JOURNAL OF MATHEMATICAL PHYSICS **53**, 032204 (2012)

MUBs inequivalence and affine planes

W. M. Kantor[a)]
Department of Mathematics, University of Oregon, Eugene, Oregon 97403, USA

(Received 25 July 2011; accepted 25 January 2012; published online 23 March 2012)

There are fairly large families of unitarily inequivalent complete sets of $N + 1$ mutually unbiased bases (MUBs) known in $\mathbb{C}^N$ for various prime powers N. The number of such sets is not bounded above by any polynomial as a function of N. While it is standard that there is a superficial similarity between complete sets of MUBs and finite affine planes, there is an intimate relationship between these large families and affine planes. This note briefly summarizes "old" results that do not appear to be well known concerning known families of complete sets of MUBs and their associated planes. © *2012 American Institute of Physics*. [http://dx.doi.org/10.1063/1.3690050]

In memory of Jaap Seidel

I. INTRODUCTION

Starting with Refs. 2, 25, 45, and 46, there has been a great deal of activity constructing, studying and using "complete sets of mutually unbiased bases" (MUBs) of $\mathbb{C}^N$, which are known to exist when N is a prime power (see Ref. 23 and the references therein). It is proved in Ref. 23 that almost all published constructions produce unitarily equivalent complete sets of MUBs, while it is also observed that there are other complete sets. The purpose of this note is to indicate the large number of other known complete sets of MUBs, together with hints of the geometric context of those constructions and non-equivalences. Almost all of these known sets fall into the same framework (Theorem 2.3 for arbitrary prime powers); the only known exceptions are in example 3.7.

Whereas sets of MUBs are usually viewed in terms of sets of vectors, it is easier to discuss automorphisms and equivalence (defined in Sec. II) by using the 1-spaces spanned by those vectors.[48] This leads to the following definitions.

An *orthoframe*[49] in $\mathbb{C}^N$ is a family of N pairwise orthogonal 1-spaces. Distinct orthoframes $\mathcal{F}_1, \mathcal{F}_2$ are called *mutually unbiased* if $|(u_1, u_2)| = 1/\sqrt{N}$ whenever u_i is a unit vector of a member of $\mathcal{F}_i$ for $i = 1, 2$. If a unit vector is taken from each member of an orthoframe the result is an orthonormal basis; orthonormal bases are called MUBs if the same is true for the corresponding orthoframes. *We will view mutually unbiased bases and mutually unbiased orthoframes as* "essentially" *the same objects.* Any family of MUBs has size at most $N + 1$. A set $\mathcal{F}$ of MUBs meeting this bound is called *complete* or *maximal*.

The construction of the sets $\mathcal{F}$ highlighted here occurred in the early 1990's. The authors of Ref. 14 did not know the physics context (in fact they were concerned with the union $\cup\mathcal{F}$ of the members of $\mathcal{F}$). Their construction method was based on connections with affine planes,[50] symplectic spreads (defined in Sec. II), sets $\mathcal{F}$ and error-correcting codes over $\mathbb{Z}_2$ or $\mathbb{Z}_4$. Symplectic spreads were also observed[31] to be related to orthogonal decompositions of the Lie algebras $\mathrm{sl}_n(\mathbb{C})$; this was recently rediscovered in Ref. 10. Relationships between symplectic spreads, $\mathbb{Z}_p$-codes for odd p, and unimodular lattices appear in Ref. 41. A number of papers, such as Ref. 42, use complete sets of MUBs for code-division multiple access in radio communication technologies. The research in Ref. 14 was initiated by Seidel's interest in sets $\mathcal{F}$ related to cubature formulas.[17,40,36]

The subject matter of this brief note has been surveyed already (e.g., in Ref. 29), but emphasizing only planes and codes, not $\mathbb{C}^N$ or $\mathbb{R}^N$. The motivation behind this note is that many of the results in

a)Electronic mail: kantor@uoregon.edu.

Ref. 14 are not widely known to the MUBs community, although Ref. 14 is referenced in several MUBs papers. In particular, Refs. 23 and 39 are essentially the only recent references that observe that there are several inequivalent complete sets of MUBs for some dimensions N. As a function of N the number of such sets is not bounded above by any polynomial (example 2.7(a)).

The simplest examples (examples 2.4, 3.5(a)) arise from 2-dimensional vector spaces, and hence from affine planes over finite fields. It is unknown whether or not there is a general relationship between complete sets of MUBs and affine planes. All known finite affine planes have prime power order; all known complete sets of MUBs have $p^n + 1$ members for some prime p. This may or may not be a coincidence,[51] but we will have nothing to say about planes or complete sets of MUBs that do not arise from a prime power. However, Remark 3.8 can be interpreted as a somewhat negative observation concerning the occurrence of an affine plane in a prime power instance.

Sections II and III deal with complete sets of MUBs in $\mathbb{C}^{p^n}$ for $p = 2$ and $p > 2$, respectively. Section IV briefly considers the situation when complex spaces are replaced by real ones. We have not discussed the quaternionic version of complete sets of MUBs. As in the real and complex cases, these are plentiful.[30]

II. COMPLETE SETS OF MUBS IN $\mathbb{C}^{2^n}$

Equip $V = \mathbb{Z}_2^n$ with its usual dot product $x \cdot y$, and $\mathbb{C}^N$, $N = 2^n$, with its usual Hermitian inner product $(,)$. Label the standard basis of $\mathbb{C}^N$ as e_v, $v \in V$. For $b \in V$, define linear transformations $X(b)$ and $Z(b)$ on $\mathbb{C}^N$ by

$$X(b) : e_v \mapsto e_{v+b} \quad \text{and} \quad Z(b) : e_v \mapsto (-1)^{b\cdot v} e_v. \tag{2.1}$$

The groups $X(V) := \{X(b) \mid b \in V\}$ and $Z(V) := \{Z(b) \mid b \in V\}$ consist of unitary transformations and are isomorphic to the additive group V. Moreover, the group $E := X(V)Z(V)\{\pm I\}$ they generate is an *extraspecial group* (or *Heisenberg group*) of order 2^{1+2n} with center $\mathcal{Z}(E) = \{\pm I\}$, which we identify with $\mathbb{Z}_2$. We also need the slightly larger group $P := E\{\pm I, \pm iI\}$ for the usual $i \in \mathbb{C}$, with center $\mathcal{Z}(P) = \{\pm I, \pm iI\}$ (see the comments preceding Proposition 2.8 below). We use the natural map $^- : P \to \overline{P} = P/\mathcal{Z}(P) \cong V \oplus V$, and therefore avoid using complex conjugation in calculations. The commutator

$$\big(X(a)Z(b)\big)^{-1}\big(X(a')Z(b')\big)^{-1}\big(X(a)Z(b)\big)\big(X(a')Z(b')\big) = a \cdot b' - a' \cdot b \tag{2.2}$$

on P determines a non-degenerate alternating bilinear form $(,)$ on the $\mathbb{Z}_2$-space $P/\mathcal{Z}(P) \cong V \oplus V \cong E/\mathcal{Z}(E)$.

If A is an abelian subgroup of P such that $\overline{A}$ is a *totally isotropic* n-space of $\overline{P}$ (i.e., $\dim\overline{A} = n$ and $(\overline{A},\overline{A}) = 0$), then the set $\mathcal{F}(A) = \mathcal{F}(\overline{A})$ of A-irreducible subspaces of $\mathbb{C}^N$ is an orthoframe. (Equivalently: $\mathcal{F}(A)$ is the set of all one-dimensional subspaces invariant under A.) Moreover, $\mathcal{F}(A)$ is invariant under P. If B is a second such subgroup of P for which $\overline{A} \cap \overline{B} = 0$, then $|(u_1, u_2)| = 2^{-n/2} = 1/\sqrt{N}$ whenever u_1 and u_2 are unit vectors in members of $\mathcal{F}(A)$ and $\mathcal{F}(B)$, respectively (Lemma 3.3 of Ref. 14): $\mathcal{F}(A)$ and $\mathcal{F}(B)$ are mutually unbiased.

Each totally isotropic n-space of $\overline{P}$ arises as some $\overline{A}$, and hence *determines a unique orthoframe* $\mathcal{F}(\overline{A})$.

A *symplectic spread* of the symplectic space $\overline{P}$ (or of $\overline{E} = E/\mathcal{Z}(E)$) is a family Σ of $N + 1$ totally isotropic n-spaces of $\overline{P}$, any two of which have intersection 0. Then every nonzero vector of $\overline{P}$ is in one and only one member of Σ (so Σ partitions the nonzero vectors). *This determines an affine plane of order N*, whose points are the vectors in $\overline{P}$ and whose lines are the translates of the members of Σ by the elements of $\overline{P}$. This is the elementary relationship between affine planes and the sets of MUBs considered in this note (see Ref. 29 and (3.3)).

The rest of this survey is concerned with the following result and its consequences and variations (such as its validity for odd characteristic).

Theorem 2.3 (Theorem 5.6 and Proposition 5.11 of Ref. 14): *Each symplectic spread* Σ *of* $\overline{P}$ *determines a complete set* $\mathcal{F}(\Sigma) = \{\mathcal{F}(\overline{A}) \mid \overline{A} \in \Sigma\}$ of $N + 1$ MUBs in $\mathbb{C}^N$ such that each member is invariant under P.

Let Σ' be another symplectic spread of $\overline{P}$. Then Σ and Σ' are equivalent under a linear transformation of $\overline{P}$ preserving the alternating bilinear form on $\overline{P}$ if, and only if,$\mathcal{F}(\Sigma)$ and $\mathcal{F}(\Sigma')$ are equivalent under a unitary transformation of $\mathbb{C}^N$. (This occurs if and only if the corresponding affine planes are isomorphic.)

Two complete sets of MUBs are called (unitarily) *equivalent* if there is a unitary transformation sending one set to the other as in the theorem.

Example 2.4: The 1-dimensional vector space $V = \mathrm{GF}(2^n)$ over a finite field $\mathrm{GF}(2^n)$ of size 2^n is also an n-dimensional vector space over $\mathrm{GF}(2) = \mathbb{Z}_2$. Let T: $\mathrm{GF}(2^n) \to \mathbb{Z}_2$ be the trace map (so that $T(x) := \sum_{i=0}^{n-1} x^{2^i}$), and use the alternating bilinear form $((a, b), (c, d)) := T(ad - bc)$ on the $2n$-space $V \oplus V = \mathrm{GF}(2^n)^2$ over $\mathrm{GF}(2)$. Then the set Σ of 1-dimensional $\mathrm{GF}(2^n)$-spaces of $V \oplus V$ is[52] a symplectic spread of $\overline{P} = V \oplus V$ (since the determinant $ad - bc$ vanishes on each of them). This produces a complete set $\mathcal{F}(\Sigma)$ of MUBs. As proved in Ref. 23, $\mathcal{F}(\Sigma)$ is equivalent to the complete sets obtained in most previous papers.

We emphasize that there is nothing mysterious about Σ: it is just the subsets $x = 0$ and $y = mx$ of $\mathrm{GF}(2^n)^2$ for $m \in \mathrm{GF}(2^n)$. This should be reminiscent of the lines through the origin in high school (cf. (3.3)). The orthoframes determined by the members of Σ are described using sums involving complex roots of unity, just as in many references such as Refs. 5, 23, and 46 (cf. (3.4) for explicit 1-spaces).

Example 2.5: Some inequivalent examples. There are many other known symplectic spreads of $\overline{P} = V \oplus V$ for suitable n. They are complicated to describe. We present an example taken from Ref. 26.

As in example 2.4, let $V = \mathrm{GF}(2^n)$ and equip the GF(2)-space $V \oplus V$ with the previous bilinear form. Assume that $n > 3$ is odd. Then *the subsets* $x = 0$ *and* $y = m^2x + mT(x) + T(mx)$ *of* $V \oplus V$, $m \in V$, *are a symplectic spread of* $V \oplus V$ *that is not equivalent to the one in* example 2.4.

The complete set of MUBs produced by this example and the one in example 2.4 are not unitarily equivalent, in view of Theorem 2.3. In order to write explicit vectors in $\mathbb{C}^{2^n}$ we would need to lift all of this from $\mathbb{Z}_2$ to $\mathbb{Z}_4$, as discussed at length in Sec. 5 of Ref. 14; cf. (3.4). (For odd prime powers a simpler example, including explicit complex vectors, appears in example 3.5(b).)

We now provide a list indicating that there are many different families with different properties. First, we need to discuss one obvious aspect of any complete set $\mathcal{F}$ of MUBs: its automorphism group $\mathrm{Aut}(\mathcal{F})$. This consists of all unitary transformations of $\mathbb{C}^N$ that send $\mathcal{F}$ to itself. We have already seen that P lies in $\mathrm{Aut}(\mathcal{F})$, inducing the identity on $\mathcal{F}$ (cf. Proposition 2.8); the same is true for all unitary matrices αI with $\alpha \in \mathbb{C}$, $|\alpha| = 1$. Using Theorem 2.3, *every automorphism of* $\mathcal{F}(\Sigma)$ *normalizes* P *and sends* Σ *to itself.* Acting by conjugation, $\mathrm{Aut}(\mathcal{F})$ then induces on $\overline{P}$ a subgroup $\overline{\mathrm{Aut}}(\mathcal{F})$ of the symplectic group (in fact, $\overline{\mathrm{Aut}}(\mathcal{F})$ is the set-stabilizer of Σ in the symplectic group of isometries of $\overline{P}$). This is part of what we will focus on when describing some pairwise inequivalent complete sets of MUBs.

Remark 2.6: In example 2.4, $\overline{\mathrm{Aut}}(\mathcal{F})$ contains all invertible semi-linear transformations $(x, y) \mapsto M(x^\sigma, y^\sigma)$ on $\mathrm{GF}(2^n)^2$ with $\sigma \in \mathrm{Aut}(\mathrm{GF}(2^n))$ and M a linear transformation on the 2-space $\mathrm{GF}(2^n)^2$ of determinant 1. (For all other *known* examples $\overline{\mathrm{Aut}}(\mathcal{F})$ is much smaller.)

For these examples $\mathrm{Aut}(\mathcal{F})$ is 3-transitive on $\mathcal{F}(\Sigma)$, and has a cyclic subgroup of order $2^n + 1$ that is transitive on $\mathcal{F}(\Sigma)$ (cf. example 2.7(c) below). There is also a cyclic subgroup of order $2^n - 1$ fixing two members of $\mathcal{F}(\Sigma)$ and permuting the remaining ones transitively (cf. example 2.7(b) below).

Example 2.7: We indicate some of the *other* known examples of complete sets of MUBs in $\mathbb{C}^N = \mathbb{C}^{2^n}$ arising from symplectic spreads of $\mathbb{Z}_2^{2n}$, together with additional remarks concerning them. We emphasize that examples (a)-(d) occur in $\mathbb{C}^{2^n}$ with $n > 3$ not a power of 2; only in (a) can n be prime. ("Unbounded" means as a function of $N = 2^n$.)

(a) Examples $\mathcal{F}(\Sigma)$ in $\mathbb{C}^{2^n}$ for which $\overline{\mathrm{Aut}}(\mathcal{F})$ *is an extension of the additive group* $\mathrm{GF}(2^n)^+$ *by a subgroup of* $\mathrm{GF}(2^n)^*\mathrm{Aut}(\mathrm{GF}(2^n))$, where $n > 3$ is not a power of 2:[34] $\mathrm{Aut}(\mathcal{F})$ has an elementary abelian subgroup of order 2^n that induces the identity on one member of $\mathcal{F}(\Sigma)$ and is transitive on the remaining ones.
The number of pairwise unitarily inequivalent complete sets of MUBs *of this sort is not bounded above by any polynomial in N.* The number of these complete sets is an increasing function of the number of prime divisors of n.
The smallest N for which there are inequivalent complete sets of MUBs obtained via Theorem 2.3 is $N = 2^5$.
Below, "unbounded" will mean as a function of N.

(b) An unbounded number of examples $\mathcal{F}(\Sigma)$ *in* $\mathbb{C}^{2^n}$ *for which* $\overline{\mathrm{Aut}}(\mathcal{F})$ *is an extension of the multiplicative group of* $\mathrm{GF}(2^n)$ *by a subgroup of* $\mathrm{Aut}(\mathrm{GF}(2^n))$, where n has at least two odd prime factors:[35] $\mathrm{Aut}(\mathcal{F}(\Sigma))$ has a cyclic subgroup of order $2^n - 1$ fixing a pair of members of $\mathcal{F}(\Sigma)$ and transitive on the remaining ones. (For many of these sets $\mathcal{F}(\Sigma)$ of MUBs each member of the indicated pair of orthoframes is sent to itself by $\mathrm{Aut}(\mathcal{F}(\Sigma))$; for others these two are interchanged.)

(c) An unbounded number of examples $\mathcal{F}(\Sigma)$ *in* $\mathbb{C}^{2^n}$ *for which* $\overline{\mathrm{Aut}}(\mathcal{F})$ *is an extension of a cyclic group of order* $2^n + 1$ *by a subgroup of* $\mathrm{Aut}(\mathrm{GF}(2^n))$, where n is neither prime nor a power of 2:[33] $\mathrm{Aut}(\mathcal{F}(\Sigma))$ has a *cyclic subgroup of order* $2^n + 1$ *that is transitive on the family* $\mathcal{F}(\Sigma)$, as in example 2.6.

(d) An unbounded number of examples $\mathcal{F}(\Sigma)$ in $\mathbb{C}^{2^n}$ *with* $n > 9$ *odd and composite, and* $\overline{\mathrm{Aut}}(\mathcal{F}) = 1$:[28] there is a great deal of structure available for these examples, enough to prove that the automorphism group $\mathrm{Aut}(\mathcal{F}(\Sigma))$ is remarkably small and nevertheless to be able to prove inequivalences.

(e) There is a symplectic spread Σ in $\mathbb{Z}_2^n$, $n \equiv 4 \pmod 8$, $n > 4$, arising from the Suzuki group $\mathrm{Sz}(2^{n/4})$ [Proposition 3.3 of Ref. 44], so that $\mathcal{F}(\Sigma)$ is a complete set of MUBs in $\mathbb{C}^{2^n}$.

Each of these families produces sets of 1-spaces of $\mathbb{C}^N$ that can be described explicitly using $\mathbb{Z}_4^n$ together with $V = \mathbb{Z}_2^n$ [Sec. 5 of Ref. 14]; cf. (3.4).

Each of the known families (b)-(e) contains fewer than $\sqrt{N}$ pairwise inequivalent complete sets of MUBs in $\mathbb{C}^N$, which is quite different from the situation in (a).

Examples (a)–(d) were obtained using what amounts to an algorithm that starts with example 2.4 and uses quadratic and alternating bilinear forms on $\mathbb{Z}_2$-spaces together with field changes (Sec. 3 of Ref. 29, Secs. 2.6 and 2.7 of Ref. 34). This approach only works in characteristic 2. There are undoubtedly large numbers of other examples yet to be found.

We have focused on P. We could just as well have used the slightly smaller extraspecial group E for the purpose of describing constructions (though not for full automorphism groups or proving inequivalence!). Namely, a preimage of a totally isotropic n-space of $\overline{E}$ is diagonalizable in $\mathbb{C}^{2^n}$ using a unique orthoframe. Moreover, it is not difficult to use extraspecial groups to test whether or not a given complete set of MUBs arises as in Theorem 2.3:

Proposition 2.8: A complete set $\mathcal{F}$ *of MUBS in* $\mathbb{C}^{2^n}$ *arises as in* Theorem 2.3 *if and only if there is an extraspecial group of* 2^{1+2n} *unitary transformations sending each member of* $\mathcal{F}$ *to itself.*

A starting point for Ref. 14 was the study of "Kerdock codes" over $\mathbb{Z}_2$ and $\mathbb{Z}_4$. In Ref. 13, the term "Kerdock codes" was redefined to be sets of $N^2 + N$ unit vectors in orthonormal bases of $\mathbb{C}^N$ determined by $\cup\mathcal{F}$ for $\mathcal{F}$ in Theorem 2.3.

III. COMPLETE SETS OF MUBS IN $\mathbb{C}^{p^n}$, $p > 2$

Consider an odd prime p and $V = \mathbb{Z}_p^n$ with its usual dot product $x \cdot y$. Equip $\mathbb{C}^N$, $N = p^n$, with its usual Hermitian inner product $(\ ,\ )$. Label the standard basis of $\mathbb{C}^N$ as e_v, $v \in V$. Let $\zeta \in \mathbb{C}$ be a primitive pth root of unity. For $b \in V$, define

$$X(b) : e_v \mapsto e_{v+b} \qquad \text{and} \qquad Z(b) : e_v \mapsto \zeta^{b\cdot v} e_v.$$

The groups $X(V) := \{X(b) \mid b \in V\}$ and $Z(V) := \{Z(b) \mid b \in V\}$ consist of unitary transformations and are isomorphic to the additive group V. Moreover, they generate an extraspecial group (or Heisenberg group) $E := X(V)Z(V)\{\zeta^j I \mid 0 \le j < p\}$ of order p^{1+2n} with center $\mathcal{Z}(E) = \{\zeta^j I \mid 0 \le j < p\}$, which we identify with $\mathbb{Z}_p$. We use the natural map $^-$ as before. The commutator (2.2) again defines a non-degenerate alternating bilinear form on $E/\mathcal{Z}(E) \cong V \oplus V$.

If A is an abelian subgroup of P such that $\overline{A}$ is a totally isotropic n-space of $\overline{E}$, then the set $\mathcal{F}(A)$ of A-irreducible subspaces of $\mathbb{C}^N$ is an orthoframe, and as before is invariant under P. If B is a second such subgroup of P for which $\overline{A} \cap \overline{B} = 0$, then $|(u_1, u_2)| = p^{-n/2} = 1/\sqrt{N}$ whenever u_1 and u_2 are unit vectors in members of $\mathcal{F}(A)$ and $\mathcal{F}(B)$, respectively.

Each totally isotropic n-space of $\overline{E}$ arises as some $\overline{A}$, and hence *determines a unique orthoframe* $\mathcal{F}(\overline{A})$. A *symplectic spread* of $\overline{E}$ is defined as before.

Theorem 2.3 *holds with P replaced by E* [Theorem 11.4, Corollary 11.6 of Ref. 14], so that any symplectic spread Σ of $\overline{E}$ produces a complete set $\mathcal{F}(\Sigma)$ of MUBs in $\mathbb{C}^{p^n}$. Example 2.4 arises as before, and produces the "usual" complete set of MUBs of $\mathbb{C}^{p^n}$;[23] $\mathrm{Aut}(\mathcal{F}(\Sigma))$ behaves as before. Proposition 2.8 holds with 2 replaced by p.

The passage from Σ to $\mathcal{F}(\Sigma)$ is slightly easier to describe in the present setting than in Sec. II. First, note that (for $p = 2$ or p odd) every symplectic spread Σ in $\overline{E} = V \oplus V$ can be assumed to be of the following type:

$$\Sigma \textit{ consists of } 0 \oplus V \textit{ and all } \{(v, Mv) \mid v \in V\} \textit{ for } M \in \mathcal{K}, \tag{3.1}$$

where $\mathcal{K}$ is a set of $|V| = p^n$ symmetric $n \times n$ matrices such that the difference of any two is nonsingular. (This was rediscovered in Theorem 4.4 of Ref. 5, without the connection (3.3) to affine planes. The relationship between symplectic spreads and MUBs was also rediscovered in Sec. 4.5.6 of Ref. 24, again without the connection to affine planes.) If $p > 2$, then

$$\begin{aligned} &\mathcal{F}(\Sigma) = \{\mathcal{F}_\infty,\ \mathcal{F}_M^{\mathcal{K}} \mid M \in \mathcal{K}\},\ \textit{where} \\ &\mathcal{F}_\infty := \{\langle e_v\rangle \mid v \in V\} \textit{ and } \mathcal{F}_M^{\mathcal{K}} := \{\langle \textstyle\sum_{v\in V} \zeta^{a\cdot v + v\cdot Mv/2} e_v\rangle \mid a \in V\}. \end{aligned} \tag{3.2}$$

(Here $v \cdot Mv/2$ is the quadratic form associated with the symmetric bilinear form $u \cdot Mv$.) The corresponding affine plane has points $(x, y) \in V \oplus V$ and the following lines:

$$x = b \textit{ and } y = Mx + b \textit{ for } b \in V,\ M \in \mathcal{K}. \tag{3.3}$$

The simplest $\mathcal{K}$ is $\mathrm{GF}(p^n)$ using M: $x \mapsto mx$. Directly verifying (without use of P) that (3.2) defines MUBs is straightforward: if $e_{a,M} := \frac{1}{\sqrt{N}} \sum_{v\in V} \zeta^{a\cdot v + v\cdot Mv/2} e_v$, then $(e_{a,M}, e_{a',M'}) = \frac{1}{N} \sum_{v\in V} \zeta^{d\cdot v + v\cdot \Delta v/2}$ with $d := a - a'$, $\Delta := M - M'$, so that $(e_{a,M}, e_{a,M}) = \frac{1}{N} N$. If $d \neq 0$ and $\Delta \neq O$, use $u = v - v'$ in the calculation

$$\begin{aligned} |(e_{a,M}, e_{a',M'})|^2 &= \tfrac{1}{N^2} \textstyle\sum_{v,v'\in V} \zeta^{d\cdot v + v\cdot \Delta v/2 - d\cdot v' - v'\cdot \Delta v'/2} \\ &= \tfrac{1}{N^2} \textstyle\sum_{u\in V} \zeta^{d\cdot u - u\cdot \Delta u/2} \sum_{v\in V} \zeta^{-v\cdot \Delta u} \\ &= \tfrac{1}{N^2} N, \end{aligned}$$

since Δ is symmetric and $\Delta u \neq 0$ for $u \neq 0$ and $M \neq M'$ in $\mathcal{K}$, while $\sum_{j=0}^{p-1} \zeta^j = 0$.

For the case $p = 2$ in Sec. II there are minor complications: the end of (3.2) is replaced by

$$\mathcal{F}_M^{\mathcal{K}} := \Big\{ \langle \sum_{v\in V} i^{2\hat{a}\cdot\hat{v} + \hat{v}\cdot\hat{M}\hat{v}} e_v\rangle \,\Big|\, a \in V \Big\}, \tag{3.4}$$

where the "hats" denote that the vector or matrix now has entries 0, 1 *viewed inside* $\mathbb{Z}_4$ (so that $\hat{a}, \hat{v} \in \mathbb{Z}_4^n$). Direct verification that we have MUBs is as before with additional bookkeeping. The difference between the situations $p = 2$ and $p > 2$ becomes even more significant when discussing known constructions.

Most known constructions for odd p are based on generalizations of fields called *semifields*: algebras satisfying the usual axioms for a field except for the associativity and commutativity of

multiplication. We refer to Refs. 7 and 32 for further information. Semifields amount to having the set $\mathcal{K}$ in (3.1) closed under addition; in this case Σ is called a "symplectic semifield spread". Every commutative semifield corresponds in a somewhat indirect manner to a symplectic semifield spread (cf. Proposition 3.8 of Ref. 32 or the end of Remark 3.6; this statement involves two different semifields). Therefore, we will refer to instances of commutative semifields as if they were examples of symplectic spreads.

There are many papers containing (among other things) surveys of commutative semifields, so we mention only two (Refs. 7 and 32). Since there recently have been new constructions for commutative odd order semifields every few months, the following list is guaranteed to be out of date.

Example 3.5: We survey the known examples of symplectic spreads of $\overline{E} \cong \mathbb{Z}_p^{2n}$ for odd p, and hence implicitly the corresponding complete sets of MUBs in $\mathbb{C}^{p^n}$ obtained as in Theorem 2.3. We give explicit complete sets of MUBs in (b).

(a) The analogue of example 2.4 uses a 2-dimensional vector space over GF(p^n). *These are the only complete sets of* MUBs *arising in* Proposition 2.8 *when* $N = p^n = p$, i.e., when $|E| = p^3$.

(b) Older families[1,18] have an unbounded number of pairwise inequivalent examples as a function of n. *We present examples not unitarily equivalent to the one in* (a) *nor to one another*, based on Ref. 3. Let V be $K = \mathrm{GF}(p^n)$ with n odd, choose an integer s relatively prime to n such that $1 \le s < n/2$, and let $T(x) := \sum_{j=0}^{n-1} x^{p^j}$, $x \in K$, be the trace map. Label the standard orthonormal basis of $\mathbb{C}^{p^n}$ as e_x, $x \in K$, with corresponding orthoframe $\mathcal{F}_\infty$. Then $\mathcal{F} := \{\mathcal{F}_\infty,\ \mathcal{F}[b] \mid b \in K\}$ *is a complete set of* MUBs, where

$$\mathcal{F}[b] := \left\{ \langle \sum_{x \in K} \zeta^{T(ax) + T(bx^{p^{n-s}+1} + b^{p^s} x^{p^s+1})/2} e_x \rangle \,\middle|\, a \in K \right\}.$$

If the exponents are written $a \cdot x + x \cdot (bx^{p^{n-s}} + b^{p^s} x^{p^s})/2$ using a dot product on K as in (3.2), the result is an equivalent set of MUBs. Allowing $s = 0$ would give (a).

(c) Families with $p = 3$ (Refs. 15, 22, 43, 38, 16, and 20): for some of these the number of pairwise inequivalent examples is unbounded as a function of n.

(d) Recent families (Refs. 47, 12, 37, 7, and 8): for some of these the number of pairwise inequivalent examples is unbounded as a function of n.

(e) There are also two families of examples not related to semifields,[4,27] the first having $p = 3$. This is very different from the situation in characteristic 2, where examples 2.7(b)–2.7(d) are fairly large families not corresponding to semifields. (Examples 2.7(a) correspond to semifields.)

The number of items in the above list attests to the amount of research occurring on this topic. Nevertheless, each of these families is associated with fewer than $\sqrt{N}$ pairwise inequivalent complete sets of MUBs in $\mathbb{C}^N$. In view of example 2.7(a), this means that at present there are far fewer complete sets that have been obtained using odd characteristic than there are using characteristic 2. As in Sec. II, there are undoubtedly large numbers of examples yet to be found.

Remark 3.6: Contrary to p. 255 of Ref. 23, *it is not the case that* "there is a natural correspondence between semifields and symplectic spreads (see for example" Proposition 3.8 of Ref. 32). The cited result in Ref. 32 only concerns commutative semifields and symplectic *semifield* spreads, not general symplectic spreads. Therefore, contrary to p. 255 of Ref. 23, it is not the case that their "mutually unbiased bases. . . are equivalent to those of" Ref. 14. Examples 2.7(b)–2.7(e) and 3.5(e) do not arise from semifields other than fields.

On the other hand, the complete sets of MUBs obtained in Ref. 23 (by using $\sum_{v \in V} \zeta^{a \cdot v + b \cdot (v * v)/2}$ in place of the vector sum in (3.2) for a commutative semifield multiplication * on V) are seen to be among those in Ref. 14 by a straightforward use of Proposition 2.8. Even simpler is to match up with (3.2): if we let ϵ_i denote the ith standard basis vector of V, then "solve" $b \cdot (x * y) = x \cdot My$ for the symmetric matrix $M = (M_{ij})$ as a function of $b \in V$ via $M_{ij} = \epsilon_i \cdot M\epsilon_j = b \cdot (\epsilon_i * \epsilon_j)$, so that $b \cdot (v * v) = v \cdot Mv$.

The complete sets of MUBs described in Ref. 23 are also obtained in Ref. 39, but the latter paper goes further:

Example 3.7: Complete sets $\mathcal{F}^f$ of MUBs in $\mathbb{C}^{3^n}$ are obtained in Ref. 39 for each odd $n \geq 5$, corresponding to the "planar functions" (Ref. 53) $f(x) = x^{(3^k+1)/2}$ on $K = \mathrm{GF}(3^n) \cong V$ (where $2n$ and k are relatively prime and $k \not\equiv \pm 1 \pmod{2n}$) [Theorem 6.2 of Ref. 16]. This time $\mathcal{F}^f$ consists of $\mathcal{F}_\infty$ and all $\mathcal{F}_b^f := \{\langle \sum_{v\in K} \zeta^{a\cdot v+b\cdot f(v)} e_v\rangle \mid a \in K\}$ for $b \in K$. A direct proof that $\mathcal{F}^f$ is a set of MUBs is similar to the one following (3.3), using $v - v' = u$ and $\zeta^{(a-a')\cdot v+(b-b')\cdot f(v)-(a-a')\cdot v'-(b-b')\cdot f(v')} = \zeta^{(a-a')\cdot u}\zeta^{(b-b')\cdot(f(v)-f(v-u))}$. It is easy to use Proposition 2.8 to show that these do not arise from symplectic spreads in any extraspecial p-group (this equivalence question is not discussed in Ref. 39). *These are the only known complete sets of* MUBs *that do not arise from symplectic spreads using extraspecial groups.* These have a property in common with complete sets arising from symplectic semifields: there is a group of N^2 automorphisms (generated by all $e_x \mapsto \zeta^{c\cdot x} e_x$ and all $e_x \mapsto \zeta^{c\cdot f(x)} e_x$, $c \in V$) having orbits of size 1 and N^2 on $\cup\mathcal{F}^f$.

This unusual family of complete sets of MUBs suggests that there are many more families yet to be discovered that are not related to extraspecial groups.

Remark 3.8: Where are the planes? Each of the known examples in Sec. II and III has at least one associated affine plane. *Where are these planes*?

For complete sets $\mathcal{F}$ of MUBs obtained as in Theorem 2.3, the answer is similar to Proposition 2.8: $\mathcal{F}$ uniquely determines a group P or E of automorphisms, hence also a symplectic spread Σ and set $\mathcal{K}$ as in (3.1), and finally an affine plane π as in (3.3). Moreover, by (3.1) and (3.3), $\mathcal{F}$ can be identified with the set Σ of parallel classes of π, and then points can be identified with $V \oplus V$, or equivalently, with (suitable!) subsets of $\cup\mathcal{F}$ consisting of one element from each member of $\mathcal{F}$.

For complete sets obtained as in example 3.7, the associated affine plane $\pi(f)$ has as points the vectors in $V \oplus V$ and as lines the sets $x = b$ and $y = f(x + a) + b$ ($a, b \in K$). It would be helpful to "see" this plane in terms of $\mathcal{F}^f$, perhaps using $\mathcal{F}^f$ as the set of $N + 1$ parallel classes of lines and (as above) "natural" subsets of $\cup\mathcal{F}^f$ corresponding to points. However, *such a description could not be invariant under the automorphism group of order* N^2 *mentioned in* example 3.7: $\pi(f)$ has no automorphism group of that order inducing the identity on one of its parallel classes.[54] In other words, there is no canonical (i.e., $\mathrm{Aut}(\mathcal{F}^f)$-invariant) way to obtain such a description from $\mathcal{F}^f$. Nevertheless, it is at least somewhat plausible that there might be an entirely different way to reconstruct $\pi(f)$ either from $\mathcal{F}^f$ or from some entirely different complete set of MUBs associated with f.

IV. COMPLETE SETS OF MUBS IN $\mathbb{R}^{2^n}$

We return to the group E in Sec. II. This time we restrict to vectors in $\mathbb{R}^N$, $N = 2^n$, and use the usual inner product $(\,,)$. There is additional structure to consider: the function $Q: E \to \mathbb{Z}_2$ given by $Q(x) = x^2 \in \mathcal{Z}(E)$ determines a quadratic form $\overline{Q} : \overline{E} \to \mathbb{Z}_2$ that polarizes to the alternating bilinear form $(\,,)$ appearing in Sec. II (i.e., $\overline{Q}(x + y) - \overline{Q}(x) - \overline{Q}(y) = (x, y)$ for all $x, y \in \overline{E}$). This time we are interested in subgroups A of E such that $\overline{A}$ is *totally singular*: $\overline{Q}(\overline{A}) = 0$ (and hence also $(\overline{A}, \overline{A}) = 0$). If $\overline{A}$ is a totally singular n-space then the set $\mathcal{F}(A) = \mathcal{F}(\overline{A})$ of A-irreducible subspaces of $\mathbb{R}^N$ is an *orthoframe*: a set of N pairwise orthogonal 1-spaces. Once again, if B is a second such subgroup of E for which $\overline{A} \cap \overline{B} = 0$, then $|(u_1, u_2)| = 1/\sqrt{N}$ whenever u_1 and u_2 are unit vectors in members of $\mathcal{F}(A)$ and $\mathcal{F}(B)$, respectively. Any family $\mathcal{F}$ of orthoframes satisfying this last property involving pairs of unit vectors has size at most $\frac{1}{2}N + 1$ [(3.9) of Ref. 14]. When equality holds we have a *complete set of* MUBs *of* $\mathbb{R}^N$. Note that such sets are smaller than the complete sets in Secs. II and III. Moreover, the factor $\frac{1}{2}$ leads us only to use vector spaces $\overline{E}$ of characteristic 2. See Ref. 9 for more information concerning sets of real MUBs.

An *orthogonal spread* of $\overline{E}$ is a family Σ of $2^{n-1} + 1$ totally singular n-spaces of $\overline{E}$ any two of which have zero intersection; every member of $\{0 \neq x \in \overline{E} \mid \overline{Q}(x) = 0\}$ lies in one and only one member of Σ. As in Theorem 2.3 there is a corresponding complete set $\mathcal{F}(\Sigma)$ of MUBs of $\mathbb{R}^N$

[Theorem 3.4 of Ref. 14]; and the equivalence part of the theorem continues to hold Proposition 3.16 of Ref. 14. However, each orthogonal spread is associated with a somewhat large number of possibly non-isomorphic affine planes [Sec. 7 of Ref. 14].

Example 4.1: All orthogonal spreads of $\mathbb{Z}_2^{2n}$ arise from symplectic spreads of $\mathbb{Z}_2^{2n-2}$, and *n must be even* (Refs. 19 or 21 or Secs. 2 and 3 of Ref. 26). One of these orthogonal spreads corresponds to example 2.4; the other known ones correspond to examples 2.7(a)–2.7(d) (note that n here corresponds to $n - 1$ in those examples). All comments about numbers of inequivalent complete sets of MUBs hold as before.

In fact the relationship with orthogonal spreads is an essential ingredient for all of the constructions in examples 2.7(a)–2.7(d).

ACKNOWLEDGMENTS

I am grateful to Mary Beth Ruskai for many very helpful comments. This research was supported in part by NSF Grant DMS 0753640.

[1] Albert, A. A., "Generalized twisted fields," Pacific J. Math. **11**, 1–8 (1961).
[2] Alltop, W. O., "Complex sequences with low periodic correlations," IEEE Trans. Inf. Theory **26**, 350–354 (1980).
[3] Bader, L., Kantor, W. M., and Lunardon, G., "Symplectic spreads from twisted fields," Boll. Unione Mat. Ital. **8-A**, 383–389 (1994).
[4] Ball, S., Bamberg, J., Lavrauw, M., and Penttila, T., "Symplectic spreads," Designs, Codes, Cryptogr. **32**, 9–14 (2004).
[5] Bandyopadhyay, S., Boykin, P. O., Roychowdhury, V., and Vatan, F., "A new proof for the existence of mutually unbiased bases," Algorithmica **34**, 512–528 (2002).
[6] Bengtsson, I., "MUBs, polytopes, and finite geometries," in *Foundations of Probability and Physics*, edited by A. Khrennikov, AIP Conference Proceedings Vol. 750 (AIP, Melville, NY, 2005), Vol. 3, pp. 63–69.
[7] Bierbrauer, J., "Commutative semifields from projection mappings," Des. Codes Cryptogr. **61**, 187–196 (2011).
[8] Bierbrauer, J. and Kantor, W. M., "A projection construction for semifields" (submitted).
[9] Boykin, P. O., Sitharam, M., Tarifi, M., and Wocjan, P., "Real mutually unbiased bases," e-print arXiv:quant-ph/0502024v2.
[10] Boykin, P. O., Sitharam, M., Tiep, P. H., and Wocjan, P., "Mutually unbiased bases and orthogonal decompositions of Lie algebras," Quantum Inf. Comput. **7**, 371–382 (2007).
[11] Budaghyan, L. and Carlet, C., "Classes of quadratic APN trinomials and hexanomials and related structures," IEEE Trans. Inf. Theory **54**, 2354–2357 (2008).
[12] Budaghyan, L. and Helleseth, T., "New commutative semifields defined by new PN multinomials," Cryptogr. Commun. **3**, 1–16 (2011).
[13] Calderbank, A. R., "Reed Muller codes and symplectic geometry," in *Recent Trends in Coding Theory and its Applications*, edited by W.-C. Li, AMS/IP Studies in Advanced Mathematics Vol. 41 (AMS, Providence, 2007), pp. 123–147.
[14] Calderbank, A. R., Cameron, P. J., Kantor, W. M., and Seidel, J. J., "$\mathbb{Z}_4$-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets," Proc. LMS **75**, 436–480 (1997).
[15] Cohen, S. D. and Ganley, M. J., "Commutative semifields, two–dimensional over their middle nuclei," J. Algebra **75**, 373–385 (1982).
[16] Coulter, R. S. and Matthews, R. W., "Planar functions and planes of Lenz-Barlotti class II," Designs, Codes, Cryptogr. **10**, 167–184 (1997).
[17] Delsarte, P., Goethals, J. M., and Seidel, J. J., "Bounds for systems of lines, and Jacobi polynomials," Philips Res. Rep. **30**, 91–105 (1975).
[18] Dickson, L. E., "On finite algebras," Göttinger Nachrichten, 358–393 (1905).
[19] Dillon, J. F., "On Pall partitions for quadratic forms" (unpublished).
[20] Ding, C. and Yuan, J., "A family of skew Paley-Hadamard difference sets," J. Comb. Theory Ser. A **113**, 1526–1535 (2006).
[21] Dye, R. H., "Partitions and their stabilizers for line complexes and quadrics," Ann. Mat. Pura. Appl. **114**, 173–194 (1977).
[22] Ganley, M. J., "Central weak nucleus semifields," Eur. J. Comb. **2**, 339–347 (1981).
[23] Godsil, C. and Roy, A., "Equiangular lines, mutually unbiased bases, and spin models," Eur. J. Comb. **30**, 246–262 (2009).
[24] Howe, R., "Nice error bases, mutually unbiased bases, induced representations, the Heisenberg group and finite geometries," Indag. Math. **16**, 553–583 (2005).
[25] Ivanović, I. D., "Geometrical description of quantal state determination," J. Phys. A **14**, 3241–3245 (1981).
[26] Kantor, W. M., "Spreads, translation planes and Kerdock sets. I, II," SIAM J. Algebraic Discrete Methods **3**, 151–165, 308–318 (1982).
[27] Kantor, W. M., "Ovoids and translation planes," Can. J. Math. **34**, 1195–1207 (1982).
[28] Kantor, W. M., "Projective planes of order q whose collineation groups have order q^2," J. Algebr. Comb. **3**, 405–425 (1994).

[29] Kantor, W. M., "Codes, quadratic forms and finite geometries," in *Different Aspects of Coding Theory*, edited by A. R. Calderbank, Proceedings of Symposia in Applied Mathematics Vol. 50 (American Mathematical Society, Providence, 1995), pp. 153–177.
[30] Kantor, W. M., "Quaternionic line-sets and quaternionic Kerdock codes," Linear Algebr. Appl. **226–228**, 749–779 (1995).
[31] Kantor, W. M., "Note on Lie algebras, finite groups and finite geometries," in *Groups, Difference Sets, and the Monster*, edited by K. T. Arasu *et al.* (de Gruyter, Berlin, 1996), pp. 73–81.
[32] Kantor, W. M., "Commutative semifields and symplectic spreads," J. Algebra **270**, 96–114 (2003).
[33] Kantor, W. M. and Williams, M. E., "New flag-transitive affine planes of even order," J. Comb. Theory Ser. A **74**, 1–13 (1996).
[34] Kantor, W. M. and Williams, M. E., "Symplectic semifield planes and $\mathbb{Z}_4$-linear codes," Trans. AMS **356**, 895–938 (2004).
[35] Kantor, W. M. and Williams, M. E., "Nearly flag-transitive affine planes," Adv. Geom. **10**, 161–183 (2010).
[36] König, H., "Isometric imbeddings of Euclidean spaces into finite-dimensional l_p-spaces," in *Banach Center Publications* (PWN-Polish Scientific, Warsaw, 1995), Vol. 34, pp. 79–87.
[37] Lunardon, G., Marino, G., Polverino, O., and Trombetti, R., "Symplectic semifield spreads of $PG(5, q)$ and the Veronese surface," Ric. Mat. **60**, 125–142 (2011).
[38] Penttila, T. and Williams, B., "Ovoids of parabolic spaces," Geom. Dedic. **82**, 1–19 (2000).
[39] Roy, A. and Scott, A. J., "Weighted complex projective 2-designs from bases: optimal state determination by orthogonal measurements," J. Math. Phys. **48**, 072110 (2007).
[40] Seidel, J. J., "Harmonics and combinatorics," in *Special Functions: Group Theoretical Aspects and Applications*, edited by R. A. Askey *et al.* (Reidel, Dordrecht, 1984), pp. 287–303.
[41] Scharlau, R. and Tiep, P. H., "Symplectic groups, symplectic spreads, codes, and unimodular lattices," J. Algebra **194**, 113–156 (1997).
[42] Strohmer, T., Heath, R. W., Jr., and Paulraj, A. J., "On the design of optimal spreading sequences for CDMA systems," in *The Thirty-Sixth Asilomar Conference on Signals, Systems & Computers*, edited by M. B. Matthews (IEEE, 2002), pp. 1434–1438.
[43] Thas, J. A. and Payne, S. E., "Spreads and ovoids in finite generalized quadrangles," Geom. Dedic. **52**, 227–253 (1994).
[44] Tits, J. "Ovoïdes et groupes de Suzuki," Arch. Math. **13**, 187–198 (1962).
[45] Wootters, W. K., "A Wigner-function formulation of finite-state quantum mechanics," Ann. Phys. **176**, 1–21 (1987).
[46] Wootters, W. K. and Fields, B. D. "Optimal state-determination by mutually unbiased measurements," Ann. Phys. **191**, 363–381 (1989).
[47] Zha, Z. and Wang, X. "New families of perfect nonlinear polynomial functions," J. Algebra **322**, 3912–3918 (2009).
[48] We do not use bases since automorphisms do not preserve bases (e.g., $Z(b)$ in (2.1) does not preserve the standard basis).
[49] We avoid the term *frame* used in Ref. 14 so as not to conflict with other uses for that word.
[50] An *affine plane of order N* is a combinatorial object consisting of a set of N^2*points*, together with $N^2 + N$ point-sets of size N called *lines*, such that any two distinct points are on a unique line. Then the lines fall into $N + 1$ "parallel classes" of size N, each of which partitions the points.
[51] See the delectable observation at the end of Ref. 6.
[52] We are identifying isomorphic vector spaces.
[53] This means that $f(x + a) - f(x) = b$ has a unique solution x for any $a \neq 0$ and b in K.
[54] Curiously, there is also a group of N^2 automorphisms of $\pi(f)$ that does not act on $\mathcal{F}^f$. (This is the group of all $(x, y) \mapsto (x + c, y + d)$, $c, d \in K$, having orbits of size N and N^2 on the set of all lines.)