J Algebr Comb (2007) 25:111–123
DOI 10.1007/s10801-006-0002-y

The limitations of nice mutually unbiased bases

Michael Aschbacher · Andrew M. Childs · Paweł Wocjan

Published online: 11 July 2006

Abstract Mutually unbiased bases of a Hilbert space can be constructed by partitioning a unitary error basis. We consider this construction when the unitary error basis is a nice error basis. We show that the number of resulting mutually unbiased bases can be at most one plus the smallest prime power contained in the dimension, and therefore that this construction cannot improve upon previous approaches. We prove this by establishing a correspondence between nice mutually unbiased bases and abelian subgroups of the index group of a nice error basis and then bounding the number of such subgroups. This bound also has implications for the construction of certain combinatorial objects called nets.

Keywords Quantum information theory · Mutually unbiased bases · Quantum designs

1. Introduction

Two orthonormal bases $\mathcal{B}$ and $\mathcal{B}'$ of the Hilbert space $\mathbb{C}^d$ are called *mutually unbiased* if and only if

$$|\langle\phi|\psi\rangle|^2 = 1/d \tag{1}$$

M. Aschbacher
Department of Mathematics, California Institute of Technology, Pasadena, CA 91125, USA
e-mail: asch@its.caltech.edu

A. M. Childs
Institute for Quantum Information, California Institute of Technology, Pasadena, CA 91125, USA
e-mail: amchilds@caltech.edu

P. Wocjan (✉)
Institute for Quantum Information, California Institute of Technology, Pasadena, CA 91125, USA
e-mail: wocjan@cs.caltech.edu

for all $|\phi\rangle \in \mathcal{B}$ and all $|\psi\rangle \in \mathcal{B}'$. (Here we use Dirac's bra-ket notation, where the ket $|\psi\rangle$ denotes a column vector, the corresponding bra $\langle\psi|$ denotes its conjugate transpose, and $\langle\phi|\psi\rangle$ denotes the standard inner product of the vectors $|\psi\rangle$ and $|\phi\rangle$.) Let $N_{\mathrm{MUB}}(d)$ denote the maximum cardinality of any set containing pairwise mutually unbiased bases (MUBs) of $\mathbb{C}^d$. It is an open question to determine $N_{\mathrm{MUB}}(d)$ for every d.

It is well known that $N_{\mathrm{MUB}}(d)$ cannot exceed $d+1$ [4, 7, 10, 12, 24]. There exist constructions that attain this upper bound when d is a prime [11], and more generally, when d is a prime power [4, 6, 14, 24, 25]. In other words, we have

$$N_{\mathrm{MUB}}(p^e) = p^e + 1 \tag{2}$$

for any prime p and $e \geq 1$.

For non-prime power dimensions, the maximal number of mutually unbiased bases $N_{\mathrm{MUB}}(d)$ is not known—even the smallest case, $d = 6$, is unresolved. The first construction of mutually unbiased bases in non-prime power dimensions appears in [14, 25]. If $d = mn$, then we have

$$N_{\mathrm{MUB}}(d) \geq \min\{N_{\mathrm{MUB}}(m), N_{\mathrm{MUB}}(n)\}\,. \tag{3}$$

For arbitrary d, let $\pi(d)$ denote the set of prime factors of d, and let d_p denote the largest power of $p \in \pi(d)$ that divides d. Then

$$N_{\mathrm{MUB}}(d) \geq \min_{p\in\pi(d)} N_{\mathrm{MUB}}(d_p) = \min_{p\in\pi(d)} d_p + 1 =: N(d)\,. \tag{4}$$

We will refer to this construction as the *reduce to prime power construction*. In particular, this result implies that $N_{\mathrm{MUB}}(d) \geq 3$ for any dimension d. (Another proof of this fact can be found in [4]. Note also that this construction is reminiscent of MacNeish's construction of $N(d) - 2$ mutually orthogonal Latin squares of order d [14, 19].)

Based on (4), one might suspect that $N_{\mathrm{MUB}}(d)$ is given by $N(d)$ for any dimension d. But this is false; a counterexample is provided by the construction in [23], which yields more MUBs for certain dimensions than the reduce to prime power construction. It was shown that for all square dimensions $d = s^2$, $N_{\mathrm{MUB}}(d) \geq N_{\mathrm{MOLS}}(s) + 2$, where $N_{\mathrm{MOLS}}(s)$ is the maximal number of mutually orthogonal Latin squares of size s. When $d = 26^2$, for example, this shows $N_{\mathrm{MUB}}(26^2) \geq 6$, whereas $N(26^2) = 5$. Note that this construction also has consequences for non-square dimensions since we can use the decomposition (3).

For prime power dimensions $d = p^e$, there are two types of constructions that attain the upper bound $d + 1$. The first is based on exponential sums in finite fields and Galois rings [14]. In [2] it was shown that a natural generalization of this construction to arbitrary dimensions cannot yield more MUBs than the reduce to prime power construction.

The second construction which attains the maximal number of MUBs in prime power dimensions is based on finding maximal commuting subsets of matrices of a unitary error basis [4]. This idea can be applied in any dimension, but it is not known

how many MUBs can be produced in this way when the dimension is not a prime power.

In this paper we concentrate on the second construction in the case in which the unitary error basis is a nice error basis. A nice error basis is a special type of unitary error basis with an underlying group structure. We show that the maximal number of MUBs produced by partitioning a nice error basis, $N_{\mathrm{NMUB}}(d)$, cannot exceed the number $N(d)$ produced by the reduce to prime power construction. This shows that if we want to construct a large number of MUBs by partitioning a unitary error basis, that basis should be *wicked* (i.e., not equivalent to any nice error basis).

Mutually unbiased bases are of interest not only as mathematical objects in their own right, but also for applications in quantum information theory. For example, quantum mechanics can be used to securely distribute a secret key by encoding information into two different mutually unbiased bases [5]. MUBs are also useful in the construction of minimal von Neumann measurements for quantum state identification [24], among other applications.

The remainder of the paper is organized as follows. In Section 2, we review the construction of mutually unbiased bases from a partition of a unitary error basis, and in particular, from a nice error basis. We also establish a connection between nice mutually unbiased bases and sets of trivially intersecting abelian subgroups of the index group of a nice error basis. In Section 3, we prove the main result by establishing a bound on the size of such sets. Then, in Section 4, we discuss examples that show the upper bound of $N(d)$ on $N_{\mathrm{NMUB}}(d)$ is achieved. In Section 5, we give a stronger bound for the particular case where the group is abelian and its structure is known. In Section 6, we point out that our results also provide bounds on the sizes of nets constructed in a particular way, and show that a complete set of nice MUBs corresponds to an affine translation plane. Finally, we conclude in Section 7 with a discussion of the results and some open problems.

2. Nice mutually unbiased bases

We will consider mutually unbiased bases constructed from certain kinds of unitary error bases. A *unitary error basis* $\mathcal{E}$ is a basis of the vector space of complex $d \times d$ matrices that is orthogonal with respect to the trace inner product. In other words, a set of unitary matrices $\mathcal{E} := \{U_1 = \mathbb{1}, U_2, \ldots, U_{d^2}\}$ is a unitary error basis iff

$$\mathrm{tr}(U_k^\dagger U_l) = d\,\delta_{k,l}, \quad k, l \in \{1, \ldots, d^2\}. \tag{5}$$

Two constructions of unitary error bases are known: nice error bases, a group-theoretic construction due to Knill [16]; and shift-and-multiply bases, a combinatorial construction due to Werner [22]. There exist nice error bases that are not equivalent to any shift-and-multiply basis, as well as shift-and-multiply bases that are wicked [15].

In this paper we are concerned primarily with nice error bases, which are unitary error bases with an underlying group structure. We will use a definition that appears different from, but is equivalent to, the one proposed by Knill (cf. [13]). To give this definition, we begin with some background material on projective representations.

Let $\mathrm{GU}_d(\mathbb{C})$ be the d-dimensional general unitary group over the complex numbers, and let $P : \mathrm{GU}_d(\mathbb{C}) \to \mathrm{PGU}_d(\mathbb{C})$ be the projection onto the projective general unitary group $\mathrm{PGU}_d(\mathbb{C}) = \mathrm{GU}_d(\mathbb{C})/Z(\mathrm{GU}_d(\mathbb{C}))$, where $Z(\cdot)$ denotes the center. A d-dimensional *projective (unitary) representation* of a finite group G is a homomorphism $\rho : G \to \mathrm{PGU}_d(\mathbb{C})$. Given any such map, one can choose a finite preimage $\hat{G}$ of $\rho(G)$ in $\mathrm{GU}_d(\mathbb{C})$ with $P(\hat{G}) = \rho(G)$. The group $\hat{G}$ is of *central type* if $|\rho(G)| = d^2$ and $\mathrm{tr}\,\hat{g} = 0$ for each $\hat{g} \in \hat{G} - Z(\mathrm{GU}_d(\mathbb{C}))$. If ρ is faithful and some (and hence each) preimage $\hat{G}$ is of central type, then we say ρ is of *central type*. Note that a finite subgroup $\hat{G} \leq \mathrm{GU}_d(\mathbb{C})$ with $|\hat{G}|/|Z(\hat{G})| = d^2$ is of central type iff the character χ of $\hat{G}$ on $\mathbb{C}^d$ is irreducible, which in turn is true iff $\chi(\hat{g}) = 0$ for each $\hat{g} \in \hat{G} - Z(\hat{G})$.

Nice error bases can be defined as follows:

Definition 1 (Nice error basis). Let G be a group of order d^2 with identity element 1. A subset $\mathcal{N} \subset \mathrm{GU}_d(\mathbb{C})$ is a *nice error basis* if there exists a projective representation $\rho : G \to \mathrm{PGU}_d(\mathbb{C})$ of central type such that $\mathcal{N} = \{U_g : g \in G\}$, with $P(U_g) = \rho(g)$ and $U_1 = 1$.

The group G is called the *index group* of the nice error basis $\mathcal{N}$. Notice that for each distinct $U_g, U_h \in \mathcal{N}$, $U_g^\dagger U_h \in U_{g^{-1}h} Z(\mathrm{GU}_d(\mathbb{C}))$, and hence is of trace 0, so $\mathcal{N}$ is a unitary error basis.

Unitary error bases can be used to produce mutually unbiased bases using the following construction:

Lemma 2. *Let $\mathcal{C} = \mathcal{C}_1 \cup \cdots \cup \mathcal{C}_n$ with $\mathcal{C}_k \cap \mathcal{C}_l = \{\mathbb{1}\}$ for $k \neq l$ be a set of $n(d-1)+1$ unitary matrices that are mutually orthogonal with respect to the trace inner product. Furthermore, let each class $\mathcal{C}_k$ of the partition of $\mathcal{C}$ contain d commuting matrices $U_{k,t}$, $0 \leq t \leq d-1$, where $U_{k,0} := \mathbb{1}$. For fixed k, let $\mathcal{B}_k$ be a basis of common eigenvectors $|\psi_k^i\rangle$ of the matrices $U_{k,j}$. Then the bases $\mathcal{B}_k$ form a set of n mutually unbiased bases, i.e.,*

$$\left|\langle \psi_k^i | \psi_l^j \rangle\right|^2 = 1/d \quad \text{for } k \neq l. \tag{6}$$

For a proof of this result, see [4, 9]. Note that such partitions of unitary error bases correspond to sets of mutually orthogonal maximal abelian subalgebras, which are studied, for example, in [21]. In Section 4 we give a shorter proof of condition (6) for the special case of $d+1$ nice error bases.

We address the question of how many mutually unbiased bases can be constructed when the set $\mathcal{C}$ in Lemma 2 is a subset of a nice error basis. We call such bases *nice mutually unbiased bases*. The main result of this paper is the following:

Theorem 3 (*Limitations of nice MUBs). Let $\mathcal{N}$ be a nice error basis of* $\mathrm{GU}_d(\mathbb{C})$ *with index group G. Then the maximal number $N_{\mathrm{NMUB}}(d)$ of mutually unbiased bases that can be obtained by partitioning a subset $\mathcal{C}$ of $\mathcal{N}$ according to Lemma 2 is at most*

$$N(d) = \min_{p \in \pi(d)} d_p + 1\,. \tag{7}$$

We prove Theorem 3 in the next section. To do so, we first establish a connection between nice error bases and trivially intersecting abelian subgroups of the index group:

Lemma 4. *Let G be the index group of a nice error basis $\mathcal{N}$ and let $\mathcal{M}$ be a set of d pairwise commuting members of $\mathcal{N}$. Then $A = P(\mathcal{M})$ is an abelian subgroup of G.*

Proof: Since the elements of $\mathcal{M}$ are mutually commuting, they can be simultaneously diagonalized. The trace orthogonality of a unitary error basis implies that the diagonals of the elements of $\mathcal{M}$, when written in their common eigenbasis, must be pairwise orthogonal as vectors in $\mathbb{C}^d$ with the standard inner product. Since there can be at most d pairwise orthogonal vectors in $\mathbb{C}^d$, $\mathcal{M}$ is a maximal commuting subset of $\mathcal{N}$. As $\mathcal{M} \subseteq \mathcal{M}' := \mathcal{N} \cap \langle \mathcal{M} \rangle$ and $M := \langle \mathcal{M} \rangle$ is abelian, $\mathcal{M} = \mathcal{M}'$ by the maximality of $\mathcal{M}$. But since P is a homomorphism, this shows that $A = P(\mathcal{M}) = P(M)$ is an abelian group. □

Given this connection, we can produce upper bounds on the number of nice MUBs by proving upper bounds on the number of trivially intersecting abelian subgroups of the index group.

3. Abelian subgroups of the index group

In this section, we establish the main result of the paper (Theorem 3) by bounding the number of trivially intersecting abelian subgroups of order d of a group G of order d^2. Throughout, we let $\mathcal{A}$ denote a set of such subgroups.

For any group H and $p \in \pi(|H|)$, let $O_p(H)$ denote the largest normal p-subgroup of H, and let $\mathrm{Syl}_p(H)$ denote the set of Sylow p-subgroups of H. Also, let

$$E_p(H) := \{h \in H : h^p = 1\} \tag{8}$$

be the set of elements of H of order 1 or p.

First we observe that G can be written as the product of two of the members of $\mathcal{A}$, and that a similar decomposition holds for certain Sylow p-subgroups.

Lemma 5. *Consider $A, B \in \mathcal{A}$ with $A \neq B$. Then $G = AB$ (and hence G is solvable). Furthermore, $P_{A,B} := O_p(A)O_p(B) \in \mathrm{Syl}_p(G)$.*

Proof: We have

$$d^2 = |G| \geq |AB| = \frac{|A||B|}{|A \cap B|} = d^2\,, \tag{9}$$

so $AB = G$. Since G can be written as the product of abelian groups, it is solvable (see for example [20, 13.3.2]). Furthermore, [20, 13.2.5] implies $P_{A,B} \in \mathrm{Syl}_p(G)$. □

Now we construct a new group G_p and a set of subgroups $\mathcal{A}_p$ that will be easier to work with.

Lemma 6. *Suppose* $|\mathcal{A}| \geq 2$. *For any* $p \in \pi(d)$, *let* $\mathcal{A}_p := \{O_p(A) : A \in \mathcal{A}\}$ *and* $G_p := \langle \mathcal{A}_p \rangle$. *Then* $|G_p| = d_p^2$, $\mathcal{A}_p$ *is a set of abelian subgroups of* G_p *of order* d_p *such that* $|A_p \cap B_p| = 1$ *for all distinct* $A_p, B_p \in \mathcal{A}_p$, *and the map* $A \mapsto O_p(A)$ *is a bijection of* $\mathcal{A}$ *with* $\mathcal{A}_p$ *(so that in particular,* $|\mathcal{A}| = |\mathcal{A}_p|$*).*

Proof: Let $A, B, C \in \mathcal{A}$ with $A \neq B$. By Lemma 5, $P_{D,E}$ is a group for all distinct $D, E \in \{A, B, C\}$. Thus, by the normality of $O_p(\cdot)$,

$$\begin{aligned} P &:= P_{A,B} O_p(C) && (10)\\ &= O_p(A) O_p(B) O_p(C) && (11)\\ &= O_p(A) O_p(C) O_p(B) && (12)\\ &= O_p(C) O_p(A) O_p(B) && (13)\\ &= O_p(C) P_{A,B}\,, && (14) \end{aligned}$$

so P is a group. Since $|P|$ divides $|P_{A,B}||O_p(C)|$, P is a p-group. Furthermore, since $P_{A,B} \in \mathrm{Syl}_p(G)$, $P = P_{A,B}$. Thus $G_p = \langle \mathcal{A}_p \rangle = P_{A,B}$ for any distinct $A, B \in \mathcal{A}$, and the lemma follows. □

Now we give the bound for the special case of p-groups, which by Lemma 6 implies a bound for all groups.

Lemma 7. *Let* d *be a power of some prime* p, *so that* G *is a* p*-group. Then* $|\mathcal{A}| \leq \min_{A \in \mathcal{A}} |E_p(A)| + 1$.

Proof: The idea of the proof is to identify a subgroup $H \leq G$ such that partitioning the non-identity elements of H according to membership in $A \in \mathcal{A}$ bounds $|\mathcal{A}|$. Let $X \leq Z(G)$ with $|X| = p$, where $Z(G)$ denotes the center of G (such a subgroup must exist because every p-group has a nontrivial center; see for example [3, 5.16]). For any fixed A, suppose $X \not\leq A$ (we will show below that such an X can always be chosen). Then let $H := E_p(AX)$.

To obtain the bound, we must compute $|H|$, $|H \cap A|$, and $|H \cap D|$ for $D \in \mathcal{D} := \mathcal{A} - \{A\}$. Note that $AX = A(AX \cap D)$ for any $D \in \mathcal{D}$ (this follows because $A(AX \cap D) = AX \cap AD$ by the modular property of groups, and $AD = G$ by Lemma 5). Furthermore, $AX \cap D$ has order p, since $p|A| = |AX| = |A(AX \cap D)| = |A||AX \cap D|/|A \cap AX \cap D| = |A||AX \cap D|$. Therefore $|H \cap D| = |E_p(AX \cap D)| = |AX \cap D| = p$. Also, $H = E_p(A)(X \cap D)$, and therefore $|H| = |E_p(A)|p$. Finally, $H \cap A = E_p(A)$, so $|H \cap A| = |E_p(A)|$. Since the non-identity elements of the various $D \in \mathcal{D}$ are distinct, we have

$$|\mathcal{D}| \leq \frac{|H| - |H \cap A|}{|H \cap D| - 1} = |E_p(A)|\,, \tag{15}$$

which shows $|\mathcal{A}| = |\mathcal{D}| + 1 \leq |E_p(A)| + 1$.

It remains to show that we can always choose X such that $X \not\leq A$. Supposing $X \leq A$, we construct $Y \not\leq A$ with $Y \leq Z(G)$ and $|Y| = p$, and use Y in place of X. Let $C, D \in \mathcal{D}$ be distinct, with $C \neq A$, and let $Y := CX \cap D$. Since $X \not\leq C$, we have $|Y| = p$ by the same argument we used to show $|AX \cap D| = p$. Since $|A \cap D| = 1$, $Y \not\leq A$. Finally, $Y \leq Z(G)$ since $y \in Y$ satisfies $y \in D$ and can also be written as $y = cx$ for $c \in C$ and $x \in X \leq Z(G)$, so it commutes with any $c'd' \in CD = G$. This completes the proof. □

Combining these results gives the following bound on the size of $\mathcal{A}$:

Lemma 8. $|\mathcal{A}| \leq \min_{p \in \pi(d), A \in \mathcal{A}} |E_p(A)| + 1$.

Proof: This follows directly from Lemmas 6 and 7. □

Now we can easily derive our main result. By Lemma 4, a partition $\mathcal{C} = \mathcal{C}_1 \cup \cdots \cup \mathcal{C}_n$ of $\mathcal{N}$ as in Lemma 2 corresponds to the set $\mathcal{A} = \{A_i : 1 \leq i \leq n\}$ of subgroups of G, where $A_i = P(\mathcal{C}_i)$. Then since $|E_p(A)| \leq d_p$ for any $A \in \mathcal{A}$, Lemma 8 implies $n = |\mathcal{A}| \leq d_p + 1$ as desired.

4. Achieving the bound

In this section we construct examples which show the upper bound of $N(d)$ on $N_{\mathrm{NMUB}}(d)$ is achieved, proving that the bound is best possible.

First, consider the case where $|\mathcal{A}| = d + 1$, i.e., there is a complete set of nice MUBs. In this case, G must be an elementary abelian group, $G = Z_p \times \cdots \times Z_p$ for some prime p.

Corollary 9. *Suppose* $|\mathcal{A}| = d + 1$. *Then G is elementary abelian.*

Proof: If $|\mathcal{A}| = d + 1$, then Lemma 8 implies $|E_p(A)| = d$ for each $A \in \mathcal{A}$. Thus every element of each $A \in \mathcal{A}$ has order 1 or p. But since $|\mathcal{A}| = d + 1$ and the distinct members of $\mathcal{A}$ intersect trivially, every element of G must appear in some $A \in \mathcal{A}$. Therefore every element of G has order 1 or p.

Now let $X \leq Z(G)$ with $|X| = p$, and choose $A \in \mathcal{A}$ with $X \not\leq A$. Arguing as in the proof of Lemma 7, $AX - A$ is partitioned by the subgroups $AX \cap D$ for $D \in \mathcal{A} - \{A\}$. As $X \leq Z(G)$, A centralizes $AX \cap D$, so $AX \cap D$ is in the center of $AD = G$. Then $A \leq \langle AX - A \rangle = \langle AX \cap D : D \in \mathcal{A} - \{A\} \rangle \leq Z(G)$, so $G = AD$ is abelian, and in particular, elementary abelian. □

Now we show that $N_{\mathrm{NMUB}}(d) = d + 1$ when $d = p^e$ is a prime power. In this case we know that G must be elementary abelian, and we want to show that this group has a nice error basis that can be partitioned according to Lemma 2. Such a partition was constructed in [4]. Here we give a nonconstructive existence proof based on some well-known group-theoretic facts and then a more concrete construction along the lines of [8].

Let Q be an extraspecial p-group of order p^{1+2e}. Then it is known that Q has a faithful irreducible representation of dimension $d = p^e$ (see [3, 34.9]). The group $G := Q/Z(Q)$ is an elementary abelian group of order d^2. The irreducible representation of Q gives rise to a projective representation of G of central type. We can regard G as a $2e$-dimensional vector space over $\mathbb{F}_p$. It is also well known (see [3, 23.10]) that there is a symplectic form $f : G \times G \to \mathbb{F}_p$ on the $\mathbb{F}_p$-space G such that for $A \leq G$, the preimage of A in Q is abelian iff A is a totally isotropic subspace of the symplectic space G. (A subspace B is called *totally isotropic* iff $f(u, v) = 0$ for all $u, v \in B$.)

We see that a set $\mathcal{A}$ of $d + 1$ abelian subgroups of order d of G partitioning G corresponds to a set $\tilde{\mathcal{A}}$ of d-dimensional totally isotropic subspaces partitioning the symplectic space G. Then by Lemma 2, $\mathcal{A}$, and hence also $\tilde{\mathcal{A}}$, determines a nice error basis $\mathcal{N}$ and a set S of $d + 1$ mutually unbiased bases of $\mathbb{C}^d$.

In fact, in our special case this can be seen without appeal to Lemma 2. Given distinct $\tilde{A}_1, \tilde{A}_2 \in \tilde{\mathcal{A}}$, pick preimages $\hat{A}_i$ of $\tilde{A}_i$ in Q and complements A_i to $Z := Z(\mathrm{GU}_d(\mathbb{C}))$ in $\hat{A}_i Z$. Since A_1 acts (by conjugation) on $\hat{A}_2$, it acts regularly on the set of 1-dimensional subspaces determined by the basis $\mathcal{B}_2$ of common eigenvectors of all $\hat{a}_2 \in \hat{A}_2$. Then the argument in the proof of Theorem 2.1 in [4] shows that $|\langle\phi|\psi\rangle|^2 = 1/d$ for all $|\phi\rangle \in \mathcal{B}_1$ and $|\psi\rangle \in \mathcal{B}_2$.

One set $\tilde{\mathcal{A}}$ can be constructed explicitly as follows. Let $\mathbb{F}_d$ be the finite field of order $d = p^e$, and let T denote the trace map from $\mathbb{F}_d$ to $\mathbb{F}_p$ (recall that the trace map is defined by $T(\eta) := \eta + \eta^p + \cdots + \eta^{p^{e-1}}$ for all $\eta \in \mathbb{F}_d$). We can make G into a 2-dimensional symplectic space over $\mathbb{F}_d$ by defining a symplectic form $g : G \times G \to \mathbb{F}_d$. We can choose g so that $f(u, v) = T(g(u, v))$ for $u, v \in G$, and let $\tilde{\mathcal{A}}$ be the set of $d + 1$ one-dimensional $\mathbb{F}_d$-subspaces of G (note that 1-dimensional subspaces are always totally isotropic). For distinct $A, B \in \tilde{A}$, $A \cap B = 0$, and so because g is 0 on A, so is $f = T \circ g$.

We will refer to (G, f) as an $\mathbb{F}_p$-structure and to (G, g) as an $\mathbb{F}_d$-structure. Let $G := H \times H$, where $H := \mathbb{F}_p^e$ is the direct product of e copies of $\mathbb{F}_p$. To define the $\mathbb{F}_d$-structure we will identify G with $G_{\mathbb{F}_d} := \mathbb{F}_d \times \mathbb{F}_d$ via a suitable map ϕ specified below.

Let $\{|k\rangle : k \in \mathbb{F}_p\}$ denote the standard basis of $\mathbb{C}^p$. Define the generalized Pauli operators

$$X := \sum_{k=0}^{p-1} |k+1\rangle\langle k|\,, \quad Z := \sum_{k=0}^{p-1} \omega^k |k\rangle\langle k|\,, \tag{16}$$

where ω is a pth root of unity. Let $(x, z) := (x_1, \ldots, x_e, z_1, \ldots, z_e)$ denote the elements of G. Define the map

$$\rho(x, z) := X^{x_1} Z^{z_1} \otimes \cdots \otimes X^{x_e} Z^{z_e}\,. \tag{17}$$

Then the set $\mathcal{N} := \{\rho(x, z) : (x, z) \in G\}$ is a nice error basis with index group G. We define the map $f : G \times G \to \mathbb{F}_p$ as

$$f((x, z), (x', z'))) := \sum_{i=1}^{e} x_i z'_i - x'_i z_i\,. \tag{18}$$

The group G together with the symplectic form f is a symplectic space of dimension $2e$ over $\mathbb{F}_p$. Using the fact $ZX = \omega XZ$ it follows that two matrices $\rho(x, z)$ and $\rho(x', z')$ commute iff $f((x, z), (x', z')) = 0$.

To view G as a 2-dimensional symplectic space over $\mathbb{F}_d$ we need to define a symplectic form $g : G_{\mathbb{F}_d} \times G_{\mathbb{F}_d} \to \mathbb{F}_d$. Furthermore, g should satisfy the condition $f(u, v) = T(g(\phi(u), \phi(v))$ for all $u, v \in G$. To do this we need some basic definitions [17]. Let $\{a_1, \ldots, a_e\}$ be a basis of the extension field $\mathbb{F}_d$ over the prime field $\mathbb{F}_p$ and $\{b_1, \ldots, b_e\}$ the dual basis, i.e.,

$$T(a_i b_j) = \delta_{ij} \,. \tag{19}$$

Define the map $\phi : G \to G_{\mathbb{F}_d}$ as

$$\phi(x_1, \ldots, x_e, z_1, \ldots, z_e) := (\alpha, \beta) \,, \tag{20}$$

where $\alpha := \sum_{i=1}^{e} x_i a_i$ and $\beta := \sum_{i=1}^{e} z_i b_i$. The symplectic form $g : G_{\mathbb{F}_d} \times G_{\mathbb{F}_d} \to \mathbb{F}_d$ can be now defined as

$$g((\alpha, \beta), (\alpha', \beta')) := \alpha\beta' - \alpha'\beta \,. \tag{21}$$

One can explicitly check that $f((x, z), (x', z')) = T(g(\phi(x, z), \phi(x', z')))$ using the property (19).

A collection of $d + 1$ one-dimensional subspaces of $G_{\mathbb{F}_d}$ is given by the lines

$$L_\Delta := \{(\alpha, \Delta\alpha) : \alpha \in \mathbb{F}_d\} \tag{22}$$

(the d lines with slope $\Delta \in \mathbb{F}_d$) and

$$L_\infty := \{(0, \beta) : \beta \in \mathbb{F}_d\} \tag{23}$$

(the line with slope ∞). Due to the discussion above, the sets

$$\mathcal{C}_\Delta := \{\rho(\phi^{-1}(\alpha, \beta)) : (\alpha, \beta) \in L_\Delta\} \,, \quad \Delta \in \mathbb{F}_d \cup \{\infty\} \tag{24}$$

form a partition of the nice error basis into $d + 1$ trivially intersecting sets containing d commuting matrices each, and hence specify a set of $N(d)$ nice MUBs of dimension $d = p^e$.

This construction also lets us achieve the upper bound of Theorem 3 in the non-prime power case, using an idea along the lines of the reduce to prime power construction. More precisely, for any dimension d there is an index group G of order d^2 with corresponding nice error basis $\mathcal{N}$ such that we can obtain $N(d)$ nice MUBs by partitioning $\mathcal{N}$ according to Lemma 2. This is seen as follows.

Let G_i be the elementary abelian group of order $p_i^{2e_i}$, ρ_i the map in (17), and $\mathcal{N}_i$ the corresponding nice error basis for $i \in \{1, \ldots, r\}$. Let $G := G_1 \times \cdots \times G_r$, $\rho := \rho_1 \otimes \cdots \otimes \rho_r$, and $\mathcal{N} := \mathcal{N}_1 \otimes \cdots \otimes \mathcal{N}_r$. Let $\mathcal{C}^{(i)} := \{\mathcal{C}_1^{(i)}, \ldots, \mathcal{C}_{p_i^{e_i}+1}^{(i)}\}$ be a partition of $\mathcal{N}_i$ into $p_i^{e_i} + 1$ commuting subsets. Choose for each i an arbitrary subset $\mathcal{D}^{(i)}$ of

$\mathcal{C}^{(i)}$ of size $N(d)$. Then the sets

$$\mathcal{D}_k := \left\{\mathcal{D}_k^{(i)} \otimes \cdots \otimes \mathcal{D}_k^{(i)} : 1 \le i \le r\right\} \tag{25}$$

for $k \in \{1, \ldots, N(d)\}$ are subsets of $\mathcal{N}$ satisfying the conditions of Lemma 2.

5. Stronger bound for abelian index groups

Although Theorem 3 is the best possible bound depending only on $|G|$, improved bounds on the size of $\mathcal{A}$ can be obtained when we know something about the structure of G. Here we produce an improved bound for the case of abelian index groups. For any $p \in \pi(d)$, define

$$\bar{E}_p(A) := \left\{a^{p^{e-1}} : a \in O_p(A)\right\} \tag{26}$$

where p^e is the exponent of $O_p(A)$. Then we have

Lemma 10. *Let G be a group of order d^2, and let $\mathcal{A}$ be a set of trivially intersecting subgroups of G of order d with the additional condition that $A \trianglelefteq G$ for each $A \in \mathcal{A}$. Suppose $|\mathcal{A}| > 2$. Then $G = A \times B$ for all distinct $A, B \in \mathcal{A}$, all members of $\mathcal{A}$ are abelian and isomorphic, and $|\mathcal{A}| \le \min_{p\in\pi(d)} |\bar{E}_p(A)| + 1$ for $A \in \mathcal{A}$.*

Proof: As in Lemma 5, $G = A_1A_2$ for all distinct $A_1, A_2 \in \mathcal{A}$. Then as $|A_1 \cap A_2| = 1$ and $A_1, A_2 \trianglelefteq G$, $G = A_1 \times A_2$. Since $|\mathcal{A}| > 2$, there is $A_3 \in \mathcal{A} - \{A_1, A_2\}$. Let $\Pi_i : A_3 \to A_i$ (for $i \in \{1, 2\}$) be the projection of A_3 onto A_i with respect to the decomposition $G = A_1 \times A_2$. As $|A_{3-i} \cap A_3| = 1$, Π_i is injective, and as $|A_3| = |A_i|$, Π_i is an isomorphism. Thus all members of $\mathcal{A}$ are isomorphic. Furthermore, let $a \in A_1$ and $b \in A_3$. Then $[a, \Pi_1(b)] = [a, b] := a^{-1}b^{-1}ab \in A_1 \cap A_3 = \{1\}$ since $A_1, A_3 \trianglelefteq G$. Since Π_1 is an isomorphism, A_1 is abelian, and therefore all members of $\mathcal{A}$ are abelian.

By Lemma 6, we may assume without loss of generality that d is a power of p. Let p^e be the exponent of $A := A_1$, and choose $X \le A_2$ with $X \cong Z_{p^e}$. Now we proceed as in the proof of Lemma 7, but with $H := \bar{E}_p(AX)$. We have $AX = A(AX \cap B)$ for all $B \in \mathcal{A} - \{A\}$, so choosing a generator b for $AX \cap B$, $\langle b^{p^{e-1}}\rangle$ is of order p in H. Furthermore, $H = \bar{E}_p(A)\langle b^{p^{e-1}}\rangle$, so as in the proof of Lemma 7, $|\mathcal{A}| \le |\bar{E}_p(A)| + 1$. Since all members of $\mathcal{A}$ are isomorphic, this bound holds for any $A \in \mathcal{A}$, and the lemma follows. □

Using this lemma, we can give a bound on the number of mutually unbiased bases constructed from any particular abelian index group. Note that abelian groups must be of the form $G = H \times H$ to be index groups of nice error bases [13]. (In the case $|\mathcal{A}| > 2$, this also follows from Lemma 10.)

Corollary 11. *Let $G = H \times H$ with $H = Z_{d_1} \times \cdots \times Z_{d_k}$, where $d_1, \ldots, d_k$ are prime powers (without loss of generality). Let $\mu_p(H) := \max\{d_j : p|d_j\}$, and let $\nu_p(H) := |\{j : d_j = \mu_p(H)\}|$. Then $|\mathcal{A}| \leq \min_{p\in\pi(d)} p^{\nu_p(H)} + 1$.*

Proof: Since any subgroup of an abelian group is normal, we can apply Lemma 10. Noting that $|\bar{E}_p(A)| = p^{\nu_p(H)}$, the result follows. □

As a simple example of this corollary, consider the index group $Z_d \times Z_d$, which has a nice error basis given by generalized Pauli operators [16]. Reference [9] showed that at most three MUBs of dimension six can be produced by partitioning the generalized Pauli operators with $d = 6$. More generally, the result above shows that a nice error basis of $Z_d \times Z_d$ can be partitioned to produce at most $\min_{p\in\pi(d)} p + 1$ mutually unbiased bases.

6. Implications for nets

In this section we show that the group-theoretic arguments of Section 3 can also be used to give upper bounds on the number of parallel classes of nets. A net is a combinatorial object that has many similar properties to a set of MUBs. Using this similarity, it was shown in [23] how to construct MUBs from nets. Our results in this section give further connections between MUBs and nets. Specifically, we present bounds on the number of parallel classes of nets constructed in a particular way, and we show that a complete set of nice mutually unbiased bases corresponds to an affine translation plane.

Definition 12 (Net). A $(d, k; \lambda)$-net is a set X of λd^2 points together with a set $\mathcal{B}$ of subsets of X (blocks) each of size λd. The set $\mathcal{B}$ is partitioned into k parallel classes, each containing d disjoint blocks. Every two non-parallel blocks intersect in exactly λ points.

The analogy between a net and a set of mutually unbiased bases is clear. A parallel class is analogous to an orthonormal basis in a collection of MUBs, and the condition that the bases be unbiased corresponds to the requirement that blocks from different parallel classes intersect in the same number of points.

A net is also referred to as an *affine design*, where "affine" indicates that every two non-parallel blocks intersect in the same number of points. We will only consider nets with $\lambda = 1$, which we refer to as (d, k)-nets.

Our results give an upper bound on the maximal number of parallel classes when we use the following construction with abelian subgroups:

Lemma 13. *Let G be a group of order d^2 together with a set $\mathcal{A}$ of subgroups of G of order d such that distinct subgroups intersect trivially. Then the incidence structure whose points are the elements of G and whose blocks are the left cosets of the subgroups defines a $(d, |\mathcal{A}|)$-net.*

We emphasize that whereas the nice MUB construction requires the subgroups to be abelian, the construction of nets does not.

Proof: Let $A \in \mathcal{A}$. Clearly the left cosets G/A form a parallel class since the cosets are a partition of G. Assume that $|\mathcal{A}| \geq 2$ and let $A, B \in \mathcal{A}$ be any two distinct subgroups. These cosets can be expressed as bA and aB for some $a \in A$ and $b \in B$ because $G = AB = BA$. It remains to show that the left cosets bA and aB intersect in exactly one point, i.e., $|bA \cap aB| = 1$.

Assume that $|bA \cap aB| \neq 1$. Then there are distinct $a', a'' \in A$ and distinct $b', b'' \in B$ such that $ba' = ab'$ and $ba'' = ab''$. But this implies that $a'(b')^{-1} = ab^{-1} = a''(b'')^{-1}$, so that $a' = a''$ and $b' = b''$, which is a contradiction. Therefore $|bA \cap aB| = 1$, which completes the proof. □

If we restrict our attention to sets $\mathcal{A}$ containing abelian subgroups, then Lemma 8 shows that (d, k)-nets constructed according to Lemma 13 must have $k \leq N(d)$.

A $(d, d+1)$-net is called an *affine plane*. Constructions of affine planes are known when d is a prime power [18]. An affine plane obtained from $d+1$ subgroups of a group G according to Lemma 13 is called an *affine translation plane*. For G abelian it is known that G must be elementary abelian for such subgroups to exist [1]. (Note that this also follows from Corollary 9.) Thus a maximal set of nice MUBs corresponds to an affine translation plane.

7. Discussion

We have shown that partitioning a nice error basis cannot produce more mutually unbiased bases than the reduce to prime power construction. This result demonstrates that novel approaches (such as the construction of [23]) are needed to improve upon the reduce to prime power construction.

The problem of determining $N_{\mathrm{MUB}}(d)$ for d not a prime power remains wide open, and although we have ruled out further progress by construction of nice MUBs, there are many alternatives. One possible avenue is to show how to extend a nice mutually unbiased basis by adding more bases that do not come from the eigenvectors of operators in the nice error basis. However, no such extension is possible when $d = 6$ [9], so it would be interesting to determine whether nice MUBs can ever be extended. Another possibility is to find ways of partitioning wicked error bases. This approach may be promising as many wicked error bases exist [15]. Finally, one could look for constructions of MUBs that are not directly based on partitioning unitary error bases, as in [23].

Acknowledgments MA is supported by the National Science Foundation under Grant No. DMS-0203417. AMC and PW are supported by the National Science Foundation under Grant No. EIA-0086038.

References

1. J. André, Über nicht-Desarguessche Ebenen mit transitiver Translationgruppe, *Math. Zeitschr.* **60** (1954), 156–186.
2. C. Archer, There is no generalization of known formulas for mutually unbiased bases, *J. Math. Phys.* **46** (2005), 022106, arxiv.org/quant-ph/0312204.
3. M. Aschbacher, *Finite Group Theory*, 2nd edition, Cambridge University Press, Cambridge, 2000.

4. S. Bandyopadhyay, P.O. Boykin, V. Roychowdhury, and F. Vatan, A new proof of the existence of mutually unbiased bases, *Algorithmica* **34** (2002), 512–528, arxiv.org/quant-ph/0103162.
5. C.H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in: *Proc. IEEE Intl. Conf. Computers, Systems, and Signal Processing,* 1984, pp. 175–179.
6. A.R. Calderbank, P.J. Cameron, W.M. Kantor, and J.J. Seidel, $\mathbb{Z}_4$-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets, *Proc. London Math. Soc.* **75** (1997), 436–480.
7. P. Delsarte, J.M. Goethals, and J.J. Seidel, Bounds for systems of lines and Jacobi polynomials, *Philips Res. Rep.* **30** (1975), 91–105.
8. K.S. Gibbons, M.J. Hoffman, and W.K. Wootters, Discrete phase space based on finite fields, *Phys. Rev. A* **70** (2004), 062101, arxiv.org/quant-ph/0401155.
9. M. Grassl, On SIC-POVMs and MUBs in dimension 6, in: *Proc. ERATO Conference on Quantum Information Science,* 2004, pp. 60–61, arxiv.org/quant-ph/0406175.
10. S.G. Hoggar, t-designs in projective spaces, *Europ. J. Combin.* **3** (1982), 233–254.
11. I.D. Ivanovic, Geometrical description of quantal state determination, *J. Phys. A* **14** (1981), 3241–3245.
12. G.A. Kabatiansky and V.I. Levenshtein, Bounds for packings on a sphere and in space, *Problems Inform. Transmission* **14**(1) (1978), 1–17.
13. A. Klappenecker and M. Rötteler, Beyond stabilizer codes I: Nice error bases, *IEEE Trans. Inf. Theory* **48** (2002), 2392–2395, arxiv.org/quant-ph/0010082.
14. A. Klappenecker and M. Rötteler, Constructions of mutually unbiased bases, in: *Proc. International Conference on Finite Fields and Applications,* 2003, pp. 137–144, arxiv.org/quant-ph/0309120.
15. A. Klappenecker and M. Rötteler, On the monomiality of nice error bases, Tech. Report CORR 2003-04, Department of Combinatorics and Optimization, University of Waterloo, April 2003, arxiv.org/quant-ph/0301078.
16. E. Knill, Non-binary unitary error bases and quantum codes, Tech. Report LAUR-96-2717, Los Alamos National Laboratory, 1996, arxiv.org/quant-ph/9608048.
17. R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Applications*, Cambridge University Press, Cambridge, 1986.
18. J.H. van Lint and R.M. Wilson, *A Course in Combinatorics*, Cambridge University Press, Cambridge, 1992.
19. H.F. MacNeish, Euler squares, *Ann. of Math.* **23**(3) (1922), 221–227.
20. W.R. Scott, *Group Theory*, Prentice Hall, Englewood Cliffs, 1964.
21. Y. Watatani, Latin squares, commuting squares, and intermediate subfactors, *Subfactors,* 1994, pp. 85–104.
22. R.F. Werner, All teleportation and dense coding schemes, *J. Phys. A* **34** (2001), 7081–7094, arxiv.org/quant-ph/0003070.
23. P. Wocjan and Th. Beth, New construction of mutually unbiased bases in square dimensions, *Quantum Inform. Comput.* **5**(2) (2005), 93–101, arxiv.org/quant-ph/0407081.
24. W.K. Wootters and B.D. Fields, Optimal state-determination by mutually unbiased measurements, *Ann. Physics* **191** (1989), 363–381.
25. G. Zauner, *Quantendesigns: Grundzüge einer nichtkommutativen Designtheorie*, Ph.D. thesis, Universität Wien, 1999.