EVIDENCE FOR AND AGAINST ZAUNER'S MUB CONJECTURE IN $\mathbb{C}^6$

GARY MCCONNELL, HARRY SPENCER, AND AFAQ TAHIR

Abstract. The problem of finding provably maximal sets of mutually unbiased bases in $\mathbb{C}^d$, for composite dimensions d which are not prime powers, remains completely open. In the first interesting case, $d = 6$, Zauner predicted that there can exist no more than three MUBs.

We explore possible algebraic solutions in $d = 6$ by looking at their 'shadows' in vector spaces over finite fields. The main result is that if a counterexample to Zauner's conjecture were to exist, then it would leave no such shadow upon reduction modulo several different primes, forcing its algebraic complexity level to be much higher than that of current well-known examples.

In the case of prime powers $q \equiv 5 \bmod 12$, however, we are able to show some curious evidence which — at least formally — points in the opposite direction. In $\mathbb{C}^6$, not even a single vector has ever been found which is mutually unbiased to a set of three MUBs. Yet in these finite fields we find sets of three 'generalised MUBs' together with an orthonormal set of four vectors of a putative fourth MUB, all of which lifts naturally to a number field.

Introduction

The notion of *mutually unbiased bases* or *MUBs* arose in physics as an optimal choice of measurement bases for quantum tomography [Sw, Iv, WF, Z]; although the concept was discovered independently in combinatorial design theory [CS, Ca, GR]. The problem of finding provably maximal sets of MUBs in $\mathbb{C}^d$ for non-prime-power dimensions d remains completely open. In the first interesting case, $d = 6$, Zauner [Z] has predicted that there can exist no more than three MUBs. Moreover there is a conjecture about orthogonal decompositions of Lie algebras [KKU] which is equivalent to saying that for any such non-prime-power d, a maximal set of $d+1$ MUBs cannot exist: see [Be1].

A priori there is no reason to expect the entries of MUB vectors over $\mathbb{C}$ to be algebraic. Indeed in $\mathbb{C}^6$ there is a catalogue of continuously parametrised families [Jam, Sz] of sets of three MUBs which outside a set of measure 0 are not unitarily equivalent to any algebraic set; showing that for arbitrary MUBs, the algebraic complexity level of the entries of the vectors can go all the way up to the transcendental. However since the equations are defined over $\mathbb{Z}$, one approach to exploring the known bounds on the number of MUBs over $\mathbb{C}^d$ is to attack the problem as an algebraic question over a general ring, and to see whether the equations can be solved there.

When studying finite systems of equations with integer coefficients, a standard technique in number theory and algebraic geometry is to look at their reductions modulo a prime number. Nambu [N], for example, also applied the same technique in a broad range of physical problems. Simplifying slightly for clarity, one looks at the image modulo p of their integer solutions, 'most' of which will survive reduction to the field $\mathbb{F}_p$ of integers modulo p. This picture naturally extends to number fields, and consequently the *absence* of a solution in a finite field can under strict conditions be used to show a corresponding failure of solvability back up in the

original number field. See [GIJM] for a recent similar approach to an affiliated problem.

The main thrust of this paper is to add a small result arising from this hitherto unexplored direction, to the already large body of evidence adduced in favour of Zauner's conjecture. Namely, in theorem 2.1 we demonstrate in a number of finite fields that sets of MUBs of size 4 in dimension 6 do not exist. Prima facie this is weak evidence that such sets of MUBs do not exist in the sorts of small degree number fields in which solutions have previously been studied: see for example [Be2, Go, ABD] and 4.2. Nevertheless, the translation back up to characteristic zero is still computationally intractable, so applying this result relies on studying each specific situation individually.

In the case of prime powers $q \equiv 5 \bmod 12$, however, proposition 2.2 points tentatively in the opposite direction. We lift a set of three generalised MUBs plus an additional set of four vectors of a putative fourth MUB, directly to solutions in a number field. Note however that we are beginning with a set of three what one might deem *hyperbolic* MUBs: where the property of unitarity is measured in terms of a *field norm*, as opposed to a complex absolute value. This formal solution is therefore *not* an MUB in complex Hilbert space; it is merely an artefact of lifting the shadow MUBs discovered in finite fields, back up to a vector space over a field of characteristic zero.

Indeed, it is important to note that when F is finite or p-adic, the sesquilinear form $\langle\ ,\ \rangle$ yields a weaker geometric structure than an inner product [Gro]. In particular, F^d will always contain isotropic vectors. Moreover, searches based on local minima of analytical functions — which have been deployed in most of the attempts to solve this problem over the complex field, for example [D, BW, Jam, Ray, Go, GrM] — are not possible at the finite field level. So there is no bijective geometric correspondence between our findings in arbitrary finite or p-adic fields, and the solutions in Hilbert spaces.

In the appendices we provide very brief notes on the results of the computer searches, the equations and their reductions, and general background reference material on the properties of these generalised MUBs.

1. The MUB problem over $\mathbb{C}$ and beyond

1.1. **State of knowledge over $\mathbb{C}$.** The MUB problem over $\mathbb{C}$ has been attacked using a mixture of geometric, combinatorial and numerical methods. To some extent these approaches have been unified under the combinatorial umbrella of frames and complex projective 2-designs: see e.g. [GR, Ca, RS, MG]. We refer to the vast body of work in the mathematical physics literature on this problem — for example [Sw, Be1, Be2, Ch, D, Ba] — for the motivation for studying Hilbert space MUBs and for various standard results about their geometry.

Before giving a generalised definition of MUBs in the next section, we set out the current state of knowledge on maximal sets of MUBs in complex Hilbert space $\mathbb{C}^d$. Let $\mathcal{M}_d\mathbb{C}$ denote the maximum number of orthonormal bases of $\mathbb{C}^d$ which can be pairwise mutually unbiased to one another.

Theorem. [All, Iv, WF, KR] *For $d \geq 2$, write $d = \prod_{i=1}^{n} p_i^{r_i}$ as a product of its prime power factors with the p_i ordered so that $p_1^{r_1} < p_2^{r_2} < \ldots < p_n^{r_n}$. Then:*

(I) $p_1^{r_1} + 1 \ \leq\ \mathcal{M}_d\mathbb{C} \ \leq\ d + 1$.

(II) *When d is a prime power, a maximal set of $d+1$ MUBs always exists in $\mathbb{C}^d$.*

The lower bound, which in the general case is currently limited to the outcome of taking tensor products [Z, Ba, ACW, KR], has in fact been marginally improved [WB] in some non-prime-power squared dimensions like $d = 676$. It should

be stressed again that no-one yet knows tight lower or upper bounds for $\mathcal{M}_d\mathbb{C}$ for any d not a power of a prime.

1.2. **Generalised definition of MUBs.** A formal definition of mutual unbiasedness may be made by analogy with the motivating complex case. For other instances of this see for example [Ch, Boy, vD][1]; and for further discussion of our case see A.2.1 and A.2.2. Throughout, $d \in \mathbb{N}$ will denote the dimension of our vector space. Let F be any field of characteristic not dividing $2d$, with an automorphic involution σ whose fixed subfield is K. For any $\alpha \in F$, $\mathrm{N}_{F/K}\alpha = \alpha\alpha^\sigma$ is the *field norm* down to K.

In the usual complex case, $F = \mathbb{C}$ and $K = \mathbb{R}$ and σ is complex conjugation. On the other hand, most of the time in this paper we shall be concerned with the case where F/K is a quadratic extension of finite fields. For a given base field $K = \mathbb{F}_{p^r}$, such an extension $F = \mathbb{F}_{p^{2r}}$ is unique up to isomorphism [Se] and has a unique cyclic K-automorphism group, or Galois group, of order 2 which fixes the base field K and is generated by the map which takes all elements of F to their p^r-th powers. This $q = p^r$-th power map is known as the *Frobenius automorphism.*

By F^d we shall always mean a *unitary space* [Gro, chapter 10]: namely, a d-dimensional vector space over F equipped with a non-degenerate *Hermitian* form defined for any pair of vectors $\mathbf{u} = (u_j), \mathbf{v} = (v_j) \in F^d$ by:

$$\langle \mathbf{u}, \mathbf{v} \rangle = \mathbf{u}^\dagger \cdot \mathbf{v} = \sum_{j=1}^{d} u_j^\sigma v_j,$$

where for any matrix M with entries in F, $M^\dagger$ denotes its conjugate transpose with respect to the involution σ. The word *basis* will always mean *orthonormal basis*, with respect to the given form; so we may write the basis set $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_d\}$ as the column vectors of a *unitary* — as defined with respect to this Hermitian form — matrix $[\mathbf{b}_1, \ldots, \mathbf{b}_d]$.

Definition 1. *Let* $\mathbf{u}, \mathbf{v} \in F^d$ *be any choice of* unit vectors*: that is, satisfying* $\langle \mathbf{u}, \mathbf{u} \rangle = \langle \mathbf{v}, \mathbf{v} \rangle = 1$. *We say that* $\mathbf{u}, \mathbf{v}$ *are* mutually unbiased *or* MU *to one another if*

$$\mathrm{N}_{F/K}\langle \mathbf{u}, \mathbf{v} \rangle \;=\; 1/d. \tag{1}$$

Let $\mathcal{B}$ *and* $\mathcal{C}$ *be any two orthonormal bases. If* $\mathrm{N}_{F/K}\langle \mathbf{b}_i, \mathbf{c}_j \rangle = 1/d$ *for every pair of vectors* $\mathbf{b}_i \in \mathcal{B}$, $\mathbf{c}_j \in \mathcal{C}$ *then we say that* $\mathcal{B}, \mathcal{C}$ *are* mutually unbiased bases.

We use the same notation as for the complex case, in that $\mathcal{M}_d F$ *will denote the size of a maximal set of MUBs in* F^d.

The definition is motivated by the situation in $\mathbb{C}^d$, in that if we require that every inner product $\langle \mathbf{b}_i, \mathbf{c}_j \rangle$ for $1 \leq i, j \leq d$ have the same absolute value, then in fact that common value is readily proven [Sw] to be $1/\sqrt{d}$.

It is important to note that in translating *particular* known algebraic solutions directly from number fields embedded in $\mathbb{C}$, down to finite and p-adic fields, at least half of the time we encounter a situation where the q-th power Frobenius automorphic involution σ does not act analogously to complex conjugation on the roots of unity. This means that the Wootters & Fields (henceforth just WF) solutions in [WF] to the equations in $\mathbb{C}$ simply *do not exist* modulo p. This is evidenced for example in the number of primes implicitly excluded from the hypotheses of proposition 3.2, and even more prominently in the tabulation of our exhaustive search results in A.1.1.

[1] Although ostensibly looking at the same question, [vD] was concerned with infinite-dimensional Hilbert spaces. The results and techniques are completely unrelated to those of this paper.

Conversely, any finite field solutions are by definition roots of cyclotomic polynomials; so this constraint is inescapable. Using a set of equations derived from the complex situation is thus rendered meaningless.

Throughout the paper, therefore, we have stuck with the *geometric* interpretation of the MUB existence question, adjusting the equations so that in each finite field they reflect the notion of an adjoint or Hermitian dot product, rather than interpreting it strictly as the specialisation of a complex algebraic variety.

The level of overdetermination in this problem is formidable. Just in the relatively tight case in proposition 2.2, even after all sensible reductions, we still begin with 150 variables over $\mathbb{F}_q$ but 231 equations. Elimination-theoretic tools like Gröbner bases had to be rejected in favour of an exhaustive search through small finite vector spaces. We have used MAGMA software [M] throughout.

2. MUBs over finite fields : implications for Zauner's conjecture

The link between the study of complex MUBs and those over quadratic extensions of finite fields is given explicitly by the correspondence between the canonical complex conjugation involution whose fixed field is $\mathbb{R}$, and the q-th power *Frobenius* involution which is the unique non-trivial automorphism of the field F fixing the base field K. It is this structural parallel which affords the possibility of analogous geometric results in the two contexts. This is explained further in 4.1.

Our attempts to explore the lower bound for $\mathcal{M}_6\mathbb{C}$ via the images of algebraic MUBs under reduction in finite fields, have led us to the following.

Theorem 2.1. *$\mathcal{M}_6\mathbb{F}_{q^2} \leq 3$ for every prime power $q = p^r$ in the set*

$$\{5, 25, 7, 49, 11, 13, 17, 19, 23, 29, 31, 37, 41\}.$$

Proof. The evidence from the numerical searches is tabulated in A.1.1. The methodology is explained in A.2. □

Theorem 2.1 supports Zauner's conjecture in a way which has not been explored before. However, as mentioned in the introduction, we also have a result which gives some slight evidence in the opposite direction.

Proposition 2.2. *Let $F = \mathbb{F}_{q^2}$ for some $q \equiv 5 \bmod 12$. Then there exists in F^6 a set $\mathcal{S}_F = \{\mathcal{B}_0, \mathcal{B}_1, \mathcal{B}_2\}$ of three pairwise mutually unbiased bases, together with an orthonormal set of four vectors which are all mutually unbiased to the three bases. In each case the solutions lift to a quadratic number field extension.*

Proof. See A.1.2 where the calculations are explained. Here, as in the rest of the paper, the initial basis set $\mathcal{B}_0$ is chosen to be the *computational basis* consisting of the d vectors $\mathbf{e}_j = (0, \ldots, 0, 1, 0, \ldots, 0)$, where the unique non-zero entry occurs at the j-th position. $\mathcal{B}_0$ is represented in matrix form by the identity matrix. An intermediate step was to lift the original solutions from the searches over finite fields, using standard p-adic techniques, up several levels in order to find the defining equations for the entries. It then became clear that they lifted not only to unramified extensions $F_\wp$ of $\mathbb{Q}_p$ but in fact all the way to a number field contained in $F_\wp$. It is also important to note that there are infinitely many possible quadratic number field extensions to which such solutions may be lifted, as we illustrate in A.1.2. □

As far as we can determine from the published literature, the arXiv, and personal communications with several other researchers active in this field (thanks to Ingemar Bengtsson, Stefan Weigert, Markus Grassl, Dan McNulty, Marcus Appleby and Dardo Goyeneche), no-one has yet been able to find a *single vector* in $\mathbb{C}^6$ which is mutually unbiased to a known set of three MUBs [Go, WM]. Indeed, using Gröbner basis techniques for varying values of d, Markus Grassl et al. have demonstrated

many cases wherein the extension of certain *non-maximal* sets of bases in $\mathbb{C}^d$ *by just a single vector* is impossible, elucidating a bewilderingly rich variety of possible outcomes given simple variations in the starting bases [GrM, §III], [De].

So the existence of this extra set of four vectors in proposition 2.2, even if it only obtains in this artificial 'hyperbolic' context, raises a natural question as to whether such a phenomenon occurs as some sort of Galois image of an actual set of MUBs, analogously for example to *ghost SICs* [AFK] in the cousin *SIC-POVM* problem [Be3].

3. Values of $\mathcal{M}_d F$ when F is a finite field

The best bounds which may be stated in full generality are as follows.

Proposition 3.1. *For any quadratic extension of finite fields F/K as above and any dimension $d \geq 2$ coprime to the characteristic p of K,*

$$1 \leq \mathcal{M}_d F \leq d+1.$$

Proof. Despite there always being at least three MUBs over $\mathbb{C}^d$ for any $d \geq 2$ — which [Ba] may be regarded simply as the eigenbases of the generalised Pauli operators X, Z and their product XZ — the lower bound in this finite field case cannot be improved upon in general. For example, see table 2 in A.1.1 in which $\mathcal{M}_3\mathbb{F}_{q^2}$ is shown to be 1 for essentially half of all q.

For the upper bound, which again is saturated in many cases, we adapt the argument from the complex case in [Iv], following the exposition in §4 of [Be1].

Define a non-degenerate Hermitian trace form $\mathrm{Tr}\left(A^\dagger B\right)$ on the matrix algebra $\mathrm{M}_{d\times d}(F)$ of degree d over F. Consider any orthonormal basis $\mathcal{B} = \{\mathbf{v}_1, \ldots, \mathbf{v}_d\}$ of F^d. The corresponding rank 1 trace 1 projectors $\pi_{\mathbf{v_k}} = \mathbf{v}_k \otimes \mathbf{v}_k^\dagger$ are orthogonal unit vectors in $\mathrm{M}_{d\times d}(F)$ under this trace form. Their endpoints span a d-simplex whose barycentre is $\frac{1}{d}\mathbb{I}$, where $\mathbb{I}$ denotes the identity matrix in $\mathrm{M}_{d\times d}(F)$. The set resulting from subtracting $\frac{1}{d}\mathbb{I}$ from each $\pi_{\mathbf{v_k}}$ spans a K^{d-1} subspace of the space $\mathcal{H}_0 \cong K^{d^2-1}$ of trace 0 Hermitian operators in $\mathrm{M}_{d\times d}(F)$. The pairwise Hermitian products between distinct shifted projectors arising from $\mathcal{B}$ are now $\frac{-1}{d}$ rather than zero.

However, given any $\mathbf{b} \in \mathcal{B}$ and $\mathbf{c} \in \mathcal{C}$ from mutually unbiased bases $\mathcal{B}$ and $\mathcal{C}$, the shifted trace product is zero:

$$\begin{aligned}
\mathrm{Tr}\big((\mathbf{b}\otimes\mathbf{b}^\dagger - \tfrac{1}{d}\mathbb{I})^\dagger(\mathbf{c}\otimes\mathbf{c}^\dagger - \tfrac{1}{d}\mathbb{I})\big) &= \mathrm{Tr}\big((\mathbf{b}\otimes\mathbf{b}^\dagger)(\mathbf{c}\otimes\mathbf{c}^\dagger)\big) - \frac{1}{d}\mathrm{Tr}\big((\mathbf{b}\otimes\mathbf{b}^\dagger + \mathbf{c}\otimes\mathbf{c}^\dagger)\big) + \mathrm{Tr}\frac{1}{d^2}\mathbb{I} \\
&= \langle\mathbf{b},\mathbf{c}\rangle\langle\mathbf{c},\mathbf{b}\rangle - \frac{2}{d} + \frac{1}{d} \\
&= 0.
\end{aligned}$$

That is to say, mutual unbiasedness between the bases down in F^d lifts to orthogonality between the corresponding translated operator subspaces in $\mathcal{H}_0$.

Hence n MUBs of F^d produce n mutually orthogonal $(d-1)$-dimensional K-subspaces inside K^{d^2-1}. If $p \mid \mathrm{char}(K)$ then for example the identity matrix lies in $\mathcal{H}_0$ and its trace product with every other matrix in $\mathcal{H}_0$ is zero, rendering degenerate the K-valued restriction to $\mathcal{H}_0$ of this trace form. However when $p \nmid \mathrm{char}(K)$, by considering a K-basis for $\mathcal{H}_0$ formed from simple F-linear combinations of the elementary matrices E_{ij} we see that the trace form remains non-degenerate; and the result follows. □

Remark. *The diagonalisation-based argument of* [Ba] *does not work here, because no Hermitian structure is possible. Indeed, the Galois group* $\mathrm{Gal}_{\overline{F}/F} \cong \widehat{\mathbb{Z}}$ *of the algebraic closure* $\overline{F}$ *of a finite field* F *is torsion-free. So in particular there is no surrogate operator for complex conjugation to match that of* $\mathrm{Gal}_{\mathbb{C}/\mathbb{R}}$.

3.1. **Values of $\mathcal{M}_d\mathbb{F}_{q^2}$ when d is a prime power.** Given any prime power dimension $d = l^k$, the next result yields a class of primes p of positive density, by Dirichlet's theorem on primes in arithmetic progressions, for which the complex WF solutions have *good reduction* over fields of characteristic p. That is to say, no singularities are introduced into the solution set in the process of reducing the coefficients of the set of defining equations modulo p.

Proposition 3.2. *Let l be a prime and k a positive integer. Let the prime $p \neq l$ and $r \geq 1$ satisfy $p^r \equiv -1 \bmod l^k$ when l is odd, or simply $p^r \equiv -1 \bmod 4$ when $l = 2$. Then writing $q = p^r$,*

$$\mathcal{M}_{l^k}\mathbb{F}_{q^2} = l^k + 1.$$

Notice that if $p^r \equiv -1 \bmod l^k$ then the same is true of p^{ar} for every odd integer a. In other words, for each particular dimension $d = l^k$, every such prime p additionally furnishes us with an infinite set of finite fields for which the statement holds.

The same techniques can be applied to more complicated sets of MUBs: we illustrate this in 4.1. Moreover, as illustrated in A.1.1, whenever we have done an exhaustive search in a prime-power dimension $d = 2, 3, 4, 5, 7$ over some finite field, we have found that all *maximal* solutions of $d + 1$ MUBs are *equivalent* — in the sense of [BWB] as explained in A.2.2 — to the reduced WF solutions, possibly modified by $\sqrt{-1}$ as in the proof below.

On the other hand, for prime powers where the structure in proposition 3.2 does not obtain, we have shown that for $d \leq 7$, $d + 1$ MUBs do *not* exist for the small primes in our searches[2]. So on the basis of this tiny body of evidence, the WF construction — with the slight modifications needed in the proof below — would seem to be universal for creating maximal sets of MUBs over finite fields. See [Ba] for a comparison with the complex case.

The sub-maximal sets in these defective dimension-prime combinations display behaviour akin to *bad reduction* of abelian varieties; although it is not because of the introduction of mod-p singularities but rather because the Hermitian form collapses. In other words, as we observed in 1.2, because the Hermitian form is encapsulated (via the Galois action) within the polynomial system, we are forced to use a different set of 'real' equations in these finite fields from that in the complex case or indeed in the finite fields in proposition 3.2. It is not clear what the 'geometric' meaning of the solutions is when there is a square root of -1 in the ground field, as is the case for example in proposition 2.2.

Given any field F and any $N \in \mathbb{N}$, let $\zeta_N \in \overline{F}$ denote a fixed primitive N-th root of unity in an algebraic closure $\overline{F}$ of F and let $\mu_N = <\zeta_N>$ be the group it generates. Similarly the symbol $\sqrt{T}$ will denote a fixed square root of a field element T inside an algebraic closure. A reference for the facts we use on finite fields is [Se].

Proof of proposition 3.2. We show by construction that the upper bound is attained; that it cannot be breached is proposition 3.1. In [WF], complete sets of l^k+1 MUBs $\{\mathcal{B}_0, \mathcal{B}_1, \ldots, \mathcal{B}_{l^k}\}$ are constructed in $\mathbb{C}^{l^k}$, where $\mathcal{B}_0$ is the computational basis represented by the identity matrix. All vector entries in the other $\mathcal{B}_k$ are of the form $\frac{\zeta_l^t}{\sqrt{l^k}}$ for some $t \in \mathbb{Z}$ when l is odd; and $\frac{i^t}{\sqrt{2^k}}$ when $l = 2$, where $i = \sqrt{-1}$.

Suppose first that l is an odd prime. The cyclic Galois group $\mathrm{Gal}_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}$ has a unique involution τ whose inversion action on μ_l is identical to that of the restriction of complex conjugation. On the other hand $\sqrt{l}$ is real and so it is fixed under

[2]Other than in the strange anomalous case $d = 7$, $p = 3$ in table 3 of A.1.1, where *a priori* we only know that solutions exist for powers of $q = p^3 = 27$, by proposition 3.2.

complex conjugation. It follows that the conjugation action on the vector entries in $\{\mathcal{B}_0, \mathcal{B}_1, \ldots, , \mathcal{B}_{l^k}\}$ is captured entirely by $\tau\colon \zeta_l \mapsto \zeta_l^{-1}$.

We have assumed that $q \equiv -1 \bmod l^k$ and $l \neq 2$, hence $\mathbb{F}_q^\times \cong \mu_{q-1}$ contains no l-th roots of unity other than 1; whereas $\mathbb{F}_{q^2}^\times \supset \mu_{q+1} \supset \mu_{l^k} \supset \mu_l$. In particular, $\mathbb{F}_{q^2} = \mathbb{F}_q(\zeta_l)$ and the q-th power Frobenius automorphism σ in the extension $\mathbb{F}_{q^2}/\mathbb{F}_q$ acts on the l-th roots of unity via inversion, since $\zeta_l^\sigma = \zeta_l^q = \zeta_l^{-1}$. It follows that any solution to the MUB equations in $\frac{1}{\sqrt{l^k}}\mathbb{Z}(\zeta_l)$ will satisfy the very same equations down in $\mathbb{F}_{q^2}$, provided that σ fixes the square root of l^k.

If k is even then l^k is a square integer; and if r is even then by the uniqueness of the quadratic extension of $\mathbb{F}_p$ the square root of $l \in \mathbb{F}_p$ must already be contained in $\mathbb{F}_q$. In such cases the norm $\mathrm{N}_{\mathbb{F}_{q^2}/\mathbb{F}_q}\sqrt{l^k} = l^k$ and consequently the behaviour exactly mimics that in the complex case.

Note also the trivial fact that when $p = 2$, so l is in fact forced to be odd, the square root of l^k — that is, 1 — is automatically in the ground field.

However if all of p, l, k and r are odd it is possible that l^k will not be a square in the base field $\mathbb{F}_q$: hence σ maps $\sqrt{l^k} \mapsto -\sqrt{l^k}$. In such cases every instance of $\sqrt{l^k}$ in the WF example must be twisted by some element $\nu \in \mathbb{F}_{q^2}$ whose norm is -1. But the norm map from $\mathbb{F}_{q^2}^\times$ to $\mathbb{F}_q^\times$ is surjective and so there are exactly $q+1$ elements of $\mathbb{F}_{q^2}^\times$ which map onto -1. Choose one such $\nu \in \mathbb{F}_{q^2}^\times$ and multiply all of the WF vector entries by ν, ignoring $\mathcal{B}_0$ of course; then once again $\mathrm{N}_{\mathbb{F}_{q^2}/\mathbb{F}_q}\nu\sqrt{l^k} = l^k$ and the set of equations derived from the geometry in $\mathbb{C}^{l^k}$ is satisfied.

When $l = 2$, so p is odd, all of the coefficients of the WF MUBs in dimension 2^k are of the form $\frac{i^a}{\sqrt{2^k}}$ for some $a \in \mathbb{Z}$. In a finite field of odd characteristic, we need the Frobenius action σ on the fourth roots of unity and on $\sqrt{2}$, where relevant, to mimic that in $\mathbb{C}/\mathbb{R}$: namely, as inversion on $i = \sqrt{-1}$ and as the identity on $\sqrt{2}$. This rules out $q \equiv 1 \bmod 4$, since then either $p \equiv 1 \bmod 4$ or r is even: either or both of which would ensure that -1 is a square in $\mathbb{F}_q$. So we are forced into the situation in the hypotheses of the proposition, where $p \equiv 3 \bmod 4$ and r is odd, which is equivalent to $q \equiv 3 \bmod 4$.

Hence all remaining possibly problematic cases for $l = 2$ reduce to k odd, r odd, $p \equiv 3 \bmod 8$ or $p \equiv 7 \bmod 8$. When $p \equiv 7 \bmod 8$, $(\frac{2}{p}) = 1$ and so the WF complex solutions behave identically down in $\mathbb{F}_{q^2}$.

When $p \equiv 3 \bmod 8$, however, the Legendre symbols $(\frac{-1}{p}) = (\frac{2}{p}) = -1$ and so both $\sqrt{-1}$ and $\sqrt{2}$ are mapped by σ to their negatives. The net action of σ is therefore to fix entries of the form $\frac{\pm i}{\sqrt{2}}$ and to flip the signs on the 'real' entries $\frac{\pm 1}{\sqrt{2}}$. So we need once again to compensate by adding in a factor whose norm is -1, and we follow the same procedure as above. □

3.2. Values of $\mathcal{M}_d\mathbb{F}_{q^2}$ when d is not a prime power.

Corollary 3.3. *Write $d = \prod_{j=1}^n l_j^{k_j}$ as a product of its prime power factors, ordered so that $l_1^{k_1} < l_2^{k_2} < \ldots < l_n^{k_n}$. Then there is a set of primes p of positive Dirichlet density together with integers $r_p \geq 1$ such that for each such pair, writing $q = p^{r_p}$:*

$$\mathcal{M}_d\mathbb{F}_{q^2} \geq l_1^{k_1} + 1.$$

Proof. We need to find a prime power $q = p^r$ which simultaneously satisfies the hypotheses of proposition 3.2 for every $l_j^{k_j}$. By the Chinese remainder theorem, if we choose a sequence of integers $a_j \bmod l_j^{k_j}$ for each j all with the same order — namely, the value $2r$ in proposition 3.2 — then this gives us a unique class $A \in (\mathbb{Z}/L\mathbb{Z})^\times$, where in principle $L = \prod_j l_j^{k_j}$. However, note that if one of the l_j is 2

then we must adjust so that the contribution to L from the j-th prime 2 is 4, $a_j = 3$ and $r = 1$ everywhere. In this case L will differ from d. By Dirichlet's theorem on primes in arithmetic progressions there are infinitely many primes p congruent to A modulo L. Such a p is then by construction congruent to $a_j \bmod l_j$ for each j.

Writing $q = p^r$, we now construct for each j a MUB over $\mathbb{F}_{q^2}^{l_j^{k_j}}$ as in the proof of proposition 3.2. We then use the argument in [KR, lemma 3] or [ACW]: take the tensor product of these component solutions, which yields a set of MUBs in dimension d over $\mathbb{F}_{q^2}$. Notice that in this last step we require the condition that the r be constant, in order to be able to tensor them over the same finite field. □

4. Applications of theorem 2.1: reduction from $\mathbb{C}$ to finite fields

4.1. **Using known solutions in $\mathbb{C}$ to search for solutions over $\mathbb{F}_{q^2}$.** One way to approach the search for four MUBs in dimension 6 is to begin with one of the many known triplets of MUBs in $\mathbb{C}^6$ whose vector entries lie in a complex algebraic number field L — see for example [ABD] — and to study its behaviour under reduction at certain admissible primes $\wp$ of the ring of integers $\mathbb{Z}_L$. We then search for more vectors over $\mathbb{F}_{q^2}/\mathbb{F}_q$ (where $q^2 = \mathrm{N}\wp$) which are MU to them all, and try to lift them back up to the extension $L_\wp$ of $\mathbb{Q}_p$. We should point out that we were unable to produce any new evidence this way along the lines of proposition 2.2.

In [Go], [Be2], [BWB] etc., many examples are detailed of sets of complex MUBs in low dimensions: there is also an online classification in [Br]. In most cases the entries are given as roots of unity or algebraic numbers of low degree [ABD]; hence they may be viewed as lying in some number field L with a fixed embedding into $\mathbb{C}$.

Choosing a prime $\wp|p$ of L at which the vector entries are $\mathbb{Z}_{L_\wp}$-units, the key requirement once again is that the action of the q-th power Frobenius map upon the vector entries reduced modulo $\wp$, should mimic that of complex conjugation in $\mathbb{C}/\mathbb{R}$. For example, it must act via inversion upon any roots of unity not in the base field. This is an unavoidable clash with the situation over $\mathbb{C}$: for a prime power $q > 3$ the $(q-1)$-th roots of unity other than ± 1 are not real; whereas they do lie in $\mathbb{F}_q$ and so the q-power map fixes them. Indeed, the more complicated the Galois action upon the entries, the higher we have to go in general, to find each prime at which Frobenius precisely replicates complex conjugation.

Locally $L_\wp$ should be the unramified quadratic extension $L_\wp/K_\mathfrak{p}$ of a base field $K_\mathfrak{p}$, writing $\wp|\mathfrak{p}|p$, such that the action of the Frobenius element $\sigma \in \mathrm{Gal}_{L_\wp/K_\mathfrak{p}}$ replicates that of complex conjugation on the L-entries of the original matrix. Let $q = N\mathfrak{p}$ denote the absolute (field-theoretic) norm of $\mathfrak{p}$: so $\mathbb{F}_q \cong \mathbb{Z}_{K_\mathfrak{p}}/\mathfrak{p}$ is the residue field of the ring of integers $\mathbb{Z}_{K_\mathfrak{p}}$ of $K_\mathfrak{p}$, with $\mathbb{F}_{q^2} \cong \mathbb{Z}_{L_\wp}/\wp$ the residue field of the ring of integers $\mathbb{Z}_{L_\wp}$ of $L_\wp$, and order 2 Galois group $\mathrm{Gal}_{\mathbb{F}_{q^2}/\mathbb{F}_q} \cong \mathrm{Gal}_{L_\wp/K_\mathfrak{p}}$.

4.2. **Examples of MUBs in $\mathbb{C}^6$ reduced modulo p: The matrices $H_1, D(0)$ from** [Go, §4]**.** We now illustrate this methodology with a couple of simple examples. These matrices require the 24-th roots of unity together with an algebraic number $b_2 = \frac{-1+2i}{\sqrt{5}}$, where $i^2 = -1$. Note that b_2 is a p-adic unit for all $p \neq 5$. So we need a prime p which allows $\mu_{24} \subseteq \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and which has a square root of 5 in $\mathbb{F}_q$ but not a square root of -1. That is, $p \equiv -1 \bmod 24$, $(\frac{5}{p}) = 1$: and $p \equiv 3 \bmod 4$ automatically by the first condition. Of the first few primes $23, 47, 71$ satisfying $p \equiv -1 \bmod 24$, only $p = 71$ contains 5 as a quadratic residue. For $q = p = 71$ in the notation of [Go], the bases were as follows. Writing $\mathbb{F}_{q^2}^\times =< \gamma > \cong C_{71^2-1}$ and $u = \gamma^{70}$ for a generator of the subgroup of elements of $\mathbb{F}_{q^2}$ of norm 1, and δ for a fixed choice of element of $\mathbb{F}_{q^2}$ of norm $1/d$ as explained in A.2.4:

$$H_1 = \delta \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ u^{54} & u^{54} & u^{6} & u^{30} & u^{30} & u^{6} \\ u^{71} & u^{35} & u^{27} & u^{63} & u^{27} & u^{63} \\ u^{54} & u^{54} & u^{30} & u^{6} & u^{6} & u^{30} \\ u^{35} & u^{71} & u^{39} & u^{51} & u^{15} & u^{3} \\ u^{35} & u^{71} & u^{15} & u^{3} & u^{39} & u^{51} \end{pmatrix} ; \quad D(0) = \delta \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & u^{36} & u^{18} & u^{54} & u^{54} & u^{18} \\ 1 & u^{18} & u^{36} & u^{18} & u^{54} & u^{54} \\ 1 & u^{54} & u^{18} & u^{36} & u^{18} & u^{54} \\ 1 & u^{54} & u^{54} & u^{18} & u^{36} & u^{18} \\ 1 & u^{18} & u^{54} & u^{54} & u^{18} & u^{36} \end{pmatrix}.$$

Acknowledgements

Initially phrasing it as a problem on Gröbner bases, Al Kasprzyk and GM began studying MUBs over finite fields in 2013. It quickly became apparent that the only computationally viable approach was an exhaustive search through the vectors themselves. This paper is the result of the faster technology now available [M]. In addition to Al Kasprzyk for helping to get the whole project running, we are grateful to Kevin Buzzard, Ian Grojnowski and Stefan Weigert for helpful conversations during the early stages, and likewise to Markus Grassl. A particular vote of thanks is due to Mike Harrison and Ingemar Bengtsson for many key observations, and helpful comments on an earlier draft. Finally, we thank the three anonymous referees for their insights, which enabled us to make the work more readable.

GM thanks Myungshik Kim and Terry Rudolph of the QOLS group at Imperial College for their continuing hospitality. AT would like to express his gratitude to the *Crankstart Internships* Programme at the University of Oxford for partially funding his work during the project.

Appendix A. The searches

A.1. **Theorem 2.1 and proposition 2.2.**

A.1.1. *Proof of theorem 2.1: limits on MUBs in finite fields.* For a field F and dimension d, suppose that $\mathcal{M}_d F = n$. As a measure of how close we can get to constructing a set of $n+1$ MUBs in F^d, we denote by $\nu_d F$ the maximal size, over all sets $\{\mathcal{B}_0, \ldots, \mathcal{B}_{n-1}\}$ of n MUBs in F^d, of an orthonormal set of vectors which are mutually unbiased to each $\mathcal{B}_k$. Here are results of the exhaustive searches for the case $d = 6$.

q	5	7	11	13	17	19	23	25	29	31	37	41	43	47	49	53
$\mathcal{M}_6\mathbb{F}_{q^2}$	3	3	3	2	3	3	3	2	3	3	2	3	3	3	2	3
$\nu_6(\mathbb{F}_{q^2})$	4	0	0	2	4	0	0	4	4	0	2	4	0	0	2	4

Table 1. Exhaustive search results in 6 dimensions.

As stated in 1.1, $\mathcal{M}_d\mathbb{C} = d + 1$ for prime powers d; and it is a corollary of the upper bound proof in proposition 3.1 that $\nu_d(\mathbb{C}) = 0$. Further, in each of the cases $d = 2, 3, 4, 5$ it is known that there is precisely one set of $d + 1$ MUBs up to equivalence [BWB]. These facts were paralleled in the results of the finite field searches wherever full MUB sets were found to exist.

d	Full $d+1$ MUBs	Partial Sets	Holds For
2	$q \equiv 3 \pmod 4$	$\mathcal{M}_2\mathbb{F}_{q^2} = 2$ for $q \equiv 1 \bmod 4$	all odd q
3	$q \equiv 2 \pmod 3$	$\mathcal{M}_3\mathbb{F}_{q^2} = 1$ for $q \equiv 1 \bmod 3$	$(3, q) = 1$
4	$q \equiv 3 \pmod 4$	$\mathcal{M}_4\mathbb{F}_{q^2} = 3$ for $q \equiv 1 \bmod 4$	$q < 240$, q odd
5	$q \equiv 4 \pmod 5$	$\mathcal{M}_5\mathbb{F}_{2^2} = 4$; $\mathcal{M}_5\mathbb{F}_{q^2} = 1$ for $q \equiv 1 \bmod 5$; $\mathcal{M}_5\mathbb{F}_{q^2} = 3$ for $q \equiv 2, 3 \bmod 5, q \neq 2$	$q < 122, (5, q) = 1$

Table 2. Exhaustive search results for $d \leq 5$.

Table 2 is valid for the ranges of q shown. The assertions for $d = 2, 3$ are a straightforward consequence of writing out the matrices with variables, incorporating the protocol detailed in A.2.3 and using proposition 3.2. In all cases where $\mathcal{M}_d\mathbb{F}_{q^2} > 1$, we find that $\nu_d\mathbb{F}_{q^2} = 0$.

Finally, our limited results for $d = 7$ are summarised in the following table.

q	2	3	4	5	8	9	11	13	17
$\mathcal{M}_7(\mathbb{F}_{q^2})$	4	8	1	2	4	3	3	8	2
$\nu_7(\mathbb{F}_{q^2})$	3	0	0	3	3	0	0	0	3

TABLE 3. Exhaustive search results in 7 dimensions.

A.1.2. *Proof of proposition 2.2: sets of three hyperbolic MUBs with a fourth set of four MU vectors.* As may be seen in table 1, for each prime power $q = p^r \equiv 5 \bmod 12$, we found in dimension 6 a set of 3 MUBs alongside a further set of 4 orthonormal vectors MU to each MUB. The first basis is always taken to be $\mathcal{B}_0$.

Lifting the solutions p-adically it became evident that they are perfectly general in characteristic zero. For example when $q \equiv 5 \bmod 24$, the extension $K(\sqrt{3})/K$ will suffice, where $K = \mathbb{Q}(i, \sqrt{6})$ and the Hermitian action is via the map $\sigma\colon \sqrt{3} \mapsto -\sqrt{3}$. So in particular the following representation reduces well in characteristic 5 mod 24:

$$\frac{1}{\sqrt{6}}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -2+\sqrt{3} & -1 & 2-\sqrt{3} & -2+\sqrt{3} & 2-\sqrt{3} \\ 1 & 1 & -2-\sqrt{3} & 1 & 1 & -2+\sqrt{3} \\ 1 & -2-\sqrt{3} & 2+\sqrt{3} & -1 & 1 & -1 \\ 1 & 1 & -2-\sqrt{3} & -2+\sqrt{3} & 1 & 1 \\ 1 & 1 & 2+\sqrt{3} & -1 & -2-\sqrt{3} & -1 \end{pmatrix},$$

$$\frac{1}{\sqrt{6}}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -2+\sqrt{3} & -1 & 2-\sqrt{3} \\ 1 & 1 & 1 & 1 & -2-\sqrt{3} & -2+\sqrt{3} \\ 1 & -2-\sqrt{3} & 2+\sqrt{3} & -2-\sqrt{3} & 2+\sqrt{3} & -1 \\ 1 & 1 & -2-\sqrt{3} & 1 & 1 & -2+\sqrt{3} \\ -2-\sqrt{3} & 1 & 2+\sqrt{3} & -2-\sqrt{3} & 2+\sqrt{3} & -1 \end{pmatrix}.$$

The four vectors, also arranged as columns in a matrix, are:

$$\frac{1}{\sqrt{6}}\begin{pmatrix} 1 & 1 & 1 & 1 \\ \omega^2(2-\sqrt{3}) & -\omega^2(2-\sqrt{3}) & -\omega(2-\sqrt{3}) & \omega(2-\sqrt{3}) \\ \omega & \omega & \omega^2 & \omega^2 \\ -\omega & \omega & \omega^2 & -\omega^2 \\ \omega^2 & \omega^2 & \omega & \omega \\ -1 & 1 & 1 & -1 \end{pmatrix},$$

where ω is a primitive cube root of unity; noting that $\sigma\colon \omega \mapsto \omega^2$.

In this case $\frac{1}{\sqrt{6}}$ is fixed under σ; whereas when $q \equiv 17 \bmod 24$ we need an extra factor of $i = \sqrt{-1}$ for each vector as in the proof of proposition 3.2.

A.2. **The search algorithms.** The exhaustive computer algorithm search routine is essentially self-explanatory. We just give a few basic background facts. The starting point in our sets of MUBs is always $\mathcal{B}_0 = \{\mathbf{e}_1, \ldots, \mathbf{e}_d\}$, represented by the identity matrix.

A.2.1. *Formal equivalence of notions of MU in $\mathbb{C}$ and $\mathbb{F}_{q^2}$.* Fix an odd prime p. The definition in (1) is formally aligned with that in the complex case: the square norm of the 'absolute value' of the Hermitian inner product of each pair of vectors from distinct bases must equal $1/d$. Hence our stipulation that $(d, p) = 1$. It is also somewhat meaningless to have d reinterpreted modulo the characteristic p. For example, if $p = 5$ and $d = 6$, then every unit vector is 'MUB to itself'. So ideally, we insist further that $d < p$.

Fix $q = p^r$ for some $r \geq 1$: we always work over the extension $\mathbb{F}_{q^2}/\mathbb{F}_q$ with Galois group generated by the Frobenius element $\sigma : x \mapsto x^q$ of order 2. Since the

quadratic extension of a finite field is unique up to isomorphism, we are assured of the existence in $\mathbb{F}_{q^2}$, if not already in $\mathbb{F}_q$, of a square root of d.

As an aside, however, we illustrate a major difference between our situation — where we are in the end searching for a solution in a number field — and those in $\mathbb{R}$ or $\mathbb{C}$ where the base field always contains $\sqrt{d}$. Let $d > 1$ be a non-square positive integer. Consider the corresponding Hermitian structure which arises via the Galois group $\mathrm{Gal}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}$. Whereas in $\mathbb{R}$ or $\mathbb{C}$ we would have $N(1/\sqrt{d}) = (1/\sqrt{d})^2 = 1/d$, here instead $N(1/\sqrt{d}) = (1/\sqrt{d})(-1/\sqrt{d}) = -1/d$. This is the context in which the *hyperbolic MUBs* arise in proposition 2.2 and A.1.2.

A.2.2. *Hadamard matrices.* Now let F/K be any quadratic extension of fields and let V be a unitary space. Given any matrix operator M on V, let $M^\dagger$ denote the Hermitian conjugate transpose of M: so in particular $\mathcal{B}$ represents an orthonormal basis if and only if its associated matrix $\mathcal{B}$ is unitary; which in turn is true iff $\mathcal{B}^\dagger\mathcal{B} = \mathcal{B}\mathcal{B}^\dagger = \mathcal{B}_0$. In view of the fact that much of the literature on this subject is phrased in these terms — see for example [Be2, Br, Go] — we note that a matrix $\mathcal{B}$ which is MU to $\mathcal{B}_0$ is often called an *F-Hadamard matrix* — or where the context is clear just a *Hadamard matrix* — drawing upon the terminology in the complex case[3].

A second basis $\mathcal{C}$ represented by another F-Hadamard matrix is then in turn MU to $\mathcal{B}$ iff the ordinary matrix product $\mathcal{B}^\dagger\mathcal{C}$ is also itself an F-Hadamard matrix. Indeed, the condition in definition 1 is identical to requiring that every entry $\langle \mathbf{b}_i, \mathbf{c}_j \rangle$ of the unitary matrix $\mathcal{B}^\dagger\mathcal{C}$ of pair-wise Hermitian dot products have that norm. Since for any unitary matrix $\mathcal{B}$ and any matrices $\mathcal{C}$, $\mathcal{D}$ it is the case that $(\mathcal{B}^\dagger\mathcal{C})^\dagger(\mathcal{B}^\dagger\mathcal{D}) = \mathcal{C}^\dagger\mathcal{D}$, including $\mathcal{B}_0$ in any set of MUBs as the first member is no restriction. This then forces all of the entries $b_j \in F$ of all other basis vectors $\mathbf{b}$ of another MUB $\mathcal{B}$, say, to satisfy $\mathrm{N}_{F/K} b_j = 1/d$. However, although when $\mathcal{B}$ and $\mathcal{C}$ are MU to one another, the basis associated to $\mathcal{D} = \mathcal{B}^\dagger\mathcal{C}$ is by definition itself MU with respect to $\mathcal{B}_0$, in most cases $\mathcal{D}$ will be MU neither to $\mathcal{B}$ nor to $\mathcal{C}$. Parenthetically, the order in which we take the Hermitian product is important: when $\mathcal{B}^\dagger\mathcal{C}$ satisfies our conditions, this nevertheless reveals nothing in particular about the unitary $\mathcal{B}\mathcal{C}^\dagger$.

A.2.3. *Transformations which preserve the MU properties: Rearrangements of the columns and rows of the MUB matrices.* [Be2, §III], [D]. Let $\mathcal{S} = \{\mathcal{B}_1, \ldots, \mathcal{B}_n\}$ be a set of MUBs in F^d which is assumed not to include $\mathcal{B}_0$, but to be MU to it. Given any basis matrix $\mathcal{B}_k \in \mathcal{S}$ we are free to rearrange the columns in any order without affecting the MU properties. This amounts to right-multiplying $\mathcal{B}_k$ by a $d \times d$ permutation matrix. Similarly and separately, we may rearrange the rows of every $\mathcal{B}_k$ for $1 \leq k \leq n$, *provided that we do an identical rearrangement on all n matrices simultaneously.* This may be effected by left-multiplying them all by *the same* permutation matrix.

By analogy with the real case, two pairs of vectors $\mathbf{u}, \mathbf{v}$ and $\mathbf{u}', \mathbf{v}'$ subtend the same 'angle' if and only if $\mathrm{N}_{F/K}\langle \mathbf{u}, \mathbf{v} \rangle = \mathrm{N}_{F/K}\langle \mathbf{u}', \mathbf{v}' \rangle$. This angle is unchanged if we multiply $\mathbf{u}$ or $\mathbf{v}$ or both by elements of F of norm 1. Regarding each $\mathcal{B}_k$ separately therefore we are free to right-multiply any or all of them by (possibly) different diagonal matrices of norm 1 elements. So in particular, we may assume without loss of generality that the first entry in every vector of every one of the $\mathcal{B}_k$ is equal to the same value, which we choose to be the quantity δ below, where $\mathrm{N}_{F/K}\delta = 1/d$.

Equally, we may multiply the rows of the bases by norm 1 elements, again provided that we use the same element on each corresponding row of each matrix at the same time. This is achieved by left-multiplying every one of the $\mathcal{B}_k$ by the

[3]Using the convention of Bengtsson *et al* in [Be2], in that Hadamard matrices are *unitary*, as opposed to *unimodular* as in say [Br]. These differ merely by a one-off normalisation by $\frac{1}{\sqrt{d}}$.

same diagonal matrix with norm 1 diagonal entries. In this way, we are able for example to ensure that the first vector of the first basis $\mathcal{B}_1$ should have all of its entries equal to δ. This was illustrated in the examples in 4.1 and A.1.2.

A.2.4. *Transformations which preserve the MU properties: Reducing the search space from d dimensions to d − 1.* We make a few obvious simplifications. The norm homomorphism N on multiplicative groups of finite fields is surjective, yielding the following short exact sequence of finite groups defining the kernel U:

$$1 \longrightarrow U \longrightarrow \mathbb{F}_{q^2}^{\times} \overset{N}{\longrightarrow} \mathbb{F}_q^{\times} \longrightarrow 1.$$

If γ is any generator for the multiplicative subgroup $\mathbb{F}_{q^2}^{\times}$ of $\mathbb{F}_{q^2}$ then $U = <\gamma^{q-1}>$ is the unique subgroup of $\mathbb{F}_{q^2}^{\times}$ of index $q-1$ (equivalently, of order $q+1$). Let $\delta \in \mathbb{F}_{q^2}^{\times}$ lie above d^{-1}; then δU is the coset containing all elements of norm $d^{-1} = N\delta = \delta^{q+1}$.

By setting the first basis to be $\mathcal{B}_0$, we may restrict our attention to vectors whose entries lie in δU. Indeed we may view $(\delta U)^d = \delta U^d$, the cartesian product of d copies of δU, as a sub*set* of $\mathbb{F}_{q^2}^d$ and focus our search within it. In accordance with the previous section, we are free to choose the first vector of our first new basis $\mathcal{B}_1$ to consist of all δ's; and moreover the first element of each of our non-$\mathcal{B}_0$ vectors also may be chosen to be δ.

Just as with the situation over the complex extension of the reals, for each vector entry we require two variables over $\mathbb{F}_q$ to constitute just one over $\mathbb{F}_{q^2}$, so that the Frobenius map may be invoked separately all the way up the p-adic tower. So we need ten variables in $\mathbb{F}_q$ for each vector in our search.

Appendix B. The equations and reduction mod p

We give a very brief outline of some facts which arise when viewing this problem through the lens of algebraic geometry. Throughout we assume we are in the context of a unitary space over a field F, where F/K is a quadratic field extension as in the text.

In order for a basis $\mathcal{C}$ to be MU to an ON basis $\mathcal{B}$, it must satisfy three separate uniform sets of highly symmetric equations: (I) equality to $\frac{1}{d}$ of the norm of each vector entry, to prove that the vectors are MU to the computational basis $\mathcal{B}_0$ — which also forces them to be unit vectors; (II) orthogonality among themselves; and (III) mutual unbiasedness to $\mathcal{B}$.

B.1. **The individual defining polynomials reduced modulo a prime.** Zauner's conjecture predicts that the ideal $\mathcal{J}$ of the polynomial ring $\mathbb{Z}[\underline{X}]$ generated by the 261 multivariate quartic and quadratic polynomials in $N = 216$ real variables defining four MUBs in $\mathbb{C}^6$, should be the whole ring $\mathbb{Z}[\underline{X}]$. This is a Gröbner basis calculation way beyond the power of any known algorithm. In particular, good reduction modulo a prime is unprovable, other than by inspection for the primes 2 and 3. So although the following result puts the reduction behaviour of the *individual* MUB defining polynomials into context, it nevertheless says nothing about the multiplicity of reduced solutions in their intersection varieties. See B.2 for the actual polynomials for $d = 2$: the general case is entirely analogous.

Proposition B.1. *The defining polynomials for a set of four MUBs over the complex numbers in dimension* 6 *are each absolutely irreducible. Consequently each polynomial is guaranteed to have good reduction outside a finite set of primes.*

Proof. Let $f(X)$ be one of the defining polynomials, where $X = \underline{X}$ denotes a tuple of variables. Choosing some high enough prime $p > 3$ we verified using MAGMA the irreducibility of f over $\mathbb{F}_p$. Examples of *simple zeroes* for f — that

is, solutions with entries in $\mathbb{F}_p$ where the Jacobian does not vanish completely — are then straightforward to construct by hand. Using [Ra, thm1] it follows therefore that $f(X)$ is *absolutely irreducible*: that is, it remains irreducible over the algebraic closure $\overline{\mathbb{F}_p}$ of $\mathbb{F}_p$.

Finally by theorem 2 of the same paper, since the degree of f is unchanged under reduction modulo p, we may lift that absolute irreducibility to $\mathbb{Q}$. That is to say, it is irreducible over $\overline{\mathbb{Q}}$. The second assertion then follows from Emmy Noether's irreducibility criteria [Sch, §V]. □

The known theoretical upper bounds for these bad primes are huge [Ra]; however in practice the set of bad primes for any known MUB solution is tiny.

B.2. **The shape of the equations in dimension $d = 2$.** We give a representative example only for dimension $d = 2$ for the sake of brevity; the systems scale to higher dimensions in an entirely predictable and uniform way. The notation for the vector entries only applies to this section.

Other than the standard assumption that the first basis of any set always be $\mathcal{B}_0$, we leave them in their most general format so as to illustrate the inherent symmetries. Representing the MUB vectors as usual by columns of a $d \times d$ matrix, we may establish the system as follows, using i as a generic symbol for a generator of the quadratic field extension F/K:

$$\mathcal{B}_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \quad \mathcal{B}_1 = \begin{pmatrix} e+i\epsilon & g+i\gamma \\ f+i\phi & h+i\chi \end{pmatrix}, \quad \mathcal{B}_2 = \begin{pmatrix} s+i\sigma & u+i\mu \\ t+i\tau & v+i\nu \end{pmatrix}.$$

We are forced to have two K-valued variables per F-valued vector entry, per basis vector: since — with an eye to lifting eventually to characteristic zero — we must explicitly build the Hermitian conjugate into the equations. Prior to any adjustments along the lines of those in A.2.3, the resulting equations are as follows.

The roman numerals refer to the introduction to this appendix. (I) First, we must ensure that all entries in all vectors have norm $\frac{1}{d}$, to ensure MUB-ness with the computational basis $\mathcal{B}_0$. This also forces them to be unit vectors. In principle this should give d inhomogeneous quadratic equations per vector, hence d^2 per basis beyond $\mathcal{B}_0$, viz.:

$$\begin{aligned} &e^2+\epsilon^2-1/2\ , \quad f^2+\phi^2-1/2\ , \quad g^2+\gamma^2-1/2\ , \quad h^2+\chi^2-1/2\ , \\ &s^2+\sigma^2-1/2\ , \quad t^2+\tau^2-1/2\ , \quad u^2+\mu^2-1/2\ , \quad v^2+\nu^2-1/2\ . \end{aligned}$$

Note that this places the candidates for MUB vector entries upon a $2d^2$-torus.

(II) Secondly, each basis must be orthonormal. By (I) they are unit vectors, so it remains to check orthogonality. There are $\binom{d}{2}$ comparisons to be made, each with real and imaginary parts, yielding a total of $d(d-1)$ extra homogeneous quadratic equations per basis; in our case:

$$\begin{aligned} &eg+\epsilon\gamma+fh+\phi\chi\ , \quad -e\gamma+\epsilon g-f\chi+\phi h\ , \\ &su+\sigma\mu+tv+\tau\nu\ , \quad -s\mu+\sigma u-t\nu+\tau v. \end{aligned}$$

(III) Finally the actual MUB-ness comparisons require a recursive structure of new equations which — in taking norms of sums of Hermitian products — gives d^2 more

inhomogeneous quartic equations per (unordered) *pair of bases*:

$$\begin{aligned}
e^2s^2 + e^2\sigma^2 + 2efst + 2ef\sigma\tau + 2e\phi s\tau - 2e\phi\sigma t + \epsilon^2 s^2 + \epsilon^2\sigma^2 - 2\epsilon fs\tau \\
+2\epsilon f\sigma t + 2\epsilon\phi st + 2\epsilon\phi\sigma\tau + f^2t^2 + f^2\tau^2 + \phi^2t^2 + \phi^2\tau^2 - 2 \ , \\
e^2u^2 + e^2\mu^2 + 2efuv + 2ef\mu\nu + 2e\phi u\nu - 2e\phi\mu v + \epsilon^2u^2 + \epsilon^2\mu^2 - 2\epsilon fu\nu + 2\epsilon f\mu v \\
+2\epsilon\phi uv + 2\epsilon\phi\mu\nu + f^2v^2 + f^2\nu^2 + \phi^2v^2 + \phi^2\nu^2 - 2 \ , \\
g^2s^2 + g^2\sigma^2 + 2ghst + 2gh\sigma\tau + 2g\chi s\tau - 2g\chi\sigma t + \gamma^2s^2 + \gamma^2\sigma^2 - 2\gamma hs\tau \\
+2\gamma h\sigma t + 2\gamma\chi st + 2\gamma\chi\sigma\tau + h^2t^2 + h^2\tau^2 + \chi^2t^2 + \chi^2\tau^2 - 2 \ , \\
g^2u^2 + g^2\mu^2 + 2ghuv + 2gh\mu\nu + 2g\chi u\nu - 2g\chi\mu v + \gamma^2u^2 + \gamma^2\mu^2 - 2\gamma hu\nu + 2\gamma h\mu v \\
+2\gamma\chi uv + 2\gamma\chi\mu\nu + h^2v^2 + h^2\nu^2 + \chi^2v^2 + \chi^2\nu^2 - 2 \ .
\end{aligned}$$

References

[All] W.O. Alltop, *Complex sequences with low periodic correlations*, IEEE Transactions on Information Theory, Vol. IT–**26**, no. 3, 350–354 (May 1980).

[ABD] Marcus Appleby, Ingemar Bengtsson and Hoan Bui Dang, *Galois Unitaries, Mutually Unbiased Bases, and MUB-Balanced States*, Quantum Information and Computation **15** (15–16) (2015), 1261–1294.

[AFK] Marcus Appleby, Steven Flammia and Gene Kopp, *Ghost SICs and the Wigner function*, in preparation.

[ACW] Aschbacher M., Childs A., Wojcan P., *The limitations of nice mutually unbiased bases*, quantph/0412066 (2004).

[Ba] 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).

[Be1] Ingemar Bengtsson, *Three ways to look at mutually unbiased bases*, AIP Conf. Proc. 889, **40** (2007); http://dx.doi.org/10.1063/1.2713445.

[Be2] Ingemar Bengtsson, Wojciech Bruzda, Asa Ericsson, Jan-Ake Larsson, Wojciech Tadej and Karol Zyczkowski, *Mutually unbiased bases and Hadamard matrices of order six*, J. Math. Phys. **48**, 052106 (2007).

[Be3] Ingemar Bengtsson, *From SICs and MUBs to Eddington*, Journal of Physics: Conference Series, IOP Publishing **254**, Nov (2010). https://doi.org/10.1088/1742-6596/254/1/012007

[Bl] Kate Blanchfield, *Orbits of mutually unbiased bases*, Journal of Physics A **47** (2014) 135303.

[Boy] P. Oscar Boykin, Meera Sitharam, Mohamad Tarifi and Pawel Wocjan, *Real Mutually Unbiased Bases*, https://arxiv.org/pdf/quant-ph/0502024v2.pdf (2005).

[BW] S. Brierley, S. Weigert. *Constructing mutually unbiased bases in dimension six*, Phys. Rev. A **79**, 052316 (2009).

[BWB] Stephen Brierley, Stefan Weigert, Ingemar Bengtsson, *All mutually unbiased bases in dimensions two to five*, Quantum Inf. Comput. **10**, 803–820 (2010).

[Br] Wojciech Bruzda, Wojciech Tadej, Karol Zyczkowski, *Complex Hadamard Matrices (an online catalogue)*: https://chaos.if.uj.edu.pl/ karol/hadamard/

[Ca] Calderbank, AR, Cameron, PJ, Kantor, WM, and Seidel, JJ. *Z4-Kerdock Codes, Orthogonal Spreads, and Extremal Euclidean Line-sets*, Proceedings of the London Mathematical Society **75**.2 (1997): 436-80.

[CS] P.J. Cameron, J.J. Seidel, *Quadratic forms over GF(2)*, Indag. Math. **35** (1973), 1–8.

[Ch] Oleg Chterental and Dragomir Dokovic, *On orthostochastic, unistochastic and qustochastic matrices*, Linear Algebra Appl. **428** (4), 1178–1201 (2008).

[De] Designolle, S. K. G., Skrzypczyk, P., Froewis, F., & Brunner, N. *Quantifying measurement incompatibility of mutually unbiased bases*, Physical Review Letters, 122(050402) doi:10.1103/PhysRevLett.122.050402 (2019).

[D] Thomas Durt, Berthold-Georg Englert, Ingemar Bengtsson, Karol Zyczkowski, *On Mutually Unbiased Bases*, Int. J. Quantum Information, **8**, 535–640 (2010); also http://arxiv.org/abs/1004.3348.

[GR] Chris Godsil, Aidan Roy, *Equiangular lines, mutually unbiased bases, and spin models*, European Journal of Combinatorics, **30** (Jan 2009), 246–262.

[Go] Dardo Goyeneche, *Mutually unbiased triplets from non-affine families of complex Hadamard matrices in dimension six*, J. Phys. A: Math. Theor. **46** 105301 (2013).

[GrM] Grassl, M., McNulty, D., Mišta, L. and Paterek, T., *Small sets of complementary observables*, Phys. Rev. A, **95**(1), 012118, (2017).

[GIJM] Gary R. W. Greaves, Joseph W. Iverson, John Jasper and Dustin G. Mixon, *Frames over finite fields: Basic theory and equiangular lines in unitary geometry*, https://arxiv.org/pdf/2012.12977.pdf (2020).

[Gro] Larry C. Grove, *Classical Groups and Geometric Algebra*, Graduate Studies in Mathematics volume 39, AMS RI (2002).

[Iv] I.D. Ivanovič, *Geometrical description of quantal state determination*, J. Phys. A, **14**: 3241–3245 (1981).

[Jam] Philippe Jaming, Máté Matolcsi, Péter Móra, Ferenc Szöllősi and Mihály Weiner, *A generalized Pauli problem and an infinite family of MUB-triplets in dimension 6*, Journal of Physics A: Mathematical and Theoretical. **42 (24)**: 245305 (2009) DOI: 10.1088/1751-8113/42/24/245305.

[KR] A. Klappenecker and M. Rötteler, *Constructions of Mutually Unbiased Bases*, in *Proceedings of the IEEE International Symposium on Information Theory*, 1740 (2005). Also at quant-ph/0309120.

[KKU] A. I. Kostrikin, I. A. Kostrikin, and V. A. Ufnarovskii, *Orthogonal decompositions of simple Lie algebras (type A_n)*, Proc. Steklov Inst. Math. (4), 113 (1983).

[M] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24**, 235–265 (1997).

[MG] Gary McConnell, David Gross, *Efficient 2-designs from bases exist*, Quantum Inf. Comput. **8** (8), 734–740 (2008).

[WM] Daniel McNulty and Stefan Weigert, *Mutually Unbiased Bases in Composite Dimensions*, in preparation.

[N] Yoichiro Nambu, *Field Theory of Galois' Fields*, in Batalin, I.A.; Isham, C.J.; Vilkovisky, G.A. (eds.) *Quantum field theory and quantum statistics: essays in honour of the sixtieth birthday of E S Fradkin. V. 1*, Adam Hilger, Bristol p. 625-636 (1987).

[Ra] Jean-François Ragot, Probabilistic absolute irreducibility test for polynomials, Journal of Pure and Applied Algebra, **172 (1)** 87-107 (2002).

[Ray] Philippe Raynal, Lü Xin and Berthold-Georg Englert, *Mutually unbiased bases in six dimensions: The four most distant bases*, Physical Review A, **83 (6)** (2011). doi = 10.1103/PHYSREVA.83.062303

[RS] Aidan Roy, A. J. Scott, *Weighted complex projective 2-designs from bases: optimal state determination by orthogonal measurements*, Journal of Mathematical Physics 48, 072110 (2007); quant-ph/0703025.

[Sch] Wolfgang M. Schmidt, *Equations over Finite Fields: An Elementary Approach*, Springer Verlag Berlin LNM 536 (1976).

[Sw] J. Schwinger, *Unitary Operator Bases*, Proceedings of the National Academy of Science **46**, 570–579 (1960).

[Se] Jean-Pierre Serre, *A Course In Arithmetic*, Springer-Verlag NY (1983).

[Sz] Ferenc Szöllősi, *A 2-parameter family of complex Hadamard matrices of order 6, induced by hypocycloids*, Proc. Am. Math. Soc. **138** (3) 921–928 (2010).

[vD] Wim van Dam and Alexander Russell, *Mutually unbiased bases for quantum states defined over p-adic numbers*, arXiv: Quantum Physics (2011) https://arxiv.org/abs/1109.0060v1

[WB] P. Wocjan and T. Beth, *New construction of MUBs in square dimensions*, Quant. Inf. Comput **5** 181 (2005); https://arxiv.org/pdf/quant-ph/0407081.pdf

[WF] William K. Wootters and Brian D. Fields, *Optimal state-determination by mutually unbiased measurements*, Ann. Phys. **191**(2), 363–381 (1989).

[Z] G. Zauner, *Quantendesigns. Grundzüge einer nichtkommutativen Designtheorie*, PhD thesis, University of Vienna (1999). English translation: *Quantum Designs: Foundations of a Non-Commutative Design Theory*, Int. J. Quantum Inf. **9**, pp. 445–507 (2011).

Controlled Quantum Dynamics Theory Group, Imperial College, London
Email address: g.mcconnell@ic.ac.uk

Churchill College, University of Cambridge
Email address: hs696@cam.ac.uk

Pembroke College, University of Oxford
Email address: afaq.tahir@pmb.ox.ac.uk