entropy

MDPI

Article

Unextendible Mutually Unbiased Bases (after Mandayam, Bandyopadhyay, Grassl and Wootters)

Koen Thas

Department of Mathematics, Ghent University, Ghent 9000, Belgium; koen.thas@gmail.com

Academic Editor: Jay Lawrence
Received: 7 September 2016; Accepted: 31 October 2016; Published: 11 November 2016

Abstract: We consider questions posed in a recent paper of Mandayam et al. (2014) on the nature of "unextendible mutually unbiased bases." We describe a conceptual framework to study these questions, using a connection proved by the author in Thas (2009) between the set of nonidentity generalized Pauli operators on the Hilbert space of N d-level quantum systems, d a prime, and the geometry of non-degenerate alternating bilinear forms of rank N over finite fields $\mathbb{F}_d$. We then supply alternative and short proofs of results obtained in Mandayam et al. (2014), as well as new general bounds for the problems considered in *loc. cit*. In this setting, we also solve Conjecture 1 of Mandayam et al. (2014) and speculate on variations of this conjecture.

Keywords: mutually unbiased bases; Pauli operator; symplectic polar space

PACS: 02.10.Ox; 02.40.Dr; 03.65.Ta; 03.65.Ud; 03.67.-a

1. Introduction

Finite-dimensional quantum systems—that is, "multiple qudits"—exhibit many interesting properties like quantum entanglement and quantum non-locality. Therefore, they play a crucial role in numerous physical applications like quantum cryptography, quantum coding, quantum cloning/teleportation and/or quantum computing, to mention just a few. As these systems live in finite-dimensional Hilbert spaces, further insights into their behavior require, obviously, a proper understanding of the structure of the associated Hilbert spaces. Within the past few years, a lot of activity in this direction has been devoted to the study of so-called mutually unbiased bases ("MUBs").

Recall that 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 conjecture, with many applications, that the theoretical upper bound $\ell + 1$ of a set of mutually unbiased bases can only be reached when ℓ is a *prime power*.

It has been suspected for a long time that there are deep connections between quantum (information) theory and finite geometry—see, for instance, Wootters [1,2] (see also [3,4] and [5–7], and references therein.)

As a specific example, proving a conjecture of Saniga and Planat [7], the author showed in [8] that the generalized Pauli operators can be identified with the points, and maximum sets of pairwise commuting members of them with the lines (or subspaces of higher dimensions) of a specific finite incidence geometry, so that the structure of the operator space can fully be inferred from the properties of the geometry in question. The incidence geometry is the geometry of a non-degenerate alternating bilinear form over a finite field, called *symplectic polar space*. Using this connection, it is easy to construct maximal sets of MUBs by just translating known results in the theory of symplectic polar spaces.

In a recent paper [9], Mandayam, Bandyopadhyay, Grassl and Wootters introduced *unextendible mutually unbiased bases* ("UMUBs") (and several variations and related concepts; details can be found in Section 3) as a natural generalization of maximal sets of mutually unbiased bases.

One of the main results of [9] reads as follows.

Theorem 1 (Mandayam et al. [9]). *Given three Pauli classes $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ belonging to a complete set $\mathcal{S}$ of classes in dimension $= 4$, there exists exactly one more maximal commuting class $\mathcal{C}$ of Pauli operators in $\mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3$. The class $\mathcal{C}$ together with the remaining two classes $\mathcal{C}_4$ and $\mathcal{C}_5$ of $\mathcal{S}$ forms an unextendible set of Pauli classes, whose common eigenbases form a weakly UMUB of order* 3.

Using the connection with the polar space, we will give a short proof of this result. Moreover, we generalize this result for all dimensions $\ell =$ prime^2 (in fact, we present a construction of a new class of maximal partial spreads of the symplectic polar space $\mathcal{W}_3(d)$ for any odd prime power d, which translates to UMUBs in the case d is a prime.) In dimension $\ell = 8$, a similar result is obtained in [9].

Motivated by Theorem 1 and the result in dimension 8, the following conjecture is then stated in [9].

Conjecture 1 (Mandayam et al. [9]). *Given $\ell/2+1$ maximal commuting Pauli classes $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_{\ell/2+1}$ belonging to a complete set $\mathcal{S}$ of classes in dimension $\ell = 2^N =: d^N$, there exists exactly one more maximal commuting class $\mathcal{C}$ of Pauli operators in $\cup_{1\le i\le \ell/2+1}\mathcal{C}_i$. The class $\mathcal{C}$ together with the remaining classes of $\mathcal{S}$ forms an unextendible set of Pauli classes of size $\ell/2+1$, whose common eigenbases form a weakly UMUB of order $\ell/2+1$.*

We will show that this conjecture is true *if and only if* $N = 2$ *or* $N = 3$. In fact, we will consider an extension of the conjecture in any characteristic d (i.e., for any prime d), and show that it is true if and only if $d = 2$ and $N = 2$ or $N = 3$. The formulation of the conjecture has to be adapted, of course, since $\ell/2$ is not an integer if ℓ is odd. Thus, we will replace $\ell/2+1 = 2^{N-1}+1$ by $d^{N-1}+1$.

We then indicate that an alternative version of the conjecture might be true and describe several new possible construction techniques to obtain weakly unextendible sets of MUBs.

At the end of the paper, we discuss a special kind of weakly unextendible set of MUBs called "Galois MUBs," which attain an optimal bound in relation to being unextendible.

2. The General Pauli Group

Let d be an odd 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 products of the form

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

where the σ_{i_k} run over the set of (generalized) Pauli matrices of $\mathbb{C}^d$. Denote $\mathbb{P}^\times = \mathbb{P} \setminus \{\mathbf{I}\}$. These operators generate a group $\mathbf{P} = \mathbf{P}_N(d)$—the *general Pauli group* or *discrete Heisenberg–Weyl group*—under ordinary matrix multiplication, which has order d^{2N+1}.

For the case of N-qubit Hilbert spaces, we refer the reader to [8]—it is completely similar (and we use the same notation).

3. Unextendible Sets of MUBs and Operator Classes

Let $\mathcal{U}$ be a set of d^2 mutually orthogonal unitary operators in $\mathbb{C}^d$ using the Hilbert–Schmidt norm: operators A and B are *orthogonal* if $\mathrm{tr}(AB^\dagger) = 0$. Assuming that $\mathcal{U}$ contains the identity operator $\mathbf{I}$, $\mathcal{U}$ constitutes a basis for the $\mathbb{C}$-vector space of $(d \times d)$-complex matrices $\mathbf{M}_{d\times d}(\mathbb{C})$. A standard construction of MUBs outlined in [10] relies on finding classes of commuting operators, with each class containing $d-1$ mutually orthogonal commuting unitary matrices different from the identity $\mathbf{I}$.

3.1. Maximal Commuting Operator Classes

A set of subsets $\{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_\ell | \mathcal{C}_j \subset \mathcal{U} \setminus \{\mathbf{I}\}\}$ of size $|\mathcal{C}_j| = d-1$ constitutes a (partial) partitioning of $\mathcal{U} \setminus \{\mathbf{I}\}$ 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 $j \neq k$.

In the rest of the paper, we sometimes use the term "Pauli classes" to refer to mutually disjoint maximal commuting classes formed out of the N-qudit Pauli group $\mathbf{P}_N(d) \leq \mathbf{U}_{d^N}(\mathbb{C})$ (in [9], only qubits are considered). The correspondence between maximal commuting operator classes and MUBs is stated in the following lemma, originally proved in [10].

Lemma 1 ([10]). *The common eigenbases of ℓ mutually disjoint maximal commuting operator classes form a set of ℓ mutually unbiased bases.*

The reference [10] only considers sets of $d+1$ mutually disjoint maximal commuting operator classes, but the proof is the same.

3.2. Unextendibility of MUBs and Operator Classes

A set of MUBs $\{B_1, B_2, \ldots, B_\ell\}$ is called *unextendible* if there does not exist another basis that is unbiased with respect to the bases $B_1, \ldots, B_\ell$.

The correspondence between MUBs and maximal commuting operator classes gives rise to a weaker notion of unextendibility, based on unextendible sets of such classes.

Definition 1 (Unextendible sets of operator classes [9]). *A set of mutually disjoint maximal commuting classes $\{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_\ell\}$ of operators drawn from a unitary basis $\mathcal{U}$ is said to be* unextendible *if no other maximal class can be formed out of the remaining operators in $\mathcal{U} \setminus (\{\mathbf{I}\} \cup \bigcup_{i=1}^{\ell} \mathcal{C}_i)$.*

The eigenbases of such an unextendible set of classes form a weakly unextendible set of MUBs, as defined below.

Definition 2 (Weakly unextendible sets of MUBs [9]). *Given a set of MUBs $\{B_1, B_2, \ldots, B_\ell\}$ that are realized as common eigenbases of a set of ℓ operator classes comprising operators from $\mathcal{U}$, the set $\{B_1, B_2, \ldots, B_\ell\}$ is* weakly unextendible *if there does not exist another unbiased basis that can be realized as the common eigenbasis of a maximal commuting class of operators in $\mathcal{U}$.*

4. Symplectic Polar Spaces and the Pauli Group

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, where d is a prime. Let F be a non-degenerate symplectic form of $\mathbf{PG}(2N-1, d)$. For F, one can choose the following canonical bilinear form [11]:

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

Here, $(X_0 : \cdots : X_{2N-1})$ and $(Y_0 : \cdots : Y_{2N-1})$ stand for homogeneous coordinates of points in $\mathbf{PG}(2N-1,d)$. 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 [11]. Here, a *totally isotropic subspace* is a linear subspace S of $\mathbf{PG}(2N-1,d)$ that vanishes under F (that is, the bilinear form is trivial once restricted to S).

One can also define this space in the underlying $2N$-dimensional vector space $V(2N,d)$ over $\mathbb{F}_d$ using a non-degenerate alternating bilinear form (which induces a symplectic form on the projective space).

Remark 1 (Number of points). *Note that* $|$ *points of* $\mathcal{W}_{2N-1}(d)| = \frac{|V(2N,d)|-1}{d-1} = d^{2N-1} + d^{2N-2} + \cdots + 1$.

In the following proposition, $[.,.]$ denotes the commutator relation in the group $\mathbf{P}$; thus, $[a,b] := a^{-1}b^{-1}ab$ for $a,b \in \mathbf{P}$ and $\mathbf{P}' := [\mathbf{P},\mathbf{P}]$ is defined as the subgroup generated by the set $\{[a,b]|a,b \in \mathbf{P}\}$.

Proposition 1 (K. Thas [8]).
(i) *The derived group* $\mathbf{P}'$ *equals the center* $Z(\mathbf{P})$ *of* $\mathbf{P}$.
(ii) *We have* $Z(\mathbf{P}) = \langle \omega \mathbf{I} \rangle$, *so that* $|Z(\mathbf{P})| = d$.
(iii) $\mathbf{P}$ *is nonabelian of exponent* d *if* d *is odd.*
(iv) $\mathbf{P}$ *is nonabelian of exponent* 4 *if* d *is* 2.
(v) *We have the following short exact sequence of groups:*

$$1 \mapsto Z(\mathbf{P}) \mapsto \mathbf{P} \mapsto V(2N,d) \mapsto 1.$$

Now, denote the natural map $\mathbf{P} \mapsto V(2N,d)$ by an overbar (and note that in $\mathbf{P}$ we use multiplicative notation, which translates into addition in $V(2N,d)$). Then, the commutator

$$[.,.] : V(2N,d) \times V(2N,d) \mapsto \langle \omega \mathbf{I}_{d^N} \rangle : (\overline{v_1}, \overline{v_2}) \mapsto [\overline{v_1}, \overline{v_2}] = [v_1, v_2]$$

defines a non-degenerate alternating bilinear form on $V(2N,d)$, and thus defines a symplectic polar space $\mathcal{W}_{2N-1}(d)$. Here, the derived group $\mathbf{P}'$ is identified with the additive group of $\mathbb{F}_d$.

Theorem 2 ([8]). *Two elements of* $\mathbb{P}^\times$ *commute if and only if the corresponding points of* $\mathcal{W}_{2N-1}(d)$ *are collinear. In other words, the commuting structure of* $\mathbf{P}$ *(and* $\mathbb{P}$*) is governed by that of the symplectic polar space* $\mathcal{W}_{2N-1}(d)$.

Two points in $\mathcal{W}_{2N-1}(d)$ are called *collinear* if there is a line in $\mathcal{W}_{2N-1}(d)$ containing them both.

Applying this result, one can easily construct sets of MUBs of maximal size $\ell + 1$ using the symplectic geometry [8].

5. Unextendible Mutually Unbiased Bases and Pauli Classes

In this section, we explain in detail the correspondence between Pauli classes and "generators" of symplectic polar spaces of [8]. It has the same proof as Theorem 2, but we make the relationship between (unextendible) commuting Pauli classes and the generators more explicit.

Theorem 3 (General connecting theorem). *Two elements of* $\mathbb{P}^\times$ *commute if and only if the corresponding points of* $\mathcal{W}_{2N-1}(d)$ *are collinear. In other words, the commuting structure of* $\mathbf{P}$ *(and* $\mathbb{P}$*) is governed by that of the symplectic polar space* $\mathcal{W}_{2N-1}(d)$. *As a corollary, "complete" partial spreads of* $\mathcal{W}_{2N-1}(d)$ *correspond to unextendible sets of operator classes in the Pauli group.*

We indicate the proof in several steps.

Let d be any prime and $N \in \mathbb{N} \setminus \{0,1\}$. Let $\mathcal{S}$ be a *partial spread* of $\mathcal{W}_{2N-1}(d)$, i.e., a set of $(N-1)$-dimensional totally isotropic subspaces that are pairwise disjoint. Throughout this, we will

call $(N-1)$-dimensional totally isotropic subspaces "generators." Let $M+1$ be the number of elements in $\mathcal{S}$, and note that $M+1 \leq d^N+1$ (equality holds when $\mathcal{S}$, by definition, is a *spread*). Then, $\mathcal{S}$ corresponds to a set of mutually unbiased bases in the associated d^N-dimensional Hilbert space, in the following way:

Step 1 To $\mathcal{S}$ corresponds a set of $M+1$ subgroups H_i, $i \in \{0,1,\ldots,M\}$, of $\mathbf{P}$ of size d^{N+1} which mutually (pairwise) intersect (precisely) in $Z(\mathbf{P})$.

Step 2 In each H_j, one chooses d^N-1 elements H_j^k ($k=1,2,\ldots,d^N-1$) which are not contained in $Z(\mathbf{P})$, so that no two such elements are in the same $Z(\mathbf{P})$-coset.

Step 3 Then, $\mathcal{U}(\mathcal{S}) := \left\{ \{H_\alpha^\beta | \beta \in \{1,2,\ldots,d^N-1\}\} \mid \alpha \in \{0,1,\ldots,M\} \right\}$ is a set of commuting unitary classes.

Step 4 If $\mathcal{S}$ is a *complete* partial spread of $\mathcal{W}_{2N-1}(d)$, that is, if $\mathcal{S}$ is not strictly contained in *another* partial spread, then $\mathcal{U}(\mathcal{S})$ is unextendible, and the corresponding set of MUBs is weakly unextendible of size $M+1$.

In particular, this construction applies when $\mathcal{U}(\mathcal{S})$ is a set of Pauli operators (each $Z(\mathbf{P})$-coset contains precisely one Pauli operator).

5.1. The Bijection ρ

Let $\mathcal{G}(\mathcal{W}_{2N-1}(d))$ be the set of generators of $\mathcal{W}_{2N-1}(d)$, and let $\mathcal{C}(\mathbb{C}^{d^N})$ be the set of commuting classes of Pauli operators (of size d^N-1). Note that, from the above, it follows that we have a *bijection*

$$\rho : \mathcal{C}(\mathbb{C}^{d^N}) \longrightarrow \mathcal{G}(\mathcal{W}_{2N-1}(d)), \tag{1}$$

which sends an element $\mathcal{U} \in \mathcal{C}(\mathbb{C}^{d^N})$ to a generator, following the scheme explained above. It is indeed a bijection: to each generator corresponds a unique maximal abelian subgroup $A \leq \mathbf{P} \leq \mathbf{U}_{d^N}(\mathbb{C})$ as above (and conversely), and each $Z(\mathbf{P})$-coset in this subgroup contains precisely one Pauli operator. Together, the set of (nontrivial) Pauli operators in A form one commuting class of Pauli operators of size d^N-1, that is, one element of $\mathcal{C}(\mathbb{C}^{d^N})$.

5.2. Prime Dimension

Now let $N=1$ (i.e., consider the case of prime dimension) and $d \neq 2$. Then, Proposition 1 tells us that $\mathbf{P}$ is a group of size d^3 and exponent d, and its center has size d—in other words, $\mathbf{P}$ is *extra-special*. In $\mathbf{P}$, one can now choose subgroups H_j^i as above, and again [10] applies. If $d=2$, the result is well known (but it can also be derived as above).

6. The Case *d* Prime, $N=2$—Small and Large Examples

If $d=p$ is a prime and $N=2$, the corresponding symplectic polar space is $\mathcal{W}_3(p) =: \mathcal{X}$, with ambient projective space $\mathbf{PG}(3,p)$, and it has two types of linear subspaces that are completely contained in $\mathcal{X}$, namely points of $\mathbf{PG}(3,p)$ and (projective) lines.

6.1. Grids and Point-Line Duals

Before proceeding, we explore some synthetic properties of $\mathcal{W}_3(\ell)$, and ℓ is any prime power now, which will makes things easy below.

Let $\mathcal{P}$ be the point set of $\mathcal{W}_3(\ell)$, $\mathcal{L}$ its line set (that is, its set of generators), and let $\mathbf{I}$ be the (symmetric) "incidence relation" on $(\mathcal{P}\times\mathcal{L}) \cup (\mathcal{L}\times\mathcal{P})$ which says that $x\mathbf{I}L$ ($L\mathbf{I}x$) if and only if the point x is on the line L. Then, this point-line geometry is a *generalized quadrangle* [12], and an extensive theory exists on these structures. Note that each line contains $\ell+1$ points and that on each point there are $\ell+1$ lines. In addition, recall the following defining projection property for generalized quadrangles: if x is a point and X a line not containing x, there is a unique line $Y\mathbf{I}x$ which meets X (and then at a unique point). We will refer to this property as "property (PR)."

Now consider the point-line geometry $\mathcal{Q}$ with line set $\mathcal{P}$, point set $\mathcal{L}$ and the same incidence relation **I**—the so-called *point-line dual* of $\mathcal{W}_3(\ell)$. Then, by Section 3.2.1 in [12], $\mathcal{Q}$ is isomorphic to the point-line geometry of an orthogonal quadric $\mathcal{Q}(4,\ell)$ in $\mathbf{PG}(4,\ell)$. Moreover, if ℓ is even, $\mathcal{Q}$ and $\mathcal{W}$ are isomorphic; see Section 3.2.1 in [12]. For all other prime powers, $\mathcal{Q}$ and $\mathcal{W}$ are not isomorphic—see loc. cit.

Let "$\perp$" denote the orthogonality relation in $\mathcal{W}_3(\ell)$; for any element $\epsilon \in \mathcal{P} \cup \mathcal{L}$, define $\epsilon^\perp := \{\epsilon' \in \mathcal{P} \cup \mathcal{L} | \epsilon' \sim \epsilon\}$, where $\epsilon' \sim \epsilon$ if there is some element E in $\mathcal{P} \cup \mathcal{L}$ such that $\epsilon \mathbf{I} E \mathbf{I} \epsilon'$; in particular, $\epsilon \sim \epsilon$. Now, for $\mathcal{E} \subseteq \mathcal{P}$ or $\mathcal{E} \subseteq \mathcal{L}$, define $\mathcal{E}^\perp := \cap_{\epsilon \in \mathcal{E}} \epsilon^\perp$. Now, let V, W be arbitrary lines of $\mathcal{W}_3(\ell)$ which do not meet. Then, $\{V,W\}^\perp = V^\perp \cap W^\perp$ consists of $\ell+1$ lines of $\mathcal{W}_3(\ell)$, which are mutually disjoint (since, by (PR), there are no triangles). If ℓ is odd, $\{V,W\}^{\perp\perp} := (\{V,W\}^\perp)^\perp$, the set of lines of $\mathcal{W}_3(\ell)$ which meet all lines of $\{V,W\}^\perp$, is $\{V,W\}$. If $\ell = 2$, there is a third line X of $\mathcal{W}_3(\ell)$ besides V, W in this set. In that case, the set of points on the lines of $\mathcal{R}_1 := \{V,W\}^\perp$ is the same as the set of points on the lines of $\mathcal{R}_2 := \{V,W\}^{\perp\perp}$, and these nine points together with the six lines of $\{V,W\}^\perp \cup \{V,W\}^{\perp\perp}$ form a (3×3)-grid $\mathcal{G}$ (see Figure 1); the aforementioned line sets $\mathcal{R}_1, \mathcal{R}_2$ are the reguli of this grid.

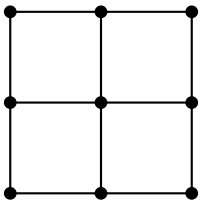

Figure 1. A (3×3)-grid.

In addition, still in the case $\ell = 2$, an easy counting exercise shows that all lines of $\mathcal{W}_3(2)$ have at least one point in common with the point set of $V \cup W \cup X$. All of these properties can essentially be found in Chapter 3 in [12].

6.2. Antiregularity

If ℓ is any odd prime power, we will use the fact that $\mathcal{W}_3(\ell)$ has no (3×3)-grids. This is a corollary of a property called "antiregularity," and can be found in Section 3.3.1(i) in [12] (in the dual version).

6.3. Regularity

If ℓ is any even prime power, we will also use the fact that in $\mathcal{W}_3(\ell)$, if U and V are lines which do not meet, then $|\{U,V\}^{\perp\perp}| = \ell + 1$, that is, U and V are contained in an $(\ell+1) \times (\ell+1)$-grid of which the line set is $\{U,V\}^\perp \cup \{U,V\}^{\perp\perp}$. We call $\{U,V\}$ a *regular* pair of lines. We already met this property for the case $\ell = 2$ in Section 6.1. Also in this case, one easily shows that every line of $\mathcal{W}_3(\ell)$ meets the $(\ell+1) \times (\ell+1)$-grid determined by U and V.

6.4. The Case $p = 2$

We start with giving an alternative and very short proof of Theorem 1 of [9] using the connection between Pauli classes and partial spreads of symplectic polar spaces.

Theorem 4 (Mandayam et al. [9])**.** *Given three Pauli classes $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ belonging to a complete set $\mathcal{S}$ of classes in dimension $= 4$, there exists exactly one more maximal commuting class $\mathcal{C}$ of Pauli operators in $\mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3$. The class $\mathcal{C}$ together with the remaining two classes $\mathcal{C}_4$ and $\mathcal{C}_5$ of $\mathcal{S}$ forms an unextendible set of Pauli classes, whose common eigenbases form a weakly UMUB of order* 3.

Proof. Interpret $\mathcal{S}$ in $\mathcal{W}_3(2)$; then, by Theorem 3 to the $\mathcal{C}_i$ correspond lines L_i of $\mathcal{W}_3(2)$ $(i = 1, \ldots, 5)$, and they form a spread. Consider the lines L_1, L_2, L_3. Then, either there is precisely one line L of $\mathcal{W}_3(2)$

meeting them all, or there are three such lines. In the latter case, the lines L_1, L_2, L_3 form a regulus of a (3×3)-grid, and, as we have seen, any line of $\mathcal{W}_3(2)$ meets the point set of such a grid, leading to the fact that L_1, L_2, L_3 would not be extendible to a spread, contradiction. Thus, we are in the former case, and the class $\mathcal{C}$ corresponding to L is the one of the statement. The set $\mathcal{C}, \mathcal{C}_4, \mathcal{C}_5$ obviously is unextendible, since extending it with a class $\widetilde{\mathcal{C}}$ would mean that the corresponding line $\widetilde{L}$ be contained in the point set of $L_1 \cup L_2 \cup L_3$, implying that there would be another line besides L meeting all of L_1, L_2, L_3, contradiction. □

We now give a short proof of another result of [9], namely Theorem 5 of that paper.

Theorem 5 (Mandayam et al. [9]). *Given an unextendible set of three Pauli classes $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ in dimension $= 4$, the nine operators in $\mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3$ can be partitioned into a different set of three maximal commuting classes $\mathcal{C}_1', \mathcal{C}_2', \mathcal{C}_3'$ such that each $\mathcal{C}_i'$ has precisely one operator in common with each $\mathcal{C}_j$, $i, j \in \{1, 2, 3\}$.*

Proof. Let L_1, L_2, L_3 be the lines corresponding to $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ in $\mathcal{W}_3(2)$; we have seen that either one or three lines are contained in $\{L_1, L_2, L_3\}^\perp$; in the latter case, an easy counting argument shows that all lines of $\mathcal{W}_3(2)$ intersect with $L_1 \cup L_2 \cup L_3$. Thus, suppose we are in the former case, and let $\{L\} := \{L_1, L_2, L_3\}^\perp$. Then, each point on L is incident with precisely one line besides L and not in $\{L_1, L_2, L_3\}$. By the projection property of generalized quadrangles, there are six lines different from L_1, L_2, L_3, which meet the six points of $L_1 \cup L_2 \cup L_3$ not on L in precisely two points. For, each point of $L_1 \cup L_2 \cup L_3$ not on L is on one of the lines of $\mathcal{W}_3(2)$ meeting $L_1 \cup L_2 \cup L_3$ in exactly two points; thus, no such point is on a line of $\mathcal{W}_3(2)$ meeting $L_1 \cup L_2 \cup L_3$ in precisely one point. Thus, the total number of lines meeting $L_1 \cup L_2 \cup L_3$ is 13, and $\{L_1, L_2, L_3\}$ is indeed extendible (since there are 15 lines in total in $\mathcal{W}_3(2)$). □

In the next subsection, we will see a general approach for constructing unextendible Pauli classes in $\mathbb{C}^{d^2}$ with d a prime number, starting from a complete set. As a corollary, we will obtain yet another proof for the result of Mandayam et al.

6.5. General Case

Theorem 6 (Existence of unextendible Pauli class sets for d prime, A). *For each prime $d = p$, there exists an unextendible set of Pauli classes $\mathcal{S}$ of size $d^2 - d + 1$ or $d^2 - d + 2$ in $\mathbb{C}^{d^2}$. The common eigenbases form a weakly UMUB of order $d^2 - d + 1$ or $d^2 - d + 2$.*

Proof. As before, we pass to $\mathcal{W}_3(p)$. Let $\mathcal{T}$ be any spread of $\mathcal{W}_3(p)$.

Now, let U be any line of $\mathcal{W}_3(p)$ which is not contained in $\mathcal{T}$; then, there are precisely $p + 1$ lines in $\mathcal{T}$ which hit U (each in exactly one point), due to the fact that the lines of $\mathcal{T}$ partition the point set of $\mathcal{W}_3(p)$. Call this line set $\mathcal{T}_U$. Now, consider the line set

$$\mathcal{T}(U) := \mathcal{T} \setminus \mathcal{T}_U \cup \{U\}. \tag{2}$$

Note that $|\mathcal{T}(U)| = p^2 - p + 1$. If it is not a complete partial spread, there is at least one other line R of $\mathcal{W}_3(p)$ not meeting any line of $\mathcal{T}(U)$, and, as a point set, it clearly must be contained in the point set "of" $\mathcal{T}_U$. Then, all lines of $\mathcal{T}_U$ meet both U and R. If yet another line R' would exist that extends $\mathcal{T}(U) \cup \{R\}$, R' would also be met by the lines of $\mathcal{T}_U$ — in other words, $R' \in \mathcal{T}_U^\perp$ while $\mathcal{T}_U = U^\perp \cap R^\perp$. As we have seen in Section 6.1, this is not possible, so only at most one line R can be added.

Translating back to Pauli classes gives the desired result. □

It is easy to see that both cases of Theorem 6 can occur (but not necessarily for every p).

As we have not used the fact that p is prime, we can translate immediately to symplectic polar spaces over any finite field.

Corollary 1. *For each prime power ℓ, there exists a complete partial spread $\mathcal{S}$ of $\mathcal{W}_3(\ell)$ of size $\ell^2-\ell+1$ or $\ell^2-\ell+2$. For ℓ even, only the case $\ell^2-\ell+1$ occurs.*

Proof. When ℓ is odd, the proof is the same as in the odd prime case. If ℓ is even, and if U and R are as above, then by Section 6.3, $\{U,R\}$ is a regular pair, so each line of $\mathcal{W}_3(\ell)$ meets the $(\ell+1)\times(\ell+1)$-grid determined by U and R. However, this implies that each of the lines of $\mathcal{T}\setminus\mathcal{T}_U$ meet some line of $\mathcal{T}_U$, contradicting the fact that $\mathcal{T}$ is a spread. Thus, even R cannot be added. □

Remark 2. *For ℓ even, we have seen this result in the literature (see, e.g., [13] and the references therein)—it would be safe to attribute this result to folklore though. We presume the odd case is somewhere as well, but the way of proving is needed below, so it is included anyhow for the sake of completeness.*

One could apply the technique in the proof of Theorem 6 multiple times to obtain examples with less elements. Indeed, this works quite well, as we will demonstrate now. We will work immediately in $\mathcal{W}_3(\ell)$, and will not restrict ourself only to the prime case. Thus, ℓ is a prime power. We *do* ask that ℓ is odd—it will be used in the proof.

Let $\mathcal{S}$ be a *classical spread* of $\mathcal{W}_3(\ell)$—by this, we mean a spread which in the point-line dual $\mathcal{Q}(4,\ell)$ corresponds to an *elliptic quadric* (c.f. Section 5.2 in [11]). Take any two lines L,M in $\mathcal{S}$, and consider the set $\mathcal{X}=\{X_0,X_1,\ldots,X_\ell\}:=\{L,M\}^\perp$; it consists of $\ell+1$ mutually disjoint lines which are not in $\mathcal{S}$. Now, for each $X_i\in\mathcal{X}$, define $\mathcal{S}_i$ to be the set of $\ell+1$ lines of $\mathcal{S}$ meeting X_i. As explained in Appendix B of this paper, for each $\mathcal{S}_i$, there is precisely one more line $\widetilde{X_i}\neq X_i$ of $\mathcal{S}$ which meets each line of $\mathcal{S}_i$. Clearly, this line must be in $\mathcal{X}$, so we can denote $\widetilde{X_i}$ by $X_{\tilde{i}}$.

Now, the following properties are immediate:

(a) $\widetilde{(\cdot)}:\{0,1,\ldots,\ell\}\longrightarrow\{0,1,\ldots,\ell\}$ is an involution, so that $|\{\mathcal{S}_0,\mathcal{S}_1,\ldots,\mathcal{S}_\ell\}|=(\ell+1)/2$;
(b) for $\mathcal{S}_i\neq\mathcal{S}_j$, we have that $\mathcal{S}_i\cap\mathcal{S}_j=\{L,M\}$ (by Section 6.2).

For the sake of convenience, we re-write the set $\{\mathcal{S}_0,\mathcal{S}_1,\ldots,\mathcal{S}_\ell\}$ as $\{\mathcal{S}_0,\mathcal{S}_1,\ldots,\mathcal{S}_{(\ell-1)/2}\}$. For each $j\in\{0,1,\ldots,(\ell-1)/2\}$ we have that $\{X_j,X_{\tilde{j}}\}^\perp=\mathcal{S}_j$.

Theorem 7. *Let ℓ be an odd prime power. Then, for any $k=0,1,\ldots,(\ell-3)/2$, there exist complete partial spreads of size $\ell^2-(k+1)\ell+(3k+2)$ in $\mathcal{W}_3(\ell)$.*

Proof. Let k be as in the statement, and consider any subset R of $\{0,1,\ldots,(\ell-1)/2\}$ of size $k+1$; for simplicity, we consider w.l.o.g. the set $\{0,1,\ldots,k\}$. Then, define the following set:

$$\mathcal{S}_R:=\mathcal{S}\setminus(\cup_{u\in R}\mathcal{S}_u)\cup_{v\in R}(\{X_v,X_{\tilde{v}}\}). \tag{3}$$

It is straightforward to see that $\mathcal{S}_R$ is a partial spread of size $\ell^2-(k+1)\ell+(3k+2)$. As for completeness, suppose we could enlarge $\mathcal{S}_R$ with some line U to another partial spread. As $\mathcal{S}$ is a spread, U, as a point set, must be contained in $\cup_{u\in R}\mathcal{S}_u$, as a point set, and it cannot be contained in $\mathcal{S}$ nor $\mathcal{S}_R$. By the Pigeon Hole Principle, some $\mathcal{S}_w$ must have at least three lines meeting U since U has $\ell+1$ points and $k+1<\frac{\ell+1}{2}$ (in case $U\in\{L,M\}^\perp$, one does not need the Pigeon Hole Principle). However, this implies the existence of a (3×3)-grid, contradiction. □

For each odd prime power ℓ, the bounds appear to be new (up to some small coincidences). For fixed ℓ, we obtain complete partial spreads of respective sizes

$$\ell^2-\ell+2,\ell^2-2\ell+5,\ell^2-3\ell+8,\ldots,\frac{\ell^2}{2}+2\ell-\frac{3}{2}. \tag{4}$$

Translating back to Pauli operators, we obtain the next result.

Theorem 8 (Existence of unextendible Pauli class sets for d prime, B)**.** *For each odd prime $d = p$ and any $k = 0, 1, \ldots, (d-3)/2$, there exists an unextendible set of Pauli classes $\mathcal{S}$ of size $d^2 - (k+1)d + (3k+2)$ in $\mathbb{C}^{d^2}$. The common eigenbases form a weakly UMUB of order $d^2 - (k+1)d + (3k+2)$.*

The construction has many variations, all using roughly the same ideas, and all giving similar (but not the same) bounds. We will come back to these variations in a forthcoming paper.

7. Solution of Conjecture 1

Motivated by Theorem 1, the following conjecture is then stated in [9].

Conjecture 2 (Mandayam et al. [9])**.** *Given $\ell/2+1$ maximal commuting Pauli classes $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_{\ell/2+1}$ belonging to a complete set $\mathcal{S}$ of classes in dimension $\ell = 2^N =: d^N$, $N \in \mathbb{N} \setminus \{0,1\}$, there exists exactly one more maximal commuting class $\mathcal{C}$ of Pauli operators in $\cup_{1 \le i \le \ell/2+1} \mathcal{C}_i$. The class $\mathcal{C}$ together with the remaining classes of $\mathcal{S}$ forms an unextendible set of Pauli classes of size $\ell/2+1$, whose common eigenbases form a weakly UMUB of order $\ell/2+1$.*

In this section, we will show that this conjecture is true *if and only if* $N = 2$ *or* $N = 3$. In fact, we will consider an extension of the conjecture in any characteristic d (i.e., for any prime d), replacing $\ell/2+1 = 2^{N-1}+1$ by $d^{N-1}+1$, and show that it is true if and only if $d = 2$ and $N = 2$ or $N = 3$.

Translated to the geometric setting, we obtain: "given $2^{N-1}+1$ elements $\alpha_1, \alpha_2, \ldots, \alpha_{2^{N-1}+1}$ belonging to a spread $\mathcal{S}$ of the polar space $\mathcal{W}_{2N-1}(2)$, there exists exactly one more generator χ which is completely contained in the union of these elements, such that χ together with the remaining elements of $\mathcal{S}$ constitutes a complete partial spread."

Note that the situation implies that χ meets each α_j, $j = 1, 2, \ldots, 2^{N-1}+1$.

We will replace $d = 2$ by any prime d and consider the same situation (immediately in the geometric setting). We will also slightly generalize the statement by replacing "exactly one" by "at least one."

Thus, let $\mathcal{S}$ be a spread of $\mathcal{W}_{2N-1}(d)$ and d be a prime. We assume that the conjecture above is true (in the more general setting).

First, suppose that $\mathcal{U}$ and $\mathcal{U}'$ are different subsets of $\mathcal{S}$, both of size $d^{N-1}+1$. Let α be a generator which meets all elements of $\mathcal{U}$ and is covered by these elements, and let α' be a generator which meets all elements of $\mathcal{U}'$ and is covered by them. Then, $\alpha \neq \alpha'$.

In the next counting argument, we will use the fact that the number of generators of $\mathcal{W}_{2N-1}(d)$ is $(d^N+1)(d^{N-1}+1)\cdots(d+1)$. Per subset of $\mathcal{S}$ of size $d^{N-1}+1$, by the conjecture, we have at least one generator meeting all of its elements and covered by them. Such a generator is never contained in $\mathcal{S}$. Thus, we have that

$$C_{|\mathcal{S}|}^{d^{N-1}+1} \cdot 1 + |\mathcal{S}| \le (d^N+1)(d^{N-1}+1)\cdots(d+1). \tag{5}$$

Here,

$$C_{|\mathcal{S}|}^{d^{N-1}+1} := \frac{(d^N+1)!}{(d^{N-1}+1)!(d^N - d^{N-1})!}. \tag{6}$$

Now, Equation (5) is equivalent to

$$\frac{(d^N+1)d^N \cdots (d^N - d^{N-1}+1) + (d^{N-1}+1)!(d^N+1)}{(d^{N-1}+1)!(d^N+1)(d^{N-1}+1)\cdots(d+1)} \le 1, \tag{7}$$

or, slightly simplified:

$$\frac{\Big((d^N+1)/(d^{N-1}+1)\Big)(d^N/d^{N-1})\cdots\Big((d^N-d^{N-1}+1)/(1)\Big)+(d^N+1)}{(d^N+1)(d^{N-1}+1)\cdots(d+1)}\leq 1. \tag{8}$$

Now, note that

$$\Big((d^N+1)/(d^{N-1}+1)\Big)(d^N/d^{N-1})\cdots\Big((d^N-d^{N-1}+1)/(1)\Big)\geq\frac{d^N+1}{d^{N-1}+1}\cdot d^{d^{N-1}}, \tag{9}$$

and that

$$(d^N+1)(d^{N-1}+1)\cdots(d+1)\leq d^{N+1}d^N\cdots d^2=d^{N(N+3)/2}. \tag{10}$$

Observe that if for some value $N=M$, we have

$$d^{d^{M-1}}\geq d^{M(M+3)/2}, \tag{11}$$

then the same inequality holds for all $M'\geq M$.

This is already enough to conclude with a contradiction for $d\geq 5$; $d=3$ and $N\geq 3$; and $d=2$ and $N\geq 6$. The cases $(d,N)=(3,2),(2,5),(2,4)$ all yield a contradiction when substituted in Equation (5); the substitution $(d,N)=(2,2)$, which is precisely the case of $\mathcal{W}_3(2)$ which was already studied before, leads to equality in Equation (5), as does the substitution $(d,N)=(2,3)$, which is the case of $\mathcal{W}_5(2)$.

Note that the cases $(d,N)=(2,2),(2,3)$ are precisely those handled in Section 3, Theorem 1 and Section 3, Theorem 3 of [9]. In the next section, we will formulate and discuss variations on Conjecture 1; to that end, we first try to generalize Theorem 6.

8. Existence of Maximal Pauli Classes

Before proceeding, let us first introduce a simple lemma about complete "partial spreads" of general incidence structures. Let $\Gamma=(\mathcal{E},t,T)$ be a triple, with $T=\{0,1,\ldots,n\}$, $n\in\mathbb{N}^\times$, and t a surjective function from the set $\mathcal{E}\neq\emptyset$ to T. For each $i\in\{0,1,\ldots,n\}$, put $\mathcal{E}_i:=t^{-1}(i)$, and call its elements the elements *of type i*. Thus,

$$\mathcal{E}=\cup_{i\in T}\mathcal{E}_i,\ \text{ and }\ |\mathcal{E}|\geq|T|. \tag{12}$$

In particular, we call elements of $\mathcal{E}_0$ "points." We now assume that for $i>0$, every element of $\mathcal{E}_i$ is a subset of $\mathcal{E}_0$. This is a natural assumption: we see each "i-space" (= element of type i) as a point set.

An *i-spread* of Γ is a partition of $\mathcal{E}_0$ in elements of type i. *Complete i-spreads* are introduced naturally as above.

The following observation is trivial.

Proposition 2. *Let $\mathcal{S}$ be an i-spread of Γ. Let χ be an element of type i which is not contained in $\mathcal{S}$, and let $\mathcal{S}_\chi$ be the subset of elements of $\mathcal{S}$, which meet χ in at least one point. Note that $\mathcal{S}_\chi$ induces a partition of the points of χ. Then, if we cannot find a set $\mathcal{T}$ of elements of type i such that*

C.1 *each element of $\mathcal{T}$ is a subset of the point set*

$$\Omega(\mathcal{S},\chi):=\cup_{U\in\mathcal{S}_\chi}U, \tag{13}$$

C.2 *the elements of $\mathcal{T}$ partition $\Omega(\mathcal{S},\chi)$,*

we have that $\mathcal{S}\setminus\mathcal{S}_\chi\cup\{\chi\}$ cannot be completed to an i-spread of Γ.

Proof. If $\mathcal{S}\setminus\mathcal{S}_\chi\cup\{\chi\}$ *could* be completed to an i-spread $\mathcal{S}'$ of Γ, $\mathcal{S}'$ must have elements which all are subsets of $\Omega(\mathcal{S},\chi)$, and which partition $\Omega(\mathcal{S},\chi)$. □

If ℓ is the maximum number of elements of type i contained in $\Omega(\mathcal{S}, \chi)$ (where both $\Omega(\mathcal{S}, \chi)$ and the elements of type i are seen as point sets) and which are pairwise disjoint, the number of elements in a maximal partial i-spread containing $\mathcal{S} \setminus \mathcal{S}_\chi \cup \{\chi\}$ is at most $|\mathcal{S}| - |\mathcal{S}_\chi| + \ell$ (note that $\ell \geq 1$ as χ itself is in $\Omega(\mathcal{S}, \chi)$.)

Remark 3 (Back to the prime case)**.** *Note that the first part of Theorem 6 is an application of the construction method of Proposition 2 (with $\chi = L$).*

8.1. $\mathcal{U}$-Sets

Motivated by Proposition 2, a *$\mathcal{U}$-set* with *carrier* χ is a set $\mathcal{S}_\chi$ of mutually disjoint generators of $\mathcal{W}_{2N-1}(d)$, which all meet some generator $\chi \notin \mathcal{S}_\chi$ such that

$$\chi \subset \cup_{Y \in \mathcal{S}_\chi} Y, \tag{14}$$

and such that $\cup_{Y \in \mathcal{S}_\chi} Y$ cannot be partitioned by a partial spread $\mathcal{P}$ of generators which includes χ.

Note that the number of elements of a $\mathcal{U}$-set is not uniquely determined by N and d (one $\mathcal{U}$-set could also have different carriers).

Proposition 3 (Existence of UMUBs)**.** *The existence of $\mathcal{U}$-sets implies the existence of complete partial spreads which are not spreads, that is, of unextendible sets of Pauli classes.*

Proof. Let $\mathcal{S}_\chi$ be a $\mathcal{U}$-set. If $\mathcal{S}_\chi$ is not contained in a spread, then we are done, so suppose it *is* contained in some spread $\mathcal{S}$. Then, by Proposition 2, we have that $\mathcal{S} \setminus \mathcal{S}_\chi \cup \{\chi\}$ cannot be completed to a spread. □

Note that this proposition can also be applied to general incidence geometries.

For the rest of this section, we suppose d is an odd prime.

Before proceeding, recall that a spread $\mathcal{S}$ (of generators) of $\mathcal{W}_{2N-1}(d)$ is *regular* if the following property is satisfied: if for every three distinct elements α, β, γ in $\mathcal{S}$, $\mathcal{L}$ is the set of lines of $\mathbf{PG}(2N-1, d)$ which meet each of α, β, γ, then there are $d-2$ further elements of $\mathcal{S}$ which meet every line in $\mathcal{L}$. By definition, $\mathcal{L}$ is called the *regulus* defined by α, β, γ. It is well known that every symplectic polar space has regular spreads.

Now, let $\mathcal{R}$ be a regular spread of $\mathcal{W}_{2N-1}(d)$. Take a generator χ which meets some $\alpha \in \mathcal{R}$ in a space of dimension $N-2$ (and note that this is possible), and let $\mathcal{R}_\chi$ be the set of elements in $\mathcal{R}$ which meet χ. Note that $|\mathcal{R}_\chi| = d^{N-1} + 1$. Now consider a generator $\beta \neq \chi, \alpha$ which contains $\chi \cap \alpha$, and which is disjoint from the elements in $\mathcal{R}_\chi \setminus \{\alpha\}$ (for the existence of such a generator, see Appendix A). Then, because $\mathcal{R}$ is a regular spread, we conjecture that $\mathcal{S}_\chi := \mathcal{R}_\chi \setminus \{\alpha\} \cup \{\beta\}$ is a $\mathcal{U}$-set with carrier χ. By Proposition 3, this would suggest that (nice) unextendible sets of Pauli classes of $\mathbb{C}^{d^N}$ always exist (ignoring possible sizes completely), that is, that complete partial spreads which are not spreads always exist in $\mathcal{W}_{2N-1}(d)$. This fact is not necessarily true for general incidence geometries which have i-spreads (using the nomenclature of above): consider, for instance, an incidence geometry for which the elements of type i precisely form *one* i-spread. Thus, although the existence of complete partial spreads is probably seen as folklore, we see the need to formalize this matter.

Remark 4. *Note that if $\mathcal{R}_\chi$ is such that there does not exist a generator besides χ which is contained in $\cup_{\vartheta \in \mathcal{R}_\chi} \vartheta$, then*

$$|\mathcal{R} \setminus \mathcal{R}_\chi \cup \{\chi\}| = d^N - d^{N-1} + 1. \tag{15}$$

Adapting the situation to the special case $d = 2$ (noting that a different definition is then needed for regular spread), we would end up with an unextendible set of Pauli classes of size $2^{N-1} + 1$.

8.2. Reformulation of Conjecture 2

We have seen that Conjecture 2 is only true when $N = 2$ or $N = 3$. On the other hand, there seems to be some evidence that the bound of that conjecture could be attained (see, e.g., the previous remark). Thus, we reformulate the conjecture as follows—we will do it in geometric terms, over all fields $\mathbb{F}_\ell$ with ℓ a prime power, but again, for the applications in quantum information theory, one takes ℓ to be prime.

Conjecture 3. *For each prime power ℓ and positive integer $N \geq 2$, there exists a spread $\mathcal{S}$ of $\mathcal{W}_{2N-1}(\ell)$ and a generator χ not in $\mathcal{S}$, such that $\mathcal{S} \setminus \mathcal{S}_\chi \cup \{\chi\}$ is a complete partial spread of size $\ell^N - \ell^{N-1} + 1$.*

When $\ell = 2$, one obtains the same bound as in Conjecture 2.

We hope to come back to this conjecture, and the construction theory of $\mathcal{U}$-sets, in the near future.

9. "Galois MUBs"

When $d = 2, 3, 5, 7$ or 11, there exist extremely exotic examples of unextendible sets of Pauli classes of size $d^2 - 1$ in $\mathbb{C}^{d^2}$ (details, constructions and references can be found in [14]). We propose calling the corresponding sets of MUBs "Galois MUBs" because they are all related to exotic two-transitive representations of special linear groups, as was first noted by Galois (see also [14]). They are extremely special amongst Pauli classes of $\mathbb{C}^{d^2}$, d being a prime, or even *all* Hilbert spaces, due to the following result.

Theorem 9 (see [12], Section 2.7)**.** *Let Γ be a generalized quadrangle of finite thick order (s, s), and let $\mathcal{C}$ be a complete partial spread of Γ. If Γ is not contained in a spread of Γ, then*

$$|\mathcal{C}| \leq s^2 - 1. \tag{16}$$

As we have seen that the points and lines of any $\mathcal{W}_3(d)$ form a generalized quadrangle, this result applies to $\mathcal{W}_3(d)$ and hence also to Pauli classes in $\mathbb{C}^{d^2}$.

Corollary 2. *A set of commuting Pauli classes of size d^2 in $\mathbb{C}^{d^2}$, d being a prime, is never unextendible.*

Remark 5. *The aforementioned examples in $d = 2, 3, 5, 7, 11$ are the only known examples which effectively reach the $(d^2 - 1)$-bound, and conjecturally they are the only ones. Geometrically, they also satisfy very extreme properties, which rightly translate to Pauli classes. Many more details on the geometric structure of partial spreads of size $s^2 - 1$ in generalized quadrangles of order (s, s) can be found in the author's paper [15].*

The next theorem, taken from the author's paper [15], says that when $d = 2$, up to isomorphism, there is only one complete partial spread of size $3 = 2^2 - 1$ in $\mathcal{W}_3(2)$.

Theorem 10 ([15])**.** *Up to isomorphism, there is only one complete partial spread of size 3 in $\mathcal{W}_3(2)$.*

Corollary 3. *Up to isomorphism, there is only one unextendible set of Pauli classes of size 3 in $\mathbb{C}^4$.*

Remark 6 (On isomorphisms)**.** *Of course, one needs to specify* what *isomorphisms between unextendible sets of Pauli classes* are*. Because of the General Connecting Theorem (and the bijection ρ), we propose saying that unextendible sets of Pauli classes $\mathcal{U}$ and $\mathcal{U}'$ in $\mathbb{C}^{d^N}$ are* isomorphic *if there exists an automorphism of $\mathcal{W}_{2N-1}(d)$ which maps the complete partial spread $\mathcal{S}(\mathcal{U})$ corresponding to $\mathcal{U}$, to the complete partial spread $\mathcal{S}(\mathcal{U}')$ corresponding to $\mathcal{U}'$. This is a natural notion of "isomorphism," since automorphisms of $\mathcal{W}_{2N-1}(d)$ preserve collinearity of points, and thus also the commuting of operators at the level of Pauli operators. One could also define isomorphisms through the general Pauli group. On the other hand, such automorphisms induce*

automorphisms of $\mathcal{W}_{2N-1}(d)$ anyhow, while the converse is not *true. Thus, one misses (many) maps which should be considered as isomorphisms in this way.*

10. Conclusions

The geometry underlying the space of the generalized Pauli operators/matrices characterizing N d-level quantum systems, with $N \geq 2$ and d any prime, is that of the symplectic polar space of rank N and order d, $\mathcal{W}_{2N-1}(d)$.

Using this connection, we have derived a short proof of a recent result of [9] on the unextendibility of MUB sets in $\mathbb{C}^4$ (their Theorem 1). Moreover, we generalized this result for all dimensions = square of a prime, and presented a construction of a class of maximal partial spreads of $\mathcal{W}_3(\ell)$ for any odd prime power ℓ, attaining new bounds in generically every case, which rightly translates to (weakly) UMUBs in the case ℓ is a prime. We also gave a very short proof of Theorem 5 of [9].

We then considered Conjecture 1 of [9], which conjecturally generalizes the aforementioned result of [9] to *any* dimension and showed that it is true *if and only if* $N = 2$ *or* $N = 3$.

We then indicated that an alternative version of the conjecture might be true and described several new construction techniques to obtain weakly unextendible sets of MUBs.

Finally, we discussed a special kind of weakly unextendible set of MUBs, called "Galois MUBs," which attain an optimal bound in relation to being unextendible.

Acknowledgments: The author wishes to thank Marcus Grassl and William K. Wootters for various interesting communications on the subject of this note.

Conflicts of Interest: The author declares no conflict of interest.

Appendix A. Properties of (Symplectic) Polar Spaces

Consider the space $\mathcal{W}_{2N-1}(d)$, d being a prime, and $N \geq 2$. We restrict ourself to the prime case because that is the class which translates to Pauli operators, but everything works when d is a prime power as well.

Appendix A.1. The Map μ

Let γ be a generator, and x a point not in γ. Then, a well-known property (of general polar spaces)—see e.g., p. 137, (c) in [16]—says that there is a unique generator on x which meets γ in an $(N-2)$-space, $\gamma(x)$ (if "$\perp$" is the orthogonality relation coming from the associated alternating form, then $\gamma(x) = x^{\perp} \cap \gamma$). Now, let γ and γ' be disjoint generators. Then, it is not hard to see that for every $(N-2)$-space δ in γ', there is precisely one point $y \in \gamma$ such that $\langle y, \delta \rangle$ is a generator ($y = \gamma \cap \delta^{\perp}$). Thus, the map

$$\mu : \gamma \longrightarrow \gamma' : z \longrightarrow \gamma'(z) \tag{A1}$$

is a bijection between the points of γ and the hyperplanes of γ'.

Appendix A.2. Generators on $(N-2)$-Spaces

Now, let α be a totally isotropic $(N-2)$-space of $\mathcal{W}_{2N-1}(d)$; it is well known that there are $d+1$ generators $g_0, \ldots, g_d$ containing α. Let β be a generator disjoint from α. By the surjectivity above, it follows that some g_i has to intersect β, and then necessarily in one point.

Appendix A.3. Structure of Spreads

Let $\mathcal{S}$ be a spread of $\mathcal{W}_{2N-1}(d)$, d being a prime, and $N \geq 2$. Let $\alpha = g_0 \in \mathcal{S}$, and let τ be an $(N-2)$-space in α. Let $g_1, \ldots, g_d$ be the other generators containing τ. By the previous paragraph, each element of $\mathcal{S} \setminus \{\alpha\}$ meets some g_i ($i \neq 0$) in precisely one point (and, conversely, each point of $g_j \setminus \tau$, $j \neq 0$, is, of course, contained in precisely one spread element.)

Appendix B. Some More Properties of $\mathcal{W}_3(d)$

As in the first appendix, for the applications in quantum information theory considered here, one wants to think of d as being prime, but everything holds when d is a prime power as well. What we *do* ask is that d is odd.

Let $\mathcal{S}$ be a classical spread of $\mathcal{W}_3(d)$; point-line dualize to obtain $\mathcal{Q}(4,d)$—$\mathcal{S}$ becomes an elliptic quadric, denoted $\mathcal{O}$. Now, let x be a point of $\mathcal{Q}(4,d)$ not contained in $\mathcal{O}$. As usual, let "$\perp$" denote the orthogonality relation associated to the defining quadratic form of $\mathcal{Q}(4,d)$ (say, corresponding to the variety with equation $X_0^2 + X_1X_2 + X_3X_4 = 0$). Then, $x^\perp \cap \mathcal{O}$ is a conic section, and since d is odd, there is precisely one other point $y \notin \mathcal{O}$ for which

$$y^\perp \cap \mathcal{O} = x^\perp \cap \mathcal{O}. \tag{B1}$$

Note that the latter expression is equal to $\{x,y\}^\perp$.

Going back to $\mathcal{W}_3(d)$ (i.e., dualizing again), we obtain that if X is a line of $\mathcal{W}_3(d)$ not in $\mathcal{S}$, and $\mathcal{S}_X$ is the set of $d+1$ lines in $\mathcal{S}$ which meet X, then there is precisely one other line Y not in $\mathcal{S}$ such that

$$\mathcal{S}_X = \{X,Y\}^\perp = X^\perp \cap Y^\perp = \mathcal{S}_Y. \tag{B2}$$

References

1. Wootters, W.K. Picturing qubits in phase space. *IBM J. Res. Dev.* **2004**, *48*, 99–110.
2. Wootters, W.K. Quantum measurements and finite geometry. *Found. Phys.* **2006**, *36*, 112–126.
3. Havlicek, H.; Saniga, M. Projective ring line of a specific qudit. *J. Phys. A* **2007**, *40*, F943–F952.
4. Havlicek, H.; Saniga, M. Projective ring line of an arbitrary single qudit. *J. Phys. A* **2008**, *41*, 015302.
5. Saniga, M.; Planat, M. Hjelmslev geometry of mutually unbiased bases. *J. Phys. A. Math. Gen.* **2006**, *39*, 435–440.
6. Saniga, M.; Planat, M.; Pracna, P. Projective ring line encompassing two-qubits. *Theor. Math. Phys.* **2008**, *155*, 905–913.
7. Saniga, M.; Planat, M. Multiple qubits as symplectic polar spaces of order two. *Adv. Stud. Theor. Phys.* **2007**, *1*, 1–4, arXiv:quant-ph/0612179.
8. Thas, K. The geometry of generalized Pauli operators of N-qudit Hilbert space, and an application to MUBs. *Europhys. Lett.* **2009**, *86*, doi:10.1209/0295-5075/86/60005.
9. Mandayam, P.; Bandyopadhyay, S.; Grassl, M.; Wootters, W.K. Unextendible mutually unbiased bases from Pauli classes. *Quantum Inf. Comput.* **2014**, *14*, 823–844.
10. Bandyopadhyay, S.; Boykin, P.O.; Roychowdhury, V.; Vatan, F. A new proof of the existence of mutually unbiased bases. *Algorithmica* **2002**, *34*, 512–528.
11. Hirschfeld, J.W.P. *Projective Geometries over Finite Fields*, 2nd ed.; Oxford University Press: Oxford, UK, 1998.
12. Payne, S.E.; Thas, J.A. *Finite Generalized Quadrangles*; Research Notes in Mathematics 110; Pitman Advanced Publishing Program: Boston, MA, USA, 1984.
13. Cimrakova, M.; De Winter, S.; Fack, V.; Storme, L. On the smallest maximal partial ovoids and spreads of the generalized quadrangles $W(q)$ and $Q(4,q)$. *Eur. J. Comb.* **2007**, *28*, 1934–1942.
14. De Winter, S.; Thas, K. Bounds on partial ovoids and spreads in classical generalized quadrangles. *Innov. Incid. Geom.* **2010**, *11*, 19–33.
15. Thas, K. Nonexistence of complete $(st - t/s)$-arcs in generalized quadrangles of order (s,t). *J. Comb. Theory Ser. A* **2002**, *97*, 394–402.
16. Ueberberg, J. *Foundations of Incidence Geometry. Projective and Polar Spaces*; Springer Monographs in Math; Springer: Berlin/Heidelberg, Germany, 2011.