# ON THE MATHEMATICAL FOUNDATIONS OF MUTUALLY UNBIASED BASES

KOEN THAS

ABSTRACT. In order to describe a setting to handle Zauner's conjecture on mutually unbiased bases (MUBs) (stating that in $\mathbb{C}^d$, a set of MUBs of the theoretical maximal size $d+1$ exists only if $d$ is a prime power), we pose some fundamental questions which naturally arise. Some of these questions have important consequences for the construction theory of (new) sets of maximal MUBs. Partial answers will be provided in particular cases; more specifically, we will analyse MUBs with associated operator groups that have nilpotence class 2, and consider MUBs of height 1. We will also confirm Zauner's conjecture for MUBs with associated finite nilpotent operator groups.

**PACs numbers**: 02.10.Hh, 02.40.Dr, 03.67.-a, 03.65.Ta, 03.65.Ud

## 1. INTRODUCTION

Two orthonormal bases $\mathcal{B}$ and $\mathcal{B}'$ of the Hilbert space $\mathbb{C}^\ell$ ($\ell \in \mathbb{N}^\times$) are *mutually unbiased* if and only if

$$|\langle\phi|\psi\rangle|^2 = 1/\ell$$

for all $|\phi\rangle \in \mathcal{B}$ and $|\psi\rangle \in \mathcal{B}'$. It is a fundamental and very famous conjecture, sometimes referred to as "Zauner's conjecture" [23] (although quite probably the conjecture already floated around before 1999), that the theoretical upper bound $\ell + 1$ of a set of mutually unbiased bases ("MUBs") can only be reached when $\ell$ is a *prime power* (see below). For each such $\ell$, examples exist — in fact, there is a rich literature in the construction theory of such examples, and even for $\ell = 6$, the first case for which the conjecture is open, many papers exist. In this paper, by $N_{\mathrm{MUB}}(\ell)$ we denote the maximal upper bound for the size of a set of MUBs in $\mathbb{C}^\ell$.

### 1.1. **Some known results and history.**

A classical result (for which we refer to [2, 4, 7, 10, 21]) is that

$$N_{\mathrm{MUB}}(\ell) \leq \ell + 1. \tag{1}$$

When $\ell$ is any prime, this upper bound is attained [9], and more generally for any prime power, the same is true — see e.g. [2, 3, 11, 17, 21, 23]. When $\ell$ is not a prime power, not much is known. As mentioned above, even when $\ell = 6$, the precise upper bound is not known. If $\ell = ab$ (for positive integers $a \neq 1$ and $b \neq 1$), then one can show that

$$N_{\mathrm{MUB}}(\ell) \geq \min\Big(N_{\mathrm{MUB}}(a), N_{\mathrm{MUB}}(b)\Big). \tag{2}$$

If we denote the set of prime factors of $\ell$ by $\Omega(\ell)$, and for each $p \in \Omega(\ell)$ we write $\ell_p$ for the largest power of $p$ that divides $\ell$, then also

$$N_{\mathrm{MUB}}(\ell) \geq \min_{p\in\Omega(\ell)}\Big(N_{\mathrm{MUB}}(\ell_p)\Big) = \min_{p\in\Omega(\ell)}\Big(\ell_p + 1\Big). \tag{3}$$

(One can find this result in [11, §4].) It is known however that the bound in (3) is not always sharp.

MUBs were introduced by Julian Schwinger in 1960 [16] under a different name. He noted in [16] that bases which are mutually unbiased represent measurements that are maximally non-commutative, in the sense that a measurement over one such basis leaves one completely uncertain as to the outcome of a measurement over a basis which is mutually unbiased with the first. Later, in [21] Wootters and Fields introduced the term "mutually unbiased bases."

*Date*: November 17, 2017.

1.2. **This note.** In an attempt to better understand the category of (maximal sets of) MUBs, and more precisely, to find the "correct setting" to attack Zauner's conjecture, some (rather subtle) questions have popped up very naturally which might be interesting in their own right (both from a physical and mathematical point of view).

For instance, one of the main tools in the construction theory of maximal sets of MUBs, after [2], is the theory of so-called "maximal commuting operator classes" (MCCs). From such an MCC (of size $d+1$), a maximal set of MUBs (of size $d+1$) can be derived, and from a maximal set of MUBs (of size $d+1$) one can also make an MCC (of size $d+1$). In this note, we will show that one has to be very careful when constructing "new" maximal MUBs through the theory of MCCs, as *nonisomorphic* MCCs could give the *same* maximal set of MUBs!

Several questions on the correspondence between MCCs and MUBs will thus be formulated, and some will be answered.

These (and the aforementioned) questions are the subject of the present note (which at the same time can be considered as a first installment in a series of papers on Zauner's conjecture).

1.3. **Outline.** In §2, we will formally introduce (sets of) mutually commuting classes (MCCs), and describe their relation to (sets of) MUBs. We will also introduce the general Pauli group, and explain how one can construct maximal sets of MUBs in any prime power dimension through symplectic geometry, an idea taken from [17]. We will also define the maps $\alpha$ and $\beta$, which are of crucial importance for the rest of this note, as they explore the subtle connection between MCCs and MUBs.

In §3, we recall the group theoretical approach due to Aschbacher, Childs and Wocjan [1], which is highly relevant for this paper. (In short, we propose a group theoretical program with an underlying geometric accent, and the results of loc. cit. also have this flavor to some extent. More details are provided in section 3.)

In the next section, §4, we pose a number of fundamental questions on the maps $\alpha$ and $\beta$.

In §5, we define a "theory of heights" for maximal sets of MCCs, which measures how far the unitary group generated by the element of a maximal set of MCCs is from an abelian group. Again, fundamental questions are posed.

Section 6 introduces the notion of *class* for a maximal set of MCCs, and for maximal sets of MUBs. It is observed that height 1 maximal MCCs agree with Zauner's conjecture. The final questions are posed.

In the next-to-last section, §7, we consider maximal MUBs $\mathcal{B}$ in $\mathbb{C}^d$ for which $\alpha(\mathcal{B})$ has nilpotence class 2. We will analyse and determine the structure of $\alpha(\mathcal{B})$, and show as a by-product that $d$ must be a prime.

In §8, we will show that maximal MUBs $\mathcal{B}$ in $\mathbb{C}^d$ for which the associated operator group $\alpha(\mathcal{B})$ is finite and nilpotent, satisfy Zauner's conjecture.

The novel ideas, notions, questions and results which appear in this note can be found in §4—§8.

1.4. **Acknowledgments.** I want to thank Markus Grassl for many helpful communications on the subject of the present paper. In particular, he provided valuable comments on the definition of "height" in §5 in a previous version of this note. I also want to thank two anonymous referees for several useful suggestions.

## 2. MUBs AND MAXIMAL COMMUTING OPERATOR CLASSES

Let $\Omega$ be a set of $d^2$ mutually orthogonal unitary operators in $\mathbb{C}^d$ containing the identity operator $\mathrm{id}$ ($d \in \mathbb{N}$, $d \neq 0, 1$) using the Hilbert-Schmidt norm: operators $A$ and $B$ are *orthogonal* if $\mathrm{tr}(AB^\dagger) = 0$. Then $\Omega$ constitutes a basis for the $\mathbb{C}$-vector space of $(d \times d)$-complex matrices $\mathbf{M}_{d\times d}(\mathbb{C})$, which one often calls, by definition, "unitary error basis." A standard construction of MUBs outlined in [2] relies on finding classes of commuting operators, with each class containing $d-1$ mutually orthogonal commuting unitary matrices different from the identity $\mathrm{id}$.

A set of subsets $\{\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_\ell | \mathcal{C}_j \subset \Omega \setminus \{\mathrm{id}\}\}$ of size $|\mathcal{C}_j| = d-1$ constitutes a (partial) partitioning of $\Omega \setminus \{\mathrm{id}\}$ into *mutually disjoint maximal commuting classes* if the subsets $\mathcal{C}_j$ are such that

(a) the elements of $\mathcal{C}_j$ commute for all $1 \leq j \leq \ell$ and
(b) $\mathcal{C}_j \cap \mathcal{C}_k = \emptyset$ for all $j \neq k$.

If $\ell = d+1$, we speak of an "MCC." By abuse of notation, we will always write that $\{\mathcal{C}_1 \cup \{\mathrm{id}\}, \dots, \mathcal{C}_{d+1} \cup \{\mathrm{id}\}\}$ is an MCC, instead of $\{\mathcal{C}_1, \dots, \mathcal{C}_{d+1}\}$.

**Lemma 2.1** ([2]). *The common eigenbases of $\ell$ mutually disjoint maximal commuting operator classes, $\ell \in \mathbb{N}$, $\ell \neq 0$, form a set of $\ell$ mutually unbiased bases.*

For the rest of this paper, if $\mathcal{B}$ is a set of MUBs of size $d+1$ in $\mathbb{C}^d$, we will call $\mathcal{B}$ a *maximal set of MUBs* or a *maximal MUB* for short.

Define the map $\beta$ from the set of all MCCs, denoted $\mathbf{MCC}$, to the set of all sets of maximal MUBs, denoted $\mathbf{MUB}$, as being the map which sends an MCC $\mathcal{U}$ to the set of MUBs $\beta(\mathcal{U})$ which arise as common eigenbases as in the previous lemma.

Conversely, consider a set $\mathcal{B}$ of $d+1$ MUBs in $\mathbb{C}^d$, $d \in \mathbb{N}$, $d \neq 0, 1$. Denote its $d+1$ bases by $\mathcal{B}_0, \mathcal{B}_1, \ldots, \mathcal{B}_d$, and for each $i = 0, 1, \ldots, d$, let

$$\mathcal{B}_i = \{\langle\psi_1^i|, \langle\psi_2^i|, \ldots, \langle\psi_d^i|\}. \tag{4}$$

Following [2], define for each $k = 0, 1, \ldots, d$ and $j = 1, 2, \ldots, d$,

$$U_j^k = \sum_{r=1}^{d} e^{2\pi i j r/d} |\psi_r^k\rangle\langle\psi_r^k|. \tag{5}$$

Then with $\mathcal{U}_y$, $y = 0, 1, \ldots, d$, defined as $\{U_j^y | j = 1, 2, \ldots, d\}$, $\{\mathcal{U}_0, \mathcal{U}_1, \ldots, \mathcal{U}_d\}$ is an MCC of size $d+1$, denoted $\alpha(\mathcal{B})$ in this note. So $\alpha$ defines a map between the set of maximal MUBs and the set of MCCs.

**Remark 2.2.** Note that $\alpha$ depends on the order of the base elements of each $\mathcal{B}_i$. So in each question we consider which regards $\alpha$, one should keep this in mind.

As a corollary of the existence of $\alpha$ and $\beta$, we have that *a maximal set of MUBs exist in $\mathbb{C}^d$ if and only if an MCC of size $d+1$ exists*.

The first questions we want to pose concerns the nature of the compositions $\alpha \circ \beta : \mathbf{MCC} \longrightarrow \mathbf{MCC}$ and $\beta \circ \alpha : \mathbf{MUB} \longrightarrow \mathbf{MUB}$.

We start with introducing the general Pauli group.

### 2.1. The general Pauli group.

Let $d$ be a prime. Let $\{|s\rangle | s = 0, 1, \ldots, d-1\}$ be a computational base of $\mathbb{C}^d$. Define the $d^2$ (generalized) *Pauli operators* of $\mathbb{C}^d$ as

$$(X_d)^a (Z_d)^b, \quad a, b \in \{0, 1, \ldots, d-1\},$$

where $X_d$ and $Z_d$ are defined by the following actions

$$X_d|s\rangle = |s+1 \mod d\rangle, \quad Z_d|s\rangle = \omega^s|s\rangle,$$

where $\omega = \exp(2i\pi/d)$.

The set $\mathbb{P}$ of generalized Pauli operators of the $N$-qudit Hilbert space $\mathbb{C}^{d^N}$ is the set $\mathbb{P}$ of $d^{2N}$ distinct tensor (Kronecker) products of the form

$$\sigma_{i_1} \otimes \sigma_{i_2} \otimes \cdots \otimes \sigma_{i_N},$$

where the $\sigma_{i_k}$ run over the set of (generalized) Pauli matrices of $\mathbb{C}^d$. Denote $\mathbb{P}^\times = \mathbb{P} \setminus \{\mathrm{id}\}$. These operators generate a group under ordinary matrix multiplication, denoted $\mathbf{P} = \mathbf{P}_N(d)$ and called the *general Pauli group* (or *discrete Heisenberg-Weyl group*). It has order $d^{2N+1}$.

If $E$ is a subset of the group $C$, $\langle E\rangle$ will denote the subgroup *generated* by the elements in $E$ (that is, $\langle E\rangle$ is the smallest subgroup of $C$ containing $E$). In the following proposition, if $G$ is a group, and $g, h \in G$, then $[g, h] := g^{-1}h^{-1}gh$; if $A$ and $B$ are subgroups of $G$, then $[A, B]$ is the subgroup generated by the elements $[a, b]$ with $a \in A$ and $b \in B$.

**Proposition 2.3** ([17]).
- (i) *The derived group $\mathbf{P}' = [\mathbf{P}, \mathbf{P}]$ equals the center $Z(\mathbf{P})$ of $\mathbf{P}$.*
- (ii) *We have $Z(\mathbf{P}) = \langle\omega \cdot \mathrm{id}\rangle$, so that $|Z(\mathbf{P})| = d$.*
- (iii) *$\mathbf{P}$ is nonabelian of exponent $d$ if $d$ is odd; if $d = 2$, $\mathbf{P}$ is nonabelian of exponent $4$.*
- (iv) *We have that the quotient $\mathbf{P}/Z(\mathbf{P})$ can be naturally seen as a $2N$-dimensional vector space $V(2N, d)$ over the finite field $\mathbb{F}_d$.*

Observe that $\mathbf{P}/Z(\mathbf{P})$ can be identified with $\mathbb{P}$ ($Z(\mathbf{P})$ corresponds to the identity operator).

Denote the natural projection map $\mathbf{P} \mapsto V(2N,d)$ by an overbar. Then the commutator

$$[.,.] : V(2N,d) \times V(2N,d) \mapsto \langle \omega \cdot \mathrm{id} \rangle : (\overline{v_1}, \overline{v_2}) \mapsto [\overline{v_1}, \overline{v_2}] = [v_1, v_2]$$

defines a non-degenerate alternating bilinear form on $V(2N,d)$ (the derived group $\mathbf{P}'$ is identified with the additive group of $\mathbb{F}_d$), so also on the corresponding projective space $\mathbf{PG}(2N-1,d)$.

### 2.2. **Symplectic polar spaces and the Pauli group.**

As in the previous subsection, $d$ is a prime.

Now consider the projective space $\mathbf{PG}(2N-1,d)$ of dimension $2N-1$, $N \geq 2$, over the field $\mathbb{F}_d$ with $d$ elements. Let $F$ be a non-degenerate symplectic form of $\mathbf{PG}(2N-1,d)$. For $F$ one can choose the following canonical bilinear form [6]:

$$(X_0Y_1 - X_1Y_0) + (X_2Y_3 - X_3Y_2) + \cdots + (X_{2N-2}Y_{2N-1} - X_{2N-1}Y_{2N-2}).$$

Then the *symplectic polar space* $\mathcal{W}_{2N-1}(d)$ consists of the points of $\mathbf{PG}(2N-1,d)$ together with all totally isotropic spaces of $F$ [6]. Here, a *totally isotropic subspace* is a linear subspace $W$ of $\mathbf{PG}(2N-1,d)$ that vanishes under $F$ (i.e., the restriction of $F$ to $W$ is trivial).

By the previous subsection, the general Pauli group $\mathbf{P}_N(d)$ naturally defines a symplectic polar space $\mathcal{W}_{2N-1}(d)$. There is a natural surjective map

$$\gamma : \mathbb{P}^{\times} \longrightarrow \text{points of } \mathcal{W}_{2N-1}(d)$$

such that operators $x$ and $y$ commute if and only if the points $\gamma(x)$ and $\gamma(y)$ of $\mathcal{W}_{2N-1}(d)$ generate a linear subspace which vanishes under $F$ — see [17, 20] for more details.

Now if $S$ is a *partition* of $\mathcal{W}_{2N-1}(d)$ in totally isotropic subspaces of (maximal) dimension $N-1$, then $\gamma^{-1}(S)$ defines an MCC of size $d^N+1$ (also denoted $\gamma^{-1}(S)$), see [17, 20] for details and also Remark 2.5 below, and hence a maximal MUB in $\mathbb{C}^{d^N}$. Many such examples exist. For further reference, we will call a partition of the aforementioned type a *spread*.

**Remark 2.4.** If $\sigma \in \mathbb{P}^{\times}$, $\langle \sigma \rangle$ is the vector line generated by $\sigma$ in $V(2N,d) \equiv \mathbf{P}/Z(\mathbf{P}) \equiv \mathbb{P}$, and this line maps to a point of $\mathcal{W}_{2N-1}(d)$.

**Remark 2.5** (On $\gamma^{-1}(\cdot)$ and scaling)**.** Let $S$ be as above, and consider again $\gamma^{-1}(S)$. In [17, 20] it is shown that it defines precisely one MCC on the set of nontrivial Pauli operators $\mathbb{P}^{\times} = \{\nu_1, \ldots, \nu_{d^{2N}-1}\}$ in $\mathbf{P}$, and this particular MCC is the one we consider. On the other hand, if $c_1, \ldots, c_{d^{2N}-1}$ are arbitrary $d$-th roots of unity in $\mathbb{C}$, then $\gamma^{-1}(S)$ also defines an MCC on $\{c_1\nu_1, \ldots, c_{d^{2N}-1}\nu_{d^{2N}-1}\}$ (and this remains valid in general; we will call this process "scaling"). But this MCC obviously should be isomorphic to the one defined on Pauli operators in any good theory of morphisms for MCCs.

## 3. Nice mutually unbiased bases

In [1], the authors introduce "nice mutually unbiased bases," which are unitary error bases with an underlying group structure. In that way, they are able to obtain nontrivial results about MUBs using (finite) unitary groups. This is exactly what we want to do, but in a more general setting.

We follow [1] below, but the definition is equivalent to the one by Knill [13].

Let $\mathbf{GU}_n(\mathbb{C})$ be the $n$-dimensional general unitary group over the complex numbers, $n \in \mathbb{N}$, $n \neq 0$, and let

$$\xi : \mathbf{GU}_n(\mathbb{C}) \ \mapsto \ \mathbf{PGU}_n(\mathbb{C}) \tag{6}$$

be the natural projection on the projective general linear group $\mathbf{PGU}_n(\mathbb{C})$ which mods out the center. An *$n$-dimensional projective unitary representation* of a finite group $G$ is a group homomorphism

$$\nu : G \ \mapsto \ \mathbf{PGU}_n(\mathbb{C}). \tag{7}$$

Let $\widetilde{G}$ be any finite preimage of $\nu(G)$ in $\mathbf{GU}_n(\mathbb{C})$ such that $\xi(\widetilde{G}) = \nu(G)$. We say $\widetilde{G}$ is of *central type* if

- $|\nu(G)| = n^2$, and
- $\mathrm{tr}(\upsilon) = 0$ for each $\upsilon \in \widetilde{G} \setminus Z(\mathbf{GU}_n(\mathbb{C}))$, where $Z(\cdot)$ denotes the center and $\mathrm{tr}(\cdot)$ the trace map.

If $\nu$ is faithful and each preimage $\widetilde{G}$ is of central type, then we say that $\nu$ is of *central type*.

Now let $G$ be a group of order $n^2$ with identity element $\mathrm{id}$ ($n \in \mathbb{N}$, $n \neq 0, 1$). (We use the notation $\mathrm{id}$ for the identity element in any group.) A subset $S \subseteq \mathbf{GU}_n(\mathbb{C})$ is a *nice error basis* if there is a projective representation $\nu : G \mapsto \mathbf{PGU}_n(\mathbb{C})$ of central type such that

$$S = \{U_g \mid g \in G\} \text{ and } U_{\mathrm{id}} = \mathrm{id}, \text{ with } \xi(U_g) = \nu(g) \quad \forall g. \tag{8}$$

The group $G$ is the *index group* of the nice error basis. It is easy to see that a nice error basis is a unitary error basis [1].

Note that by the very definition, a nice error basis (with index group $G$) is endowed with a group structure (once having passed to the projective group), since for all $g, h \in G$ we have

$$\xi(U_g U_h) = \xi(U_g)\xi(U_h) = \nu(g)\nu(h) = \nu(gh) = \xi(U_{gh}). \tag{9}$$

So $\xi(S)$ carries a natural group structure.

The main theorem of [1] reads as follows:

**Theorem 3.1** ([1]). *Let $S$ be a nice error basis of $\mathbf{GU}_d(\mathbb{C})$ with index group $G$. Then the maximal number of MUBs that can be obtained by partitioning a subset of $S$ according to the beginning of §2 is at most*

$$\min_{p \in \Omega(d)}(d_p + 1). \tag{10}$$

In what follows, we will denote $\mathbf{GU}_n(\mathbb{C})$ by $\mathbf{U}_n(\mathbb{C})$.

**Remark 3.2.** In [1], the authors study certain finite groups $G$ of size $d^2$, with families $\mathcal{A}$ of trivially intersecting abelian subgroups of size $d$, the main objective being to bound $|\mathcal{A}|$ (from above) in function of $\Omega(d)$ (see [1, §3]). We will try to get a hold on the general situation in which a group $G$ is generated by the subgroups in $\mathcal{A}$, where $\mathcal{A} = d + 1$, without initial assumptions on $|G|$. While the authors of [1] try to understand maximal families $\mathcal{A}$ in the case $|G| = d^2$, the extremal case $|\mathcal{A}| = d + 1$ coming from affine planes of order $d$ (see section 5), we will try to understand $\Omega(d)$ in function of a "height," given that $|\mathcal{A}|$ is maximal (see again section 5).

## 4. The maps $\alpha$ and $\beta$

Take an element $\mathcal{B}$ in $\mathbf{MUB}$, and consider $\alpha(\mathcal{B}) = \{\mathcal{U}_0, \mathcal{U}_1, \ldots, \mathcal{U}_d\}$; recall Remark 2.2 (we use the notation of above, with $d \in \mathbb{N}$ and $d \neq 0, 1$). As each element $U_1^j$ with $j = 0, 1, \ldots, d$ has $d$ different eigenvalues, it follows that up to scaling the image of $\alpha(\mathcal{B})$ under $\beta$ is unique (that is, is $\mathcal{B}$ again). So $\alpha$ is injective.

In order to understand the correspondence between maximal MUBs and MCCs, we need to understand the map $\beta$ as well. What first comes to mind is the question whether $\beta$ is injective — i.e., could it happen that two different (nonisomorphic) MCCs give rise to the same maximal MUB under $\beta$? When attacking Zauner's conjecture from the viewpoint of MCCs, it would be very valuable to have a canonical correspondence between maximal MUBs and MCCs, but unfortunately, $\beta$ is *not* injective: *very* structurally different MCCs could map to the same maximal MUB. As each MCC generates a group, this means for instance that nonisomorphic groups can carry the same MUB structure.

This has important implications for the construction theory of maximal MUBs: one has to be very careful when constructing "new" maximal MUBs through the theory of MCCs (and the map $\beta$), as nonisomorphic MCCs could give the same MUB!

**Remark 4.1.** Note that for any maximal MUB $\mathcal{B}$, $\beta^{-1}(\mathcal{B})$ is not empty, since $\alpha(\mathcal{B}) \in \beta^{-1}(\mathcal{B})$. So $\beta$ is surjective.

Before proceeding, we need to express what "isomorphic MCCs" means. (In [20] this notion was already discussed in the special case of MCCs consisting of Pauli operators; there, a finer definition can be given than the one we propose here in the general context.)

For any MCC $\widetilde{\mathcal{U}} = \{\widetilde{\mathcal{U}}_0, \ldots, \widetilde{\mathcal{U}}_d\}$ of size $d + 1$, $d \in \mathbb{N}$ and $d \neq 0, 1$, define $A(\widetilde{\mathcal{U}}) \leq \mathbf{U}_d(\mathbb{C})$ to be the group generated by the elements of $\cup_{i=0}^{d} \widetilde{\mathcal{U}}_i$. We will call it the *operator group* associated to $\widetilde{\mathcal{U}}$.

So let $\mathcal{U}$ and $\mathcal{U}'$ be MCCs, and let $\Omega$, respectively $\Omega'$, be the set of operators of $\mathcal{U}$, respectively $\mathcal{U}'$. Then we call $\mathcal{U}$ and $\mathcal{U}'$ *isomorphic* if modulo scaling there exists an isomorphism $\varrho : A(\mathcal{U}) \mapsto A(\mathcal{U}')$ which maps $\Omega$ to $\Omega'$. (By "modulo scaling" we mean that one first is allow to re-scale $\Omega$.)[1]

**QUESTION 4.2.** *Consider a maximal MUB $\mathcal{B}$. List invariants of the elements of $\beta^{-1}(\mathcal{B})$.*

Now let $d$ be a prime, $N > 1$ a positive integer, and let $S$ be a spread of $\mathcal{W}_{2N-1}(d)$ (they always exist); then we have seen that $\gamma^{-1}(S)$ is an MCC of size $d^N + 1$, so $\beta(\gamma^{-1}(S)) =: \mathcal{B}_S$ is a maximal MUB of order $d^N + 1$. Now $\gamma^{-1}(S)$ and $\alpha(\mathcal{B}_S)$ both are elements of $\beta^{-1}(\mathcal{B})$, but they cannot be isomorphic for various reasons. One being that as $\gamma^{-1}(S)$ is a subset of the general Pauli group $\mathbf{P}_N(d)$, all its elements are trivial or have order $d$. While obviously $\alpha(\mathcal{B}_S)$ contains elements of order $d^N$ (as each $\mathcal{U}_j$ is a cyclic group of order $d^N$).

So the list of all possible orders of the operators associated to an element of $\beta^{-1}(\mathcal{B})$ is *not* an invariant! Moreover, $A(\gamma^{-1}(S))$, the Pauli group, is a $d$-group of exponent $d$, while $A(\alpha(\mathcal{B}_S))$ is a $d$-group of exponent $d^N$, so the associated (isomorphism classes of) groups aren't invariants as well.

This indicates that the sets $\beta^{-1}(\mathcal{B})$ behave rather mysteriously.

## 5. A THEORY OF HEIGHTS?

In order to work with an induction hypothesis, it could be valuable to introduce a notion of "height" for any MCC, which measures how far the generated group is from an abelian group. Ideally, the heights would be nonzero integers, and height $1$ would be the case where the group *is* abelian. In many papers concerning MUBs (see, for instance, Wootters [22]), it has been conjectured or at least has been expressed as a hope, that one can associate a finite projective or affine plane of order $d$ to a maximal set of MUBs (of size $d + 1$). The central conjecture in the theory of finite projective planes is the statement that each such plane's order is a prime power; see Thas [18] for a far-reaching discussion. Passing to the language of MCCs $\mathcal{U} = \{U_0, \ldots, U_d\}$, each $U_i$ should define a parallel class of lines in an associated affine plane of order $d$. When $\xi(A(\mathcal{U}))$ is small (minimally of size $d^2$), we will see in Theorem 5.3 below that this is precisely what happens: the proof observes that the elements of $\xi(A(\mathcal{U}))$ then naturally define the points of an affine plane of order $d$, and the left cosets of each $\xi(U_i)$ define a parallel class of lines. The theory of affine translation planes then ends the proof. (A related result in Aschbacher et al. [1], see section 3, is proved in the same way.) In that sense, and motivated by Theorem 5.3, "height" also measures how far the point-line geometry defined by

- Points: the elements of $\xi(A(\mathcal{U}))$,
- Lines: left cosets of the $\xi(U_i)$s;
- Incidence: natural,

is from an affine (translation) plane.

So let $\mathcal{U} = \{\mathcal{U}_0, \mathcal{U}_1, \ldots, \mathcal{U}_d\}$ be an MCC of size $d + 1$, with $d \in \mathbb{N}$, $d \neq 0, 1$. The *height* of $\mathcal{U}$ is the value

$$\rho(\mathcal{U}) := \frac{|\xi(A(\mathcal{U}))|}{d^2} \in \mathbb{Q}_{\geq 1} \cup \{\infty\}. \tag{11}$$

Recall from §3 that

$$\xi(A(\mathcal{U})) = A(\mathcal{U})/(A(\mathcal{U}) \cap Z(\mathbf{U}_d(\mathbb{C}))). \tag{12}$$

At this point, I have no idea whether a height is always contained in $\mathbb{N} \cup \{\infty\}$, or even $\mathbb{N}$, and these are the first questions to be handled. Each of the questions below comes with a more subtle twin, motivated by the previous section.

**QUESTION 5.1.** *Let $\mathcal{U}$ be an MCC of size $d + 1$.*

(a) *Is $\rho(\mathcal{U})$ always finite? (That is, is $A(\mathcal{U})$ always a finite group?)*
(b) *Is $\rho(\widetilde{\mathcal{U}})$ finite for some element $\widetilde{\mathcal{U}} \in \beta^{-1}(\beta(\mathcal{U}))$? (In other words, given $\mathcal{U}$, is there some other MCC $\widetilde{\mathcal{U}}$ of finite height which gives rise to the same maximal MUB?)*

A positive answer on either questions would reduce the problem to one in finite (unitary) group theory.

[1] Probably other (better) definitions exist, but it is in any case compatible with the one of [20] in the special case of Pauli operators.

**Question 5.2.** *Let $\mathcal{U}$ be an MCC of size $d+1$.*

(a) *Is $\rho(\mathcal{U})$ always a positive integer, or $\infty$?*
(b) *If not all elements of $\beta^{-1}(\beta(\mathcal{U}))$ have infinite weight, is $\rho(\widetilde{\mathcal{U}})$ a positive integer for some element $\widetilde{\mathcal{U}} \in \beta^{-1}(\beta(\mathcal{U}))$?*

MUBs which are associated to an MCC of height $1$ can be easily handled; we will do this after the next definition.

If $A$ and $B$ are subsets of a group $(C,\cdot)$, by $AB$ we will denote the subset $\{a\cdot b|a\in A, b\in B\}$.

**Theorem 5.3** (Height 1)**.** *If $\mathcal{B}$ is a maximal MUB of size $d+1$, $d\in\mathbb{N}$, $d\neq 0,1$, and $\mathcal{U}\in\beta^{-1}(\mathcal{B})$, then $d$ is a prime power if $\mathcal{U}$ has height $1$.*

*Proof.* Suppose that $\mathcal{U}$ has height $1$; then $|\xi(A(\mathcal{U}))| = d^2$. Denote $A(\mathcal{U})\cap Z(\mathbf{U}_d(\mathbb{C}))$ by $Y$.

Now note the following properties (for all $i\neq j$ in $\{0,1,\ldots,d\}$):

$$\begin{cases} \mathcal{U}_i \cap Y & = \{\mathrm{id}\}, \\ Y\mathcal{U}_i \cap Y\mathcal{U}_j & = Y. \end{cases} \tag{13}$$

The first property is trivial. For the second property, consider $V\in\mathcal{U}_i^\times, W\in\mathcal{U}_j^\times$, and suppose $yV = y'W\neq\mathrm{id}$ for $y,y'\in Y$. Then $VW^{-1}\in Y$, that is, $V$ and $W$ differ only by a scalar factor, obviously a contradiction.

It now follows easily that

$$A(\mathcal{U}) = \bigcup_{0\leq i\leq d} Y\mathcal{U}_i. \tag{14}$$

We hence have the next property for all $i\neq j$ in $\{0,1,\ldots,d\}$:

$$\langle\mathcal{U}_i\rangle \leq Y\mathcal{U}_i. \tag{15}$$

For, suppose $\langle\mathcal{U}_i\rangle \not\leq Y\mathcal{U}_i$; then by (14), $\langle\mathcal{U}_i\rangle$ contains elements of the form $yL$, with $L\in\mathcal{U}_j^\times$, $j\neq i$, and $y\in Y$. As the elements of $\mathcal{U}_i$ mutually commute, $\langle\mathcal{U}_i\rangle$ is abelian, so $yL$ commutes with any element of $\mathcal{U}_i$, and then $L$ also does, contradiction. So for each $i$, we have that $\langle\mathcal{U}_i\rangle\leq Y\mathcal{U}_i$, so

$$\xi(\langle\mathcal{U}_i\rangle) = \langle\mathcal{U}_i\rangle Y/Y = Y\mathcal{U}_i/Y \tag{16}$$

is a group of size $d$.

Passing to $\xi(A(\mathcal{U}))$, we obtain that if $i\neq j$, then $\xi(\langle\mathcal{U}_i\rangle)$ and $\xi(\langle\mathcal{U}_j\rangle)$ both are groups of size $d$, and they intersect in $\{\mathrm{id}\}$. So

$$|\xi(A(\mathcal{U}))| = |\cup_{i=0}^{d}\xi(\langle\mathcal{U}_i\rangle)|. \tag{17}$$

So in this way we get $d+1$ subgroups of $\xi(A(\mathcal{U}))$ of size $d$, two by two intersecting only in $\{\mathrm{id}\}$. It follows by [12, §1.1] that $\xi(A(\mathcal{U}))$ must be elementary abelian. Hence $d$ is a prime power. ■

Taken that $\rho(\mathcal{U})\neq\infty$, one way to study these questions could be to consider the subgroups $\langle\mathcal{U}_i,\mathcal{U}_j\rangle$ $(i\neq j)$ and try to find out how the commutator $[\mathcal{U}_i,\mathcal{U}_j]$ looks like (so that one can estimate the order of $\langle\mathcal{U}_i,\mathcal{U}_j\rangle$). It seems that even in special cases this becomes a hard task. This motivates us to consider the nilpotence and solvability class of the groups generated by the MCCs associated to one given maximal MUB: both properties express how far a group is from being abelian (in an entirely different fashion than the height function), and the latter case is the case with trivial commutators. Also, we have seen in the discussion starting with Proposition 2.3, that we used specific group theoretical properties of the general Pauli group to construct the map $\gamma$, and to define the associated symplectic polar space, in section 2.2. In cases of low nilpotence class, geometries constructed from groups and forms, similarly as in section 2.2, or from a group coset construction such as in the beginning of section 5, tend to have interesting structural geometric properties which often are sufficient to force the group to be a $p$-group for some prime $p$. Another example besides the aforementioned symplectic polar spaces and affine translation planes in which this idea can be illustrated, is the case of *elation generalized quadrangles* [19]. This is a type of point-line geometry which is constructed as a group coset geometry similarly as affine translation planes are, and in the finite case, it is a conjecture that the group be a $p$-group (see [18] and [19, chapter 3]). In case that the group is nilpotent, this can indeed be verified using the extra geometric information the nilpotence yields. We refer to the monograph [19], and especially its chapter 5, for proofs of these and other related results. We note that $\mathcal{W}_{2N-1}(d)$ is an elation generalized quadrangle if $N=2$.

## 6. MUBs of class 2

Let $G$ be any group. Then define $G^{(0)} := G$ and $G^{(n)} := [G, G^{(n-1)}]$ for all $n \in \mathbb{N}$; in particular, $G^{(1)} := [G, G] = G'$. If $G^{(n)} = \{\mathrm{id}\}$ for some such $n$, then we say that $G$ has *nilpotence class* $n$ if $n$ is the minimum natural number for which this property holds. Nilpotence class 1, e.g, implies that $G$ is abelian. Now define $G^{[0]} := G$ and $G^{[n]} := [G^{[n-1]}, G^{[n-1]}]$ for all $n \in \mathbb{N}$; in particular, $G^{[1]} := [G, G] = G^{(1)}$. If $G^{[m]} = \{\mathrm{id}\}$ for some $m$, then we say that $G$ has *solvability class* $m$ if $m$ is the minimum natural number for which this property holds.

We say that an MCC $\mathcal{U}$ has *nil-class*, respectively *sol-class*, $m \in \mathbb{N} \cup \{\infty\}$ if $A(\mathcal{U})$ has nilpotence class, respectively solvability class, $m$. If we speak of the class of an MCC without mentioning the type, we mean both nil- and sol-class. The nil-class is denoted by $\mathrm{nilcl}(\mathcal{U})$, the sol-class by $\mathrm{solcl}(\mathcal{U})$. (Class $\infty$ means that $A(\mathcal{U})$ is not nilpotent/solvable.)

A maximal MUB $\mathcal{B}$ has *nil/sol-class* $n \in \mathbb{N} \cup \{\infty\}$ if $n = \min\{\mathrm{nil/solcl}(\mathcal{U}) | \mathcal{U} \in \beta^{-1}(\mathcal{B})\}$.

**Proposition 6.1.** *A maximal MUB always has nil/sol-class at least* 2.

*Proof.* If $\mathcal{B}$ has nil/sol-class 1, this means that some $\mathcal{U} \in \beta^{-1}(\mathcal{B})$ has nil/sol-class 1, so that $A(\mathcal{U})$ is abelian. On the other hand, in [2] it is remarked that if $O \neq \mathrm{id}$ is an operator in an MCC, $O$ only commutes with the elements of the unique commuting class to which it belongs. So $A(\mathcal{U})$ cannot be abelian. ■

Any MCC $\mathcal{U}$ of order $d^N + 1$ which exists solely of elements from the general Pauli group $\mathbf{P}_N(d)$ of order $d^{2N+1}$ (that is, which arises from the symplectic polar space), has the property that $A(\mathcal{U}) = \mathbf{P}_N(d)$, and as we have seen the general Pauli group has nilpotence class 2. Here $d$ is a prime, and $N$ a positive integer. So nil/sol-class 2 MUBs *do* exist.

**Question 6.2.** *Can Zauner's conjecture be verified for MUBs of nil/sol-class* 2*?*

Working with general MCCs of sol-class 2, this already appears to be difficult. In this context, it would be interesting to known the nil/sol-classes of the presently known examples of maximal MUBs — in any case, class 2 maximal MUBs are obviously fundamental to understand. So we propose the following important special case.

**Question 6.3.** *Let $\mathcal{B}$ be a maximal MUB of size $d+1$, $d \in \mathbb{N}$, $d \neq 0, 1$, and suppose that $\alpha(\mathcal{B})$ has class* 2*. Is $d$ a prime power? What can be said about the structure of $\alpha(\mathcal{B})$?*

We will consider this question for the nil-class, in the next section.

**Question 6.4.** *Let $\mathcal{B}$ be a maximal MUB of size $d+1$, and suppose that $\alpha(\mathcal{B})$ has class $m < \infty$. Is $d$ a prime power?*

For nil-class, we will solve the question completely in §8. Given the specific properties used in section 8 to accomplish this, I am not sure the question for sol-class is in reach for the moment.

## 7. Maximal MUBs $\mathcal{B}$ with $\alpha(\mathcal{B})$ having nil-class 2

We start with a number of lemmas which, once pieced together, will reveal the structure of MUBs of nil-class 2. So rather than only proving that $d$ is a prime power in low nilpotence class, revealing that structure is a main objective here. There are much shorter proofs for the prime power property in more general settings — see §8. In this particular case, the structure will even lead to the fact that the dimension is a prime.

### 7.1. Some structural lemmas.

**Lemma 7.1.** *Let $A$ and $D$ be $(m \times m)$-matrices with $m \in \mathbb{N} \setminus \{0, 1\}$, and suppose $D$ is diagonal with all different nonzero diagonal entries. If $AD = DA$, then $A$ also is diagonal.*

*Proof.* Write $A = (a_{ij})$ and $D = (d_{ij})$. Then $AD = DA$ implies that for $u, v \in \{1, \ldots, m\}$, we have $a_{uv}d_{vv} = a_{uv}d_{uu}$. So if $a_{uv} \neq 0$, it follows that $u = v$. ■

**Corollary 7.2.** *Let $\mathcal{B}$ have nil-class* 2*, with $A(\mathcal{U})$ having nil-class* 2 *and $\mathcal{U} \in \beta^{-1}(\mathcal{B})$. If $C \in Z(A(\mathcal{U}))$, then $C$ is diagonal. In particular, if $C \in [A(\mathcal{U}), A(\mathcal{U})]$, it is diagonal.* ■

**Corollary 7.3.** *If $A, B \in A(\mathcal{U})$, we have that $[A, B]$ is diagonal.* ■

If in particular $A \in \mathcal{U}_0$, then $A$ is diagonal, so that $[A, B] \neq \mathrm{id}$ if $B \in \mathcal{U}_i$, $i \neq 0$.
The following lemma will be quite useful.

**Lemma 7.4.** *Let $AD = rDA$ with $A$ an $(m \times m)$-matrix ($m \in \mathbb{N} \setminus \{0,1\}$), $D$ a diagonal $(m \times m)$-matrix with two by two different $\neq 0$ diagonal entries and $r \in \mathbb{C} \setminus \{0,1\}$, that is, $[A, D] = r \cdot \mathrm{id}_m \in Z(\mathbf{U}_m(\mathbb{C}))$. Then $A$ has the structure of a permutation matrix, i.e., $A \in \mathbb{C} \wr S_m$.*

*Proof.* Writing $A = (a_{ij})$ and $D = (d_{ij})$, we have that if $u, v$ are different elements of $\{1, 2, \ldots, m\}$, then

$$a_{uv}d_{vv} \ = \ r \cdot a_{uv}d_{uu}, \tag{18}$$

so that $a_{uv} \neq 0$ would imply that $d_{vv} = rd_{uu}$. If we also assume that $a_{uk} \neq 0$ for some $k \neq v$, then $a_{uk}d_{kk} = ra_{uk}d_{uu}$, implying $d_{kk} = rd_{uu} = d_{vv}$, contradiction. So if $a_{uv} \neq 0$, then $a_{uk} = 0$ for all $k \neq v$. From the fact that $A$ is nonsingular follows that each row and column had exactly one $\neq 0$ entry, whence the claim. ■

7.2. **The underlying permutations.** From now on, $\mathcal{B}$ is a maximal MUB of size $d+1$ in $\mathbb{C}^d$, and we suppose that $\alpha(\mathcal{B}) =: \mathcal{U}$ has nil-class 2. Then since the generator $U_1^0$ of $\mathcal{U}_0$ is a diagonal matrix with $d$ different eigenvalues, by Corollary 7.2 we know that the center of $A(\mathcal{U})$ consists of diagonal matrices. Inspired by Proposition 2.3(ii), we introduce the next "diagonal property." In subsection 7.4 we will show that it always holds *for every MCC*. That is the reason why we postpone it to subsection 7.4.

[**Assumption DIAG**] *From now on, we suppose that*

$$Z(A(\mathcal{U})) \ \leq \ Z(\mathbf{U}_d(\mathbb{C})), \tag{19}$$

*that is, $Z(A(\mathcal{U}))$ consists of scalar matrices.*

Take any $A \in A(\mathcal{U})$; then since $A(\mathcal{U})$ has nil-class 2, $[A, U_1^0] \leq Z(A(\mathcal{U}))$, so that $[A, U_1^0] = r \cdot \mathrm{id}_d$ for some nonzero $r$. By Lemma 7.4, we may conclude that $A$ has the structure of a permutation matrix. Suppose the underlying permutation of $\{1, 2, \ldots, d\}$ is $\sigma$. This means that for any $l \in \{1, 2, \ldots, d\}$, the only nonzero element in the $l$-th row of $A$ is $a_{l\sigma(l)}$. Write $(u_{ij})$ for $U_1^0$; then from $AU_1^0 = r \cdot U_1^0 A$, we deduce

$$a_{w\sigma(w)}u_{\sigma(w)\sigma(w)} \ = \ r \cdot u_{ww}a_{w\sigma(w)} \quad \forall w, \tag{20}$$

so that the fact that $a_{w\sigma(w)} \neq 0$ implies that

$$\frac{u_{\sigma(w)\sigma(w)}}{u_{ww}} = r \quad \forall w. \tag{21}$$

Applying the definition of $U_1^0$ (through the map $\alpha$), we conclude that

$$e^{\frac{2\pi i}{d}(\sigma(x)-x)} \ = \ e^{\frac{2\pi i}{d}(\sigma(y)-y)} \quad \forall x, y. \tag{22}$$

Put $\sigma(1) - 1 =: s$, and observe that $s \in \mathbb{N}$. Then for all $x \in \{1, 2, \ldots, d\}$, we have that

$$\sigma(x) - x \ = \ s \mod d. \tag{23}$$

It follows easily that $\sigma$ is defined as follows (in terms of $s$), where below $m \in \{1, 2, \ldots, d\}$.

$$\begin{cases} \text{If } m + s \leq d, & \text{then } \sigma(m) = m + s; \\ \text{If } m + s > d, & \text{then } \sigma(m) = m + s - d. \end{cases} \tag{24}$$

When $s = 1$, we denote the corresponding permutation by $\tau$; $\tau$ defines a regular cycle of size $d$. Note that $\tau$ corresponds to the shift operator $\widehat{X}$, which acts on the standard base $\{|1\rangle, |2\rangle, \ldots, |d\rangle\}$ as

$$\widehat{X}|k\rangle = |k + 1 \mod d\rangle \quad \forall k \in \{1, 2, \ldots, d\}. \tag{25}$$

**Lemma 7.5.** *For any element $B$ of $A(\mathcal{U})$, the underlying permutation is an element of $\langle\tau\rangle$, which is a regular group of size $d$. Moreover, if $\pi$ is the natural projection of $A(\mathcal{U})$ on the symmetric group $S_d$, then*

$$\pi(A(\mathcal{U})) \;=\; \langle\tau\rangle. \tag{26}$$

*Proof.* The fact that $\pi(A(\mathcal{U})) \;\leq\; \langle\tau\rangle$ is obvious. Now consider a commuting class $\mathcal{U}_i$, with $i \neq 0$; by assumption, $\mathcal{U}_i$ is a group of order $d$. Suppose by way of contradiction that $\pi(\mathcal{U}_i) \neq \langle\tau\rangle$. Then $\mathcal{U}_i$ has nontrivial elements which are projected on the identity matrix in $\langle\tau\rangle$ (since $\pi$ is a group morphism), that is, nontrivial diagonal elements. But those commute with any element in $\mathcal{U}_0$, contradicting the definition of MCC. So for each $\mathcal{U}_j$, $j \neq 0$,

$$\pi(\mathcal{U}_j) \;=\; \langle\tau\rangle. \tag{27}$$

■

7.3. **Obtaining that $d$ is a prime.** Now suppose $d$ is not a prime; write $d = d_1 \cdot d_2$, with $d_1$ and $d_2$ positive integers, both different from $1$ and $d$. Let $\omega$, as before, be a primitive $d$-th root of unity.

Let $i \in \{1, 2, \ldots, d\}$. By the above, each element $\rho$ of $\mathcal{U}_i$ is of the form $(\widehat{X})^u(\widetilde{Z})^v$, where $(u, v) \in \mathbb{N}\times\mathbb{N}$, $\widehat{X}$ is as in §7.2, and where the operator $\widetilde{Z}$ acts on the standard base $\{|1\rangle, |2\rangle, \ldots, |d\rangle\}$ as

$$\widetilde{Z}|k\rangle = \omega^{f(k)}|k\rangle. \tag{28}$$

Here $f : \{1, 2, \ldots, d\} \mapsto \{1, 2, \ldots, d\}$ is some unknown function. (Note that $\rho$ indeed has this form, since it has the structure of a permutation matrix, with entries integer powers of $\omega$.)

Now let $(Z_d)^b$, $b \in \mathbb{N}^\times$, be an arbitrary element of $\mathcal{U}_0^\times$. Then for each $|k\rangle$ in the standard base we have:

$$\begin{cases} (Z_d)^b \cdot \Big((\widehat{X}^u)(\widetilde{Z})^v\Big)|k\rangle & = \omega^{b(k+u)}\omega^{vf(k)}|k+u \mod d\rangle, \\ \\ \Big((\widehat{X}^u)(\widetilde{Z})^v\Big) \cdot (Z_d)^b|k\rangle & = \omega^{bk}\omega^{vf(k)}|k+u \mod d\rangle. \end{cases} \tag{29}$$

So the right-hand sides are equal (for all $|k\rangle$) if and only if $bu \equiv 0 \mod d$. Each element of $\mathcal{U}_0$ commutes with $(Z_d)^b$. However, if for instance $b = d_1$ and $u = d_2$, we find an element in $\mathcal{U}_i^\times$ which also commutes with $(Z_d)^b$, contradiction with the definition of MCC. It is important to note here that by the proof of Lemma 7.5, we may indeed substitute an arbitrary value in $u$, since $\mathcal{U}_i$ projects onto $\langle\tau\rangle$ by $\pi$.

We have shown that $d$ must be a prime.

7.4. **The diagonal assumption for general MCCs.** In this subsection, we show that (DIAG) is satisfied in the setting of the previous section. In fact, we will show that (DIAG) is *always* satisfied for *general* MCCs, as an application of Schur's Lemma on irreducible linear representations (in characteristic $0$).

So let $\mathcal{U} = \{\mathcal{U}_0, \ldots, \mathcal{U}_d\}$ be an MCC in $\mathbb{C}^d$ and consider the identical map

$$\rho : A(\mathcal{U}) \mapsto A(\mathcal{U}) \leq \mathbf{U}_d(\mathbb{C}), \tag{30}$$

which sends each element of $A(\mathcal{U})$ to the corresponding unitary matrix in $\mathbf{U}_d(\mathbb{C})$.

By definition of $A(\mathcal{U})$, $\rho$ is a faithful linear representation of $A(\mathcal{U})$. Suppose $W \neq \{\mathbf{0}\}$ is a $\mathbb{C}$-linear subspace of $V = \mathbb{C}^d$ which is $A(\mathcal{U})$-invariant. Fix some nonzero vector $\mathbf{x} \in W$. Then for all $A \in \cup_i\mathcal{U}_i$, we have that $cA \cdot \mathbf{x}^T \in W$ with $c \in \mathbb{C}$. So for every $\mathbb{C}$-linear combination $\sum_{A\in\cup_i\mathcal{U}_i} c_A A$, we have that

$$\Big(\sum_{A\in\cup_i\mathcal{U}_i} c_A A\Big)\cdot\mathbf{x}^T \;\in\; W. \tag{31}$$

As $\cup_i\mathcal{U}_i$ is a basis for $\mathbf{M}_{d\times d}(\mathbb{C})$ (cf. section 2), it follows that $W = V$. So $\rho$ is an *irreducible* representation. By Schur's Lemma [15], it now follows that the only elements in $\mathbf{U}_d(\mathbb{C})$ which commute with each element in $A(\mathcal{U})$ are scalar matrices. We have proved the following proposition:

**Proposition 7.6.** *Let $\mathcal{U}$ be an MCC in $\mathbb{C}^d$, and consider $A(\mathcal{U})$. Then the center $Z(A(\mathcal{U}))$ consists of scalar matrices. In particular, if $A(\mathcal{U})$ is finite, $Z(A(\mathcal{U}))$ is a cyclic group.*

*Proof.* The general statement has already been proven. For the finite case, note that $Z(A(\mathcal{U}))$ is isomorphic to a finite subgroup of $\mathbb{C}^\times$. ■

So (DIAG) is indeed true in general.

## 8. Finite nilpotent MUBs satisfy Zauner's conjecture

Let $\mathcal{B}$ be a maximal MUB of size $d+1$ in $\mathbb{C}^d$, and suppose that $\alpha(\mathcal{B}) =: \mathcal{U}$ has nil-class $m < \infty$, and furthermore that $A(\mathcal{U})$ is finite. In this section we will show that $d$ is a prime power. In contrast with the previous section, we do not focus on the structure of $\alpha(\mathcal{B})$, but we solely concentrate on Zauner's conjecture.

### 8.1. Finite nilpotent MUBs.

Since $A(\mathcal{U})$ is nilpotent and finite, $A(\mathcal{U})$ is isomorphic to the direct product of its Sylow subgroups (see [5, Theorem 3.5, p. 23]):

$$A(\mathcal{U}) \;\cong\; S_{p_1} \times \cdots \times S_{p_k}, \tag{32}$$

where $\{p_1, \ldots, p_k\}$ is the set of distinct primes dividing $|A(\mathcal{U})|$, and for each $p_i$, $S_{p_i}$ is the Sylow $p_i$-subgroup of $A(\mathcal{U})$. It immediately follows that if $\alpha \in A(\mathcal{U})^\times$ has order $p_i^n$ and $\beta \in A(\mathcal{U})^\times$ has order $p_j^m$, with $p_i \neq p_j$, then $[\alpha, \beta] = \mathrm{id}$. So take $\delta \in \mathcal{U}_u^\times$ and $\phi \in \mathcal{U}_v^\times$ with $u \neq v$. Then we can take suitable powers $\delta^a \neq \mathrm{id}$ of $\delta$ and $\phi^b \neq \mathrm{id}$ of $\phi$ so that $[\delta^a, \phi^b] = \mathrm{id}$, contradiction with the definition of MCC.

It follows that $|\{p_1, \ldots, p_k\}| = 1$, that is, $|A(\mathcal{U})|$, and hence $d$, is a prime power.

### 8.2. Generalizations (group-like MCCs).

At no point in the previous subsection have we used the actual definition of $\alpha(\mathcal{B})$; rather, we only used the fact that each $\mathcal{U}_i$ is a group. So call an MCC $\mathcal{U} = \{\mathcal{U}_0, \ldots, \mathcal{U}_d\}$ in $\mathbb{C}^d$ "group-like" if each $\mathcal{U}_i$ is a group. Call it *group-like at* $\mathcal{U}_j$ if $\mathcal{U}_j$ is a group (recall that in our notation each commuting class contains $\mathrm{id}$). The next results follows immediately from the previous subsection.

**Proposition 8.1.** *If $\mathcal{U}$ is an MCC in $\mathbb{C}^d$ so that $A(\mathcal{U})$ is finite and nilpotent, and such that it is group-like at at least two elements, then $d$ is a prime power. In particular, if $A(\mathcal{U})$ is group-like, the same conclusion holds.* ■

**Proposition 8.2.** *Let $\mathcal{U}$ be an MCC in $\mathbb{C}^d$ so that $A(\mathcal{U})$ is finite and nilpotent, and suppose there are elements $\alpha \in \mathcal{U}_i^\times$ and $\beta \in \mathcal{U}_j^\times$ with $i \neq j$, such that $\langle \alpha \rangle \leq \mathcal{U}_i$ and $\langle \beta \rangle \leq \mathcal{U}_j$. Then $d$ is a prime power.*

## References

[1] Aschbacher M, Childs, A M and Wocjan P 2007 J. Algebraic Combin. **25** 111–123

[2] Bandyopadhyay S, Boykin, P O, Roychowdhury V and Vatan F 2002 Algorithmica **34** 512–528

[3] Calderbank A R, Cameron P. J., Kantor W. M. and Seidel J. J. 1997 Proc. London Math. Soc. **75** 436–480

[4] Delsarte P, Goethals P M and Seidel J J 1975 Philips Res. Rep. **30** 91–105

[5] Gorenstein D 1980 *Finite groups. Second edition* Chelsea Publishing Co. New York

[6] Hirschfeld J W P 1998 *Projective Geometries over Finite Fields (2nd Edition)* Oxford Mathematical Monographs (New York: Oxford University Press)

[7] Hoggar S G 1982 European J. Combin. **3** 233–254

[8] Hughes D R and Piper F C *Projective Planes* Grad. Texts in Math. (New York Heidelberg Berlin: Springer-Verlag)

[9] Ivanovic I D 1981 J. Phys. A **14** 3241–3245

[10] Kabatiansky G A and Levenshtein V I 1978 Problems Inform. Transmission **14** 1–17

[11] Klappenecker A and Rötteler M 2005 Proc. 2005 IEEE International Symposium on Information Theory 1740–1744 (Preprint `quant-ph/0502031`)

[12] Knarr N *Translation Planes* 1995 Lecture Notes in Mathematics (New York Heidelberg Berlin: Springer-Verlag)

[13] Knill E 1996 Tech. Report LAUR-96-2717 Los Alamos National Laboratory

[14] Mandayam P, Bandyopadhyay S, Grassl M and Wootters W K 2014 Quantum Inf. Comp **14** 0823–0844

[15] Schur I 1905 *Neue Begründung der Theorie der Gruppencharaktere*, Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin 406–432

[16] Schwinger J 1960 Proc. Nat. Acad. Sci. U. S. A. **46** 570

[17] Thas K 2009 Europhys. Lett. (EPL) **86** 60005

[18] Thas K 2011 in: Surveys in Combinatorics London Math. Soc. Lecture Note Ser. **392** Cambridge University Press pp. 235–331

[19] Thas K 2012 *A Course on Elation Quadrangles* EMS Series of Lectures in Mathematics (European Math. Soc.: Zürich)

[20] Thas K 2016 Entropy **18** 395

[21] Wootters W K and Fields B D 1989 Ann. Phys. **191** 363–381

[22] Wootters W K 2006 Found. Phys. **36** 112–126

[23] Zauner G 1999 *Quantendesigns: Grundzüge einer nichtkommutativen Designtheorie* Ph. D. Thesis (Universität Wien)

Department of Mathematics, Ghent University, Krijgslaan 281, S25, B-9000 Ghent, Belgium
*E-mail address*: `koen.thas@gmail.com`