Mutually unbiased bases as submodules and subspaces

Joanne L. Hall* and Jan Štovíček†
Department of Algebra
Charles University in Prague
186 75 Praha 8, Sokolovska 83, Czech Republic
*Email: hall@karlin.mff.cuni.cz
†Email: stovicek@karlin.mff.cuni.cz

Abstract—Mutually unbiased bases (MUBs) have been used in several cryptographic and communications applications. There has been much speculation regarding connections between MUBs and finite geometries. Most of which has focused on a connection with projective and affine planes. We propose a connection with higher dimensional projective geometries and projective Hjelmslev geometries. We show that this proposed geometric structure is present in several constructions of MUBs.

I. INTRODUCTION

Mutually unbiased bases (MUBs) are a structure first defined in a quantum physics context in 1960 [22]. Since then MUBs have been used in quantum key distribution protocols [3], [21], and can be used to construct signal sets then MUBs have been used in quantum key distribution defined in a quantum physics context in 1960 [22]. Since it is complete sets of MUBs that are of most use in the communications applications. While constructions of complete sets of MUBs in $\mathbb{C}^d$ is called complete, it is complete sets of MUBs that are of most use in the communications applications. While constructions of complete sets of MUBs in $\mathbb{C}^d$ are known when $d$ is a prime power [26], it is unknown if such complete sets exist in non-prime power dimensions.

There has been much speculation regarding connections between MUBs and finite geometries [2], [19], [20], [25]. Most of this has focused on a connection with projective and affine planes.

The evidence for connections between MUBs and finite geometries falls into two categories: counting arguments [20], [19], and structures which construct both MUBs and finite geometries. These structures include planar functions [18], [12], symplectic spreads [11] as well as specific affine planes [8], [17].

We investigate higher dimensional projective geometries and show that some sets of MUBs may be regarded as subspaces. Note that in order for these higher order projective geometries to exist, a projective plane of the appropriate size must also exist. If all MUBs are subspaces of larger projective geometries, then a connection between MUBs and projective planes would be proven. Alas we do not go so far.

It has been shown that complete sets of MUBs are equivalent to orthogonal decompositions of the Lie algebra $sl_n(\mathbb{C})$ [4], however finding orthogonal decompositions of Lie algebras is as difficult a task as finding sets of MUBs. Some work has been done classifying Lie Algebras using projective geometry [15], but these results have as yet not been applied to decompositions of $sl_n(\mathbb{C})$.

Some sets of MUBs have been shown to have an Abelian group structure [13], [10]. We go further by showing that some complete sets of MUBs may be regarded as submodules of the appropriate free module, and as subspaces of a projective geometry over that module.

II. PRELIMINARIES

A. Constructions of MUBs

We investigate three non-equivalent constructions of MUBs. This first construction is based on planar functions over a finite field. For more on planar functions see for example [5]. Let $\omega_p := e^{2\pi i/p}$.

Theorem 1 (Planar function construction): [18, Thm 4.1]
Let $\mathbb{F}_q$ be a field of odd characteristic $p$. Let $II(x)$ be a planar function on $\mathbb{F}_q$. Let $V_a := \{v_{ab} : b \in \mathbb{F}_q\}$ be the set of vectors

$$v_{ab} = \frac{1}{\sqrt{q}} \left( \omega_p^{tr(aII(x)+bx)} \right)_{x \in \mathbb{F}_q} \quad (1)$$

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

The following construction has been shown to be equivalent to the planar function construction when using $II(x) = x^2$ [9]. We highlight it as the submodule and subspaces structure appear in a different way to the planar function construction.

Theorem 2 (Alltop construction): [1][12, Thm 1]
Let $\mathbb{F}_q$ be a finite field of odd characteristic $p \geq 5$. Let $V_a := \{v_{ab} : b \in \mathbb{F}_q\}$ be the set of vectors

$$v_{ab} := \frac{1}{\sqrt{q}} \left( \omega_p^{tr((x+a)^3 + b(x+a))} \right)_{x \in \mathbb{F}_q} \quad (2)$$

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

The next construction stems from a symplectic spread.
This is familiar as the left axioms of a vector space. All \( \mathbb{R} \)-modules. An (left and right) rings, thus all modules in consideration are both left and right \( \mathbb{F} \)-modules in Galois rings [24, §14].

The next construction uses Galois rings.

**Theorem 4 (Galois ring construction):** [12, Thm 3] Let \( GR(4, n) \) be Galois ring of characteristic 4 and Teichmüller set \( T_n \). Let \( i = \omega_4 = \sqrt{-1} \). Let \( V_a := \{ v_{ab} : b \in T_n \} \) be the set of vectors

\[
\tilde{v}_{ab} := \frac{1}{\sqrt{n}} \left( i^{r(a+b)}x_{ab} \right)_{x \in T_n}
\]

with \( a, b \in \mathbb{F}_q \). The standard basis \( E \) along with the sets \( V_a, a \in T_n \), form a complete set of \( 2^n + 1 \) MUBs in \( C^n \).

These are not the only known constructions of complete sets of MUBs [11], but are good starting point for an investigation.

### B. Algebraic Structures

Let \( R \) be a ring with unity, a left \( R \)-module is an Abelian group, \( M \), together with a product \( R \times M \to M \) which satisfies the following: for all \( r_1, r_2 \in R \) and \( a_1, a_2 \in M \)

\[
\begin{align*}
1 \cdot a &= a, \\
(r_1 r_2) a &= r_1 (r_2 a) \\
(r_1 + r_2) a &= r_1 a + r_2 a \\
r(a_1 + a_2) &= r a_1 + r a_2
\end{align*}
\]

This is familiar as the left axioms of a vector space. All \( \mathbb{F} \)-modules where \( \mathbb{F} \) is a field are vector spaces. Theorem 4 uses a ring to construct MUBs, hence we need the more general object of a module. We are only concerned with commutative rings, thus all modules in consideration are both left and right modules. An (left and right) \( R \) module is free if it is isomorphic to \( R^d \) for some \( d \).

The trace map, familiar from finite fields, may also be used from finite fields. The trace map, familiar from finite fields, may also be used. The trace map familiar from finite fields, may also be used. The trace map familiar from finite fields, may also be used

**Theorem 5:** [24, Thm 7.12, 14.34,14.37] The trace map, \( tr : GR(p^n, 1) \to GR(p^n, 1) \) has the following properties:

1) For all \( r \in GR(p^n, 1) \) and \( x \in GR(p^n, n) \), \( vtr(x) = tr(vx) \).

2) \( tr(\alpha) = 0 \) if and only if there exists \( \beta \in R' \) such that \( \alpha = \beta - \phi(\beta) \).

where \( \phi \) is the generalized Frobenius automorphism. Note that \( GR(p^n, 1) \cong \mathbb{F}_{p^n} \).

For further on Galois rings and fields we refer the reader to [24].

### C. Geometric Structures

The geometric structures we are investigating are projective geometries, \( PG(d-1, q) \), defined over a finite field and projective Hjelmslev geometries \( PHG(d-1, GR(4, 1)) \), defined over a Galois ring.

Let \( M \) be an \( R \) module that is a submodule of \( R^d \). If \( R \) is a field, then any submodule is a subspace of \( R^d \). If \( R \) is a Galois ring then any free submodule is a subspace of \( R^d \) [14].

**Definition 6:** The projective geometry constructed from \( \mathbb{F}_q \). \( PG(d-1, q) \) is the set of subspaces of \( \mathbb{F}_q^d \). \( \tilde{x} \) is a point of \( PHG(d-1, q) \) and represents all vectors \( \rho \tilde{x} \) in \( \mathbb{F}_q^d \) such that \( \rho \in \mathbb{F}_q^* \) and at least one of the entries of \( \tilde{x} \) is non-zero.

**Definition 7:** [23] The projective Hjelmslev geometry constructed from \( GR(4, 1), PHG(d-1, 14) \) is the set of subspaces of \( GR(4, 1)^d \). \( \tilde{x} \) is a point of \( PHG(d-1, GR(4, 1)) \) and represents all vectors \( \rho \tilde{x} \) in \( GR(4, 1)^d \) such that \( \rho \in \text{unit of } GR(4, 1) \) and at least one of the entries of \( \tilde{x} \) is a unit of \( GR(4, 1) \).

Note that \( PG(d-1, q) \cong PHG(d-1, \mathbb{F}_q) \).

### III. MUBS AS SUBMODULES AND SUBSPACES

#### A. Conjecture

**Proposal 8:** Let \( X \) be a complete set of MUBs which contains the standard basis in \( C^n \). Let \( N \) be the set containing all the vectors from \( X \), except the standard basis vectors. Let the vectors in \( N \) be of the form \( \omega \tilde{x} \) where \( \omega \in \mathbb{F}_q \), \( \omega \) is a \( q \)-th root of unity, and \( \tilde{x} \in \mathbb{Z}_q^d \). Let \( \circ \) represent component wise multiplication, let

\[
\tilde{v} \circ \tilde{u} = \frac{\tilde{v} \circ \tilde{u}}{[\tilde{v} \circ \tilde{u}]}
\]

and let \( N' = \{ u \circ \tilde{v} : \tilde{u}, \tilde{v} \in N \} \), \( M = \{ \tilde{x} : \omega \tilde{x} \in N \} \), and \( M' = \{ \tilde{x} - \tilde{y} : \tilde{x}, \tilde{y} \in M \} \). Let \( U' \subset M' \) be the set containing the vectors from \( M' \) for which every entry is a non-unit.

1) Then \( N' \) is a \( \mathbb{Z}_q \)-module.

2) Then \( M' \setminus U' \) is the set of vectors representing a subspace of a projective geometry over \( \mathbb{Z}_q \).

We show this proposal is true for each of the constructions of MUBs mentioned in section II-A. This proposal says nothing about the existence of MUBs which are not constructed from a ring. All projective geometries and projective Hjelmsev geometries of dimension greater than 2 have an algebraic structure [6, §1.4],[14]. It may be the same for complete sets of MUBs.

MUBs for which the set of vectors forms a group under point-wise multiplication, has been shown to be equivalent to a relative difference set in an abelian group [9]. Our construction differs in that the module structure is in the set of vectors generated by point-wise multiplication. This may extend to set \( N' \) in Proposal 8.

#### B. Counting

Much of the evidence for connections between MUBs and geometric structures stems from similarities in cardinality.
We show that Proposal 8 is plausible in general by using cardinalities.

**Lemma 2.84**. To show that it is a module \( F \) to scalar multiplication on the set \( r \), we have shown that \(<a, b, c, d>\). Let \( r \in \mathbb{F}_p \) and \( \bar{v}_{ab} \in N \), \( r * \bar{v}_{ab} \in N \). The properties of \( \mathbb{F}_p \) ensure that the module axioms are satisfied.

2. Part 1. shows that \( M \) is a submodule, and thus forms a subspace of \( \mathbb{F}_p^N \). The counting results of Lemma 10 show the size of the subspace.

For all \( a, b, c, d \in \mathbb{F}_q \), any element in \( \bar{v}_{ef} \in M \) can be constructed as \( \bar{v}_{ef} = \bar{v}_{ab} \hat{\circ} \bar{v}_{cd} \) for some \( \bar{v}_{ab}, \bar{v}_{cd} \in M \). Thus in the definition of Proposal 8, \( N = N' \) and \( M = M' \). Hence Proposal 8 holds for planar function MUBs.

**Theorem 12**: Let \( X \) be the complete set of MUBs in \( \mathbb{C}^n \) generated by the Alltop construction (Thm 2). Let \( S \subset X \) be the set of vectors \( \hat{x} = \frac{1}{\sqrt{d}} \omega_p^x \) where \( \hat{x} \in \mathbb{F}_p^\prime \). Let \( T := \{ \hat{x} : \omega_p^x \in N \} \). Let \( S' = \{ \hat{v} \hat{\circ} \hat{u} : \hat{v}, \hat{u} \in S \} \) and \( T' = \{ \hat{x} + \hat{y} : \hat{x}, \hat{y} \in T \} \).

1) \((S', \hat{\circ})\) is an \( \mathbb{F}_p\)-module.
2) \( T' \) is a 2\( n \)-1 dimensional subspace of \( PG(p^n - 1, p) \).

**Proof**: Let \( \bar{v}_{ab}, \bar{v}_{cd} \) be as defined in equation (2). We now show that \( S' = N' \) and \( T' = M' \), with \( M, N \) from Theorem 11.

\[
\bar{v}_{ab} \hat{\circ} \bar{v}_{cd} = \frac{1}{q} \sum_{x \in \mathbb{F}_p} \omega_p^{3(a-c)x^2+(3a^3-3a^2c+bc-d)x+(a^3-c^3+ba-bc-d)} \tag{13}
\]

which is a quadratic in \( x \). \( x^2 \) is a planar function, hence Theorem 11 may be used.

This result highlights that structures which are not present in sets of vectors of the MUBs, may be present in another way, see also [17].

We use essentially the same proof for the structure of the MUBs generated by Theorem 3.

**Theorem 13**: Let \( X \) be the complete set of MUBs in \( \mathbb{C}^n \) generated by the construction of Theorem 3. Let \( N \subset X \) be the set of vectors \( \hat{x} = \frac{1}{\sqrt{d}} \omega_p^x \) where \( \hat{x} \in \mathbb{F}_p^\prime \). Let \( M := \{ \hat{x} : \omega_p^x \in N \} \)

1) \((N, \hat{\circ})\) is an \( \mathbb{F}_p\)-module.
2) \( M \) is a 2\( n \)-1 dimensional subspace of \( PG(p^n - 1, p) \).

**Proof**: 1. We use the operations \( \hat{\circ} \) and \( * \) as in Theorem 11. From equation 3,

\[
\bar{v}_{ab} \hat{\circ} \bar{v}_{cd} = \frac{1}{\sqrt{q}} \left( \omega_p^{\Pi(a+c)x+(b+d)x^2} \right)_{x \in \mathbb{F}_q} \tag{14}
\]

with \( a, b, c, \in \mathbb{F}_q \). Let \( \phi(b) = b^p \) be the Frobenius automorphism [24, §7.1], then \( b^{p^n} = \phi^{p^{n-1}}(b) \) and hence
\( \phi^{p^{r-1}}(b + d) = \phi^{p^{r-1}}(b) + \phi^{p^{r-1}}(d) \). Using this fact we can rearrange equation (14)

\[
\hat{u}_{\alpha} \hat{v}_{\beta} = \frac{1}{\sqrt{q}} \left( i^{Tr(\alpha x)} \right)_{x \in T_n}
\]

with \( a, b \in \mathbb{F}_q \). Showing that \( \hat{u}_{\alpha} \hat{v}_{\beta} \in N \). As with Theorem 11, we use the operation \( \ast \) and see that \( N \) is an \( \mathbb{F}_p \) module.

2. The proof is the same as for Theorem 11.

As with Theorem 11, we find that \( M = M' \) and \( N' = N \) for \( M, M', N, N' \) as in Proposal 8.

These three structures based on finite fields all conform to the structure of Proposal 8.

D. Even dimensions

Theorem 14: Let \( X \) be the complete set of MUBs in dimension \( d = 2^n \) generated by the Galois ring construction [12]. Let \( N \subset X \) be the set of vectors \( \tilde{x} = \frac{1}{\sqrt{d}} \tilde{\bar{x}} \) where \( \bar{x} \in GR(4,1)^{2^n} \). Let \( M := \{ \tilde{x} : \tilde{\bar{x}} \in N \} \).

1) \( N \) is a \( GR(4,1) \)-module.

2) \( M \) is a \( 2^{2n-1} \) dimensional subspace of \( PHG(2^n - 1, GR(4,1)) \).

Proof: 1. Let \( \alpha = a + 2b \) and \( \beta = c + 2d \) where \( a, b, c, d \in T_n \) the Teichmuller set of \( GR(4, n) \). Then equation (4) becomes

\[
\hat{v}_{\alpha} := \frac{1}{\sqrt{2^{n}}} \left( i^{Tr(\alpha x)} \right)_{x \in T_n}
\]

\( \alpha \in GR(4, n) \). Let \( \hat{\circ} \) be as in Proposal 8

\[
\hat{v}_{\alpha} \hat{v}_{\beta} = \frac{1}{\sqrt{2^{n}}} \left( i^{Tr(\alpha + \beta x)} \right)_{x \in T_n}
\]

\( \hat{v}_{\alpha} \hat{v}_{\beta} \in M \). \( \hat{v}_{0} \) is the identity, \( \hat{v}_{\alpha} \hat{v}_{-\alpha} = \hat{v}_{0} \).

Let \( \ast \) be the operation \( GR(4, 1) \times N \) that corresponds to scalar multiplication on \( M \).

\[
r \ast \hat{v}_{\alpha} := \frac{1}{\sqrt{2^{n}}} \left( i^{Tr(\alpha x)} \right)_{x \in T_n}
\]

and hence \( r \ast \hat{v}_{\alpha} \in M \), for all \( r \in GR(4, 1) \). Hence \( M \) is a submodule.

2. Part 1. shows that \( M \) is a module. To show \( M \) is free we need that for every \( \tilde{\bar{x}} \) such that \( 2\tilde{\bar{x}} = 0 \), there exists \( \tilde{\bar{a}} \) such that \( 2\tilde{\bar{a}} = \tilde{\bar{x}} \). Thus we require that \( \alpha \) is such that

\[
2Tr(\alpha x) = Tr(2\alpha x) = 0
\]

for all \( x \in T_n \). then there exists \( \beta \in M \) such that \( \alpha = 2\beta \). Reverting to the \( p \)-adic notation, let \( \alpha = a + 2b \) and \( \beta = c + 2d \), then \( 2\beta = 0 + 2a \) and \( 2\beta = 0 + 2c \). Hence we need to show that if \( Tr(2\alpha x) = 0 \) for all \( x \in T_n \), then \( \alpha = 0 \).

Using Theorem 5.2, we see that this is equivalent to showing that for all \( x \in T_n \), there exists \( \gamma = (e + 2f) \in GR(4, n) \) such that

\[
2ax = e + 2f - \phi(e + 2f)
\]

\[
2ax = e + 2f - e^2 - 2f^2
\]

where \( a, x, e, f \in T_n \). This simplifies to

\[
ax = f - f^2
\]

If \( a = 0 \), then we have solved our problem. Assume \( a \neq 0 \), then there exists \( x \in T_n \) such that \( ax = 1 \). Thus we require a solution to

\[
0 = f^2 - f + 1
\]

This is a monic irreducible polynomial of degree 2, and hence has possible solution only in \( GR(4, 2) \). Let \( h(f) = f^2 - f + 1 \), then \( GR(4, 2) = Z_4[f]/(h(f)) \), and hence \( T_2 = \{ 0, 1, \xi, \xi + 3 \} \) where \( \xi \) is a root of \( h(f) \). From equation (22)

\[
\xi - \xi^2 = \xi - \xi - 3 = 1
\]

\[
\xi^2 - \xi^4 = \xi^2 - \xi = 3
\]

Hence if \( ax \in \{ \xi, \xi + 3 \} \), then equation (22) has no solution. We require that equation (22) holds for fixed \( a \) and all \( x \in T_n \), hence we require that \( a = 0 \), which shows that \( M \) is a free submodule. And thus by construction forms a subspace of \( PHG(2^n - 1, GR(4,1)) \). The counting results of Lemma 10 show the size of the subspace.

Note that \( GR(p^s, 1) \cong Z_{p^s} \), and as with Theorem 11, \( M = M' \) and \( N = N' \), thus the conditions of Proposal 8 are satisfied.

IV. CONCLUSION

We have shown that several sets of MUBs display the algebraic structure of a module and the geometric structure of a subspace of a projective Hjelmslev geometry. There are also counting results to show that this geometric structure may be true in general. Of particular note is that these structures may not arise from the sets of vectors which define the MUBs, but from the sets of vectors derived from component wise multiplication.

We have not covered all possible constructions of MUBs, but have shown sufficient evidence that this is a structure worthy of more thorough investigation.

REFERENCES


