CARLETON UNIVERSITY

SCHOOL OF
MATHEMATICS AND STATISTICS

HONOURS PROJECT

TITLE: Mutually Unbiased Bases

AUTHOR: Abrar Kazi

SUPERVISOR: Jason Crann

DATE: August 25, 2020

Mutually Unbiased Bases

Abrar Kazi

August 25, 2020

Abstract

Two orthonormal bases E and F of $\mathbb{C}^d$ are mutually unbiased if $|\langle e, f\rangle|^2 = \frac{1}{d}, \forall e \in E, f \in F$. A set of mutually unbiased bases (MUBs) is a set of pairwise mutually unbiased orthonormal bases. We give a proof of the main result concerning MUBs, that there are $d+1$ of them in $\mathbb{C}^d$ for any prime power d, using the approach of matrix algebras and the symplectic geometry of finite fields.

1 Introduction

Definition 1 *Two orthonormal bases $E = \{e_0, \ldots, e_{d-1}\}$ and $F = \{f_0, \ldots, f_{d-1}\}$ of $\mathbb{C}^d$ are mutually unbiased if*

$$|\langle e_i, f_j\rangle|^2 = \frac{1}{d}, \forall i, j = 0, \ldots, d-1.$$

A set of orthonormal bases is mutually unbiased if it is pairwise mutually unbiased, and we refer to the bases as MUBs.

Several methods are known for constructing MUBs. In [6], a direct construction is given using Weil sums and exponential sums to handle the cases of odd and even prime power dimensions respectively. The theory of difference sets can also be applied to construct MUBs, and it has been shown that if there exists a semi-regular (d, m, d, λ)-relative difference set, then there exists a collection of $m+1$ MUBs in $\mathbb{C}^d$ [4].

In this paper we present a proof of the main existence result of MUBs in finite-dimensional Hilbert spaces:

Theorem 1 *If $d = p^n$, where p is a prime and n is a positive integer, then there is a collection of $d+1$ MUBs in $\mathbb{C}^d$.*

We prove the result using the approach of matrix algebras and the symplectic geometry of finite fields. In Section 2, we gather some preliminary definitions and results. Our proof begins in Section 3 with some useful results about Maximal Abelian *-Subalgebras (*-MASAs) of matrix algebras. Section 4 shows how *-MASAs can be used to construct MUBs. Section 5 shows how the Weyl representation can be used to generate *-MASAs from subgroups of certain finite

groups. Finally, section 6 proves existence results about the required subgroups, with the aid of finite fields, completing the proof of Theorem 1.

One application of mutually unbiased bases to quantum information is to perform optimal state-determination. Determining a mixed quantum state in $\mathbb{C}^d$ requires measurements with respect to at least $d+1$ bases, and if these bases are mutually unbiased, then the uncertainty of the measured state is minimized [10]. Another application is for determining whether a system of quantum states is entangled. If $d+1$ MUBs exist is $\mathbb{C}^d$, they can be used to guarantee whether or not the system is entangled. Even just two MUBs provide a more robust test for entanglement than other methods, such as the use of Bell inequalities, and can be used to identify maximally entangled states up to a noise threshold of 50% [9]. MUBs are also related to complex Hadamard matrices. Notions of equivalence can be defined for both MUBs and Hadamard matrices, and two MUBs are equivalent if and only if their corresponding Hadamard matrices are equivalent [1].

2 Preliminaries

We assume the reader is familiar with linear algebra in complex inner product spaces at the level of [5].

The adjoint A^* of a matrix (or vector) A is its conjugate transpose. The inner product on $\mathbb{C}^d$ is $\langle v_1, v_2\rangle = v_1^* v_2$. We will sometimes use bra-ket notation, where $|v\rangle = v$ and $\langle v| = v^*$.

A *-algebra will always refer to a unital subalgebra of $M_d(\mathbb{C})$, for some $d \in \mathbb{N}$, closed under the adjoint operation. The following definitions will concern matrices from such algebras.

The standard inner product on $M_d(\mathbb{C})$ is the Hilbert-Schmidt inner product, defined by $\langle A, B\rangle = tr(A^*B)$.

A normal matrix A is one that commutes with its adjoint: $A^*A = AA^*$. A unitary matrix A is one that satisfies $A^* = A^{-1}$, or equivalently $\langle Ae_i|Ae_j\rangle = \delta_{ij}$.

A subalgebra $\mathcal{A}$ is maximal abelian if it is not properly contained in a larger abelian algebra. A representation $\phi : G \to M_d(\mathbb{C})$ is a group homomorphism from a finite group to a matrix algebra. A representation is unitary if $\phi(g)$ is unitary $\forall g \in G$. We write $\langle \mathcal{S}\rangle$ to denote the algebra generated by a set $\mathcal{S}$.

If $\mathcal{S} \subseteq M_d(\mathbb{C})$ then its commutant is $\mathcal{S}' = \{A \in M_d(\mathbb{C}) : AS = SA, \forall S \in \mathcal{S}\}$, the set of matrices which commute with all elements of $\mathcal{S}$. Its bicommutant is $\mathcal{S}'' = (\mathcal{S}')'$.

Proposition 2 *If $\mathcal{A}$ is an algebra such that $\mathcal{A} = \mathcal{A}'$, then it is maximal abelian.*

Proof. Let $\mathcal{B}$ be an abelian algebra with $\mathcal{A} \subseteq \mathcal{B}$. Let $B \in \mathcal{B}$ and $A \in \mathcal{A}$. Since A is also in $\mathcal{B}$, A and B commute. The choice of A was arbitrary, so $AB = BA, \forall A \in \mathcal{A}$, which implies $B \in A' = A$. Thus, $\mathcal{B} \subseteq \mathcal{A}$ and $\mathcal{A} = \mathcal{B}$. □

Proposition 3 *For any set $\mathcal{S}$, $\mathcal{S}' = \langle S\rangle'$.*

Proof. Since $\mathcal{S} \subseteq \langle \mathcal{S} \rangle$, if B commutes with all elements of $\langle \mathcal{S} \rangle$, then it commutes with all elements of S, so $\langle \mathcal{S} \rangle' \subseteq \mathcal{S}'$. Conversely, suppose B commutes with all elements $\mathcal{S}$, and let $A \in \langle \mathcal{S} \rangle$ be arbitrarily chosen. Since $\mathcal{S}$ generates $\langle \mathcal{S} \rangle$, $A = \sum_{i=1}^{n} A_{i,1} \dots A_{i,m_n}$, where $A_{i,j} \in \mathcal{S}$. Then

$$AB = \left(\sum_{i=1}^{n} A_{i,1} \dots A_{i,m_i} \right) B = \sum_{i=1}^{n} A_{i,1} \dots A_{i,m_i} B = \sum_{i=1}^{n} A_{i,1} \dots B A_{i,m_i}$$
$$= \dots = \sum_{i=1}^{n} B A_{i,1} \dots A_{i,m_i} = B \left(\sum_{i=1}^{n} A_{i,1} \dots A_{i,m_i} \right) = BA,$$

so B commutes with all elements of $\langle S \rangle$. Thus, $\mathcal{S}' \subseteq \langle \mathcal{S} \rangle'$, and $\mathcal{S}' = \langle S \rangle'$. $\square$

As seen in the proof above, if a claim holds for the generating set of an algebra, it will often hold for the entire algebra. This concept is used implicitly throughout this paper.

The tensor product of $A \in M_{d_1}(\mathbb{C})$ and $B \in M_{d_2}(\mathbb{C})$ is an operator $A \otimes B \in M_{d_1}(\mathbb{C}) \otimes M_{d_2}(\mathbb{C}) \cong M_{d_1 d_2}(\mathbb{C})$. $\mathcal{A}^{\otimes n}$ is a tensor space produced by taking the tensor product of n copies of $\mathcal{A}$. The tensor product is bilinear and associative. One can easily verify that $(A \otimes B)(C \otimes D) = (AB \otimes CD)$ and $(A \otimes B)^* = A^* \otimes B^*$, so multiplication and adjoint of tensor products are performed componentwise.

The trace of a matrix $A \in M_d(\mathbb{C})$ is $tr(A) = \sum_{k=0}^{d-1} \langle e_k, Ae_k \rangle$, where $e_0, \dots, e_{d-1}$ is any orthonormal basis of C^d (trace is independent of basis choice). A useful fact about the trace is that $tr(AB) = tr(BA)$ for any matrices A and B (not necessarily square) such that AB and BA are well defined.

3 Maximal Abelian *-Subalgebras

Definition 2 *Let $E = \{e_0, \dots, e_{d-1}\}$ be a basis for $\mathbb{C}^d$. Let $\boldsymbol{\lambda} = (\lambda_0, \dots, \lambda_{d-1}) \in \mathbb{C}^d$. Then $diag_E(\boldsymbol{\lambda}) : \mathbb{C}^d \to \mathbb{C}^d$ is the linear operator with eigenvectors $e_0, \dots, e_{d-1}$ and corresponding eigenvalues $\lambda_0, \dots, \lambda_{d-1}$ (i.e. $diag_E(\boldsymbol{\lambda})$ is diagonalizable with respect to basis E). We write $diag_E(\mathbb{C}^d) = \{diag_E(\boldsymbol{\lambda}) : \boldsymbol{\lambda} \in \mathbb{C}^d\}$.*

The elements of $diag_E(\mathbb{C}^d)$ have the following properties:

1. $diag_E(\boldsymbol{\lambda}) + diag_E(\boldsymbol{\lambda}') = diag_E(\boldsymbol{\lambda} + \boldsymbol{\lambda}')$
2. $c \cdot diag_E(\boldsymbol{\lambda}) = diag_E(c\boldsymbol{\lambda})$
3. $diag_E(\boldsymbol{\lambda}) diag_E(\boldsymbol{\lambda}') = diag_E(\boldsymbol{\lambda}\boldsymbol{\lambda}')$, where $\boldsymbol{\lambda}\boldsymbol{\lambda}' = (\lambda_0 \lambda_0', \dots, \lambda_{d-1} \lambda_{d-1}')$

Thus, $diag_E(\mathbb{C}^d)$ is a subalgebra of $M_d(\mathbb{C})$. Furthermore, it is abelian by property 3 since $\boldsymbol{\lambda}\boldsymbol{\lambda}' = \boldsymbol{\lambda}'\boldsymbol{\lambda}$.

Lemma 4 *If $\mathcal{A}$ is a *-MASA of $M_d(\mathbb{C})$, then $\mathcal{A} = diag_E(\mathbb{C}^d)$ for some orthonormal basis E.*

Proof. First, we show all elements of $\mathcal{A}$ are normal. Let $A \in \mathcal{A}$. Since $\mathcal{A}$ is a *-algebra, $A^* \in \mathcal{A}$, and since $\mathcal{A}$ is abelian, $AA^* = A^*A$, so A is normal. Now let $\{A_1, \ldots, A_k\}$ be a basis for $\mathcal{A}$. Since $A_1, \ldots, A_k$ are normal and commute, there exists an orthonormal basis E of $\mathbb{C}^d$ such that $A_1, \ldots, A_k$ can be simultaneously diagonalized with respect to E [2], so $A_1, \ldots, A_k \in diag_E(\mathbb{C}^d)$. Since $\{A_1, \ldots, A_k\}$ spans $\mathcal{A}$, $\mathcal{A} \subseteq diag_E(\mathbb{C}^d)$. On the other hand, Since $\mathcal{A}$ is maximal abelian, $\mathcal{A} = diag_E(\mathbb{C}^d)$ □

By Lemma 4, if we refer to $diag_E(\mathbb{C}^d)$ as a *-MASA, it is understood that E is an orthonormal basis of $\mathbb{C}^d$.

Lemma 5 *If $E = \{e_0, \ldots, e_{d-1}\}$ is an orthonormal basis of $\mathbb{C}^d$, then $diag_E(\mathbb{C}^d) =$*

$span\{|e_i\rangle\langle e_i| : 0 \leq i \leq d-1\}$

Proof. First note that

$$\left(\sum_{i=0}^{d-1} \lambda_i |e_i\rangle\langle e_i|\right) |e_j\rangle = \sum_{i=0}^{d-1} \lambda_i \langle e_i|e_j\rangle |e_i\rangle = \lambda_j |e_j\rangle, \forall j = 0, \ldots, d-1,$$

so by definition,

$$diag_E(\lambda_0, \ldots, \lambda_{d-1}) = \sum_{i=0}^{d-1} \lambda_i |e_i\rangle\langle e_i|.$$

Then

$$\begin{aligned} diag_E(\mathbb{C}^d) &= \{diag_E(\boldsymbol{\lambda}) : \boldsymbol{\lambda} \in \mathbb{C}^d\} \\ &= \left\{\sum_{i=0}^{d-1} \lambda_i |e_i\rangle\langle e_i| : (\lambda_0, \ldots, \lambda_{d-1}) \in \mathbb{C}^d\right\} \\ &= span\{|e_i\rangle\langle e_i| : 0 \leq i \leq d-1\}. \end{aligned}$$

□

4 From Quasi-orthogonal *-MASAs to Mutually Unbiased Bases

Definition 3 *Two subalgebras $\mathcal{A}, \mathcal{B}$ of $M_d(\mathbb{C})$ are quasi-orthogonal if $\mathcal{A} \ominus \mathbb{C}I \perp \mathcal{B} \ominus \mathbb{C}I$, where $\mathcal{A} \ominus \mathbb{C}I = \{A \in \mathcal{A} : \langle I, A\rangle = tr(A) = 0\}$.*

Now we show how *-MASAs that are quasi-orthogonal give rise to MUBs.

Lemma 6 *If E is an orthonormal basis of $\mathbb{C}^d$, then*

$$diag_E(\mathbb{C}^d) \ominus \mathbb{C}I = span\{|e_i\rangle\langle e_i| - \frac{1}{d}I\}.$$

Proof. Let $\mathcal{A} = diag_E(\mathbb{C}^d) \ominus \mathbb{C}I = \{A \in diag_E(\mathbb{C}^d) : \langle I, A\rangle = tr(A) = 0\}$. Then since $diag_E(\mathbb{C}^d) = span\{|e_i\rangle\langle e_i| : 0 \leq i \leq d-1\}$ by Lemma 5, $\mathcal{A} = span\{proj_{\mathcal{A}}(|e_i\rangle\langle e_i|) : 0 \leq i \leq d-1\}$, where $proj_{\mathcal{A}}$ is the projection onto $\mathcal{A}$, treating $M_d(\mathbb{C})$ as a Hilbert space under the Hilbert-Schmidt inner product.

We will show that $proj_{\mathcal{A}}(|e_i\rangle\langle e_i|) = |e_i\rangle\langle e_i| - \frac{1}{d}I$. Note that $|e_i\rangle\langle e_i| = (|e_i\rangle\langle e_i| - \frac{1}{d}I) + \frac{1}{d}I$. We show that $|e_i\rangle\langle e_i| - \frac{1}{d}I \in \mathcal{A}$. Since $|e_i\rangle\langle e_i|, I \in diag_E(\mathbb{C}^d)$, $|e_i\rangle\langle e_i| - \frac{1}{d}I \in diag_E(\mathbb{C}^d)$. Also,

$$tr(|e_i\rangle\langle e_i| - \frac{1}{d}I) = tr(|e_i\rangle\langle e_i|) - tr(\frac{1}{d}I) = tr(\langle e_i|e_i\rangle) - \frac{1}{d}tr(I) = 0.$$

Thus, $|e_i\rangle\langle e_i| - \frac{1}{d}I \in \mathcal{A}$. Now note that since $\langle I, A\rangle = 0, \forall A \in \mathcal{A}$, we have $\frac{1}{d}I \in \mathcal{A}^{\perp}$. Therefore, $proj_{\mathcal{A}}(|e_i\rangle\langle e_i|) = |e_i\rangle\langle e_i| - \frac{1}{d}I$. □

Theorem 7 *Let $diag_{E_1}(\mathbb{C}^d)$, $diag_{E_2}(\mathbb{C}^d)$ be two *-MASAs. Then $diag_{E_1}(\mathbb{C}^d)$ and $diag_{E_2}(\mathbb{C}^d)$ are quasi-orthogonal if and only if E_1 and E_2 are mutually unbiased.*

Proof. By Lemma 6, $diag_{E_i}(\mathbb{C}^d) \ominus \mathbb{C}I = span\{|e_k^i\rangle\langle e_k^i| - \frac{1}{d}I\}$. Then

$$\begin{aligned}
&diag_{E_1}(\mathbb{C}^d) \ominus \mathbb{C}I \perp diag_{E_2}(\mathbb{C}^d) \ominus \mathbb{C}I \\
\iff &\left\langle |e_k^1\rangle\langle e_k^1| - \frac{I}{d}, |e_l^2\rangle\langle e_l^2| - \frac{I}{d} \right\rangle = 0, \ \forall k, l \\
\iff &tr\left(\left(|e_k^1\rangle\langle e_k^1| - \frac{I}{d}\right)\left(|e_l^2\rangle\langle e_l^2| - \frac{I}{d}\right)\right) = 0, \ \forall k, l \\
\iff &tr(|e_k^1\rangle\langle e_k^1|e_l^2\rangle\langle e_l^2|) - \frac{1}{d}tr(|e_k^1\rangle\langle e_k^1|) - \frac{1}{d}tr(|e_l^2\rangle\langle e_l^2|) + \frac{1}{d^2}tr(I) = 0, \ \forall k, l \\
\iff &tr(\langle e_l^2|e_k^1\rangle\langle e_k^1|e_l^2\rangle) - \frac{1}{d}tr(\langle e_k^1|e_k^1\rangle) - \frac{1}{d}tr(\langle e_l^2|e_l^2\rangle) + \frac{1}{d^2}tr(I) = 0, \ \forall k, l \\
\iff &\overline{\langle e_k^1|e_l^2\rangle}\langle e_k^1|e_l^2\rangle - \frac{1}{d} = 0, \ \forall k, l \\
\iff &|\langle e_k^1, e_l^2\rangle|^2 = \frac{1}{d}, \ \forall k, l.
\end{aligned}$$

Thus, $\mathcal{A}_1$ and $\mathcal{A}_2$ are quasi-orthogonal if and only if E_1 and E_2 are mutually unbiased. □

In general, given m quasi-orthogonal *-MASAs in $M_d(\mathbb{C})$, one can construct a set of m MUBs.

5 The Weyl Representation on $\mathbb{Z}_d^2$

Let $U, V \in M_d(\mathbb{C})$ be defined by

$$Ue_k = e_{k+1}, \ Ve_k = e^{2\pi ik/d}e_k, \ k \in \mathbb{Z}_d$$

where $\{e_k\}$ is the standard basis and addition is mod d. Note that $U^d = V^d = I$, and U, V are unitary since

$$\langle Ue_k, Ue_{k'}\rangle = \langle e_{k+1}, e_{k'+1}\rangle = \delta_{k+1,k'+1} = \delta_{k,k'}, \forall k, k' \in \mathbb{Z}$$

$$\langle Ve_k, Ve_{k'}\rangle = \langle e^{2\pi ik/d}e_k, e^{2\pi ik'/d}e_{k'}\rangle = e^{2\pi i(k'-k)/d}\langle e_k, e_{k'}\rangle = \delta_{k,k'}, \forall k, k' \in \mathbb{Z}.$$

Thus, $x \to U^x, x \to V^x$ are unitary representations on $\mathbb{Z}^d$.

Definition 4 *The Weyl representation $W : \mathbb{Z}_d^2 \to M_d(\mathbb{C})$ is defined by*

$$W(z) = W(x, y) = U^x V^y,\ z = (x, y) \in \mathbb{Z}_d^2.$$

In this section we will show how the Weyl representation can be used to generate quasi-orthogonal maximal abelian *-subalgebras.

Lemma 8

$$V^y U^x = e^{2\pi ixy/d} U^x V^y, \forall x, y \in \mathbb{Z}_d.$$

Proof. We show that the two sides have the same action on basis vectors. Note, $\forall k \in \mathbb{Z}_d$,

$$U^x V^y e_k = U^x (e^{2\pi ik/d})^y e_k = e^{2\pi iky/d} U^x e_k = e^{2\pi iky/d} e_{k+x},$$

so we have

$$\begin{aligned} V^y U^x e_k &= V^y e_{k+x} = (e^{2\pi i(k+x)/d})^y e_{k+x} = e^{2\pi iky/d + 2\pi ixy/d} e_{k+x} \\ &= e^{2\pi ixy/d}(e^{2\pi iky/d} e_{k+x}) = e^{2\pi ixy/d}(U^x V^y e_k) = [e^{2\pi ixy/d} U^x V^y] e_k. \end{aligned}$$

□

Corollary 9

$$W(z)W(z') = e^{2\pi ix'y/d} W(z + z'), \forall z, z' \in \mathbb{Z}_d^2.$$

Proof.

$$\begin{aligned} W(z)W(z') &= U^x V^y U^{x'} V^{y'} \\ &= e^{2\pi ix'y/d} U^x U^{x'} V^y V^{y'} && \text{By Lemma 8} \\ &= e^{2\pi ix'y/d} U^{x+x'} V^{y+y'} \\ &= e^{2\pi ix'y/d} W(z + z'). \end{aligned}$$

□

Note that Corollary 9 shows that W is a projective representation, meaning a representation up to multiplication by complex numbers of modulus 1.

Definition 5 *The canonical bilinear symplectic form on $\mathbb{Z}_d^2$ (scaled by a factor of $\frac{2\pi}{d}$) is*

$$\Delta(z', z) = \frac{2\pi}{d}(x'y - y'x).$$

Lemma 10 *The following relations hold for all $z, z' \in \mathbb{Z}_d^2$:*

1. $W(z)^* = e^{2\pi ixy/d} W(-z)$
2. $W(z)W(z') = e^{i\Delta(z',z)} W(z')W(z)$
3. $\langle W(z), W(z') \rangle = d\delta_{z,z'}$

Proof. 1.

$$\begin{aligned}
&(e^{2\pi ixy/d} W(-z))W(z) \\
=&e^{2\pi ixy/d} e^{-2\pi ixy/d} W(-z+z) && \text{By Corollary 9} \\
=&W(0) = I.
\end{aligned}$$

So

$$\begin{aligned}
e^{2\pi ixy/d} W(-z) &= W(z)^{-1} \\
&= W(z)^* && \text{Since } W(z) \text{ is unitary.}
\end{aligned}$$

2.

$$\begin{aligned}
W(z)W(z') &= e^{2\pi ix'y/d} W(z+z') && \text{By Corollary 9} \\
&= e^{2\pi ix'y/d} W(z'+z) \\
&= e^{2\pi ix'y/d} e^{-2\pi ixy'/d} W(z')W(z) && \text{By Corollary 9} \\
&= e^{2\pi i(x'y - xy')/d} W(z')W(z) \\
&= e^{i\Delta(z',z)} W(z')W(z).
\end{aligned}$$

3.

$$\begin{aligned}
\langle W(z), W(z') \rangle &= tr(W(z)^* W(z')) \\
&= tr(e^{2\pi ixy/d} W(-z)W(z')) && \text{By Part 1} \\
&= e^{2\pi ixy/d} tr(e^{-2\pi ix'y/d} W(z'-z)) && \text{By Corollary 9} \\
&= e^{2\pi ixy/d} e^{-2\pi ix'y/d} tr(U^{x'-x} V^{y-y'}) \\
&= e^{2\pi i(x-x')y/d} tr(U^{x'-x} V^{y-y'}).
\end{aligned}$$

We will simplify $tr(U^{x'-x}V^{y'-y})$. Let $x'' = x' - x, y'' = y' - y$. Note that

$tr(A) = \sum_{k=0}^{d-1} \langle e_k, Ae_k \rangle$.

$$\begin{aligned}
tr(U^{x'-x}V^{y'-y}) = tr(U^{x''}V^{y''}) &= \sum_{k=0}^{d-1} \langle e_k, U^{x''}V^{y''}e_k \rangle \\
&= \sum_{k=0}^{d-1} \langle e_k, e^{2\pi iky''/d} e_{k+x''} \rangle \\
&= \sum_{k=0}^{d-1} e^{2\pi iky''/d} \langle e_k, e_{k+x''} \rangle \\
&= \sum_{k=0}^{d-1} e^{2\pi iky''/d} \delta_{k,k+x''} = \sum_{k=0}^{d-1} e^{2\pi iky''/d} \delta_{0,x''} \\
&= \delta_{x,x'} \sum_{k=0}^{d-1} e^{2\pi iky''/d} = \delta_{x,x'} \sum_{k=0}^{d-1} (e^{2\pi iy''/d})^k \\
&= \begin{cases} d\delta_{x,x'} & y'' = 0 \\ \delta_{x,x'} \dfrac{1-(e^{2\pi iy''/d})^d}{1-e^{2\pi iy''/d}} & y'' \neq 0 \end{cases} \\
&= \begin{cases} d\delta_{x,x'} & y'' = 0 \\ 0 & y'' \neq 0 \end{cases} \\
&= d\delta_{x,x'}\delta_{y'',0} = d\delta_{x,x'}\delta_{y,y'} = d\delta_{(x,y),(x',y')} = d\delta_{z,z'}.
\end{aligned}$$

Therefore, $\langle W(z), W(z') \rangle = de^{2\pi i(x-x')y/d}\delta_{z,z'} = d\delta_{z,z'}$.

□

From Part 3 of Lemma 10, we obtain:

Corollary 11 *$\{W(z) : z \in \mathbb{Z}_d^2\}$ is an orthogonal basis of $M_d(\mathbb{C})$ and $\left\{ \frac{W(z)}{\sqrt{d}} : z \in \mathbb{Z}_d^2 \right\}$ is an orthonormal basis.*

Lemma 12 *If H is a subgroup of $\mathbb{Z}_d^2$, then $\langle W(H) \rangle$ is a *-algebra.*

Proof. First note that $W(0) = I$, where $0 \in H$ is the additive identity. To show $\langle W(H) \rangle$ is closed under taking adjoints, it suffices to show $W(h)^* \in \langle W(H) \rangle, \forall h \in H$.

$$\begin{aligned}
& h \in H \\
\Rightarrow & -h \in H && \text{Since } H \text{ is a group} \\
\Rightarrow & W(-h) \in W(H) \\
\Rightarrow & e^{2\pi ixy/d} W(-h) \in \langle W(H) \rangle \\
\Rightarrow & W(h)^* \in \langle W(H) \rangle && \text{By Lemma 10, Part 1.}
\end{aligned}$$

□

Definition 6 *If H is a subgroup of $\mathbb{Z}_d^2$, its symplectic complement is*

$$H^\Delta = \{z \in \mathbb{Z}_d^2 : \Delta(z,h) \in 2\pi\mathbb{Z}\ \forall h \in H\}.$$

Note that H^Δ is a subgroup of $\mathbb{Z}_d^2$. If $H = H^\Delta$, then we say H is Lagrangian.

Lemma 13 *Let $d \in \mathbb{N}$ and H be a subgroup of $\mathbb{Z}_d^2$. Then $\langle W(H^\Delta)\rangle = W(H)'$.*

Proof. First we show $\langle W(H^\Delta)\rangle \subseteq W(H)'$. By Part 2 of Lemma 10 and the definition of H^Δ,

$$\forall z \in H, z' \in H^\Delta, W(z)W(z') = e^{i\Delta(z',z)}W(z')W(z) = W(z')W(z),$$

so $W(H^\Delta) \subseteq W(H)'$ and thus $\langle W(H^\Delta)\rangle \subseteq W(H)'$.

Now we show $W(H)' \subseteq \langle W(H^\Delta)\rangle$. Let $X \in W(H)'$. Since $\left\{\frac{W(z)}{\sqrt{d}} : z \in \mathbb{Z}_d^2\right\}$ is an orthonormal basis of $M_d(\mathbb{C})$ by Corollary 11, we can write

$$X = \sum_{z\in\mathbb{Z}_d^2} \left\langle \frac{W(z)}{\sqrt{d}}, X \right\rangle \frac{W(z)}{\sqrt{d}} = \frac{1}{d}\sum_{z\in\mathbb{Z}_d^2} \langle W(z), X\rangle W(z).$$

Let $h \in H$. Since $X \in W(H)'$, $XW(h) = W(h)X$. On the other hand,

$$\begin{aligned} XW(h) &= \frac{1}{d}\sum_{z\in\mathbb{Z}_d^2} \langle W(z), X\rangle W(z)W(h) \\ &= \frac{1}{d}\sum_{z\in\mathbb{Z}_d^2} \langle W(z), X\rangle e^{i\Delta(h,z)}W(h)W(z) \qquad \text{By Lemma 10, Part 2} \\ &= W(h)\left[\frac{1}{d}\sum_{z\in\mathbb{Z}_d^2} \langle W(z), X\rangle e^{i\Delta(h,z)}W(z)\right]. \end{aligned}$$

Thus,

$$\begin{aligned} &\frac{1}{d}\sum_{z\in\mathbb{Z}_d^2} \langle W(z), X\rangle e^{i\Delta(h,z)}W(z) = X = \frac{1}{d}\sum_{z\in\mathbb{Z}_d^2} \langle W(z), X\rangle W(z) \\ \Rightarrow &\frac{1}{d}\sum_{z\in\mathbb{Z}_d^2} [\langle W(z), X\rangle (e^{i\Delta(h,z)} - 1)]W(z) = 0. \end{aligned}$$

Since $\{W(z) : z \in \mathbb{Z}_d^2\}$ is linearly independent, and the choice of h was arbitrary, $\langle W(z), X\rangle(e^{i\Delta(h,z)} - 1) = 0, \forall h \in H, z \in \mathbb{Z}_d^2$. Thus, $\forall z \in \mathbb{Z}_d^2$,

$$\langle W(z), X\rangle \neq 0 \Rightarrow \forall h \in H, e^{i\Delta(h,z)} = 1 \Rightarrow z \in H^\Delta,$$

and so $\{z \in \mathbb{Z}_d^2 : \langle W(z), X\rangle \neq 0\} = \{z \in H^\Delta : \langle W(z), X\rangle \neq 0\}$. Finally,

$$\begin{aligned} X &= \frac{1}{d}\sum_{z\in\mathbb{Z}_d^2} \langle W(z), X\rangle W(z) \\ &= \frac{1}{d}\sum_{\substack{z\in\mathbb{Z}_d^2 \\ \langle W(z),X\rangle\neq 0}} \langle W(z), X\rangle W(z) \\ &= \frac{1}{d}\sum_{\substack{z\in H^\Delta \\ \langle W(z),X\rangle\neq 0}} \langle W(z), X\rangle W(z) \in \langle W(H^\Delta)\rangle. \end{aligned}$$

□

Lemma 14 *If H is a subgroup of $\mathbb{Z}_d^2$, then $\langle W(H)\rangle = span(W(H))$.*

Proof. First note $\langle W(H)\rangle = \langle span(W(H))\rangle$. If we show that $span(W(H))$ is an algebra, then $\langle span(W(H))\rangle = span(W(H))$, completing the proof.

$Span(W(H))$ is a vector space, so it remains to show it is closed under multiplication, specifically that $W(h_1)W(h_2) \in span(W(H)), \forall h_1, h_2 \in H$.

$$\begin{aligned} & h_1, h_2 \in H \\ \Rightarrow & h_1 + h_2 \in H && \text{Since } H \text{ is a group} \\ \Rightarrow & W(h_1 + h_2) \in W(H) \\ \Rightarrow & e^{2\pi i x_2 y_1/d} W(h_1 + h_2) \in span(W(H)) \\ \Rightarrow & W(h_1)W(h_2) \in span(W(H)) && \text{By Corollary 9.} \end{aligned}$$

□

Lemma 15 *If H is a subgroup of $\mathbb{Z}_d^2$, then $\langle W(H)\rangle$ is maximal abelian if and only if H is Lagrangian.*

Proof. First note that $\langle W(H)\rangle' = W(H)' = \langle W(H^\Delta)\rangle$, where the second equality is from Lemma 13.

If H is Lagrangian, then $H = H^\Delta$ and $\langle W(H)\rangle' = \langle W(H^\Delta)\rangle = \langle W(H)\rangle$, so $\langle W(H)\rangle$ is maximal abelian.

Conversely, suppose $\langle W(H)\rangle$ is maximal abelian, so $\langle W(H)\rangle' = \langle W(H)\rangle$. Then $\langle W(H^\Delta)\rangle = \langle W(H)\rangle$, so by Lemma 14, $span(W(H^\Delta)) = span(W(H))$. By Corollary 11, $\{W(z) : z \in \mathbb{Z}_d^2\}$ is linearly independent, so $span(W(H^\Delta)) = span(W(H)) \Rightarrow W(H^\Delta) = W(H)$. Finally, by part 3 of Lemma 10, W is injective, so $W(H^\Delta) = W(H) \Rightarrow H^\Delta = H$, showing that H is Lagrangian. □

Lemma 16 *If H is a subgroup of $\mathbb{Z}_d^2$, then $\langle W(H)\rangle \ominus \mathbb{C}I = span(W(H \setminus \{0\}))$.*

Proof. By Lemma 14, $\langle W(H)\rangle \ominus \mathbb{C}I = Span(W(H)) \ominus \mathbb{C}I$. Then

$$\begin{aligned} Span(W(H)) \ominus \mathbb{C}I &= \{A \in Span(W(H)) : \langle I, A\rangle = 0\} \\ &= \left\{ \sum_{h\in H} c_h W(h) : c_h \in \mathbb{C}, \forall h \in H, \left\langle I, \sum_{h\in H} c_h W(h) \right\rangle = 0 \right\}. \end{aligned}$$

Note that

$$\begin{aligned} &\left\langle I, \sum_{h\in H} c_h W(h) \right\rangle = 0 \\ \iff &\sum_{h\in H} c_h \langle W(0), W(h)\rangle = 0 \\ \iff &\sum_{h\in H} c_h d\delta_{0,h} = 0 \\ \iff &c_0 = 0. \end{aligned}$$

Thus,

$$\begin{aligned} Span(W(H)) \ominus \mathbb{C}I &= \left\{ \sum_{h\in H} c_h W(h) : c_h \in \mathbb{C}, \forall h \in H, c_0 = 0 \right\} \\ &= \left\{ \sum_{h\in H\setminus\{0\}} c_h W(h) : c_h \in \mathbb{C}, \forall h \in H \right\} \\ &= Span(W(H \setminus \{0\})). \end{aligned}$$

□

Lemma 17 *If H_1 and H_2 are subgroups of $\mathbb{Z}_d^2$ such that $H_1 \cap H_2 = \{0\}$, then $\langle W(H_1)\rangle$ and $\langle W(H_2)\rangle$ are quasi-orthogonal.*

Proof. Note that $(H_1\setminus\{0\})\cap(H_2\setminus\{0\}) = \emptyset$, so if $h_1 \in H_1\setminus\{0\}$ and $h_2 \in H_2\setminus\{0\}$, then $h_1 \neq h_2$. Thus, since $\{W(z) : z \in \mathbb{Z}_d^2\}$ is orthogonal, we have

$$\begin{aligned} &W(h_1) \perp W(h_2), \forall h_1 \in H_1 \setminus \{0\}, h_2 \in H_2 \setminus \{0\} \\ \iff &span(W(H_1 \setminus \{0\})) \perp span(W(H_2 \setminus \{0\})) \\ \iff &\langle W(H_1)\rangle \ominus \mathbb{C}I \perp \langle W(H_2)\rangle \ominus \mathbb{C}I \qquad \text{By Lemma 16.} \end{aligned}$$

□

Combining Lemmas 12, 15, and 17 gives us the following theorem.

Theorem 18 *If H_1 and H_2 are Lagrangian subgroups of $\mathbb{Z}_d^2$ such that $H_1 \cap H_2 = \{0\}$, then $\langle W(H_1)\rangle$ and $\langle W(H_2)\rangle$ are quasi-orthogonal *-MASAs.*

In general, given m Lagrangian subgroups of $\mathbb{Z}_d^2$ that are "disjoint" (in the sense that their pairwise intersection is $\{0\}$), one can construct m quasi-orthogonal *-MASAs in $M_d(\mathbb{C})$.

6 Disjoint Lagrangian Subgroups

In this section we consider the problem of finding disjoint Lagrangian subgroups of certain finite groups in order to construct MUBs for $M_d(\mathbb{C})$, where $d = p^n$ is a prime power. We consider two cases, the first being for d prime, the second for d being a higher prime power ($n \geq 2$).

6.1 d prime

We consider the group $\mathbb{Z}_d^2$. Note that since d is prime, $\mathbb{Z}_d$ is a finite field and $\mathbb{Z}_d^2$ is a vector space over $\mathbb{Z}_d$.

Definition 7 *If $z \in \mathbb{Z}_d^2 \setminus \{0\}$, then $H_z = \{sz : s \in \mathbb{Z}_d\}$. We call H_z a ray.*

Note that rays are subgroups of $\mathbb{Z}_d^2$. If $s' \in \mathbb{Z}_d \setminus \{0\}$, then $H_{s'z} = H_z$.

Lemma 19 *If $H_{z_1} \neq H_{z_2}$, then $H_{z_1} \cap H_{z_2} = \{0\}$.*

Proof. Clearly $0 \in H_{z_1} \cap H_{z_2}$. Now let $z \in H_{z_1} \cap H_{z_2}$ and suppose $z \neq 0$. Then $z = s_1 z_1 = s_2 z_2$ where $s_1, s_2 \neq 0$, so $z_1 = s_1^{-1} s_2 z_2$ and $H_{z_1} = H_{z_2}$, contradiction. Thus, $H_{z_1} \cap H_{z_2} = \{0\}$. □

Since each $z \in \mathbb{Z}_d^2 \setminus \{0\}$ belongs to a ray (namely H_z) and the rays are disjoint when restricted to $\mathbb{Z}_d^2 \setminus \{0\}$, they partition $\mathbb{Z}_d^2 \setminus \{0\}$. Since $|\mathbb{Z}_d^2 \setminus \{0\}| = d^2 - 1$ and each ray contains $d - 1$ points of $\mathbb{Z}_d^2 \setminus \{0\}$, there are $d + 1$ rays.

Lemma 20 *$\forall z \in \mathbb{Z}_d^2 \setminus \{0\}$, H_z is Lagrangian.*

Proof. We need to show $H_z^\Delta = H_z$, that is, $\forall z' \in \mathbb{Z}_d^2, z' \in H_z^\Delta \iff z' \in H_z$. Note that all operations will be performed modulo d.

$$\begin{aligned}
& z' \in H_z^\Delta \\
\iff & \Delta(z', sz) \in 2\pi\mathbb{Z}, \forall s \in \mathbb{Z}_d \\
\iff & \frac{2\pi}{d}(sx'y - sxy') \in 2\pi\mathbb{Z}, \forall s \in \mathbb{Z}_d \\
\iff & s(x'y - xy') \in d\mathbb{Z}, \forall s \in \mathbb{Z}_d \\
\iff & s(x'y - xy') = 0, \forall s \in \mathbb{Z}_d \\
\iff & x'y - xy' = 0 \\
\iff & x'y = xy'.
\end{aligned}$$

Since $z \neq 0$, WLOG suppose $x \neq 0$. Then $x' = s'x$ where $s' = x'x^{-1}$, and so,

$$x'y = xy' \iff s'xy = xy' \iff s'y = y' \iff y' = s'y.$$

Then, $y' = s'y$, together with $x' = s'x$, implies $\exists s \in \mathbb{Z}_d, x' = sx, y' = sy$. Conversely, $\exists s \in \mathbb{Z}_d, x' = sx, y' = sy$, together with $x' = s'x$, implies $y' = s'y$. Finally,

$$y' = s'y \iff \exists s \in \mathbb{Z}_d, x' = sx, y' = sy \iff z' \in H_z.$$

□

Therefore, there exist $d+1$ disjoint Lagrangian subgroups of $\mathbb{Z}_d^2$, and hence one can construct a set of $d+1$ MUBs for $M_d(\mathbb{C})$.

6.2 $d = p^n$ for p prime

We will consider the group $(\mathbb{Z}_p^n)^2$. First, we define the Weyl representation on $(\mathbb{Z}_p^n)^2$ and prove analogues of some of the results in Section 5.

Let $U, V \in M_p(\mathbb{C})$ be defined as in Section 5. Recall that the Weyl representation $W : \mathbb{Z}_p^2 \to M_p(\mathbb{C})$ is defined as

$$W(z) = W(x,y) = U^x V^y,\ z = (x,y) \in \mathbb{Z}_p^2.$$

Then the Weyl representation $W : (\mathbb{Z}_p^n)^2 \to [M_p(\mathbb{C})]^{\otimes n} \cong M_{p^n}(\mathbb{C}) = M_d(\mathbb{C})$ is defined as

$$W(z) = W(x,y) = W((x_1,\ldots,x_n),(y_1,\ldots,y_n)) = \bigotimes_{j=1}^{n} W(x_j,y_j),$$

where $z = (x,y) = ((x_1,\ldots,x_n),(y_1,\ldots,y_n)) \in (\mathbb{Z}_p^n)^2$.

Recall that the symplectic form on $\mathbb{Z}_p^2$ is defined as $\Delta(z',z) = \frac{2\pi}{p}(x'y - y'x)$. Then the bilinear symplectic form on $(\mathbb{Z}_p^n)^2$ is defined as

$$\Delta(z',z) = \sum_{j=1}^{n} \Delta((x_j',y_j'),(x_j,y_j)).$$

Equivalently, $\Delta(z',z) = \frac{2\pi}{p}(x'\cdot y - y'\cdot x)$, where $\cdot$ is the dot product.

We prove the analogue of Corollary 9 for the Weyl representation on $(\mathbb{Z}_p^n)^2$.

Lemma 21

$$W(z)W(z') = e^{2\pi i x'\cdot y/p} W(z+z'), \forall z, z' \in (\mathbb{Z}_p^n)^2.$$

Proof.

$$\begin{aligned}
W(z)W(z') &= \bigotimes_{j=1}^{n} W(x_j,y_j) \bigotimes_{j=1}^{n} W(x_j',y_j') \\
&= \bigotimes_{j=1}^{n} W(x_j,y_j)W(x_j',y_j') \\
&= \bigotimes_{j=1}^{n} e^{2\pi i x_j' y_j/p} W(x_j+x_j', y_j+y_j') \\
&= \prod_{j=1}^{n} e^{2\pi i x_j' y_j/p} \bigotimes_{j=1}^{n} W(x_j+x_j', y_j+y_j') \\
&= e^{2\pi i \sum_{j=1}^{n} x_j' y_j/p} W(z+z') \\
&= e^{2\pi i x'\cdot y/p} W(z+z').
\end{aligned}$$

□

Analogues of Parts 1 and 2 of Lemma 10 follow from Lemma 21. The proofs of the analogues are the same as the original proofs except with xy replaced with $x \cdot y$ and d replaced with p.

Now we prove the analogue of Lemma 10 Part 3 for the Weyl representation on $(\mathbb{Z}_p^n)^2$.

Lemma 22

$$\langle W(z'), W(z) \rangle = d\delta_{z',z}, \forall z, z' \in (\mathbb{Z}_p^n)^2.$$

Proof.

$$\begin{aligned}
\langle W(z'), W(z) \rangle &= tr(W(z')^* W(z)) \\
&= tr\left(\left(\bigotimes_{j=1}^{n} W(x_j', y_j') \right)^* \bigotimes_{j=1}^{n} W(x_j, y_j) \right) \\
&= tr\left(\bigotimes_{j=1}^{n} W(x_j', y_j')^* W(x_j, y_j) \right) \\
&= \prod_{j=1}^{n} tr(W(x_j', y_j')^* W(x_j, y_j)) \\
&= \prod_{j=1}^{n} \langle W(x_j', y_j'), W(x_j, y_j) \rangle \\
&= \prod_{j=1}^{n} p\, \delta_{x_k', x_k} \delta_{y_k', y_k} = p^n \prod_{j=1}^{n} \delta_{x_k', x_k} \prod_{j=1}^{n} \delta_{y_k', y_k} \\
&= p^n \delta_{x',x} \delta_{y',y} = d\delta_{z',z}.
\end{aligned}$$

□

Analogues for all other results from Section 5 follow from the results proven in this section. The proofs of the analogues are the same as the original proofs except with xy replaced with $x \cdot y$, $\mathbb{Z}_d$ replaced with $\mathbb{Z}_p^n$, and d replaced with p where appropriate.

In particular, we have an analogue of Theorem 18.

Theorem 23 *If H_1 and H_2 are Lagrangian subgroups of $(\mathbb{Z}_p^n)^2$ such that $H_1 \cap H_2 = \{0\}$, then $\langle W(H_1) \rangle$ and $\langle W(H_2) \rangle$ are quasi-orthogonal *-MASAs.*

In general, given m disjoint Lagrangian subgroups of $(\mathbb{Z}_p^n)^2$, one can construct m quasi-orthogonal *-MASAs in $M_d(\mathbb{C})$. We now show how to construct such subgroups using finite fields.

Let $\mathbb{F}_{p^n}$ be the finite field of p^n elements. Note that $\mathbb{F}_{p^n}$ is also an n-dimensonal vector space over the subfield $\mathbb{F}_p$.

Definition 8 *The trace of $x \in \mathbb{F}_{p^n}$ is*

$$\text{tr } x = \sum_{i=0}^{n-1} x^{p^i}.$$

It turns out that $\text{tr } x \in \mathbb{F}_p,\ \forall x \in \mathbb{F}_{p^n}$. Furthermore, trace is linear if $\mathbb{F}_{p^n}$ is viewed as a vector space ([7], Theorem 2.23).

For a basis $B = \{b_1, \ldots, b_n\}$ of $\mathbb{F}_{p^n}$, and an element x of $\mathbb{F}_{p^n}$, we write $(x)_B \in \mathbb{Z}_p^n$ to denote the coordinate vector of x with respect to B. We let $(x)_{bi}$ denote the i^{th} component of $(x)_B$. That is, $x = \sum_{i=1}^n (x)_{bi} b_i$. Note that $x \mapsto (x)_B$ is a group isomorphism from $(\mathbb{F}_{p^n}, +)$ to $(\mathbb{Z}_p^n, +)$.

Let $E = \{e_1, \ldots, e_n\}$ be a basis for $\mathbb{F}_{p^n}$. Then there exists a unique *dual* basis $F = \{f_1, \ldots, f_n\}$ defined by the property $\text{tr } e_i f_j = \delta_{ij}$ ([3], pg. 14).

Note that $x = \sum_{i=1}^n (x)_{ei} e_i \Rightarrow \text{tr}(x f_j) = \sum_{i=1}^n (x)_{ei} tr(e_i f_j) = \sum_{i=1}^n (x)_{ei} \delta_{ij} = (x)_{ej}$, or simply $(x)_{ei} = \text{tr}(x f_i)$.

Definition 9 *If $z \in (\mathbb{F}_{p^n})^2 \setminus \{0\}$, then $H_z = \{((sx)_E, (sy)_F) : s \in \mathbb{F}_{p^n}\}$.*

H_z is a subgroup of $(\mathbb{Z}_p^n)^2$, since $x \mapsto (x)_B$ is an isomorphism. The subgroups are disjoint when restricted to $(\mathbb{Z}_p^n)^2 \setminus 0$, with the proof being similar to that of Lemma 19. A counting argument similar to that in Section 6.1 shows that there are $d + 1$ subgroups.

Lemma 24 *$\forall z \in (\mathbb{F}_p^n)^2 \setminus \{0\}$, H_z is Lagrangian.*

Proof. We need to show $H_z^\Delta = H_z$, that is, $\forall v \in (\mathbb{Z}_p^n)^2, v \in H_z^\Delta \iff v \in H_z$. Note that for any $v \in (\mathbb{Z}_p^n)^2$, there exist unique $x', y' \in \mathbb{F}_{p^n}$ such that $v = ((x')_E, (y')_F)$. All operations will be performed modulo p. Then,

$$\begin{aligned}
& v \in H_z^\Delta \\
\iff & \Delta\big(((x')_E, (y')_F), ((sx)_E, (sy)_F)\big) \in 2\pi\mathbb{Z}, \forall s \in \mathbb{F}_{p^n} \\
\iff & \frac{2\pi}{d}((x')_E \cdot (sy)_F - (sx)_E \cdot (y')_F) \in 2\pi\mathbb{Z}, \forall s \in \mathbb{F}_{p^n} \\
\iff & (x')_E \cdot (sy)_F - (sx)_E \cdot (y')_F \in d\mathbb{Z}, \forall s \in \mathbb{F}_{p^n} \\
\iff & (x')_E \cdot (sy)_F - (sx)_E \cdot (y')_F = 0, \forall s \in \mathbb{F}_{p^n} \\
\iff & (x')_E \cdot (sy)_F = (sx)_E \cdot (y')_F, \forall s \in \mathbb{F}_{p^n}.
\end{aligned}$$

We inspect $(x')_E \cdot (sy)_F$.

$$\begin{aligned}
&(x')_E \cdot (sy)_F \\
=&\sum_{i=1}^{n} (x')_{ei}(sy)_{fi} \\
=&\sum_{i,j=1}^{n} (x')_{ei}(sy)_{fj}\delta_{ij} \\
=&\sum_{i,j=1}^{n} (x')_{ei}(sy)_{fj}\mathrm{tr}(e_i f_j) \\
=&\mathrm{tr}\left[\sum_{i,j=1}^{n} ((x')_{ei}e_i(sy)_{fj}f_j)\right] \\
=&\mathrm{tr}\left[\sum_{i=1}^{n}((x')_{ei}e_i)\sum_{j=1}^{n}((sy)_{fj}f_j))\right] \\
=&\mathrm{tr}(x'sy) = \mathrm{tr}(sx'y).
\end{aligned}$$

Likewise, $(sx)_E \cdot (y')_F = \mathrm{tr}(sxy')$. Thus,

$$\begin{aligned}
&(x')_E \cdot (sy)_F = (sx)_E \cdot (y')_F, \forall s \in \mathbb{F}_{p^n} \\
\iff &\mathrm{tr}(sx'y) = \mathrm{tr}(sxy'), \forall s \in \mathbb{F}_{p^n} \\
\iff &\mathrm{tr}(sx'y) - \mathrm{tr}(sxy') = 0, \forall s \in \mathbb{F}_{p^n} \\
\iff &\mathrm{tr}(s(x'y - xy')) = 0, \forall s \in \mathbb{F}_{p^n} \\
\iff &\mathrm{tr}(f_i(x'y - xy')) = 0, \forall i \in \{1, \ldots, n\} \\
\iff &(x'y - xy')_{ei} = 0, \forall i \in \{1, \ldots, n\} \\
\iff &x'y - xy' = 0 \\
\iff &x'y = xy'.
\end{aligned}$$

The proof that $x'y = xy' \iff v \in H_z$ is the same as in Lemma 20 with $\mathbb{F}_{p^n}$ in place of $\mathbb{Z}_d$ and v in place of z', since that proof only relied on $\mathbb{Z}_d$ being a field and the fact that $z' \neq 0$. □

Therefore, there exist $d+1$ disjoint Lagrangian subgroups of $(\mathbb{Z}_p^n)^2$, and hence one can construct a set of $d+1$ MUBs for $M_d(\mathbb{C})$.

7 Conclusion

Mutually unbiased bases have many applications in quantum information theory, especially when there exist $d+1$ such bases in $\mathbb{C}^d$, which is the maximum possible. In this paper, we gave a proof that when d is a prime power, this maximum is attained. We did this by showing that given m quasi-orthogonal

maximal abelian *-subalgebras of $M_d(\mathbb{C})$, one can construct m MUBs of $\mathbb{C}^d$, and given m disjoint Lagrangian subgroups of $(\mathbb{Z}_d)^2$ (or $(\mathbb{Z}_p^n)^2$), one can construct m quasi-orthogonal *-MASAs. The converse to this statement is that the existence of m MUBs in $\mathbb{C}^d$ implies the existence of m disjoint Lagrangian subgroups of G^2, for some abelian group G of order d. If this is true, then something can be said about non-prime power dimensions as well. For example, the fact that one can not find more than 3 disjoint Lagrangian subgroups of $(\mathbb{Z}_6)^2$ would suffice to prove that only 3 MUBs exist in $\mathbb{C}^6$, which is widely believed to be the case.

References

[1] Thomas Durt, Berthold-Georg Englert, Ingemar Bengtsson, and Karol Zyczkowski. On mutually unbiased bases. *International Journal of Quantum Information*, 2010.

[2] Joel Feldman. Families of commuting normal matrices. `http://www.math.ubc.ca/~feldman/m512/matrices.pdf`, 2000.

[3] Kathleen S. Gibbons, Matthew J. Hoffman, and William K. Wootters. Discrete phase space based on finite fields. *Physical Review A*, 2004.

[4] Chris Godsil and Aidan Roy. Equiangular lines, mutually unbiased bases, and spin models. *European Journal of Combinatorics*, 2009.

[5] Kenneth Hoffman and Ray Kunze. *Linear Algebra*. Pearson, 1971.

[6] Andreas Klappenecker and Martin Rötteler. Constructions of mutually unbiased bases. *Finite Fields and Applications*, 2004.

[7] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. Cambridge University Press, 1996.

[8] K. R. Parthasarathy. On estimating the state of a finite level quantum system. *Infinite Dimensional Analysis, Quantum Probability and Related Topics*, 2004.

[9] Christoph Spengler, Marcus Huber, Stephen Brierley, Theodor Adaktylos, , and Beatrix C. Hiesmayr. Entanglement detection via mutually unbiased bases. *Physical Review A*, 2012.

[10] William K Wootters and Brian D Fields. Optimal state-determination by mutually unbiased measurements. *Annals of Physics*, 1989.