therefore a relation algebra.

It must be noted that the operations of Lemma 6.4 are sufficient, but not necessary for a relation algebra.

6.2.2 Properties of relation algebras

The *Identity* relation on the set X is given by

$$I_X := \{(x, x) : x \in X\}. \tag{6.6}$$

The *Universal* relation on the set X is given by

$$U_X := \{(x, y) : x, y \in X\}. \tag{6.7}$$

Definition 6.5. An algebra $\mathfrak{M} = \langle \mathcal{M}, +, \bar{}, ;, \breve{}, I\rangle$ of relational type is *finite* if $\mathcal{M}$ is a finite set.

If $\mathcal{M}$ is a finite set of relations on X then, X is not necessarily finite.

Definition 6.6. [52, Ex 3.3.7] A relation algebra $\mathfrak{M} = \langle \mathcal{M}, +, \bar{}, ;, \breve{}, I\rangle$ is *symmetric* if $A = \breve{A}$ for all elements of $\mathcal{M}$.

Definition 6.7. [82, §5.2] An element, A, of a relation algebra $\mathfrak{M} = \langle \mathcal{M}, +, \bar{}, ;, \breve{}, I\rangle$ is an *atom* if $A + R \neq A$ for all elements $R \in \mathcal{M}$ and $A; R \neq A$ for some $R \in \mathcal{M}$. The set of atoms may be denoted $\mathcal{A}t(\mathfrak{M})$. An algebra $\mathfrak{M}$ is *atomic* if for every $R \in \mathcal{M}$ there exists an $A \in \mathcal{A}t(\mathfrak{M})$ such that $A + R = R$.

Since an algebra is closed under the four operations $+, \bar{}, ;, \breve{}$, an atomic relation algebra may be defined by its atoms.

A *ternary* relation T on a set X is a subset of $X \times X \times X$. Let

$$U := \{x : \exists y, \exists z, Txyz \vee Tyxz \vee Tyzx\}, \tag{6.8}$$

then U is the *field* of T. $U \subseteq X$. Ternary relations may be reduced to binary relations. For example:

$$Q := \{(a, b) : a, b \in U, \forall_x \forall_y [Taxy \Leftrightarrow Tbyx] \vee [Txay \Leftrightarrow Tybx]\}. \tag{6.9}$$

Definition 6.8. [82, §6.26] Let T be a ternary relation. Let U be the field of T and Q as defined in equation (6.9). Then $\mathfrak{Cm}(T) := \langle \mathcal{S}b(U), \cup, \bar{}, ;, \breve{}, I\rangle$ is the *complex* algebra of T, where

the operations $\cup, ^-$ are defined as in Lemma 6.4, and $;, \breve{}$ abd I are defined as

$$R;S := \{c : \exists r, \exists s, [r \in R, s \in S, Trsc]\} \tag{6.10}$$

$$\breve{R} := \{b : \exists r, [r \in R, Qrb]\} \tag{6.11}$$

$$I := \{a : a \in U, \forall r, \forall s, [[Tars \vee Tras] \Rightarrow r = s]\}. \tag{6.12}$$

The elements of a $\mathfrak{Cm}(T)$ are subsets of U, not binary relations. $\mathfrak{Cm}(T)$ is an algebra of relational type, but depending on T it may not satisfy all the axioms of a relation algebra.

6.2.3 Relation Algebras constructed from projective planes

There are two classes of relation algebras that have been constructed using the structure of projective planes: the Lyndon and Jonsson algebras [82, 52]. We construct the Jonsson and Lyndon algebras and discuss some of their properties.

Jonsson Algebra

Definition 6.9. [82, §6.31] Let $\mathcal{P}$ be a projective plane of order at least 2. Let e be a point not in $\mathcal{P}$. Let U be the set of points of $\mathcal{P}$ in union with $\{e\}$. Let T be the ternary relation consisting of all triples (a, b, c) of distinct collinear points of $\mathcal{P}$ and triples of the form (e, a, a), (a, e, a), (a, a, e) with $a \in U$.

The Jonsson algebra of $\mathcal{P}$ is $\mathfrak{Cm}(T)$.

The Jonsson algebra is an algebra of relational type. Axioms $R_1 - R_3$ and $R_5 - R_{10}$ hold for all Jonsson algebras. If $\mathcal{P}$ is of order 2, then axiom R_4 also holds and the Jonsson algebra is a relation algebra.

Lemma 6.10. *[82, §6.31]The Jonsson algebra is symmetric. If $\mathcal{P}$ is a projective plane of order 3 or greater then the Jonsson algebra is non-associative in the operation ;.*

Since the elements of $\mathfrak{Cm}(T)$ are subsets of U, each $\{a\}$, $a \in U$ is an atom of $\mathfrak{Cm}(T)$. If the projective plane is finite, then there is a finite number of atoms, and hence $\mathfrak{Cm}(T)$ is finite.

$\{e\}$ is the identity element I since

$$R;I = R \iff R = \{p : \exists r, \exists i, [r \in R, i \in I, Trip]\} \tag{6.13}$$

and $Trer$ for all $r \in U$.

Thus for $\mathcal{P}$ a finite projective plane of order 3 or greater the Jonsson algebra is an algebra of relational type that is symmetric, atomic, finite and non-associative.

Lyndon Algebra

Definition 6.11. [79, §3][52, §4.5] A Lyndon algebra $\mathfrak{L}_n = \langle \mathcal{L}, \cup, \bar{}, ;, \breve{}, I \rangle$ of order n is a finite relation algebra with $n+2$ atoms, $I, a_0, a_1, \ldots, a_n$. Composition is defined by

$$a_i ; a_i = a_i \cup I \tag{6.14}$$

$$a_i ; a_j = \sum_{k \neq i,j} a_k \quad \text{for } i \neq j. \tag{6.15}$$

All atoms of $\mathfrak{L}$ are self converse, $\breve{a_i} = a_i$. Operations $\cup$, and $\bar{}$ are as defined in Lemma 6.4.

Lemma 6.12. *[79, §3][52, §4.5] Let $n \geq 3$. $\mathfrak{L}_n$ is a relation algebra.*

$\mathfrak{L}_n$ may be constructed on 4 or less atoms, but associativity does not hold.

The Lyndon algebra may be constructed as the complex algebra of a ternary relation. This construction differs from the Jonsson algebra by the inclusion of the triples of the form (a, a, a) in the ternary relation.

Definition 6.13. [82, §6.32] Let $\mathcal{P}$ be a projective geometry of order at least three. Let e be a point not in $\mathcal{P}$. Let U be the set of points of $\mathcal{P}$ and $\{e\}$. Let T' be the ternary relation consisting of all triples (a, b, c) of distinct collinear points of $\mathcal{P}$ and triples of the form (e, a, a), (a, e, a), (a, a, e), (a, a, a) with $a \in U$.

$\mathfrak{L}(\mathcal{P})$ is $\mathfrak{Cm}(T')$.

Theorem 6.14. *$\mathfrak{L}(\mathcal{P})$ as given in Definition 6.13 is a Lyndon algebra $\mathfrak{L}_n$ where n is the number of points in the projective plane. Each atom a_i is a point of the projective plane, and I represents a set containing a point not in the plane, $\{e\}$.*

Proof. The atoms of $\mathfrak{L}_n$ and $\mathfrak{L}(\mathcal{P})$ are the points of $\mathcal{P}$ and $I = \{e\}$. The operations $\cup$, $\bar{}$ are the same for both $\mathfrak{L}_n$ and $\mathfrak{L}(\mathcal{P})$.

Let $R = \{r\}$ and $S = \{s\}$ be atomic relations of $\mathfrak{L}(\mathcal{P})$. Then $R;S$ is all points on the line rs except r and s, which is consistent with equation (6.15). $R;R = \{r, e\} = R \cup I$, which is consistent with equation (6.14). Thus ; is the same operation for both $\mathfrak{L}_n$ and $\mathfrak{L}(\mathcal{P})$.

From equation (6.11)

$$\breve{R} = \{b : \exists r \in R, \forall x \in U, \forall y \in U, [[T'rxy \Leftrightarrow T'byx] \vee [T'xry \Leftrightarrow T'ybx]]. \tag{6.16}$$

If $T'rxy$ then either r, x, y are collinear or $T'rrr$, $T'rre$, or $T'rer$. If $T'byx$ then b, x, y are collinear, $T'bbb$, $T'bbe$, or $T'beb$. Thus $b = r$ and $\breve{R} = R$.

All operations on $\mathfrak{L}(\mathcal{P})$ are the same as for $\mathfrak{L}_n$, hence $\mathfrak{L}(\mathcal{P}) = \mathfrak{L}_n$. □

The following result shows that the Lyndon algebra has a unique set of properties.

Theorem 6.15. *[79][82, Thm 347] $\mathfrak{L}$ is the Lyndon algebra of a projective geometry with at least four points on every line if and only if $\mathfrak{L}$ is a relation algebra that is complete, atomic, symmetric, I is an atom of $\mathfrak{L}$ and $a; a = a + I$ for every atom.*

In particular if $\mathcal{P}$ is a line with $n + 1$ points, then the Lyndon algebra is representable if and only if a projective plane of order n exists.

Discussion

Both the Jonsson and Lyndon algebras have different properties depending on whether the underlying geometry has three or more points on a line. It is possible that other relation algebras can be constructed from the structure of projective or affine planes, but that is beyond the scope of this project.

6.3 Relation Algebras constructed from MUBs

We now construct some algebras of relational type using the structure of MUBs.

Definition 6.16. Let $\mathcal{X}$ be the union of the vectors in a set of MUBs. The relations on these vectors can be defined using the inner product:

$$U := \{(a, b) : a, b \in \mathcal{X}\} \quad \text{Universality,} \tag{6.17}$$

$$\emptyset := \{\ \} \quad \text{Empty,} \tag{6.18}$$

$$I := \{(a, a) : a \in \mathcal{X}\} \quad \text{Identity,} \tag{6.19}$$

$$O := \{(a, b) : |\langle a|b\rangle|^2 = 0\} \quad \text{Orthogonality,} \tag{6.20}$$

$$N := \{(a, b) : |\langle a|b\rangle|^2 = \frac{1}{d}\} \quad \text{Non-orthogonality.} \tag{6.21}$$

$\mid$	I_x	O_x	N_{xy}	N_{yx}	N_{yz}
I_x	I_x	O_x	N_{xy}	N_{yx}	N_{yz}
O_x	O_x	$O_x \cup I_x$	N_{xy}	$\emptyset$	$\emptyset$
N_{xy}	$\emptyset$	$\emptyset$	$\emptyset$	$O_x \cup I_x$	N_{xz}
N_{yx}	N_{yx}	N_{yx}	$O_y \cup I_y$	$\emptyset$	$\emptyset$
N_{yz}	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$

Figure 6.1: Cayley table of atomic relations in $\mathfrak{R}$.

Lemma 6.17. *Let $\mathcal{M} = \{U, \emptyset, I, \bar{I}, O, \bar{O}, N, \bar{N}\}$ as defined in equations (6.17 -6.21). Then $\mathfrak{M} = \langle \mathcal{M}, \cup, ^-, |, ^\smile, I\rangle$ is a relation algebra with operations union $\cup$, complement $^-$, composition $|$, and converse $^\smile$, defined as in Lemma 6.4.*

Proof. By Lemma 6.4, $\mathfrak{M}$ obeys axioms $R_1 - R_{10}$ and is therefore a relation algebra. □

This relation algebra structure exists for any set of at least two MUBs in any dimension. In order for the algebraic structure to be useful in finding MUBs, or finding links between projective planes and MUBs, the relations need to be more specific. The relations need to contain information about how many MUBs are in the set and their dimension. Thus we split the original relations to reflect membership of each base. Let $\mathcal{B}_x$ be the x^{th} base in a set of MUBs, then relations may be defined as:

$$I_x = \{(a, a) : a \in \mathcal{B}_x\}, \tag{6.22}$$

$$O_x = \{(a, b) : a, b \in \mathcal{B}_x \wedge a \neq b\}, \tag{6.23}$$

$$N_{xy} = \{(a, b) : a \in \mathcal{B}_x, b \in \mathcal{B}_y\}. \tag{6.24}$$

Lemma 6.18. *Let $\mathcal{X}$ be the union of vectors in a set of n MUBs. Let $\mathcal{R}$ be the set of relations generated by the atomic relations I_x, O_x, N_{xy}, $1 \leq x, y \leq n$. Then $\mathfrak{R} = \langle \mathcal{R}, \cup, ^-, |, ^\smile, I\rangle$ is a relation algebra with operations union, $\cup$, complement, $^-$, composition, $|$, and converse $^\smile$, as in Lemma 6.4.*

Proof. By generating the set of relations using $\cup$ we ensure it is closed under $^-$. I_x and O_x are symmetric relations. $\breve{N}_{xy} = N_{yx}$, which shows closure under $^\smile$. The Cayley table of the atoms under $|$ (Figure 6.1), in conjunction with closure under $\cup$ shows closure under $|$. □

$\mathfrak{R}$ is not symmetric, and does not satisfy $A|A = A \cup I$ for any element of R. Thus $\mathfrak{R}$ is neither a Jonsson nor a Lyndon algebra.

$\mathfrak{R}$ does not contain any information about the dimension. Different relations may be required for this. Both the Lyndon and Jonsson algebras are symmetric, thus if we are trying to construct a Lyndon or Jonsson algebra, then $\mathfrak{R}$ may not be worth further investigation.

6.4 Conclusion

6.4.1 Findings

The algebras constructed from the structure of MUBs do not share any similarities with algebras constructed from projective planes. Perhaps this is a small piece of evidence pointing to MUBs and projective planes being non-equivalent. However we have not conducted an exhaustive investigation of relation algebras from the structure of MUBs.

The Jonsson and Lyndon algebras have different properties, even though they are constructed from the same geometric structure. They also have different properties depending on the size of the projective plane. This may be similar to the WF and Alltop type MUBs, although the MUBs are equivalent, the Alltop construction fails when d is a power of 3.

6.4.2 Further directions

Question 6.19. *What relational algebra structures can be constructed for complete sets of MUBs.*

A ternary relation that reflects base membership may yield a relation algebra with similarities to the Jonsson or Lyndon algebras.

Chapter 7

MUBs and Group Rings

This chapter has been published as a section of [46].

7.1 Introduction

7.1.1 Motivation

Difference sets can be represented as elements in group rings [11]. Theorem 2.78 connects relative difference sets and MUBs [42].[1] We investigate MUBs using group rings.

A vector can be written as a formal sum

$$\sum_{i=1}^{d} a_i s_i \tag{7.1}$$

where a_i are elements of a field, and s_i are basis vectors. In the case of MUBs the field is $\mathbb{C}$. A group ring is a set of formal sums where the a_i are elements of a ring, and the s_i are elements of a group. This structural similarity and connections from Theorem 2.78 lead to the representation of the vectors of MUBs as group ring elements.

7.1.2 Aim

In this chapter we use group rings to investigate the algebraic structure of MUBs. By representing the vectors as group ring elements we aim to establish an algebraic structure for a set of MUBs.

[1] Although the publication date of [42] is after that of [46] on which this chapter is based, a preprint was available.

From Theorem 2.65 we know that MUBs can be constructed from relative difference sets, which can be represented as group ring elements. We choose a different interpretation of group ring elements in the hope for a more general result than Theorem 2.65.

From Theorem 2.86 we know that, under component-wise multiplication, specific sets of MUBs have a group structure. Using the convolution product of a group ring may yield an algebraic structure for more sets of MUBs.

7.2 Definitions and preliminary results

Definitions and properties of group rings may be found in standard works on algebra for example [40, 74].

Definition 7.1. [74, §2.1] Let $\mathbb{K}$ be a ring and G be a group. Then the *group ring* $\mathbb{K}[G]$ is the set of formal linear combinations

$$\alpha = \sum_{x \in G} a_x x \quad \text{where } a_x \in \mathbb{K} \text{ and } x \in G. \tag{7.2}$$

A difference set D of a group G may be represented as an element of a group ring:

$$D = \sum_{x \in G} a_x x \quad \text{where } a_x \in \mathbb{K},\ x \in G,\ \ a_x = 1_{\mathbb{K}} \text{ for } x \in D, \text{ and } a_x = 0 \text{ otherwise.} \tag{7.3}$$

Definition 7.2. [74, §2.1] Let $\alpha = \sum_{x \in G} a_x x$ and $\beta = \sum_{y \in G} b_y y$ be elements of $\mathbb{K}[G]$. Then the *convolution product* is defined as:

$$\alpha * \beta = \sum_{x \in G} \sum_{y \in G} a_x b_y (x + y) = \sum_{z \in G} \left(\sum_{x+y=z} a_x b_y \right) z. \tag{7.4}$$

The elements of G may be thought of as labels on each component of a vector. By choosing these labels from a finite group we take advantage of the algebraic structure.

We represent vectors in $\mathbb{C}^q$ as members of a group ring $\mathbb{C}[\mathbb{F}_q]$ using the additive group of $\mathbb{F}_q$. Thus $a_x, b_y \in \mathbb{C}$ and $x, y \in \mathbb{F}_q$. When constructing MUBs we are interested only in the direction of the vectors, not their magnitude, so a modified version of convolution is used.

Definition 7.3. Normalised convolution, $\hat{*}$ is defined as:

$$\alpha\hat{*}\beta = \mu \ : \exists c{\in}\mathbb{C},\ \alpha{*}\beta = c\mu \tag{7.5}$$

Lemma 7.4. *[74, p85] If G is a commutative group, and $\mathbb{K}$ is a commutative ring, then $\mathbb{K}[G]$ is commutative.*

Definition 7.5. [40, 1.3.17] A *monoid* $\langle M, \star\rangle$ is a set M closed under a binary operation $\star$ which is associative, and has an identity element.

If a monoid is also commutative then it is a *commutative monoid*; if every element has an inverse, then it is a group.

7.3 Group ring representation of MUBs

7.3.1 Representing vectors as group ring elements

Vectors of a set of MUBs can be represented as elements of a group ring. This is shown with an example.

Let $\mathcal{N}_2$ be the set of vectors of 3 MUBs in $\mathbb{C}^2$ [112] in union with $\{\vec{0}\}$. These vectors can be generated using the Galois ring construction or the Pauli Matrix construction.

$$\begin{aligned}\mathcal{N}_2 \ = \ & \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}, \right. \\ & \left. \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\}. \end{aligned} \tag{7.6}$$

Consider the elements of $\mathcal{N}_2$ to be elements of the group ring $\mathbb{C}[\mathbb{Z}_2]$. To avoid confusion with elements of $\mathbb{C}$ we denote the elements of $\mathbb{Z}_2$ as μ and ν. Let

$$\begin{aligned} \vec{s}_0 &= 1\mu + 0\nu, \\ \vec{s}_1 &= 0\mu + 1\nu, \\ \vec{v}_{00} &= \tfrac{1}{\sqrt{2}}(1\mu + 1\nu), \\ \vec{v}_{01} &= \tfrac{1}{\sqrt{2}}(1\mu - 1\nu), \\ \vec{v}_{10} &= \tfrac{1}{\sqrt{2}}(1\mu + i\nu), \\ \vec{v}_{11} &= \tfrac{1}{\sqrt{2}}(1\mu - i\nu), \\ \vec{0} &= 0\mu + 0\nu. \end{aligned} \tag{7.7}$$

$\hat{*}$	$\vec{0}$	$\vec{s}_0$	$\vec{s}_1$	$\vec{v}_{00}$	$\vec{v}_{01}$	$\vec{v}_{10}$	$\vec{v}_{11}$
$\vec{0}$	$\vec{0}$	$\vec{0}$	$\vec{0}$	$\vec{0}$	$\vec{0}$	$\vec{0}$	$\vec{0}$
$\vec{s}_0$	$\vec{0}$	$\vec{s}_0$	$\vec{s}_1$	$\vec{v}_{00}$	$\vec{v}_{01}$	$\vec{v}_{10}$	$\vec{v}_{11}$
$\vec{s}_1$	$\vec{0}$	$\vec{s}_1$	$\vec{s}_0$	$\vec{v}_{00}$	$\vec{v}_{01}$	$\vec{v}_{11}$	$\vec{v}_{10}$
$\vec{v}_{00}$	$\vec{0}$	$\vec{v}_{00}$	$\vec{v}_{00}$	$\vec{v}_{00}$	$\vec{0}$	$\vec{v}_{00}$	$\vec{v}_{00}$
$\vec{v}_{01}$	$\vec{0}$	$\vec{v}_{01}$	$\vec{v}_{01}$	$\vec{0}$	$\vec{v}_{01}$	$\vec{v}_{01}$	$\vec{v}_{01}$
$\vec{v}_{10}$	$\vec{0}$	$\vec{v}_{10}$	$\vec{v}_{11}$	$\vec{v}_{00}$	$\vec{v}_{01}$	$\vec{s}_1$	$\vec{s}_0$
$\vec{v}_{11}$	$\vec{0}$	$\vec{v}_{11}$	$\vec{v}_{10}$	$\vec{v}_{00}$	$\vec{v}_{01}$	$\vec{s}_0$	$\vec{s}_1$

Figure 7.1: Cayley table of $\langle \mathcal{N}_2, \hat{*} \rangle$ [46, Prop 3].

The Cayley table of $\langle \mathcal{N}_2, \hat{*} \rangle$ in Figure 7.1 shows that $\langle \mathcal{N}_2, \hat{*} \rangle$ is associative, commutative and has $\vec{s}_0$ as an identity element. Hence when considered as elements of $\mathbb{C}[\mathbb{F}_2]$, $\langle \mathcal{N}_2, \hat{*} \rangle$ forms a commutative monoid.

7.3.2 Group ring structure of WF type MUBs

Structure of vectors of WF type MUBs

We begin with some examples.

Let $d = 3, 5, 7$. The vectors of WF type MUBs in union with $\{\vec{0}\}$, when considered as elements of the group ring $\mathbb{C}[\mathbb{Z}_d]$, form a commutative monoid.

Let $d = 9$. The vectors of WF type MUBs in union with $\{\vec{0}\}$, when considered as elements of the group ring $\mathbb{C}[\mathbb{Z}_3 \times \mathbb{Z}_3]$, form a commutative monoid. Using the group ring $\mathbb{C}[\mathbb{Z}_9]$ does not produce a closed structure.

Let $d = 4$. The vectors of Galois ring MUBs in union with $\{\vec{0}\}$, when considered as elements of the group ring $\mathbb{C}[\mathbb{Z}_2 \times \mathbb{Z}_2]$, form a commutative monoid. Using the group ring $\mathbb{C}[\mathbb{Z}_4]$ does not produce a closed structure.

The vectors forming a commutative monoid holds generally for WF type MUBs when the vectors of WF type MUBs are represented as elements of the group ring $\mathbb{C}(\mathbb{F}_q)$, using the additive group of $\mathbb{F}_q$. We begin with some specific Lemmas before showing the monoid structure.

Let B_a be the a^{th} base of WF type MUBs constructed using equation (2.79)

$$B_a = \{\vec{v}_{a0}, \vec{v}_{a1} \dots \vec{v}_{a(p-1)}\} \tag{7.8}$$

$$\vec{v}_{ab} = \left(\chi\left(ax^2 + bx\right)\right)_{x\in\mathbb{F}_q}. \tag{7.9}$$

Let v_{ab_z} be the z^{th} entry in vector $\vec{v}_{ab}$,

$$v_{ab_z} = \chi(az^2 + bz). \tag{7.10}$$

We begin by first expanding out the convolution product:

$$(\vec{v}_{ab}\hat{*}\vec{v}_{cd})_z = k\sum_{x+y=z} v_{ab_x} v_{cd_y} \tag{7.11}$$

$$= k\sum_{x\in\mathbb{F}_q} v_{ab_x} v_{cd_{z-x}} \tag{7.12}$$

$$= k\sum_{x\in\mathbb{F}_q} \chi\left(ax^2 + bx + c(z-x)^2 + d(z-x)\right) \tag{7.13}$$

$$= k\sum_{x\in\mathbb{F}_q} \chi\left((a+c)x^2 + (b - c2z - d)x + (cz^2 + dz)\right). \tag{7.14}$$

Here $k \in \mathbb{C}$ is chosen to normalise the vectors. It is important to note that $a, b, c, d, x, y, z \in \mathbb{F}_q$. χ is a mapping from $\mathbb{F}_q$ to $\mathbb{C}$.

There are several possibilities for the solution to $\vec{v}_{ab}\hat{*}\vec{v}_{cd}$:

- $\vec{v}_{ef}$ for some $e, f \in \mathbb{F}_q$, (Lemma 7.6)
- a member of the standard basis, (Lemma 7.8)
- $\vec{0}$, (Lemma 7.9)
- a vector which is not contained in the set of MUBs. (Not possible by Lemma 7.11)

Equation (7.14) will be used in the following results to show the various solutions to $\vec{v}_{ab}\hat{*}\vec{v}_{cd}$.

Lemma 7.6. *For $a + c \neq 0$*

$$\vec{v}_{ab}\hat{*}\vec{v}_{cd} = \vec{v}_{ef} \tag{7.15}$$

where $e = c - c^2(a+c)^{-1}$ and $f = c(a+c)^{-1}(b-d) + d$.

Proof. Let $\vec{v}_{ab}\hat{*}\vec{v}_{cd} = \vec{\gamma}$.

Using equation (7.14) and Theorem 2.33 we find that

$$\gamma_z = k\chi\left(cz^2 + dz - \frac{(b-2cz-d)^2}{4(a+c)}\right)\eta(a+c)G(\eta,\chi) \tag{7.16}$$

$$= k\chi\left(\left(c - \frac{c^2}{a+c}\right)z^2 + \left(\frac{c(b-d)}{a+c} + d\right)z - \frac{(b-d)^2}{4(a+c)}\right)\eta(a+c)G(\eta,\chi). \tag{7.17}$$

All of the terms without a z will be a scalar on the entire vector, which will be factored out by choosing appropriate k.

$$\gamma_z = \chi\left(z^2(c - c^2(a+c)^{-1}) + z(c(a+c)^{-1}(b-d) - d)\right) \tag{7.18}$$

Thus $\vec{\gamma} = \vec{v}_{ef}$ with $e = c - c^2(a+c)^{-1}$ and $f = c(a+c)^{-1}(b+d) - d$. □

Corollary 7.7. *For $a + c \neq 0$*

$$\vec{v}_{a0}\hat{*}\vec{v}_{c0} = \vec{v}_{e0} \tag{7.19}$$

with $e = c - c^2(a+c)^{-1}$.

Lemma 7.8. *For $a + c = 0$, $c \neq 0$*

$$\vec{v}_{ab}\hat{*}\vec{v}_{cd} = \vec{s}_r \tag{7.20}$$

with $r = (b-d)(2c)^{-1}$.

Proof. If $a + c \neq 0$ then

$$(\vec{v}_{ab}\hat{*}\vec{v}_{cd})_z = k\chi\left((cz^2 + dz) - \frac{(b - c2z - d)^2}{4(a+c)}\right)\eta(a+c)G(\eta,\chi). \tag{7.21}$$

Since $\chi(x) \neq 0$ and $\eta(x) \neq 0$ equation (7.21) can only equal 0 if $G(\eta,\chi) = 0$. By Theorem 5.3, $G(\eta,\chi) = 0$ if and only if χ is a trivial character. But χ is not trivial, thus the left hand side of equation (7.21) can never equal 0. Thus if $a + c \neq 0$, $\vec{v}_{ab}\hat{*}\vec{v}_{cd} \neq \vec{s}_r$.

If $a + c = 0$ then equation (7.14) becomes

$$(\vec{v}_{ab}\hat{*}\vec{v}_{cd})_z = k\sum_{x\in\mathbb{F}_q}\chi\left((b-2cz-d)x + cz^2 + dz\right). \tag{7.22}$$

If $b - 2cz - d \neq 0$, then from Theorem 5.4

$$k\sum_{x\in\mathbb{F}_q}\chi\left((b-2cz-d)x + cz^2 + dz\right) = 0. \tag{7.23}$$

If $b - 2cz - d = 0$, then when allowing for the factor k to be chosen,

$$k \sum_{x \in \mathbb{F}_q} \chi(cz^2 + dz) = 1. \tag{7.24}$$

For each combination of b, d, c there is exactly one value of z for which $b-2cz-d = 0$. Let $r = (b-d)(2c)^{-1}$ then $\vec{v}_{ab} \hat{*} \vec{v}_{cd} = \vec{s}_r$ when $a + c = 0$. Because 0 does not have a multiplicative inverse, if $c = 0$ then r has no solution, hence $c \neq 0$. If $b = d$ then $r = 0$. □

Corollary 7.9.

$$\vec{v}_{0b} \hat{*} \vec{v}_{0d} = \begin{cases} \vec{0} & \text{for } b \neq d, \\ \vec{v}_{0b} & \text{for } b = d. \end{cases} \tag{7.25}$$

Proof. From equation (7.14) we see that if $b - d \neq 0$ then

$$(\vec{v}_{0b} \hat{*} \vec{v}_{0d})_z = k \sum_{x \in \mathbb{F}_q} \chi\left((b-d)x + dz\right) = 0 \tag{7.26}$$

for each z. Thus $\vec{v}_{0b} \hat{*} \vec{v}_{0d} = \vec{0}$.

If $b = d$ then

$$(\vec{v}_{0b} \hat{*} \vec{v}_{0b})_z = k \sum_{x \in \mathbb{F}_q} \chi(bz) = v_{0b_z}. \tag{7.27}$$

□

Lemma 7.10. $\vec{s}_0 \hat{*} \vec{v}_{ab} = \vec{v}_{ab}$.

Proof. Obvious. □

Lemma 7.11. *If* $\vec{v}_{ab} \hat{*} \vec{v}_{cd} = \vec{v}_{ef}$ *then* $\vec{v}_{ag} \hat{*} \vec{v}_{cd} = \vec{v}_{eh}$ *where* $h = f + \frac{(g-b)c}{a+b}$.

Proof. From equation (2.79)

$$v_{ab_x} = \frac{1}{\sqrt{q}} \chi\left(ax^2 + bx\right) \qquad v_{cd_y} = \frac{1}{\sqrt{q}} \chi\left(cy^2 + dy\right). \tag{7.28}$$

Let $g = b + m$ then

$$v_{ag_x} = \frac{1}{\sqrt{q}} \chi\left(ax^2 + gx\right) = \chi\left(ax^2 + bx + mx\right) = \chi(mx) v_{ab_x}. \tag{7.29}$$

Then using equation (7.14) and Theorem 2.33 we get $a_2 = a + c$, $a_1 = b - c2z - d$, $a_0 = cz^2 + dz$.

$$v_{ef_z} = \chi\left((cz^2 + dz) - \frac{(b - c2z - d)^2}{4(a+c)}\right) \eta(a+c) G(\eta, \chi). \tag{7.30}$$

Let $\vec{v}_{ag} \hat{*} \vec{v}_{cd} = \vec{v}_{e'h}$:

$$\begin{aligned} v_{e'h_z} &= k \sum_{x \in \mathbb{F}_q} \chi\left(ax^2 + gx + c(z-x)^2 + d(z-x)\right) && (7.31)\\ &= k \sum_{x \in \mathbb{F}_q} \chi\left(ax^2 + bx + mx + c(z-x)^2 + d(z-x)\right) && (7.32)\\ &= k \sum_{x \in \mathbb{F}_q} \chi\left((a+c)x^2 + (b - c2z - d + m)x + (cz^2 + dz)\right). && (7.33) \end{aligned}$$

Then using Theorem 2.33 we get $a_2 = a + c$, $a_1 = b - c2z - d + m$, $a_0 = cz^2 + dz$.

$$\begin{aligned} v_{e'h_z} &= k\chi\left((cz^2 + dz) - \frac{(b - c2z - d + m)^2}{4(a+c)}\right)\eta(a+c)G(\eta,\chi) && (7.34)\\ &= k\chi\left((cz^2 + dz) - \frac{(b - 2cz - d)^2}{4(a+c)} - \frac{2m(b - 2cz - d) + m^2}{4(a+c)}\right)\eta(a+c)G(\eta,\chi) && (7.35)\\ &= k\chi\left(\frac{-2m(b - 2cz - d) - m^2}{4(a+c)}\right) v_{ef_z} && (7.36)\\ &= k\chi\left(\frac{mcz}{a+c}\right)\chi\left(\frac{2m(d-b) - m^2}{4(a+c)}\right) v_{ef_z}. && (7.37) \end{aligned}$$

Thus we have that $v_{e'h_z}$ is a scalar multiple of v_{ef_z}. $h = f + \frac{mc}{a+c}$, $e' = e$, and the other term is cleared by k. □

We have now shown enough results to show the structure of the vectors.

Theorem 7.12. *The vectors in a complete set of WF type MUBs in union with $\{\vec{0}\}$, when considered as elements of $\mathbb{C}[\mathbb{F}_q]$ form a commutative monoid under $\hat{*}$.*

Proof. Closure: By induction. Lemma 7.7 gives the base set, and Lemma 7.11 gives the inductive step.

Associativity: $\mathbb{C}[\mathbb{F}_q]$ is a ring, so we know that convolution is associative.

Identity: Lemma 7.10 shows that $\vec{s}_0$ is the identity element.

Commutativity: Lemma 7.4.

Corollary 7.9 shows that not every element has an inverse, thus the vectors do not form a group. □

This result is weaker that that of Theorem 2.79, which finds a group.

Structure of bases of WF MUBs

We can look at the structure of the set of MUBs as a set of bases, rather than as a set of vectors.

There is the special case of $v_{0b}\hat{*}v_{0d} = \vec{0}$. According to the definition of $\hat{*}$, $\vec{0}$ represents all vectors. We could choose it to represent v_{00}.

Theorem 7.13. *The bases in a complete set of WF type MUBs, without B_0 form an Abelian group under $\hat{*}$.*

Proof. Associativity, Identity and Commutativity, are the same as for Theorem 7.12

Closure: Lemma 7.7 shows that the only way for $v_{ab}\hat{*}v_{cd} = v_{0f}$ is if $a = 0$. This then combined with closure in Theorem 7.12 provides closure in the group.

Inverse: Lemma 7.8. □

This is similar to Theorem 2.164 which finds that the Pauli matrix MUBs in odd dimensions without the standard basis forms a group. This adds further evidence to Conjecture 2.67, that the Pauli matrix MUBs in odd dimensions are equivalent to the WF MUBs.

Lemma 7.14. *Let B_a be the a^{th} base of WF type MUBs as generated by equation (2.79) and E the standard basis.*

For $a + c \neq 0$

$$B_a\hat{*}B_c = B_e \qquad e = c - c^2(a+c)^{-1}. \tag{7.38}$$

For $a + c = 0$, $c \neq 0$

$$B_a\hat{*}B_c = E. \tag{7.39}$$

$$B_a\hat{*}E = B_a. \tag{7.40}$$

$$B_0\hat{*}B_0 = B_0 \cup \{\vec{0}\}. \tag{7.41}$$

Proof. From Lemma 7.6 if $a + c \neq 0$ then $v_{ab}\hat{*}v_{cd} = v_{ef}$ with $e = c - c^2(a+c)^{-1}$ and $f = c(a+c)^{-1}(b-d) - d$. Thus e only depends on a and c, and hence $B_e \subseteq B_a\hat{*}B_c$.

Choose any $f \in \mathbb{F}_q$, then for fixed $a, c, (b-d)$, we can choose d such that $f = c(a+c)^{-1}(b-d) - d$. Thus $B_e \supseteq B_a\hat{*}B_c$.

Therefore $B_a\hat{*}B_c = B_e$.

Then use similar logic applied to Lemmas 7.8, 7.9 and 7.10. □

This result shows that the complete set of MUBs does not form a closed algebraic structure.

Corollary 7.15. *The bases in a complete set of WF type MUBs in union with* $\{B_0 \cup \{\vec{0}\}\}$ *form a commutative monoid under* $\hat{*}$.

7.3.3 Group ring structure of Alltop MUBs

All the previous results only apply to WF type MUBs. The same techniques are now applied to Alltop type MUBs.

Let A_a be the a^{th} base of the Alltop type MUBs as constructed using equation (2.81).

$$A_a = \{\vec{u}_{a0}, \vec{u}_{a1} \dots \vec{u}_{a(p-1)}\} \tag{7.42}$$

$$\vec{u}_{ab} = \left(\chi\left((x+b)^3 + a(x+b)\right)\right)_{x\in\mathbb{F}_q}. \tag{7.43}$$

Let $\xi := \vec{u}_{ab}\hat{*}\vec{u}_{cd}$, then

$$\xi_z = k\sum \chi\left((x+b)^3 + a(x+b) + (z-x+d)^3 + c(z-x+d)\right). \tag{7.44}$$

This then expands out to a polynomial $a_3x^3 + a_2x^2 + a_1x + a_0$,

$$a_3 = 0 \tag{7.45}$$

$$a_2 = 3(z+d+b) \tag{7.46}$$

$$a_1 = 3b^2 + a - 3(z+d)^2 - c \tag{7.47}$$

$$a_0 = b^3 + (z+d)^3 + ab + cz + cd \tag{7.48}$$

which can then be substituted into Theorem 2.33.

The coefficient a_2 is dependant on z, thus $\eta(a_2)$ is not a constant. Hence $\xi \neq \vec{u}_{ef}$ for any $e, f \in \mathbb{F}_q$. A cubic equation has at most three distinct roots, thus at most three positions in the vector ξ may be 0. Alltop type MUBs do not occur in dimensions less than 5, hence ξ is neither a standard basis vector nor $\vec{0}$.

Representing Alltop type MUBs as elements of a group ring does not result in a closed algebraic structure.

7.3.4 Group ring structure of Galois ring MUBs

Let G_a be the a^{th} base of Galois ring type MUBs in $\mathbb{C}^{2^r}$ constructed using equation (2.111)

$$G_a = \{\vec{v}_{a0}, \vec{v}_{a1} \dots \vec{v}_{a(p-1)}\} \tag{7.49}$$

$$\vec{v}_{ab} = (\chi((a+2b)x))_{x\in\mathcal{T}_r}. \tag{7.50}$$

Let v_{ab_z} be the z^{th} entry in vector $\vec{v}_{ab}$,

$$v_{ab_z} = \chi((a+2b)z). \tag{7.51}$$

We expand out the convolution product.

$$(\vec{v}_{ab}\hat{*}\vec{v}_{cd})_z = k\sum_{x+y=z} v_{ab_x}v_{cd_y} \tag{7.52}$$

$$= k\sum_{x\in\mathcal{T}_r} v_{ab_x}v_{cd_{z-x}} \tag{7.53}$$

$$= k\sum_{x\in\mathcal{T}_r} \chi((a+2b-c-2d)x + (c+2d)z) \tag{7.54}$$

$$= k\chi((c+2d)z)\sum_{x\in\mathcal{T}_r} \chi((a+2b-c-2d)x). \tag{7.55}$$

Using Lemma 2.57, the sum may only be explicitly calculated when $a+2b-c-2d \in 2\mathcal{T}_r$. Thus we cannot know if the Galois ring MUBs form a closed algebraic structure using $\hat{*}$. We have a computational example to show that it is possible. This is in contrast to using component-wise multiplication which does not work at all (Theorem 2.87).

7.4 Conclusion

7.4.1 Findings

A set of WF type MUBs, when represented as elements of the group ring $\mathbb{C}[\mathbb{F}_q]$, form a commutative monoid. A set of Alltop type MUBs does not form a similar closed algebraic structure. In Theorem 2.65 it is shown that that WF and Alltop MUBs are equivalent, thus the lack of a closed structure in the Alltop MUBs suggests that the monoid is a peculiarity of the WF type MUBs, and not a property of MUBs in general.

When a specific base is removed from a set of WF type MUBs a group is formed. This mirrors Theorem 2.67 which shows a similar result with the Pauli matrix MUBs in odd dimensions using component-wise multiplication.

Due to the lack of knowledge about character sums, it is not shown whether Galois ring type MUBs form an algebraic structure when represented as group ring elements.

7.4.2 Further Directions

When examined in Chapter 3 the WF and Alltop type MUBs both reveal MOLS, however the MOLS do not come from the vectors, but rather from differences between the vectors. Perhaps the same may be said for the monoid structure.

Question 7.16. *Is there an algebraic structure if the inner product vectors of a set of MUBs are represented as group ring elements?*

WF type MUBs are a special case of planar function MUBs. The monoid structure may occur in all sets of planar function MUBs. The group structure may also occur when a specific base is dropped from the set of MUBs.

Question 7.17. *Do all the planar function MUBs have similar algebraic properties?*

The Pauli matrix MUBs have not been investigated here. Perhaps there will be an algebraic structure. This may help to determine the equivalence of the WF and Pauli matrix MUBs.

Further knowledge of sums over Galois rings, may show an algebraic structure of the Galois ring MUBs.

Chapter 8

Conclusion

8.1 Findings

The research questions investigated in this thesis have been open for a number of years.

Research Question 8.1. *Are mutually unbiased bases intimately linked with mutually orthogonal Latin squares?*

It has been 7 years since the publication of the SPR conjecture [96], and even longer since a connection between finite geometries and MUBs was foreshadowed [112].

Research Question 8.2. *Do all complete sets of mutually unbiased bases have an algebraic structure?*

It has been 30 years since an algebraic structure (Galois field) was first used to construct a set of MUBs [59].

There are many research groups taking various approaches to these questions, and yet they are still open. In this thesis some significant progress has been made, which can be built upon to answer these questions in the future.

Complete sets of MOLS were constructed from two complete sets of MUBs. The MUBs tested are generated by a Galois field. The MOLS are also generated using a Galois field. This may have nothing to do with the MUB's structure, only the properties of Galois fields. The MOLS structure comes from the inner products of pairs of vectors, which in both cases can be described by a planar function. This shows that planar functions are not necessary to construct MUBs, but are sufficient in describing the angles between vectors.

Analogous properties of Hjelmslev planes and MUBs, and gaps in knowledge about Hjelmslev planes motivated investigation of Hjelmslev planes. The sub-structures of a Hjelmslev plane over a Galois ring, and a combinatorial algorithm for generating Hjelmslev planes were developed. The analogous properties of MUBs and conics in Hjelmslev planes are not valid in even dimensions, making a strong connection between MUBs and conics in Hjelmslev planes unlikely.

The planar function construction of MUBs was generalised by using an automorphism on the additive group of a Galois field. However it is unclear if this generalisation is non-equivalent to the original MUBs.

Relation algebras were constructed from the structure of MUBs which do not share any similarities with algebras constructed from projective planes. However we have not conducted an exhaustive investigation of relation algebras from the structure of MUBs.

A set of WF type MUBs, when represented as elements of the group ring $\mathbb{C}[\mathbb{F}_q]$, form a commutative monoid. A set of Alltop type MUBs when similarly represented does not form a closed algebraic structure. In Theorem 2.65 it is shown that that WF and Alltop MUBs are equivalent, thus the lack of a closed structure in the Alltop MUBs suggests that the monoid is a peculiarity of the WF type MUBs, and not a property of MUBs in general.

Complete sets of MOLS and complete sets of MUBs are 'similar in spirit', but perhaps this is not an inherent feature of MUBs and MOLS. All the known constructions of MUBs rely on algebraic structures which exist only in prime power dimensions. The connection may not be with MOLS, but with the algebraic structures which generate both MOLS and MUBs.

8.2 Implications for applications

The applications of MUBs rely on complete sets of MUBs; we have neither found new complete sets nor shown the non-existence of complete sets of MUBs. Thus the results on MUBs have no immediate practical implications.

The generalised planar function construction of MUBs may be used if it can be shown that it provides new sets of MUBs.

The new results on Hjelmslev planes have implications for the applications of Hjelmslev planes, such as constructing codes over rings.

8.3 Further directions

This research has not answered either of the two research questions, but has provided results in many directions. Many specific questions have been raised that give directions for future research.

Planar functions are not necessary in constructing the vectors of a set of MUBs, as in the planar construction, but are sufficient in describing the angles between the vectors, as in both Alltop and planar function constructions.

Question 8.3. *Are there sets of vectors which cannot be constructed by planar functions, but the angles between the vectors can be described by planar functions?*

The Alltop construction may be unique in this respect. In even dimensions planar functions cannot be used, but a differentially 1-uniform function has been shown to construct MUBs in even prime power dimensions.

Question 8.4. *Are there sets of vectors which cannot be constructed by differentially* 1*-uniform functions, but the angles between the vectors can be described by differentially* 1*-uniform functions?*

Hjelmslev planes are a largely unexplored structure. There are many aspects of Hjelmslev planes which have not been investigated.

Question 8.5. *What are the permissible neighbourhood structures of a Hjelmslev plane?*

Question 8.6. *For what sizes do non-uniform Hjelmslev planes exist?*

The applications of Hjelmslev planes are only just emerging. The SP analogy regarding conics in Hjelmslev planes does not hold in even dimensions making a deep connection unlikely. There are many unexplored aspects of Hjelmslev planes which may have stronger connections.

Question 8.7. *Can a Hjelmslev plane be used to construct mutually unbiased bases?*

We already know the answer is yes in two special cases, as planar functions construct projective planes which are trivial Hjelmslev planes, and Galois rings construct both Hjelmslev planes and MUBs in even dimensions. There are many different Hjelmslev planes, constructed using different algebraic structures, for which no connection with MUBs has yet been established.

There is still much to be done looking at the equivalences of constructions of MUBs. Conjecture 2.67 and Corollary 2.68 suggest the Pauli matrix MUBs are a different method for constructing the WF and Galois ring MUBs. The generalised planar function construction is yet to be shown to be equivalent or non-equivalent to the planar function construction of MUBs.

Question 8.8. *Can non-equivalent sets of MUBs be generated from the same planar function?*

More knowledge about character sums would enable an algebraic test for equivalence. Explicit computation of examples may show that there are non-equivalent MUBs which are based on the same planar function.

The relation algebras that were constructed from the structure of sets of MUBs are not the only possible relation algebras. Different constructions may yield a relation algebra with similarities to the relation algebras constructed from MOLS.

Question 8.9. *What relational algebra structures can be constructed from a complete set of MUBs?*

When examined in Chapter 3 the WF and Alltop type MUBs both reveal MOLS, however the MOLS do not come from the vectors, but rather from differences between the vectors. Perhaps the same may be said for the monoid structure. There may be a monoid when differences between the vectors of Alltop MUBs are examined.

Question 8.10. *Is there an algebraic structure if the inner product vectors of a set of MUBs are represented as group ring elements?*

WF type MUBs are a special case of planar function MUBs. The monoid structure may occur in all sets of planar function MUBs.

Question 8.11. *Do all the planar function MUBs have similar algebraic properties?*

Computation showed a commutative monoid for the Galois ring MUBs in small dimensions. This may be the case more generally.

It would seem from the volume of research, that finding MUBs is a hard problem; a problem that will require many small results, before it is completely solved.

Index

Bibliography

[1] W.O. Alltop. Complex sequences with low periodic correlations. *IEEE Transactions on Information Theory*, 26(3):350–354, 1980.

[2] D.M. Appleby. *Foundations of Probability and Physics-5*, chapter SIC-POVMS and MUBs: Geometrical Relationships in prime dimensions, pages 223–232. Number 1101 in AIP Conference proceedings. AIP, 2008.

[3] C Archer. There is no generalization of known formulas for mutually unbiased bases. *Journal of Mathematical Physics*, 46(022106), 2005.

[4] R.A. Bailey, P.J. Cameron, P. Dobcsànyi, J.P. Morgan, and L.H. Soicher. *DesignTheory.org*. U.K. Engineering and Physical Sciences Research Council, `http://designtheory.org`, updated on 2009-09-17.

[5] 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.

[6] M. Le Bellac. *A Short Introduction to Quantum Information and Quantum Computation*. Cambridge University Press, 2006.

[7] I. Bengtsson. Three ways to look at mutually unbiased bases. *arXiv:quant-ph*, 0610216v1, 2006.

[8] I. Bengtsson, W. Bruzda, Å. Ericsson, J. Larsson, W. Tadej, and K. Życzkowski. Mutually unbiased bases and Hadamard matrices of order six. *Journal of Mathematical Physics*, 48(052106):1–21, 2007.

[9] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[10] D. Best and H. Kharaghani. Unbiased complex Hadamard matrices and bases. *Cryptography and Communications*, 2:199–209, 2010.

[11] T. Beth, D. Jungnickel, and H. Lenz. *Design Theory: Volume 1*. Cambridge University Press, second edition, 1999.

[12] A. Blokhuis, D. Jungnikel, and B. Schmidt. Proof of the prime power conjecture for projective planes of order n with Abelian collineation groups of order n^2. *Proceedings of the American Mathematical Society*, 130:1473–1476, 2002.

[13] H. Bohr. Johannes Hjelmslev in memoriam. *Acta Mathematica*, 83(1):vii–ix, 1964.

[14] G. Boole. *The Laws of Thought*. Chicago: Open Court Publishing Company, reprint of *An investigation of the laws of thought, on which are founded the mathematical theories of logic and probabilities*, 1854 edition, 1916.

[15] S. Brierley, S. Weigert, and I. Bengtsson. All mutually unbiased bases in dimensions two to five. *Quantum Information and Computing*, 10(9):803–820, 2010.

[16] R.H. Bruck and H.J. Ryser. The nonexistence of certain finite projective planes. *Canadian Journal of Mathematics*, 1:88–93, 1949.

[17] D. Bruß. Optimal eavesdropping in quantum cryptography with six states. *Physical Review Letters*, 81(14):30183021, 1998.

[18] P. Butterley and W. Hall. Numerical evidence for the maximum number of mutually unbiased bases in dimension six. *Physics Letters A*, 369(1):5–8, 2007.

[19] C. Carlet. *Coding theory, Cryptography and Related Areas*, chapter One-weight Z_4-linear codes, pages 57–72. Springer, Berlin, 2000.

[20] C. Carlet and C. Ding. Highly nonlinear mappings. *Journal of Complexity*, 20:205–244, 2004.

[21] N. Cerf, M. Bourenname, A. Karlsson, and N. Gisin. Security of quantum key distribution using d-level systems. *Physics Review Letters*, 88(127902):1–4, 2002.

[22] V. Chvàl and R. Jurga. Tangents of conics in Hjelmslev planes over a local ring of even characteristic. *Mathematica Slovaca*, 48(1):69–78, 1998.

[23] C.J. Colbourn and J.H. Dinitz, editors. *Handbook of Combinatorial Designs*. Chapman and Hall/CRC Press, second edition, 2007.

[24] C.J. Colbourn, T. Kløve, and A.C.H. Ling. Permutation arrays for powerline communication and mutually orthogonal Latin squares. *IEEE Transactions on Information Theory*, 50(6):1289–1291, 2004.

[25] M. Combescure. Block-circulant matrices with circulant blocks, Weil sums, and mutually unbiased bases. II. The prime power case. *Journal of Mathematical Physics*, 50:032104, 2009.

[26] R.S. Coulter and R.W. Matthews. Bent polynomials over finite fields. *Bulletin of the Australian Mathematical Society*, 56(3):429–437, 1997.

[27] R.S. Coulter and R.W. Matthews. Planar functions and planes of Lenz-Barlotti class II. *Designs, Codes and Cryptography*, 10(2):167–184, 1997.

[28] A. Cronheim. Dual numbers, Witt vectors and Hjelmslev planes. *Geometriae Dedicata*, 7(3):287–302, 1978.

[29] J. Delahaye. The Science behind Sudoku. *Scientific American*, 294:80–87, June 2006.

[30] P. Dembowski. *Finite Geometries*. Classics in Mathematics. Springer, reprint of the 1968 edition, 1997.

[31] P. Dembowski and T.G. Ostrom. Planes of order n with collineation groups of order n^2. *Mathematische Zeitschrift*, 103(3):239–258, 1968.

[32] C. Ding and J. Yuan. A family of skew Hadamard difference sets. *Journal of Combinatorial Theory, Series A*, 113:1526–1535, 2006.

[33] D.A. Drake. On n-uniform Hjelmslev planes. *Journal of Combinatorial Theory*, 9:267–288, 1970.

[34] D.A. Drake. Near affine Hjemslev planes. *Journal of Combinatorial Theory (A)*, 16:34–50, 1974.

[35] D.A. Drake. Existence of parallelisms and projective extensions for strongly n-uniform near affine Hjelmslev planes. *Geometriae Dedicata*, 3(2):191–214, 1974.

[36] D.A. Drake. Nonexistence results for finite Hjelmslev planes. *Abhandlungen aus dem Mathematischen Seminar der Universitt Hamburg*, 40:100–110, 1974.

[37] D.A. Drake. Constructions of Hjelmslev planes. *Journal of Geometry*, 10(1):179–193, 1977.

[38] D.A. Drake and E.E. Shult. Construction of Hjelmslev planes from (t, k) nets. *Geometriae Dedicata*, 5(3):377–392, 1976.

[39] J.V. Field. *The MacTutor history of mathematics archive*. University of St Andrews, Scotland, `http://www-history.mcs.st-andrews.ac.uk/`, updated on 2011-04-01.

[40] J.B. Fraleigh. *A First Course in Abstract Algebra*. Addison-Wesley, sixth edition, 1999.

[41] K.S. Gibbons, M.J. Hoffman, and W.K. Wootters. Discrete phase space based on finite fields. *Physical Review A*, 70(062101):1–23, 2004.

[42] C. Godsil and A. Roy. Equiangular lines, mutually unbiased bases, and spin models. *European Journal of Combinatorics*, 30(1):246–262, 2009.

[43] A. Granville and K. Soundararajan. Large character sums: Pretentious characters and the Pólya-Vinogradov theorem. *Journal of the American Mathematical Society*, 20:357–384, 2007.

[44] M. Grassl. On SIC-POVMs and MUBs in Dimension 6. In *Proceedings of the 2004 ERATO Conference on Quantum Information Science*, pages 60–68, 2004. Arxiv: 0406175v2.

[45] J.L. Hall and A. Rao. Constructing a 2-uniform projective Hjelmslev plane. *Submitted*.

[46] J.L. Hall and A. Rao. The algebraic structure of mutually unbiased bases. In *International Symposium on Information Theory and its Applications*. SITA, IEEE, 2008.

[47] J.L. Hall and A. Rao. Mutually orthogonal Latin squares from the inner products of vectors in mutually unbiased bases. *Journal of Physics A*, 43(13):135302, 2010.

[48] J.L. Hall and A. Rao. Comment on 'Mutually Unbiased Bases, orthogonal Latin squares, and hidden-variable models'. *Physical Review A*, 83(036101):1–2, 2011.

[49] P. Halmos. *Naive set theory*. The university series in undergraduate mathematics. Van Nostrand, Princeton, N.J, 1960.

[50] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, and P. Sole. The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes. *IEEE Transactions on Information Theory*, 40(2):301–319, 1994.

[51] Y. Hiramine. On planar functions. *Journal of Algebra*, 133:103–110, 1990.

[52] R. Hirsch and I. Hodkinson. *Relation Algebras by Games*, volume 147 of *Studies in Logic and the Foundations of Mathematics*. Elsevier, 2002.

[53] J. Hjelmslev. Die Geometrie der Wirklichkeit. *Acta Mathematica*, 40(1):35–66, 1916. German.

[54] S.G. Hoggar. t-Designs with general angle set. *European Journal of Combinatorics*, 13:257–271, 1992.

[55] T. Honold and I. Landjev. On arcs in projective Hjelmslev planes. *Discrete Mathematics*, 231(1-3):265–278, 2001.

[56] T. Honold and I. Landjev. *Codes Over Rings*, volume 6 of *Series on Coding Theory and Cryptology*, chapter Linear codes over finite chain rings and projective Hjelmslev geometries, pages 60–124. World Scientific, 2009.

[57] K.J. Horadam. *Hadamard Matrices and Their Applications*. Princeton University Press, Princeton, New Jersey, 2007.

[58] D.R. Hughes and F.C. Piper. *Projective Planes*. Springer-Verlag, New York, 1973.

[59] I.D. Ivanovic. Geometrical description of quantal state determination. *Journal of Physics A: Mathematical and General*, 14:3241–3245, 1981.

[60] P. Jaming, M. Matolcsi, and P. Móra. The problem of mutually unbiased bases in dimension 6 . *Cryptography and Communications*, 2(2):211–220, 2010.

[61] P. Jaming, M. Matolcsi, P. Móra, F. Sz ollösi, and M. Weiner2. A generalized Pauli problem and an infinite family of MUB-triplets in dimension 6 . *Journal of Physics A: Mathematical and Theoretical*, 42(245305):1–26, 2009.

[62] J.L.Massey and T. Mittelholzer. *Sequences II : methods in communication, security and computer science*, chapter Welch's bound and sequence sets for code-division multiple-access systems, pages 63–78. Springer-Verlag, New York, 1993.

[63] D. Keppens. Polarities in finite 2-uniform projective Hjelsmlev planes. *Geometriae Dedicata*, 24(1):51–76, 1987.

[64] A. Klappenecker and M. Rötteler. Constructions of mutually unbiased bases. *Lecture Notes in Computer Science*, 2948:137–144, 2003.

[65] A. Klappenecker and M. Rötteler. Mutually unbiased bases are complex projective 2-designs. In *Proceedings. International Symposium on Information Theory*, pages 1740–1744. ISIT 2005, IEEE, September 2005.

[66] E. Kleinfeld. Finite Hjelmslev planes. *Illinois Journal of Mathematics*, 3(3):403–407, 1959.

[67] A.B. Klimov, C. Muñoz, and J.L. Romero. Geometrical approach to the discrete Wigner function in prime power dimensions. *Journal of Physics A: Mathematical and General*, 39(46):14471–14497, 2006.

[68] W. Klingenberg. Projektive und affine Ebenen mit Nachbarelementen. *Mathematische Zeitschrift*, 60(1):384, 1954. German.

[69] W. Klingenberg. Desarguessche Ebenen mit Nachbarelemten. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 20(1-2):97–111, 1955. German.

[70] A. Kreuzer. *Projective Hjelmslev-Räume*. PhD thesis, Technische Universität München, 1988. German.

[71] A. Kreuzer. A system of axioms for projective Hjelmslev spaces. *Journal of Geometry*, 40(1-2):125–147, 1991.

[72] P.V. Kumar, R.A. Scholtz, and L.R. Welch. Generalized bent functions and their properties. *Journal of Combinatorial Theory, Series A*, 40(1):90–107, 1985.

[73] C.W.H. Lam. The Search for a Finite Projective Plane of Order 10. *The American Mathematical Monthly*, 98(4):305–318, 1991.

[74] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer, New York, revised third edition, 2002.

[75] D.C. Lay. *Linear Algebra and it Applications*. World Student Series. Addisson-Wesley Publishing Company, second edition, 2000.

[76] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, second edition, 1997.

[77] H. Lüneberg. Affine Hjelmslev-Ebenen mit transitiver Translationsgruppe. *Mathematische Zeitschrift*, 79(1):260–288, 1962. German.

[78] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*, 4:686–689, 2010.

[79] R.C. Lyndon. Relation algebras and projective geometries. *Michigan Mathematics Journal*, 8(1):21–28, 1961.

[80] H.F. MacNeish. Euler squares. *The Annals of Mathematics*, 23(3):221–227, 1922.

[81] F.J. Macwilliams and N.J. Sloane. *The Theory of Error Correcting Codes*. Elsevier Science, 1977.

[82] R.D. Maddux. *Relation Algebras*, volume 150 of *Studies in Logic and the Foundations of Mathematics*. Elsivier, 2006.

[83] A. De Morgan. On the syllogism, no IV, and on the logic of relations. *Transactions of the Cambridge Philosophical Society*, 10:331–358, 1860.

[84] M.A. Nielsen and I.L. Chuang. *Quantumn Computation and Quantum Information*. Cambridge University Press, 2000.

[85] T. Paterek, B. Dakić, and Č. Brukner. Mutually unbiased bases, orthogonal Latin squares, and hidden-variable models. *Physical Review A*, 79(012109):1–6, 2009.

[86] T. Paterek, M. Pawlowski, M. Grassl, and Č. Brukner. On the connection between mutually unbiased bases and orthogonal Latin squares. *Physica Scripta*, 2010(014031):1–4, 2010.

[87] A. Peres. *Quantum Theory: Concepts and Methods*, volume 72 of *The Fundemental Theories of Physics*. Kluwer Academic Publishers, Dordecht, 1998.

[88] C.S. Pierce. *Writings of Charles S. Peirce : a chronological edition*, volume 4, chapter Note B: the logic of relatives, pages 453–466. Bloomington : Indiana University Press, 2000. Original publication, *Studies in Logic by members of the John Hopkins University*. Boston : Little, Brown and Co, 1883.

[89] A. Pott. *Finite Geometry and Character Theory*, volume 1601 of *Lecture Notes in Mathematics*. Springer, 1995.

[90] A. Rao, D. Donovan, and J.L. Hall. Mutually orthogonal Latin squares and mutually unbiased bases in dimensions of odd prime power. *Cryptography and Communications*, 2(2):221–231, 2010.

[91] J.M. Renes, R. Blume-Kohout, A.J. Scott, and C.M. Caves. Symmetric informationally complete quantum measurements. *Journal of Mathematical Physics*, 45(6):2171–2180, 2004.

[92] R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[93] A. Roy and A.J. Scott. Weighted complex projective 2-designs from bases: Optimal state determination by orthogonal measurements. *Journal of Mathematical Physics*, 48(072110):1–24, 2007.

[94] M. Saniga and M. Planat. Viewing sets of mutually unbiased bases as arcs of finite projective planes. *Chaos Solutions and Fractals*, 26(5):1267–1270, 2005.

[95] M. Saniga and M. Planat. Hjelmslev geometry of mutually unbiased bases. *Journal of Physics A: Mathematical and General*, 39(2):435–440, 2006.

[96] M. Saniga, M. Planat, and H. Rosu. Mutually unbiased bases and finite projective planes. *Journal of Optics B: Quantum and Semiclassical Optics*, 6:L19–L20, 2004.

[97] V. Scarani, A. Ac̆in, G. Ribordy, and N. Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical Review Letters*, 92(057901):1–4, 2004.

[98] F.W.K. Ernst Schröder. *Vorlesungen ber die Algebra der Logik : Exakte Logik. Vol. 3, Algebra und Logik der Relative*. Leipzig : B. G. Teubner, 1895. German.

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

[100] A.J. Scott and M. Grassl. Symmetric informationally complete positive-operator-valued measures: A new computer study. *Journal of Mathematical Physics*, 51(042203):1–16, 2010.

[101] N.J.A. Sloane. *A Library of Orthogonal Arrays*. `http://www2.research.att.com/~njas/oadir/`, Updated 2007.

[102] A. Penfold Street and D. J. Street. *Combinatorics of Experimental Design*. Oxford Science Publications. Oxford University Press, Oxford, 1987.

[103] P. Suppes. *Axiomatic set theory*. The University series in undergraduate mathematics. New York : Dover Publications, 1960.

[104] L.N. Trefethen and D. Bau III. *Numerical Linear Algebra*. Society for Industrial and Applied Mathematics, Philadelphia, 1997.

[105] J.D. Trimmer. The present situation in quantum mechanics: A translation of Schrödinger's 'cat paradox' paper. *Proceedings of the American Philosophical Society*, 124(5):323–338, 1980.

[106] F.D. Veldkamp. *Handbook of Incidence Geometry*, chapter Geometry over rings, pages 1033– 1084. Elsevier Science, 1995.

[107] Z.X. Wan. *Lectures on finite fields and Galois rings*. World Scientific, New Jersey, 2003.

[108] S. Weigert and T. Durt. Affine constellations without mutually unbiased counterparts. *Journal of Physics A: Mathematical and Theoretical*, 43(402002):1–8, 2010.

[109] L.R. Welch. Lower bounds on the maximum cross correlation of signals. *IEEE Transactions on Information Theory*, 20(3):397–399, 1974.

[110] P. Wocjan and T. Beth. New construction of mutually unbiased bases in square dimensions. *Quantum Information and Computing*, 5(2):93–101, March 2005.

[111] W. Wootters. Quantum measurements and finite geometry. *Foundations of Physics*, 36(1):112–126, 2006.

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

[113] P. Xia, S. Zhou, and G.B. Giannakis. Achieving the Welch bound with difference sets. *IEEE Transactions on Information Theory*, 51(5):1900–1907, 2005.

[114] K. Yang, T. Helleseth, P.V. Kumar, and A.G. Shanbhag. On the wieght hierarchy of Kerdock codes over Z_4. *IEEE Transactions on Information theory*, 42(5):1587–1593, 1996.

[115] J. Yuan, C. Carlet, and C. Ding. The weight distribution of a class of linear codes from perfect nonlinear functions. *IEEE Transactions on Information Theory*, 52(2):712–717, 2006.

[116] G. Zauner. *Quantendesigns*. PhD thesis, Universitat Wien, 1999. German.