William M. Kantor*

On maximal symplectic partial spreads

DOI 10.1515/advgeom-2017-0033. Received 13 January, 2016

Abstract: New types of maximal symplectic partial spreads are constructed.

Keywords: Partial spread, orthogonal space, symplectic space.

2010 Mathematics Subject Classification: 51A50, 51E20

Communicated by: G. Korchmáros

1 Introduction

This paper concerns partial spreads that are maximal among the symplectic ones. Since very few papers concern maximal symplectic partial spreads in dimension > 4 [13], we will emphasize those dimensions. The largest and most obvious type of maximal partial spread of a $2n$-dimensional symplectic $\mathbb{F}_q$-space is a spread, of size $q^n + 1$, which we will not consider here. (However, there are relatively few known types of symplectic spreads; see [17] for a survey as of 2012.)

On the other hand, when n is even Grassl [13] initially conjectured that the smallest possible size of a maximal symplectic partial spread is $q^{n/2} + 1$, and he provided examples of this size for all even q and n. However, when $2n = 8$ this conjecture is not correct: Grassl later produced computer-generated counterexamples of size 61, 62, 63 and 64 when $2n = q = 8$. Families of counterexamples using Suzuki–Tits ovoids are in Section 7.4. It still seems plausible that Grassl's conjecture may be correct if $2n > 8$ or if q is odd. Thus far all counterexamples to this conjecture have size greater than $q^{n/2}/2$.

Most of our examples are based on standard properties of orthogonal or symplectic spaces, involving either orthogonal spreads or the standard method for obtaining them (Sections 4, 5 and 6), or partial $\mathrm{O}^+(8, q)$-ovoids and triality (Section 7). Almost half of this paper is concerned with spaces of dimension 4 or 8, where we can use points as crutches: the Klein correspondence in dimension 4 [26, p. 196] and triality in dimension 8 [29] turn sets of points into sets of subspaces (of dimension 2 or 4). In dimension > 4 our results are summarized in Table 1; the pairs of dimensions of the form $4n$, $4n - 2$ arise from orthogonal partial spreads and are explained in Section 6.

Maximal symplectic partial spreads have a straightforward use in Quantum Physics for finding sets of mutually unbiased bases (MUBs) in complex vector spaces [20; 13]. Appendix A provides a brief description of this connection to Quantum Physics, the sense in which these are maximal sets of MUBs, and the fact that sets of *real* MUBs arise if the underlying field has order 2 and the symplectic partial spread is also an orthogonal partial spread.

Tables of computer-generated sizes of maximal symplectic partial spreads in $\mathbb{F}_q^{2n}$ are given in [5; 13] for very small n and q. A few of these are special cases of constructions given here. However, since those tables contain integer intervals that consist of sizes of these partial spreads, it is clear that new types of construction techniques are needed in all dimensions.

Acknowledgement: I am grateful to Markus Grassl for stimulating my interest in maximal symplectic partial spreads by pointing out the scarcity of examples in dimension > 4.

Funding: This research was supported in part by a grant from the Simons Foundation.

***Corresponding author: William M. Kantor,** University of Oregon, Eugene, OR 97403, USA; Northeastern University, Boston, MA 02115, USA, email: kantor@uoregon.edu

2 Background

The letter q will always denote a prime power, while n, m, k, s and i will be integers.

Dimensions	Parity of q	Size	Restrictions	Theorems
$4m$	arbitrary	$q^{2m} - q^m + (2, q-1)$		3.1
$4mk$, $4mk-2$	even	$q^{2mk-k} + 1$	$m > (k+1)/2$	4.6, 6.3
$4k$, $4k-2$	even	$q^k + 1$ [a]		5.2, 6.2
$4k$	even	$2q^k + 1$		5.2
8 and 6	even	$q^3 - q^2 + 1$	$q \geq 4$	7.2, 7.14
8 and 6	even	n_s [b]	$1 \leq s \leq q/5$	7.3, 7.14
8 and 6	even	$n_4 - 1$	$q > 16$	7.3, 7.14
8 and 6	even	$q^2 + 1$		7.7, 7.14
8 and 6	even	$2q^2 + 1$		7.10, 7.14
8 and 6	even	$q^2 + q + 1$	$q = 2^{2e+1} > 2$	7.11, 7.14
8 and 6	even	$q^2 - q + 1$	$q = 2^{2e+1} > 2$	7.12, 7.14
8 and 6	even	$q^2 - sq + 2s - 1$	$q = 2^{2e+1} > 2$ $1 < s \leq 2^e - 1$	7.13, 7.14
6	arbitrary	$q^3 - q^2 + 1$		8.1

Table 1: Maximal symplectic partial spreads: dimension ≥ 6 over $\mathbb{F}_q$

[a] This corresponds to the excluded possibility $m = 1$ in dimensions $4mk$, $4mk-2$

[b] $n_s = q^3 - sq^2 + (s-1)(q+2) + \binom{s}{2}(q-2) + 1$

See [26] for the standard properties of the symplectic and orthogonal vector spaces used here. We name geometries using their isometry groups. We will be concerned with singular vectors and totally singular (t.s.) subspaces of orthogonal spaces, and totally isotropic (t.i.) subspaces of symplectic spaces. A subspace of an orthogonal space is *anisotropic* if it contains no nonzero singular vector — and hence has dimension ≤ 2. In characteristic 2, an orthogonal vector space is also a symplectic space, t.s. subspaces are also t.i. subspaces, and the set of singular vectors in a t.i. subspace is a t.s. subspace of codimension 1.

Types of maximal t.s. subspaces

The n-dimensional t.s. subspaces of an $O^+(2n, q)$-space are of two types, with two such subspaces of the same type if and only if their intersection has dimension $\equiv n \pmod 2$. Each t.s. $n-1$-space is contained in one member of each type. We will be concerned with subspaces intersecting in 0, so that n will be even.

A triality map for an $O^+(8, q)$-space [29] permutes the t.s. subspaces, sending singular points to a type of t.s. 4-spaces and non-perpendicular pairs of points to pairs of 4-spaces having zero intersection.

Partial ovoids and partial spreads

A *partial ovoid* of an orthogonal space is a set Ω of t.s. points such that each maximal t.s. subspace contains at most one point in the set; Ω is an *ovoid* if it meets every such subspace. A *partial spread* in a $2n$-dimensional vector space V is a set Σ of n-spaces any two of which have only 0 in common; Σ is a *spread* if every vector is

in a member of Σ. If V is a $2n$-dimensional symplectic or orthogonal vector space, a *symplectic or orthogonal partial spread* Σ is a partial spread consisting of t.i. or t.s. n-spaces; Σ is a *symplectic or orthogonal spread* if every vector or every singular vector is in a member of Σ. This paper concerns *maximal* symplectic or orthogonal partial spreads: maximal with respect to inclusion. In some situations we will even obtain symplectic maximal partial spreads: maximal partial spreads that happen to be symplectic.

Two symplectic partial spreads are *equivalent* if there is a semilinear automorphism of the symplectic geometry sending one partial spread to the other. If Σ is a set of subspaces of an $\mathrm{Sp}(2n, q)$-space, then $\mathrm{Sp}(2n, q)_\Sigma$ is its set-stabilizer in the symplectic group $\mathrm{Sp}(2n, q)$. There are similar definitions for orthogonal spaces and for the automorphism group of a symplectic or orthogonal partial spread.

3 Maximal partial $\mathrm{Sp}(4m, q)$-spreads

Our most general result is the following

Theorem 3.1. *For any q and $m \geq 1$, an $\mathrm{Sp}(4m, q)$-space has a maximal symplectic partial spread of size $q^{2m} - q^m + (2, q-1)$.*

We begin with notation. Let $F = \mathbb{F}_{q^{2m}} \supset E = \mathbb{F}_{q^m} \supset K = \mathbb{F}_q$, with trace map $T\colon F \to K$, so that $T(xy)$ is a nondegenerate symmetric K-bilinear form on F. By dimension arguments, the E-subspace $\{x \in F \mid T(xE) = 0\}$ is θE for some $\theta \in F$.

Equip the K-space $V = F^2$ with the nondegenerate alternating K-bilinear form $f((x, y), (x', y')) := T(xy') - T(x'y)$. Then V is an $\mathrm{Sp}(4m, q)$-space.

Let Σ be the desarguesian symplectic spread of V consisting of the t.i. 2-spaces $[x = 0]$ and $[y = ax]$ for $a \in F$. Let $Z_\star < V$ be the t.i. $2m$-space $(E, \theta E) = E \oplus \theta E$ (which is t.i. since $T(E\theta E) = 0$).

Let $\Sigma_\star \subset \Sigma$ consist of the members of Σ met nontrivially by $Z_\star$ (namely, the $2m$-spaces $[x = 0]$ and $[y = a\theta x]$ for $a \in E$). We need information concerning some transversals of $\Sigma_\star$:

Lemma 3.2. *There are exactly $(2, q-1)$ t.i. $2m$-spaces of V that meet each member of $\Sigma_\star$ in an m-space. If there are two such subspaces then they intersect in 0.*

Proof. If Z is such a subspace let $Z \cap [y = 0] = (U, 0)$ and $Z \cap [x = 0] = (0, W)$ for m-dimensional K-subspaces U and W of F. Since $Z = (U, 0) + (0, W)$ is t.i. we have $T(UW) = 0$.

Since $Z \cap [y = a\theta x]$ (for $a \in E$) consists of the vectors $(u, a\theta u)$ with $u \in U$, we see that $W = \theta U$ (using $a = 1$) and W is closed under multiplication by elements of E. Then W is an E-subspace of F. Let $U = \alpha E$, $\alpha \in F^*$, so that $W = \theta\alpha E$. Then $0 = T(UW) = T(\alpha\theta\alpha E)$, so that $\alpha^2\theta \in \theta E$. Thus, there are $(2, q-1)$ choices for the coset $\alpha F^* \in F^*/E^*$, and hence also $(2, q-1)$ choices for $Z = (U, W) = (\alpha E, \theta\alpha E)$.

This argument reverses: if the coset αE^* has order at most 2, then $Z := (\alpha E, \theta\alpha E)$ is a t.i. $2m$-space that meets each member of $\Sigma_\star$ in an m-space. Moreover, each member of $\Sigma - \Sigma_\star$ has 0 intersection with Z.

Finally, if there are two such subspaces $Z_\star = (E, \theta E)$ and $(\alpha E, \theta\alpha E)$, then $\alpha \notin E$ and these have intersection 0. □

Proof of Theorem 3.1. Let Σ and $\Sigma_\star$ be as above. By the lemma, there are t.i. $2m$-spaces Z (if q is even) or Z, Z' (if q is odd) such that $\Sigma_\star$ is the set of elements of Σ met nontrivially by either of these $2m$-spaces. Then

$$\Sigma^\bullet := \begin{cases} (\Sigma - \Sigma_\star) \cup \{Z\} & \text{if } q \text{ is even} \\ (\Sigma - \Sigma_\star) \cup \{Z, Z'\} & \text{if } q \text{ is odd} \end{cases}$$

is a symplectic partial spread of size $q^{2m} - q^m + (2, q-1)$.

Maximality: Suppose that X is a t.i. $2m$-space meeting each member of $\Sigma^\bullet$ in zero. Since Σ is a spread, the set Σ_X of members of Σ meeting X nontrivially must be contained in $\Sigma_\star$. If $(\star)$ $\Sigma_X = \Sigma_\star$ *and* $\dim X \cap Y = 0$ *or* m *for each* $Y \in \Sigma$, then $X = Z$ or Z' by Lemma 3.2, which contradicts the fact that $X \notin \Sigma^\bullet$.

We count in order to prove $(\star)$. Let a_i be the number of $Y \in \Sigma$ such that $\dim X \cap Y = i$, where $1 \le i \le 2m-1$. Since the intersections $X \cap Y$ produce a partition of $X - \{0\}$,

$$\sum_1^{2m-1} a_i(q^i - 1) = q^{2m} - 1 \quad \text{and} \quad \sum_1^{2m-1} a_i = |\Sigma_X| \le |\Sigma_\star| = q^m + 1.$$

There cannot be two subspaces of X of dimension $> m$ and $\ge m$ having zero intersection. Thus, if $a_k \ne 0$ for some $k > m$ then $a_k = 1$ and $a_i = 0$ whenever $m \le i \le 2m-1$, $i \ne k$. This produces the contradiction $q^{2m} - 1 = (q^k - 1) + \sum_1^{m-1} a_i(q^i - 1) \le (q^k - 1) + \sum_1^{m-1} a_i(q^{m-1} - 1) \le (q^k - 1) + (q^m + 1 - 1)(q^{m-1} - 1)$.

Thus, $a_k = 0$ for $k > m$, and $q^{2m} - 1 = \sum_1^m a_i(q^i - 1) \le \sum_1^m a_i(q^m - 1) \le (q^m + 1)(q^m - 1)$. Then $a_i = 0$ for $i < m$ and $a_m = q^m + 1$, as required. □

Remarks 3.3. When $2m = 4$ the theorem is a special case of [5; 28] and Theorem 9.1, which suggests the question: *Can more than one subset like $\Sigma_\star$ be removed in* Theorem 3.1?

The last part of the proof showed that *a partition of the nonzero vectors of $\mathbb{F}_q^{2m}$ induced by a set of proper subspaces has size at least $q^m + 1$, with equality if and only if the subspaces all have dimension m.*

4 Orthogonal spreads

Let V be an $O^+(4m, q)$-space (for even q and $4m \ge 8$) with quadratic form Q. Then V has an orthogonal spread Σ (first proved in [11], then rediscovered in [12]; cf. [16; 18]), and $|\Sigma| = q^{2m-1} + 1$. This leads to our simplest examples:

Proposition 4.1. *Σ is a maximal partial spread of size $q^{2m-1} + 1$, and is symplectic.*

Proof. For even q, t.s. subspaces are also t.i., so Σ is symplectic. *Maximality*: since $2m > 2$, the quadratic form induced by Q on any $2m$-space has a nontrivial zero. Thus, every $2m$-space has nonzero intersection with some member of Σ. □

Remark 4.2. If $d = 2^{2m}$ and $q = 2$ then $|\Sigma| = \frac{1}{2}d + 1$ (this should be compared to [20]).

Remark 4.3. *If $m > 3$ then there is a maximal symplectic partial spread in V of size $q^{2m-1} + 1$ that is not equivalent to an orthogonal spread.* For, let $X \in \Sigma$, let H be a hyperplane of X and let $z \in H^\perp$ be nonsingular. Then it is not difficult to check that $(\Sigma - \{X\}) \cup \{\langle H, z\rangle\}$ behaves as stated.

Lemma 4.4. *Let $E = \mathbb{F}_q \subseteq F = \mathbb{F}_{q^k}$ with q even. If X is an E-subspace of an orthogonal F-space and $|X| > q^{k^2+k}$, then X contains a nonzero F-singular vector.*

Proof. We are given an F-space V equipped with a quadratic form Q and associated bilinear form $f(,)$; both forms have values in F not in E. The symbol $\perp$ will refer to the F-space V, while $\langle\ \rangle_L$ refers to spanning an L-subspace for $L = E$ or F.

For $i = 1, \dots, k+1$, we will construct E-linearly independent vectors $x_1, \dots, x_i \in X$ and an E-subspace X_i such that $\langle x_1, \dots, x_i\rangle_E \le X_i \le \langle x_1, \dots, x_i\rangle_F^\perp \cap X$ and $|X_i| \ge |X|/|F|^i$. (In particular, $x_1, \dots, x_{k+1} \in \langle x_1, \dots, x_{k+1}\rangle_F^\perp \cap X$.)

Let $0 \ne x_1 \in X$ and $X_1 := \langle x_1\rangle_F^\perp \cap X$. Then $x_1 \in X_1$ (since q is even and hence V is symplectic) and $|X_1| = |\langle x_1\rangle_F^\perp||X|/|\langle x_1\rangle_F^\perp + X| \ge |\langle x_1\rangle_F^\perp||X|/|V| = |X|/|F|$.

For induction, let $1 \le i \le k$ and assume that we have $x_1, \dots, x_i$ and X_i. Then $|X_i| \ge |X|/|F|^i > q^{k^2+k}/(q^k)^k \ge |\langle x_1, \dots, x_i\rangle_E|$. Let $x_{i+1} \in X_i - \langle x_1, \dots, x_i\rangle_E$ and $X_{i+1} := \langle x_{i+1}\rangle_F^\perp \cap X_i$. Then $x_{i+1} \in X_{i+1} \le \langle x_{i+1}\rangle_F^\perp \cap \langle x_1, \dots, x_i\rangle_F^\perp \cap X$ and $|X_{i+1}| = |\langle x_{i+1}\rangle_F^\perp||X_i|/|\langle x_{i+1}\rangle_F^\perp + X| \ge (|X|/|F|^i)/|F|$, as needed for induction.

Since $\langle x_1, \dots, x_{k+1}\rangle_E$ is in $\langle x_1, \dots, x_{k+1}\rangle_E^\perp \cap X$ and has size $q^{k+1} > |F|$, the additive map $\langle x_1, \dots, x_{k+1}\rangle_E \to F$ obtained by restricting Q has nonzero kernel. □

Remarks 4.5. The preceding argument did not require anything about the nature of the quadratic form, which could even have a large radical.

Although the argument used the fact that all vectors are isotropic, it can still be used for unitary spaces and orthogonal spaces of odd characteristic. One minor difference is that we need to know that X_i has an isotropic vector $x_{i+1} \in X_i - \langle x_1, \dots, x_i \rangle_E$. This is clear if X_i is the span of its isotropic vectors; and that holds unless $X_i/\operatorname{rad} X_i$ is anisotropic, hence of dimension 1 or (in the orthogonal case) 2. Thus, there is a choice x_{i+1} for each i if we replace the condition $|X| > q^{k^2+k}$ by $|X| > (q^2)^{k^2+k+1}$ for unitary spaces and by $|X| > q^{k^2+k+2}$ for orthogonal spaces.

These observations do not, however, lead to useful unitary or odd characteristic orthogonal analogues of the next theorem: unfortunately, there is no unitary spread in dimension ≥ 6 [27] and no known odd characteristic orthogonal spread in dimension > 8.

Theorem 4.6. *If q is even and $m > (k+1)/2$, then $\mathbb{F}_q^{4mk}$ has a maximal partial spread of size $q^{2mk-k}+1$ that is orthogonal and hence also symplectic.*

Proof. Let V be an $\mathrm{O}^+(4m, q^k)$-space with quadratic form Q, and let Σ be an orthogonal spread in V. Let $T\colon \mathbb{F}_{q^k} \to \mathbb{F}_q$ be the trace map. Then $Q'(v) := T(Q(v))$ is a quadratic form that turns V into an $\mathrm{O}^+(4mk, q)$-space. Moreover, Σ is still an orthogonal partial spread in this space, of size $(q^k)^{2m-1}+1$.

Maximality: If X is an $\mathbb{F}_q$-subspace of V of dimension $2mk$, then $|X| = q^{2mk} > q^{k^2+k}$. By Lemma 4.4, X contains a nonzero $\mathbb{F}_{q^k}$-singular vector that must lie in some member of the $\mathrm{O}^+(4m, q^k)$-spread Σ. Thus, X has nonzero intersection with some member of Σ. □

Question 4.7. *Is every $\mathrm{O}^+(4m, q^k)$-spread also a maximal orthogonal partial spread in an $\mathrm{O}^+(4mk, q)$-space?*

This seems plausible since it is correct when either $m > (k+1)/2$ (by Theorem 4.6) or $m = 2$ [13] (cf. Theorem 5.2(i)).

Remarks 4.8. If $q = 2$ and $d = 2^{2mk}$ with $m > (k+1)/2$, then the maximal symplectic partial spreads in Theorem 4.6 have size $\frac{1}{2^k}d + 1$, resembling Remark 4.2. Grassl's computer data [13] suggests much more: *for even q there appears to be a maximal symplectic partial spread of size $2^i + 1$ in $\mathrm{Sp}(2n, q)$-space whenever $q^{n/2} + 1 \leq 2^i + 1 \leq q^n + 1$.*

We will need the following elementary observation several times:

Lemma 4.9. *If Σ is a maximal orthogonal partial spread of an $\mathrm{O}^+(4m, q)$-space with q even and $m \geq 2$, then it is also a maximal symplectic partial spread.*

Proof. Suppose that $Y \notin \Sigma$ is a t.i. $2m$-space such that $\Sigma \cup \{Y\}$ is a symplectic partial spread. The quadratic form on V restricts to a semilinear map on the t.i. subspace Y; the kernel is a t.s. subspace Y_0 of dimension $\geq 2m-1$. If $\dim Y_0 = 2m$ then $Y = Y_0$ must have the same type as the members of Σ (cf. Section 2).

In any case let W be the t.s. $2m$-space containing Y_0 having the same type as the members of Σ. By maximality, $\Sigma \cup \{W\}$ is not an orthogonal partial spread, so that $W \cap X \neq 0$ for some $X \in \Sigma$. Since $\dim W \cap X \equiv 2m \pmod 2$ we have $\dim W \cap X \geq 2$. Since Y_0, $W \cap X \leq W$ and $\dim Y_0 \geq 2m-1$, it follows that $Y_0 \cap (W \cap X) \neq 0$ and hence that $Y \cap X \neq 0$. This contradicts the fact that $\Sigma \cup \{Y\}$ is a partial spread. □

5 The embedding $\mathrm{O}^+(4, q^k) < \mathrm{Sp}(4k, q)$

Example 5.1. *If q is even then an $\mathrm{Sp}(4, q)$-space has a maximal symplectic partial spread of size $q+1$ that is also a maximal orthogonal partial spread.*

Proof. An $\mathrm{O}^+(4, q)$-space has $(q+1)^2$ singular points partitioned by exactly two orthogonal spreads Σ, $\Sigma^\dagger$, arising from the two types of t.s. 2-spaces (cf. Section 2); each member of Σ and each member of $\Sigma^\dagger$ meet nontrivially. Possibly the most elementary (and most opaque) way to see that these are maximal symplectic spreads is to count the number of t.i. lines containing at least one singular point. There are $2|\Sigma| + (q+1)^2(q-1) = (q^2+1)(q+1)$ such lines, which is exactly the total number of t.i. lines. □

Theorem 5.2. *Let q be even and $k \geq 1$.*

(i) *An $\mathrm{Sp}(4k, q)$-space has a maximal symplectic partial spread of size $q^k + 1$ that is also a maximal orthogonal partial spread.*

(ii) *An $\mathrm{Sp}(4k, q)$-space has a maximal symplectic partial spread of size $2q^k + 1$.*

Proof. (i) The preceding example produces a maximal symplectic partial spread Σ of an $\mathrm{Sp}(4, q^k)$-space V that is also a maximal orthogonal partial spread, and $|\Sigma| = q^k + 1$. Viewed over $\mathbb{F}_q$ (using a trace map T as in the proof of Theorem 4.6) the set Σ again is an orthogonal partial spread. It is a maximal symplectic partial spread by [13], and hence also a maximal orthogonal partial spread.

We include slightly more detail: in [13] the $\mathbb{F}_q$-space $(\mathbb{F}_{q^k}^2)^2$ is equipped with the alternating bilinear form $((u, v), (u', v')) := T(u \cdot v' - u' \cdot v)$. The partial spread Σ consists of the t.i. subspaces $\{(0, 0, y_1, y_2) \mid y_1, y_2 \in \mathbb{F}_{q^k}\}$ and $\{(x_1, x_2, x_2\alpha, x_1\alpha) \mid x_1, x_2 \in \mathbb{F}_{q^k}\}$ for each $\alpha \in \mathbb{F}_{q^k}$. These are t.s. $2k$-spaces for the quadratic form $Q(u, v) := T(u \cdot v)$. In the preceding example, $\Sigma^\dagger$ is Σ^j, where $j\colon (x_1, x_2, y_1, y_2) \mapsto (x_1, y_1, x_2, y_2)$.

(ii) Choose any $Z \in \Sigma$. Obtain a new symplectic partial spread $\Sigma^\bullet$ by removing Z and then, for each 1-dimensional $\mathbb{F}_{q^k}$-subspace W of Z, adjoining one 2-dimensional t.i. $\mathbb{F}_{q^k}$-subspace that contains W and is different from both Z and the member of $\Sigma^\dagger$ containing W. This produces a maximal symplectic partial spread of the $\mathbb{F}_{q^k}$-space V [5, Remark 2.12(2)].

In fact *$\Sigma^\bullet$ is also a maximal symplectic partial spread of the $\mathbb{F}_q$-space V*. For, let X be a t.i. $2k$-dimensional $\mathbb{F}_q$-subspace of V having zero intersection with all members of $\Sigma^\bullet$. By (i), X has nonzero intersection with some member of Σ, which therefore must be Z. Then X has nonzero intersection with some $\mathbb{F}_{q^k}$-point W of Z and hence with the adjoined $\mathbb{F}_{q^k}$-space in $\Sigma^\bullet$ containing W, which is a contradiction. □

The proof of (i) in [13] uses a neat computational idea. It would be interesting to have a more geometric proof.

Example 5.3. Theorem 5.2(i) points to a general construction (compare Remarks 7.8). Let $V = \mathbb{F}_q^{4m}$ be an orthogonal, symplectic or unitary space. Let X and Y be t.i./t.s. $2m$-spaces with zero intersection, and let Σ_X be a partial spread (of m-spaces) of X. Each $A \in \Sigma_X$ determines another m-space $A' := A^\perp \cap Y$, and $A + A'$ is a t.i./t.s. $2m$-space. Then $\Sigma := \{A + A' \mid A \in \Sigma_X\}$ *is a partial spread of the same type as the underlying space V*. (If $A \neq B \in \Sigma_X$ then $V = X \oplus Y = (A \oplus B) \oplus (A' \oplus B')$, so that $A \oplus A'$ and $B \oplus B'$ have zero intersection.)

When Σ_X is a maximal partial spread (or even a spread), some of these partial spreads may be maximal orthogonal, symplectic or unitary partial spreads of size $q^m + 1$ (as in Theorem 5.2(i) and Theorem 7.7), but we do not see how to prove that. (See Question 7.6 for instances of such symplectic partial spreads that are *not* maximal. As noted earlier, there is no unitary spread in dimension ≥ 6 by [27].)

6 Projections

Let q be even. A key ingredient of [16; 17; 18] is the fact that there is a natural transition between $\mathrm{O}^+(4m, q)$-spreads and $\mathrm{Sp}(4m - 2, q)$-spreads. This uses any nonsingular point z of an $\mathrm{O}^+(4m, q)$-space and projects into the symplectic space $z^\perp/z$. This procedure also applies to orthogonal and symplectic partial spreads:

Lemma 6.1. *Let z be a nonsingular point of an $\mathrm{O}^+(4m, q)$-space V.*

(i) *If Σ is a maximal orthogonal partial spread of V, then $\Sigma/z := \{\langle z^\perp \cap X, z\rangle/z \mid X \in \Sigma\}$ is a maximal symplectic partial spread of the $\mathrm{Sp}(4m - 2, q)$-space $z^\perp/z$.*

(ii) *If Σ' is a maximal symplectic partial spread of $z^\perp/z$, then there is a maximal orthogonal partial spread Σ of V such that $\Sigma' = \Sigma/z$. Moreover, Σ is a maximal symplectic partial spread.*

(iii) *If Σ_1 is a maximal orthogonal partial spread of V and z_1 is a nonsingular point of V, then Σ/z and Σ_1/z_1 are equivalent symplectic partial spreads if and only if Σ_1 is the image of Σ under an automorphism of the orthogonal geometry of V that sends z to z_1.*

Proof. (i) *Σ/z is a symplectic partial spread*: If X and Y are distinct members of Σ and $\langle z^\perp \cap X, z\rangle \cap \langle z^\perp \cap Y, z\rangle \neq z$, then $z \in \langle x, y\rangle$ for some points $x \in z^\perp \cap X$, $y \in z^\perp \cap Y$. Then x and y are perpendicular to z and hence to one another, so that $\langle x, y\rangle$ is t.s. whereas z is nonsingular.

Maximality: Suppose that $(\Sigma/z) \cup \{U/z\}$ is a larger symplectic partial spread for some t.i. $2m$-space U of V containing z. Let U_0 be the hyperplane of U consisting of singular vectors. The members of Σ all have the same type (cf. Section 2). Let $\hat{U}$ be the t.s. $2m$-space of that type containing U_0. Then $\hat{U}$ meets each $X \in \Sigma$ in at most a 1-space and hence only in 0 (by Section 2, $1 \geq \dim(\hat{U} \cap X) \equiv 2m \pmod 2$ and hence $\hat{U} \cap X = 0$). Thus, $\Sigma \cup \{\hat{U}\}$ is an orthogonal partial spread properly containing Σ, whereas Σ is assumed to be maximal.

(ii) Choose a type of t.s. $2m$-space of V. If $U/z \in \Sigma'$ let U_0 be the hyperplane of singular vectors of the t.i. $2m$-space U, and let $\hat{U}$ be the t.s. $2m$-space containing U_0 of the chosen type. Then the set Σ consisting of these subspaces $\hat{U}$ is an orthogonal partial spread: since distinct members of Σ meet in at most a 1-space and have the same type they have intersection 0. Clearly $\Sigma' = \Sigma/z$.

Maximality: If Σ^+ is an orthogonal partial spread properly containing Σ, then Σ^+/z properly contains $\Sigma/z = \Sigma'$, whereas Σ' is maximal.

The final statement follows from Lemma 4.9.

(iii) As a consequence of Witt's Lemma [26, p. 57], an equivalence from Σ/z to Σ_1/z_1 lifts first to $z^\perp \to z_1^\perp$ and then to an automorphism of the orthogonal geometry on V sending $z \to z_1$ and $\Sigma \to \Sigma_1$. The converse is clear. □

By (iii), a maximal orthogonal partial spread Σ produces many inequivalent maximal symplectic partial spreads for different choices of z, where the number of inequivalent ones requires knowledge of the automorphism group of Σ. This was crucial in [16; 17; 18].

Theorem 6.2. *If $k \geq 2$ then there is a maximal partial* $\mathrm{Sp}(4k-2, q)$*-spread of size $q^k + 1$.*

Proof. Use Lemma 6.1(i) and Theorem 5.2(i). □

Theorem 6.3. *If $m > (k+1)/2$ then there is a maximal partial* $\mathrm{Sp}(4mk-2, q)$*-spread of size $q^{2mk-k} + 1$.*

Proof. Use Lemma 6.1(i) and Theorem 4.6. □

Example 6.4. By Lemma 6.1(ii), the set of sizes of maximal partial $\mathrm{Sp}(6, 4)$-spreads is contained in the set of sizes of maximal partial $\mathrm{Sp}(8, 4)$-spreads. This can be compared with the list in [13].

7 8-dimensional partial spreads

In $\mathrm{O}^+(8, q)$-spaces, triality [29] allows us to use more easily visualized points and partial ovoids in place of partial spreads: a triality map sends orthogonal (partial) ovoids to orthogonal (partial) spreads. We will use this to produce maximal partial $\mathrm{Sp}(8, q)$-spreads when q is even.

7.1 8-dimensional ovoids

Spreads and ovoids are known in $\mathrm{O}^+(8, q)$-spaces when q is prime, a power of 2 or 3, or $\equiv 2 \pmod 3$ (some of these ovoids are described in [15]). They have size $q^3 + 1$.

Lemma 7.1. *Let Ω be an ovoid in an $\mathrm{O}^+(8, q)$-space V, where $q > 2$. Let $a \notin \Omega$ be a singular point that is the only singular point in $\langle a^\perp \cap \Omega\rangle^\perp$. (Examples appear below in Appendix* B *for all even $q > 2$.) Then $\Omega^\bullet := (\Omega - (a^\perp \cap \Omega)) \cup \{a\}$ is a maximal orthogonal partial ovoid of size $q^3 - q^2 + 1$.*

Proof. Clearly $\Omega^\bullet$ is an orthogonal partial ovoid. If b is a singular point not perpendicular to any member of $\Omega^\bullet$ then $b^\perp \cap \Omega \subseteq a^\perp \cap \Omega$. Since both of these sets have size $q^2 + 1$ (e.g., by [15, p. 1196]), we obtain the contradiction that both a and b are the singular point in $\langle a^\perp \cap \Omega\rangle^\perp$. □

Applying triality τ to the preceding lemma produces a maximal orthogonal partial spread $\Omega^{\bullet\tau}$ of size q^3-q^2+1 in an $\mathrm{O}^+(8,q)$-space when $q>2$. If q is even then $\Omega^{\bullet\tau}$ is also a maximal symplectic partial spread by Lemma 4.9:

Theorem 7.2. *If $q>2$ is even then an $\mathrm{O}^+(8,q)$-space has a maximal symplectic partial spread of size q^3-q^2+1.*

We can imitate the preceding result and remove several sets $a^\perp\cap\Omega$ by using a specific type of ovoid.

Theorem 7.3. *If q is even and $1\le s\le q/5$, then an $\mathrm{O}^+(8,q)$-space has a maximal orthogonal partial spread of size $n_s:=q^3-sq^2+(s-1)(q+2)+\binom{s}{2}(q-2)+1$. There is also a maximal orthogonal partial spread of size n_4-1 if $q>16$. These are also maximal symplectic partial spreads.*

Proof. As in Theorem 7.2 we will construct maximal orthogonal ovoids. Since this the only part of this paper involving detailed computations, those computations have been postponed to Appendix B.

For the ovoid Ω in Appendix B, Example B.13(i) provides us with many sets $\mathcal{S}$ of s singular points disjoint from Ω together with the sizes $|\bigcap_{p\in\mathcal{S}'}p^\perp\cap\Omega|$ for all $\mathcal{S}'\subseteq\mathcal{S}$. Then

$$\Omega_s^\bullet:=(\Omega-\bigcup_{p\in\mathcal{S}}(p^\perp\cap\Omega))\cup\mathcal{S}$$

is an orthogonal partial ovoid of size $(q^3+1)-s(q^2+1)+\binom{s}{2}(2q)-\binom{s}{3}(q+2)+\cdots\pm\binom{s}{s}(q+2)+|\mathcal{S}|=\{(q^3+1)-s(q^2+1)+\binom{s}{2}(2q)\}-(q+2)+s(q+2)-\binom{s}{2}(q+2)+(1-1)^s(q+2)+s$.

Maximality of $\Omega_s^\bullet$: Suppose that b is a singular point not perpendicular to every member of $\Omega_s^\bullet$. Since Ω is an orthogonal ovoid, $b^\perp\cap\Omega$ must be contained in $\bigcup_{p\in\mathcal{S}}(p^\perp\cap\Omega)$. By Lemma B.2, $s(5q-5)\ge\sum_{p\in\mathcal{S}}|b^\perp\cap p^\perp\cap\Omega|\ge|b^\perp\cap\Omega|=q^2+1$, which contradicts our assumption that $s\le q/5$.

The same argument can be used for Example B.13(ii), producing the stated additional maximal orthogonal partial spreads. Use Lemma 4.9 for the final assertion. □

The preceding proof should be compared to the proofs of Theorem 7.13 and the more elementary Theorem 9.1. In those proofs the needed intersection sizes are known for simple geometric reasons. Here there does not seem to be a geometric explanation for the various intersection sizes occurring in Appendix B.

7.2 4- and 5-dimensional orthogonal ovoids

The next 8-dimensional partial spreads (in Theorem 7.7) arise from small-dimensional ovoids.

Example 7.4. *If Ω is an $\mathrm{O}^-(4,q)$-ovoid (i.e., an elliptic quadric) in an $\mathrm{O}^-(4,q)$-subspace W of a nondegenerate orthogonal $\mathbb{F}_q$-space V, then Ω is a maximal orthogonal partial ovoid of V.*

Proof. If x is any point of V then $x^\perp\cap W$ contains a hyperplane of W and hence contains either $p^\perp\cap W$ for a singular point p of W or $n^\perp\cap W$ a nonsingular point n of W. Each such hyperplane of W contains a singular point of W, and hence meets Ω nontrivially. □

A more general version of this example is a simple consequence of 5-dimensional results in [1; 3] (also see Lemma C.1):

Lemma 7.5. *If Ω is an ovoid in an $\mathrm{O}(5,q)$-subspace of a nondegenerate orthogonal $\mathbb{F}_q$-space V, then Ω is a maximal orthogonal partial ovoid of V.*

Proof. Once again we will show that *each point x of V is perpendicular to some point in Ω*. We may assume that $U:=\langle\Omega\rangle\not\le x^\perp$, so that $H:=x^\perp\cap U$ is a hyperplane of U. By the preceding example, we may also assume that U is not of type $\mathrm{O}^-(4,q)$.

If H has type $\mathrm{O}^+(4,q)$ then H contains a t.s. line, and each t.s. line of U meets each ovoid of U (by definition; cf. Section 2).

If H has type $\mathrm{O}^-(4,q)$ then its set Λ of singular points is a classical quadric. Then $\Lambda\cap\Omega\ne\emptyset$ by [1; 3].

Thus, H is degenerate. If there is a singular point y in its radical rad H, then every t.s. line of U on y meets Ω at a point perpendicular to y.

Finally, if rad H is a nonsingular point then q is even and the radical r of U is in H (since all hyperplanes of U not containing its radical are nonsingular). Let "bar" denote the projection map $U \to U/r$. Then $\overline{H}$ is a tangent or secant plane of the ovoid $\overline{\Omega}$ in the 4-space $\overline{U}$, so that $\overline{H}$ contains 1 or $q+1$ points of $\overline{\Omega}$. If T/r is one of these points, then the line T has a unique singular point, and this lies in both $H \le x^{\perp}$ and Ω. □

Question 7.6. *Which ovoids in orthogonal spaces are partial ovoids in all larger-dimensional orthogonal spaces over the same field?*

This requires that $(*)$ all hyperplanes of the smaller orthogonal space meet the ovoid. *Perhaps* this does not hold for any ovoids of $O^+(6,q)$-spaces that span the underlying 6-space (and there are, indeed, many such ovoids for which $(*)$ does not hold). However, $(*)$ does hold for some of the known $O^+(8,q)$ ovoids: those in [7, Theorem 3.9] or in [15, Section 7] and Appendix B.

Theorem 7.7. *Let q be a prime power.*

(i) *There are inequivalent maximal partial $O^+(8,q)$-spreads Σ of size q^2+1:*
  (a) *One for which $O^+(8,q)_\Sigma$ has a subgroup $SL(2,q^2)$ acting 2-transitively on Σ; and*
  (b) *One occurring when q is odd but not prime and for which $O^+(8,q)_\Sigma$ is intransitive on Σ.*

(ii) *If $q=2^e$ then there are inequivalent maximal partial $Sp(8,q)$-spreads Σ of size q^2+1 that are orthogonal partial spreads:*
  (a) *One for which $Sp(8,q)_\Sigma$ has a subgroup $SL(2,q^2)$ acting 2-transitively on Σ; and*
  (b) *One occurring when $e>1$ is odd and for which $Sp(8,q)_\Sigma$ has a subgroup $Sz(q)$ acting 2-transitively on Σ.*

Proof. Let τ be a triality map for an $O^+(8,q)$-space V. For Ω in the preceding example or lemma, $\Sigma = \Omega^\tau$ is a maximal orthogonal partial spread of V.

For (ia) use an elliptic quadric and its group of isometries. For (ib) there are other choices for Ω in Lemma 7.5, such as those in [15, Section 5].

If q is even then the only known choices for Ω in Lemma 7.5 are an elliptic quadric (Example 7.4) and a Suzuki–Tits ovoid (cf. Appendix C). The stated groups arise from subgroups of $\Omega^+(8,q)$ acting on Ω.

The various partial spreads are inequivalent as orthogonal partial spreads, since the corresponding maximal orthogonal partial ovoids $\Sigma^{\tau^{-1}} = \Omega$ are inequivalent.

In order to prove symplectic inequivalence in (ii), we use the isomorphism of $Sp(8,q)$ and $O(9,q)$ geometries. We may assume that the partial spreads in (iia) and (iib) lie in hyperplanes of an $O(9,q)$-space. They span these hyperplanes (two members of a partial spread already span). Hence, an element of $\Gamma O(9,q)$ sending one of our partial spreads to the other one respects the orthogonal geometries of these hyperplanes. We just saw that this is not the case. □

Remarks 7.8. We excluded $q=2$ in (iib) since that produces the same partial spread as in (iia). Part (iia) is a very special case of a result of Grassl (cf. Theorem 5.2). Is there an analogous generalization of (iib)?

Note that $Sp(8,q)_\Sigma$ contains subgroups $SL(2,q^2)\times SL(2,q^2)$ in (iia) and $Sz(q)\times O(3,q) \cong Sz(q)\times SL(2,q)$ in (iib).

In both (i) and (ii) there are t.s. 4-spaces X, Y such that the members of Σ meet X and Y in spreads of each (cf. Example 5.3).

See [22] for a survey of $O(5,q)$-ovoids.

7.3 Extending a partial spread

How can one search for maximal symplectic partial spreads? One obvious answer is to start with a symplectic or orthogonal partial spread and try to extend it to a maximal one (this was the computational method used to

produce the table in [13]). The instances considered below may have extensions to maximal ones other than the ones we provide.

Once again, points are easier to deal with than subspaces.

7.3.1 $O^-(4, q)$-ovoids

A simple example of an orthogonal partial ovoid is $(\Omega - \{p\}) \cup \{x\}$, where p is a point in the set Ω of singular points of an $O^-(4, q)$-space U and $x \notin U$ is a singular point in $(p^\perp \cap U)^\perp - U^\perp$ in a larger orthogonal space.

Proposition 7.9. *For any q an $O^+(8, q)$-space has a maximal orthogonal partial ovoid of size $2q^2 + 1$.*

Proof. In an $O^+(8, q)$-space V consider anisotropic 2-spaces A, A' and a totally singular 2-space $\langle p, p' \rangle$ such that $\langle A, A', p, p' \rangle = A \perp A' \perp \langle p, p' \rangle$. Let $E = \langle A, p \rangle$ and $E' = \langle A', p' \rangle$, and let x be a point of $\langle p, p' \rangle - \{p, p'\}$.

Let U and U' be non-perpendicular $O^-(4, q)$-subspaces of V such that $E'^\perp > U > E$ and $E^\perp > U' > E'$. (In order to construct these, note that p and p' are in t.s. lines $\neq \langle p, p' \rangle$ of the $O^+(4, q)$-space $(A \perp A')^\perp$. Choose singular points $u, u' \in (A \perp A')^\perp - \langle p, p' \rangle$ perpendicular to p' and p, respectively, but not to each other. Then $U := A \perp \langle p, u \rangle = \langle E, u \rangle$ and $U' := A' \perp \langle p', u' \rangle = \langle E', u' \rangle$ are non-perpendicular $O^-(4, q)$-subspaces such that $U = \langle A, p, u \rangle < \langle A', p' \rangle^\perp = E'^\perp$ and $U' < E^\perp$ behave as required.)

If Ω and Ω' are the sets of singular points of U and U', respectively, we claim that

$$\Omega^\bullet := (\Omega - \{p\}) \cup (\Omega' - \{p'\}) \cup \{x\}$$

behaves as stated in the lemma. Clearly, $|\Omega^\bullet| = q^2 + q^2 + 1$.

Orthogonal partial ovoid: $x^\perp \cap U = p^\perp \cap U = E$ has only one singular point p, and $p \notin \Omega^\bullet$. Suppose that there are perpendicular singular points $y \in \Omega - E$ and $y' \in \Omega' - E'$. Since $y \in U < E'^\perp$ and $y' < E^\perp$, while E and E' are perpendicular, we obtain to the contradiction that $\langle y, E \rangle = U$ and $\langle y', E' \rangle = U'$ are perpendicular.

Maximality: Suppose that h is a singular point such that $h^\perp \cap \Omega^\bullet = \emptyset$. Then $h^\perp \cap U$ is a hyperplane of U and hence contains a singular point, which must be p. Then $h^\perp \cap U = p^\perp \cap U = E$. Also $h^\perp \cap U' = E'$. Now $h \in \langle E, E' \rangle^\perp = \langle p, p' \rangle$, which contradicts the assumption that h is not perpendicular to $x \in \Omega^\bullet$. □

Theorem 7.10. *For any q an $O^+(8, q)$-space has a maximal orthogonal partial spread Σ of size $2q^2 + 1$. If q is even then Σ is symplectic.*

Proof. Applying triality to the proposition proves the first part, while Lemma 4.9 implies the second part. □

When q is even, Theorem 5.2(ii) contains another maximal symplectic partial spread of size $2q^2 + 1$ that need not be orthogonal.

Note that these examples, and others in this section, would have been more awkward to describe using t.s. 4-spaces instead of points.

7.3.2 Suzuki–Tits ovoids

Another example of an orthogonal partial ovoid is $(\Omega - \{p\}) \cup \{x\}$, where p is a point of a Suzuki–Tits ovoid Ω in an $O(5, q)$-space U and $x \notin U$ is a singular point in $(p^\perp \cap U)^\perp - U^\perp$ (cf. Appendix C). This time it is easier to extend this to a maximal orthogonal partial ovoid of an $O^+(8, q)$-space. In the next section we will see further advantages of Ω over an elliptic quadric.

Theorem 7.11. *If $q = 2^{2e+1} > 2$ then an $O^+(8, q)$-space has a maximal orthogonal partial spread Σ of size $q^2 + q + 1$ that is symplectic.*

Proof. By triality and Lemma 4.9, we need to construct a maximal orthogonal partial ovoid of the stated size in an $O^+(8, q)$-space V containing U. The radical r of U is also the radical of the 3-space $U^\perp$, and $(p^\perp \cap U)^\perp =$

$\langle p, U^\perp\rangle = p \perp U^\perp$ for $p \in \Omega$. Each singular point in the 4-space $(p^\perp \cap U)^\perp$ lies on a t.s. line containing p and meeting $U^\perp$ in one of its $q+1$ singular points.

For each singular point x_0 in $U^\perp$ let x be any point in $\langle p, x_0\rangle - \{p, x_0\}$. Let X be the resulting set of $q+1$ points x. We claim that

$$\Omega^\bullet := (\Omega - \{p\}) \cup X$$

behaves as required. Clearly, $|\Omega^\bullet| = q^2 + q + 1$.

Orthogonal partial ovoid: $x^\perp \cap U = p^\perp \cap U$ since $x_0^\perp \geq U$. Then $x^\perp \cap \Omega = \{p\}$. No two members of X are perpendicular since no two singular points in $U^\perp$ are.

Maximality: Suppose that h is a singular point such that $h^\perp \cap \Omega^\bullet = \emptyset$. Then $h^\perp \cap U$ is a hyperplane of U that cannot contain a point of $\Omega - \{p\}$. By Lemma C.1, $h^\perp \geq h^\perp \cap U = p^\perp \cap U$. Then $h \in (p^\perp \cap U)^\perp = \langle p, U^\perp\rangle$, so that h lies on one of the above lines $\langle p, x_0\rangle$, whereas $h^\perp \cap X = \emptyset$. □

7.4 Smaller maximal partial spreads using Suzuki–Tits ovoids

We will describe counterexamples to Grassl's conjecture, which was stated in the Introduction. Grassl has also found counterexamples to his conjecture in an $\mathrm{Sp}(8,8)$-space by using a computer search.

Theorem 7.12. *If $q = 2^{2e+1} > 2$ then there is a maximal partial $\mathrm{O}^+(8,q)$-spread of size $q^2 - q + 1$; this is also a maximal partial $\mathrm{Sp}(8,q)$-spread.*

Proof. In view of triality and Lemma 4.9, it suffices to construct a maximal partial $\mathrm{O}^+(8,q)$-ovoid of size $q^2 - q + 1$. We use the notation in Section 7.3.2 and Appendix C.

Let Ω be a Suzuki–Tits ovoid in an $\mathrm{O}(5,q)$-space U. Embed U into an $\mathrm{O}^+(8,q)$-space V.

Let $\Omega^\bullet := (\Omega - (x^\perp \cap \Omega)) \cup \{x\}$ for a singular point x of U not in Ω (this uses $\dim U > 4$). Then $|\Omega^\bullet| = q^2 - q + 1$ and $\Omega^\bullet$ is an orthogonal partial ovoid of U and hence of V.

Maximality: Suppose that h is a singular point of V such that $h^\perp \cap \Omega^\bullet = \emptyset$. We will consider the possibilities for the hyperplane $h^\perp \cap U$ of U in Lemma C.1. We have $h^\perp \cap \Omega \subseteq x^\perp \cap \Omega$ since $h^\perp \cap \Omega^\bullet = \emptyset$. Also, $\Omega^\perp = U^\perp < x^\perp$ since $x \in U = \langle\Omega\rangle$.

Case 1. $h^\perp \cap \Omega = \{p\}$ for some $p \in x^\perp \cap \Omega$. Then $h^\perp \cap U = p^\perp \cap U$ since Lemma C.1 implies that $p^\perp \cap U$ is the only hyperplane of U meeting Ω just in p. Then $h^\perp \geq h^\perp \cap U = p^\perp \cap U$ implies that $h \in \langle p, U^\perp\rangle \leq x^\perp$, whereas h is assumed not to be perpendicular to $x \in \Omega^\bullet$.

Case 2. $|h^\perp \cap \Omega| = q+1$. Since $h^\perp \cap \Omega \subseteq x^\perp \cap \Omega$ for sets of size $q+1$, we have $h^\perp \geq \langle h^\perp \cap \Omega\rangle = \langle x^\perp \cap \Omega\rangle$. Since $x^\perp \cap \Omega$ projects into a plane of U/r we are in the situation of Lemma C.1(ii). Then $\langle x^\perp \cap \Omega\rangle = x^\perp \cap U$ by the end of Lemma C.1(ii). Now $h \in \langle x, U^\perp\rangle \leq x^\perp$, which produces the same contradiction as before.

Case 3. $1 < |h^\perp \cap \Omega| < q+1$. Since $h^\perp \cap \Omega$ lies in a set $x^\perp \cap \Omega$ that projects into a plane of U/r, this contradicts the irreducibility in Lemma C.1(iii). □

We can go further (mimicking the proofs of Theorems 7.3 and 9.1):

Theorem 7.13. *An $\mathrm{O}^+(8,q)$-space has a maximal orthogonal partial spread of size $q^2 - sq + 2s - 1$ whenever $q = 2^{2e+1}$ and $1 < s \leq \sqrt{q/2} - 1$. Each of these is a maximal partial symplectic spread.*

In particular, there is a maximal partial $\mathrm{Sp}(8,q)$-spread of size $q^2 - \sqrt{q^3/2} + q + \sqrt{2q} - 3$.

Proof. Once again we will construct maximal partial $\mathrm{O}^+(8,q)$-ovoids. Let Ω, U, V and $r = \mathrm{rad}\, U$ be as before. Choose distinct $a, b \in \Omega$. Then $\{a,b\}^\perp \cap U$ is a nondegenerate plane containing r whose $q+1$ singular points x form a conic. These points produce $q+1$ subspaces $\langle x, a, b, r\rangle = x^\perp \cap U$ that induce a partition of $\Omega - \{a,b\}$ using $q+1$ circles $\Omega_x := x^\perp \cap \Omega$ of the inversive plane $\mathfrak{I}(\Omega)$ determined by Ω [10, Section 6.4].

Let $\mathcal{S}$ be any set of s singular points $x \in \{a,b\}^\perp$. We will show that

$$\Omega^\bullet := \Big(\Omega - \bigcup_{x\in\mathcal{S}} \Omega_x\Big) \cup \mathcal{S} \subset U$$

is a maximal partial ovoid of the stated size.

1. $|\Omega^\bullet| = (q^2+1) - 2 - |\mathcal{S}|(q-1) + |\mathcal{S}|$.

2. *Partial ovoid*: If $x \in \mathcal{S}$ then $\Omega_x = x^\perp \cap \Omega$ was replaced by x, and all such x lie in a conic of $\{a,b\}^\perp \cap U$.

3. *Maximality*: Suppose that h is a singular point of V such that $h^\perp \cap \Omega^\bullet = \emptyset$. Then $h^\perp \cap \Omega \subseteq \bigcup_{x\in\mathcal{S}} \Omega_x$. Lemma C.1 contains several possibilities for $h^\perp \cap \Omega$.

Case 1. $h^\perp \cap \Omega = \{p\}$ for some $p \in \Omega$. Then $p \in \Omega_x$ for some $x \in \mathcal{S} \subset \Omega^\bullet$. By Lemma C.1, $h^\perp \cap U = p^\perp \cap U \leq h^\perp$. Then $h \in \langle p, U^\perp\rangle \leq x^\perp$, whereas h is assumed not to be perpendicular to $x \in \Omega^\bullet$.

Case 2. $h^\perp \cap \Omega$ is a circle of $\mathcal{I}(\Omega)$. If $h^\perp \cap \Omega$ contains $\{a,b\}$ then $h^\perp \cap \Omega = \Omega_x \subset x^\perp$ for some $x \in \mathcal{S}$ since the circles Ω_y, $y \in \{a,b\}^\perp$, induce a partition of $\Omega - \{a,b\}$. Then $h^\perp$ contains $\langle \Omega_x\rangle = x^\perp \cap U$ by Lemma C.1(ii), which again produces the contradiction $h \in \langle x, U^\perp\rangle \leq x^\perp$.

If $h^\perp \cap \Omega$ does not contain $\{a,b\}$ then it meets each circle Ω_x, $x \in \mathcal{S}$, in at most two points. This produces the contradiction $q+1 = |h^\perp \cap \Omega| \leq 2|\mathcal{S}| = 2s$.

Case 3. $h^\perp \cap \Omega$ is an orbit of a cyclic group $T < G$ of order $|h^\perp \cap \Omega| = q \pm \sqrt{2q} + 1$ (Lemma C.1(iii)). Note that $|T|$ divides q^2+1 and hence is relatively prime to $q(q-1)$, the order of the stabilizer in G of a circle [25, Theorem 9]. Thus, given circles C_1 and C_2, at most one element of T can send C_1 to C_2.

For each $t \in T$ we have $h^\perp \cap \Omega = (h^\perp \cap \Omega)^t \subseteq \bigcup_{x\in\mathcal{S}} \Omega_x^t$, involving two sets of s circles: $\{\Omega_x \mid x \in \mathcal{S}\}$ and $\{\Omega_x^t \mid x \in \mathcal{S}\}$. For an ordered pair x, y of distinct elements of $\mathcal{S}$ there is at most one such $t \neq 1$ with $\Omega_x^t = \Omega_y$. Thus, if we choose t to be one of at least $|T| - 1 - s(s-1) \geq q - \sqrt{2q} - s(s-1) > 0$ elements of T that do not behave this way for all x, y, then we will have two disjoint sets of s circles, with the union of each set containing $h^\perp \cap \Omega$. Since distinct circles meet in at most two points, $q \pm \sqrt{2q} + 1 = |h^\perp \cap \Omega| \leq s \cdot s \cdot 2$, which is not the case.

Case 4. $\Lambda := h^\perp \cap \Omega$ has size $q+1$ but is not a circle, and its stabilizer in G has a cyclic subgroup T of order $q-1$ fixing two points c, d and transitive on $\Lambda - \{c,d\}$ (Lemma C.1(iv)). By Remark C.2(ii), given circles C_1 and C_2, at most one element of T can send C_1 to C_2 unless $C_1 = C_2$ is one of the two circles fixed by T.

We have $\Lambda - \{c,d\} \subseteq \bigcup_{x\in\mathcal{S}} \Omega_x$ and $\Lambda - \{c,d\} \subseteq \bigcup_{y\in\mathcal{S}} \Omega_y^t$ whenever $1 \neq t \in T$. If Ω_y^t arises from two such t then Ω_y is one of the two circles fixed by T (by Remark C.2(ii)), and $\Omega_y - \{c,d\}$ and $\Lambda - \{c,d\}$ are disjoint; then Ω_y is not needed for our union of Ω_x to contain $\Lambda - \{c,d\}$ and hence can be deleted. After at most two T-invariant circles have been deleted, we can choose one of at least $|T| - 1 - s(s-1) = q - 2 - s(s-1) > 0$ elements $t \in T$ such that $\Omega_x^t \neq \Omega_y$ for all remaining Ω_x, Ω_y (with $x, y \in \mathcal{S}$). Then we obtain two disjoint sets of at least $s-2$ circles with the union of each set containing $\Lambda - \{c,d\}$. This produces the contradiction $(q+1) - 2 \leq (s-2)\cdot(s-2)\cdot 2$. □

We have proved, more generally, that *$\Omega^\bullet$ is a maximal partial ovoid of any nonsingular orthogonal $\mathbb{F}_q$-space containing U*, since every hyperplane of U has nonempty intersection with $\Omega^\bullet$ (cf. Question 7.6).

7.5 Sp(6, q)-space consequences

Theorem 7.14. *For even $q > 2$, an* Sp$(6,q)$*-space has maximal symplectic partial spreads of size*

(i) $n_1 = q^3 - q^2 + 1$,

(ii) $q^2 + 1$,

(iii) $2q^2 + 1$,

(iv) $q^2 + q + 1$ *if* $q = 2^{2e+1}$,

(v) $q^2 - q + 1$ *if* $q = 2^{2e+1}$,

(vi) $q^2 - sq + 2s - 1$ *if* $q = 2^{2e+1}$ *and* $1 < s \leq \sqrt{q/2} - 1$,

(vii) n_r *if* $1 \leq r \leq q/5$ (*where* n_r *is defined in* Theorem 7.3), and

(viii) $n_4 - 1$ if $q \geq 16$.

Proof. Use Lemma 6.1(i) together with Theorems 7.2, 7.7, 7.10, 7.11, 7.12, 7.13 and 7.3. □

8 6-dimensional partial spreads

We again consider arbitrary characteristic. In characteristic 2 the examples in the next theorem already appear in Theorem 7.14(i), but here we use an entirely different method to prove maximality.

Theorem 8.1. *If q is a prime power then an* $\mathrm{Sp}(6,q)$*-space has a maximal symplectic partial spread of size* q^3-q^2+1.

Proof. In an $\mathrm{Sp}(6,q)$-space let Σ be a desarguesian spread preserved by $G=\mathrm{SL}(2,q^3)=\mathrm{Sp}(2,q^3)<\mathrm{Sp}(6,q)$. Let $X\in\Sigma$. Let U be a t.i. 3-space such that $U\cap X=L$ is a line. If Σ_U is the set of members of Σ met nontrivially by U, then we will show that $\Sigma^\bullet:=(\Sigma-\Sigma_U)\cup\{U\}$ *is a maximal symplectic partial spread of size* q^3-q^2+1.

If U meets $Y\in\Sigma-\{X\}$ nontrivially then $U\cap Y$ must meet $U\cap X=L$ trivially and hence is a point; the number of such points is the number $|\Sigma-\{X\}|=q^2$ of points in U not in L. Thus, $|\Sigma_U|=q^2+1$ and $\Sigma^\bullet$ is a symplectic partial spread of size q^3+1-q^2.

The set-stabilizer G_X of X has order $q^3(q^3-1)$. It has an abelian normal subgroup Q of order q^3 inducing 1 on X and a cyclic subgroup S of order q^3-1 transitive on $X-\{0\}$ and hence also on the q^2+q+1 lines L of X. Then $|G_L|=q^3(q-1)$.

Since Q is transitive on $\Sigma-\{X\}$ it is transitive on the q^3 points in $\{L^\perp\cap Y\mid Y\in\Sigma-\{X\}\}$, and hence also on the q t.i. 3-spaces $\langle L,L^\perp\cap Y\rangle\neq X$ containing L (where once again $Y\in\Sigma-\{X\}$). Then $|G_U|=q^2(q-1)$. Moreover, Q_U has order q^2 and is the subgroup $Q_{[L]}$ of Q that fixes each t.i. 3-space containing L. Each of the q orbits of $Q_{[L]}$ on $\Sigma-\{X\}$ spans one of the q t.i. 3-spaces $\neq X$ containing L.

Maximality: Assume that $W\notin\Sigma^\bullet$ is a t.i. 3-space such that $\Sigma^\bullet\cup\{W\}$ is a symplectic partial spread. Then $\Sigma_W\subseteq\Sigma_U$ since Σ is a spread. Clearly, W meets each member of Σ in 0, a point or a line. Since W has $q^2+q+1>|\Sigma_U|\geq|\Sigma_W|$ points, some intersection is a line, and it is unique (since two lines of W would meet nontrivially). Thus, W arises in the same manner as U, and G_W acts on $\Sigma_W=\Sigma_U$.

Since $|\Sigma_U|=q^2+1$ does not divide $|G|$, G_W cannot move X. Then $G_U,G_W\leq G_X$. Since the q nontrivial orbits of $Q_{[L]}$ on Σ correspond to the t.i. 3-spaces $\neq X$ containing L, we cannot have $W\cap X=L$.

However, the cyclic group S is transitive on the lines L of X and (by conjugation) on the corresponding subgroups $Q_{[L]}$. Then $Q_{[W\cap X]}$ and $Q_{[L]}$ are distinct subgroups of order q^2. They generate a subgroup of Q of order $>q^2=|\Sigma_X|-1$, which is a final contradiction. □

9 4-dimensional partial spreads

Finally, we survey families of maximal partial spreads of $\mathrm{Sp}(4,q)$-spaces. See [5; 13] for lists and tables of known families. As noted in Section 1, we can use more easily visualized points in $\mathrm{O}(5,q)$-space instead of lines in $\mathrm{Sp}(4,q)$-space due to the Klein correspondence [26, p. 196]. The following result involves a much simpler version of the arguments used in Theorems 7.3 and 7.13.

Theorem 9.1 ([5, p. 1940], [28, Theorem 6.6]). (i) *For odd q an* $\mathrm{Sp}(4,q)$*-space has a maximal partial spread of size* $q^2-sq+3s-1$ *whenever* $1\leq s<(q+1)/2$.

(ii) *For even q an* $\mathrm{Sp}(4,q)$*-space has a maximal partial spread of size* $q^2-sq+2s-1$ *whenever* $1\leq s<(q+1)/2$.

Proof. We will construct maximal partial $\mathrm{O}(5,q)$-ovoids. Let Ω be an $\mathrm{O}^-(4,q)$ ovoid in a 4-dimensional subspace U. Choose distinct $a,b\in\Omega$, so that the set C of singular points in $\langle a,b\rangle^\perp$ is a conic.

(i) If $x\in C$ then $\Omega_x:=x^\perp\cap\Omega$ is a conic in the nondegenerate 3-space $\langle x^\perp\cap\Omega\rangle$. The line $\Omega_x^\perp$ contains exactly two singular points x,x' for a fixed-point-free involution $x\mapsto x'$ of C, and $\Omega_x=\Omega_{x'}$.

Let $\mathcal{S}$ be any set of $s<(q+1)/2$ points $x\in C$ such that the conics Ω_x, $x\in\mathcal{S}$, are distinct (i.e., $\mathcal{S}\cap\mathcal{S}'=\emptyset$). We claim that $\Omega^\bullet:=(\Omega-\bigcup_{x\in\mathcal{S}}\Omega_x)\cup\bigcup_{x\in\mathcal{S}}\{x,x'\}$ *is a maximal partial* $\mathrm{O}(5,q)$*-ovoid of the stated size.*

1. $|\Omega^\bullet|=(q^2+1)-2-|\mathcal{S}|(q-1)+2|\mathcal{S}|$.

2. *Orthogonal partial ovoid*: If $x\in\mathcal{S}$ then Ω_x was replaced by the subset $\{x,x'\}$ of the conic C.

3. *Maximality*: Suppose that h is a singular point such that $h^\perp \cap \Omega^\bullet = \emptyset$. Then $h^\perp \cap \Omega \subseteq \bigcup_{x\in\mathcal{S}} \Omega_x$, and $h^\perp \cap \Omega$ is either a point or a circle of the inversive plane $\mathfrak{I}(\Omega)$ determined by Ω [10, Section 6.4].

If $h^\perp \cap \Omega$ is a point p then $h^\perp \cap U = p^\perp \cap U$. Then $h \in (h^\perp \cap U)^\perp = (p^\perp \cap U)^\perp = \langle p, U^\perp\rangle$, which has just one singular point p, whereas $p \in \Omega$ is either in $\Omega^\bullet$ or is perpendicular to some $x \in \mathcal{S}$.

Thus, $h^\perp \cap \Omega$ is a circle. If $h^\perp \cap \Omega = \Omega_x$ with $x \in \mathcal{S}$, then $h \in \Omega_x^\perp = \langle x, x'\rangle$, whereas $h \notin \{x, x'\}$. Thus, $h^\perp \cap \Omega$ is a circle lying in the union of s circles of $\mathfrak{I}(\Omega)$, each of which it meets at most twice. This produces the contradiction $q + 1 = |h^\perp \cap \Omega| \le 2s$.

(ii) This is proved as above but is simpler: if x is a singular point in $\{a, b\}^\perp$ then $(x^\perp \cap \Omega)^\perp$ contains just one singular point; no permutation $x \mapsto x'$ is involved. □

Example 9.2. A maximal partial ovoid of size $3q - 1$ in $\mathrm{Sp}(4, q)$-space, $q \ge 4$, is constructed in [5, p. 1939]. The proof in that paper shows that this is a maximal partial ovoid in $\mathrm{Sp}(2m, q)$-space for all $m \ge 2$.

This partial ovoid is the set of points in $\bigcup_1^3(\langle x_i, y_{i+1}\rangle - \{x_i, y_{i+1}\}) \cup \{x, y\}$ (subscripts mod 3), where x_1, x_2, x_3, x are four points of X and y_1, y_2, y_3, y are four points of Y for t.i. 2-spaces X, Y intersecting in 0, with each pair x_i, y_i perpendicular and x, y not perpendicular.

Dualizing [26, p. 196] produces a maximal symplectic partial spread of size $3q - 1$ in $\mathrm{Sp}(4, q)$-space for even $q \ge 4$.

Example 9.3. For arbitrary q there are integer intervals that consist of sizes of maximal $\mathrm{Sp}(4, q)$ partial spreads [24; 23]. While the ideas used in those papers resemble much more intricate versions of those in the theorem, it is not clear whether those papers contain the above examples.

Example 9.4. There is a maximal partial spread of size $q^2 - 1$ in $\mathrm{Sp}(4, q)$-space for $q \in \{3, 5, 7, 11\}$. This is constructed using a subgroup of $\mathrm{Sp}(2, q) = \mathrm{SL}(2, q)$ sharply transitive on $\mathbb{F}_q^2 - \{0\}$ [21; 9; 6]. It is contained in the non-symplectic spread of $\mathbb{F}_q^4$ corresponding to the associated affine irregular nearfield plane.

10 Concluding remarks

The preceding examples make it clear that there are rather few known types of maximal symplectic partial spreads. There are amazingly few known types in odd characteristic, especially in view of the tables in [5; 13]. We mentioned a number of symplectic partial spreads whose maximality has yet to be decided.

Other examples are in [19, Theorem 1.2] and [8]: if q is odd then an $\mathrm{Sp}(8, q)$-space has an $\mathrm{SL}(2, q^3)$-invariant partial spread of size $q^3 + 1$ that is fundamental for the existence of a ${}^3D_4(q)$ generalized hexagon. This symplectic partial spread is probably maximal, but no proof seems to be known. When q is even the maximality of the analogous symplectic partial spread is a special case of Proposition 4.1.

We have mostly ignored inequivalence questions. Suppose that q is even. The number of inequivalent orthogonal spreads in $\mathrm{O}^+(4m, q)$-spaces is not bounded above by any polynomial in q^m [18]; these produce inequivalent maximal symplectic partial spreads in Proposition 4.1 and Theorems 4.6 and 6.3. In addition, there are at least q^{q^k}/q^{4k^2} inequivalent examples in Theorem 5.2(ii), $\binom{q-1}{s}/q^{30}$ for each pair q, s in Theorem 7.3, $(q-1)^{q+1}/q^{30}$ in Theorem 7.11, $\binom{q+1}{s}/q^{30}$ for each pair q, s in Theorem 7.13, $\binom{q+1}{s}/q^{11}$ for each pair q, s in Theorem 9.1 and $(q-2)(q-3)/6 \log q$ in Example 9.2.

Appendices

A Mutually unbiased bases

Equip $\mathbb{C}^N$ with its usual hermitian inner product $(,)$. Orthonormal bases $\mathcal{B}_1$ and $\mathcal{B}_2$ are called *mutually unbiased* if $|(u_1, u_2)| = 1/\sqrt{N}$ whenever $u_i \in \mathcal{B}_i$ for $i = 1, 2$. Any set of MUBs (mutually unbiased bases) has size at most $N + 1$.

For a prime p set $V = \mathbb{Z}_p^n$ (row vectors) with its usual dot product $x \cdot y$. Consider $\mathbb{C}^N$, $N = p^n$, with the standard basis labeled $\mathcal{B}_\infty := \{e_v \mid v \in V\}$ and the usual hermitian inner product $(,)$. Let $\zeta \in \mathbb{C}$ be a primitive p^{th} root of unity (so that $\zeta = -1$ if $p = 2$).

The MUBs mentioned in Section 1 can be described using sets $\mathcal{S}$ of symmetric $n \times n$ matrices M such that the difference of any two is nonsingular; explicit sets $\mathcal{S}$ are in [4; 17; 13]. Each partial symplectic spread Σ can be written (after a choice of bases) as the subspaces of $V \oplus V$ of the form $O \oplus V$ or $(V \oplus O)\left(\begin{smallmatrix} I & M \\ O & I \end{smallmatrix}\right)$ for M varying through a set $\mathcal{S}$ as above. (The alternating bilinear form is $((x, y), (x', y')) = x \cdot y' - x' \cdot y$.)

Let $Q_M \colon V \to \mathbb{Z}_p$ be a quadratic form associated with the symmetric bilinear form $uM \cdot v$ on V, so that $Q_M(u+v) = Q_M(u) + Q_M(v) + uM \cdot v$ for all $u, v \in V$. If $p > 2$ then $Q_M(v) = vM \cdot v/2$. If $p = 2$ use $Q_M(v) = vU_M \cdot v$, where U_M is obtained from M by replacing all entries below the diagonal by 0. If

$$\mathcal{F}(\Sigma) := \{\mathcal{B}_\infty, \mathcal{B}_M^{\mathcal{S}} \mid M \in \mathcal{S}\}, \quad \mathcal{B}_M^{\mathcal{S}} := \left\{ \frac{1}{\sqrt{N}} \sum_{v \in V} \zeta^{a \cdot v + Q_M(v)} e_v \;\middle|\; a \in V \right\}, \tag{A.1}$$

then $\mathcal{F}(\Sigma)$ is a set of MUBs when $p > 2$. If $p = 2$ then $\mathcal{F}(\Sigma)$ is a set of real MUBs (i.e., in $\mathbb{R}^N$) provided that Σ is an orthogonal partial spread. Using the quadratic form $Q((x, y)) = x \cdot y$ this means that $\mathcal{S}$ consists of skew-symmetric matrices M (i.e., symmetric with zero diagonal, so that $Q((x, xM)) = 0$).

Complex MUBs also arise when $p = 2$. Let

$$\widehat{\mathcal{B}}_M^{\mathcal{S}} := \left\{ \frac{1}{\sqrt{N}} \sum_{v \in V} i^{2\hat{a} \cdot \hat{v} + \hat{v}\hat{M} \cdot \hat{v}} e_v \;\middle|\; a \in V \right\}, \tag{A.2}$$

where "hats" denote that the vector or matrix has entries 0, 1 *viewed inside* $\mathbb{Z}_4$ (so that $\hat{a}, \hat{v} \in \mathbb{Z}_4^n$). Then $\{\mathcal{B}_\infty, \widehat{\mathcal{B}}_M^{\mathcal{S}} \mid M \in \mathcal{S}\}$ is again a set of MUBs.

See [4; 17] for proofs and the related finite group framework. Our maximal symplectic partial spreads produce sets of MUBs that are maximal within that framework. It is not at all clear that these are also maximal as sets of MUBs in $\mathbb{C}^N$, though this may be the case if Σ is sufficiently large.

B Desarguesian ovoids in $O^+(8, q)$-space

In order to prove Theorem 7.3 we will consider a specific orthogonal ovoid in an $O^+(8, q)$-space with $q > 2$ even. Let $F = \mathbb{F}_{q^3} \supset K = \mathbb{F}_q$, with trace map $T \colon F \to K$ and norm $N \colon F \to K$. Then $Q(a, \beta, \gamma, d) := ad + T(\beta\gamma)$ turns $V := K \oplus F \oplus F \oplus K$ into an $O^+(8, q)$-space.

The $q^3 + 1$ points $\langle (0, 0, 0, 1) \rangle$ and $\langle (1, t, t^{q+q^2}, N(t)) \rangle$, $t \in F$, form an ovoid Ω on which $G := \mathrm{SL}(2, q^3)$ acting 3-transitively. In [15, p. 1204] this is called a *desarguesian ovoid* (since it arises from a desarguesian spread of an $\mathrm{Sp}(6, q)$-space using Lemma 6.1(ii) and triality), and it is observed that G has exactly two orbits of singular points of V, one of which is Ω. If $q > 2$ and p is any singular point not in Ω, then $\langle p^\perp \cap \Omega \rangle = p^\perp$ [15, p. 1204], as required in Lemma 7.1.

Notation B.1. Let $\pi \in F$ with $T(\pi) = 0 \neq T(\pi^{1+q})$. Use the nondegenerate symmetric K-bilinear form $T(xy)$ on F to see that $\pi^q \notin \{t \in F \mid T(\pi t) = 0\} = K + K\pi$.

Lemma B.2. *If p_1 and p_2 are distinct singular points not in Ω, then $|p_1^\perp \cap p_2^\perp \cap \Omega| \leq 5q - 5$.*

Proof. By the transitivity of G we may assume that $p_1 = \langle(0, 0, \pi, 0)\rangle$ and $p_2 = \langle(a, \beta, \gamma, d)\rangle$ for some a, β, γ, d. We need to estimate the number of solutions t to the equations

$$T(t\pi) = 0 = aN(t) + d + T(\beta t^{q+q^2} + \gamma t)$$

corresponding to points $\langle(1, t, t^{q+q^2}, t^{1+q+q^2})\rangle$. By (B.1) we can write $t = u + v\pi$ with $u, v \in K$. Then the second equation is

$$aN(u + v\pi) + d + T(\beta[u + v\pi]^{q+q^2} + \gamma[u + v\pi]) = 0,$$

which expands to

$$a\{u^3 + uv^2T(\pi^{q+q^2}) + v^3N(\pi)\} + d + u^2T(\beta) + uvT(\beta\pi) + v^2T(\beta\pi^{q+q^2}) + uT(\gamma) + vT(\gamma\pi) = 0. \tag{B.3}$$

For each u this is a K-polynomial in v of degree at most three, and hence has at most three roots $v \in K$ if it is not the zero polynomial. Let B be the number of "bad" u for which this polynomial in v is the zero polynomial. Then $|p_1^\perp \cap p_2^\perp \cap \Omega| \le (q - B)3 + Bq + 1$ (the last term occurs since $\langle(0, 0, 0, 1)\rangle$ may be in the intersection). We will show that $B \le 2$, which produces the bound in the lemma.

The coefficients of our polynomial show that, for a "bad" u, we must have $aN(\pi) = 0$, $T(\beta\pi^{q+q^2}) = 0$, $uT(\beta\pi) + T(\gamma\pi) = 0$ and $u^2T(\beta) + uT(\gamma) + d = 0$. If $T(\beta\pi) \neq 0$ then there is one "bad" u, while if $T(\beta\pi) = T(\gamma\pi) = 0$ then there are at most two "bad" u unless $T(\beta) = T(\gamma) = d = 0$.

Thus, we must show that $T(\beta\pi^{q+q^2}) = T(\beta\pi) = T(\gamma\pi) = T(\beta) = T(\gamma) = 0$ cannot all occur. Since $T(\beta) = T(\beta\pi) = 0$, by (B.1) we have $\beta = x\pi$ with $x \in K$. Then $0 = T(\beta\pi^{q+q^2}) = xT(N(\pi))$, so that $x = 0$. Similarly, since $T(\gamma) = T(\gamma\pi) = 0$ we have $\gamma = y\pi$ with $y \in K$. Now $p_2 = \langle(0, 0, y\pi, 0)\rangle = p_1$, which is not the case. □

Notation B.4. Let $\Omega_0 \subset \Omega$ consist of $\langle(0, 0, 0, 1)\rangle$ and $\langle(1, t, t^{q+q^2}, t^{1+q+q^2})\rangle$, $t \in K$. There are $(q + 1)^2$ singular points in $\Omega_0^\perp$, all having the form $\langle(0, \beta, \gamma, 0)\rangle$ with $T(\beta) = T(\gamma) = T(\beta\gamma) = 0$. The sets Ω_0 and $\Omega_0^\perp$ are acted on by a naturally embedded subgroup $G_0 = \mathrm{SL}(2, q)$ of G containing the transformations

$$\begin{aligned} u_s &: (a, \beta, \gamma, d) \mapsto (a, \beta + sa, \gamma + as^2 + \beta^q s + \beta^{q^2} s, d + as^3 + T(\beta)s^2 + T(\gamma)s) \\ j &: (a, \beta, \gamma, d) \mapsto (d, \gamma, \beta, a) \end{aligned}$$

with $s \in K$. These act on each of the $q + 1$ lines $\langle(0, \beta, 0, 0), (0, 0, \beta, 0)\rangle$ with $T(\beta) = 0 \neq \beta$ that partition the $(q + 1)^2$ singular points in $\Omega_0^\perp$, sending

$$\begin{aligned} u_s &: (0, \beta, \gamma, 0) \mapsto (0, \beta, \gamma + \beta s, 0) \\ j &: (0, \beta, \gamma, 0) \mapsto (0, \gamma, \beta, 0). \end{aligned} \tag{B.5}$$

Definition B.6. An *ordinary* point is a singular point in $\Omega_0^\perp$ of the form $\langle(0, \beta, \gamma, 0)\rangle$ such that either $\beta = 0$ and $T(\gamma^{1+q}) \neq 0$, or $T(\beta^{1+q}) \neq 0$ (recall that $T(\beta) = T(\gamma) = T(\beta\gamma) = 0$). Since any $\beta \in F^*$ has characteristic polynomial $x^3 + T(\beta)x^2 + T(\beta^{1+q})x + N(\beta)$, the ordinary requirement can fail for some β, γ if and only if $q \equiv 1 \pmod 3$. Moreover, if $\beta \in F - K$ then $\beta^q \in \beta K \iff \beta^{q-1} \in K \iff \beta^{(q-1, q^2+q+1)} \in K \iff \beta^3 \in K \iff T(\beta^{1+q}) = 0$.

For π in (B.1), since $T((a\pi + \pi^q)(a\pi + \pi^q)^q) = (a^2 + a + 1)T(\pi^{1+q})$ all points of the line $\langle(0, a\pi + \pi^q, 0, 0), (0, 0, a\pi + \pi^q, 0)\rangle$, $a \in K$, are ordinary if and only if $a^2 + a + 1 \neq 0$, so that all points are ordinary if $q \equiv 2 \pmod 3$, but there are two lines of this form all of whose points are not ordinary when $q \equiv 1 \pmod 3$.

The significance of ordinary points is the following

Lemma B.7. *If p is an ordinary point then*

(i) *p has the form $\langle(0, 0, \gamma, 0)\rangle$ with $T(\gamma) = 0$ or $\langle(0, \beta, a\beta, 0)\rangle$ with $T(\beta) = 0$ and $a \in K$, and*

(ii) *$p^g = \langle(0, 0, \pi', 0)\rangle$ for some $g \in G_0$, where π' behaves as π does in* (B.1)*: $T(\pi') = 0 \neq T(\pi'^{1+q})$.*

Proof. We may assume that $p = \langle(0, \beta, \gamma, 0)\rangle$ with $\beta \neq 0$.

(i) Since p is ordinary, we have seen that $\beta^q \notin K\beta$, so that β and β^q span $\ker T$. Write $\gamma = k\beta + b\beta^q$ with $k, b \in K$. Then $0 = T(\beta\gamma) = bT(\beta^{1+q})$ implies that $b = 0$.

(ii) By (B.5), $p^{u_k j} = \langle(0, 0, \beta, 0)\rangle$ behaves as stated. □

Lemma B.8. *If p_1, p_2 and p_3 are pairwise non-perpendicular ordinary points, then*

(i) $|p_1^\perp \cap p_2^\perp \cap \Omega| = 2q$ *and*

(ii) $|p_1^\perp \cap p_2^\perp \cap p_3^\perp \cap \Omega| = q + 2$.

Proof. By Lemma B.7(ii) we may assume that p_1 has the form $\langle(0, 0, \pi, 0)\rangle$ and $p_2 = \langle(0, \beta, \gamma, 0)\rangle$, where $T(\beta) = T(\gamma) = T(\beta\gamma) = 0$. Also $T(\beta\pi) \neq 0$ since p_1 and p_2 are not perpendicular. All $(0, 0, 0, 1)$ and $(1, t, t^{q+q^2}, N(t))$, $t \in K$, are in each of the stated intersections, so we will focus on vectors $(1, t, t^{q+q^2}, N(t))$ with $t = u + v\pi \notin K$ that lie in an intersection.

(i) Here (B.3) states that

$$uvT(\beta\pi) + v^2 T(\beta\pi^{q+q^2}) + vT(\gamma\pi) = 0. \tag{B.9}$$

Since $T(\beta\pi) \neq 0$, each $v \neq 0$ determines a unique u. This argument reverses: the intersection size is $(q + 1) + (q - 1)$.

Before continuing we massage (B.9). By Lemma B.7(i), $\gamma = k\beta$ for some $k \in K$. Since $\dim \ker T = 2$ we can write $\beta = x\pi + y\pi^q$ with $x, y \in K$. Since $0 \neq T(\beta\pi) = yT(\pi^{1+q})$ we have $y \neq 0$ and $\beta \in ((x/y)\pi + \pi^q)K$. We may assume that $\beta = a\pi + \pi^q$ with $a \in K$. Then

$$p_2 = \langle(0, a\pi + \pi^q, k(a\pi + \pi^q), 0)\rangle. \tag{B.10}$$

Also $T(\beta\pi) = T(\pi^{1+q})$, so that (B.9) becomes

$$uT(\pi^{1+q}) + v[aN(\pi) + T(\pi^{2q+q^2})] + kT(\pi^{1+q}) = 0. \tag{B.11}$$

(ii) We may assume that $p_3 = \langle(0, \beta', \gamma', 0)\rangle$ with $\gamma' = k'\beta'$ and $\beta' = a'\pi + \pi^q$ for some $k', a' \in K$. Then $(a + a')(k + k')T(\pi\pi^q) = T(\beta\gamma' + \gamma\beta') \neq 0$ since p_2 and p_3 are not perpendicular. Then $a \neq a'$, and the two versions of (B.11) imply that

$$v = \frac{k + k'}{a + a'} \frac{T(\pi^{1+q})}{N(\pi)}, \quad u = k + \frac{k + k'}{a + a'}\left(a + \frac{T(\pi^{2q+q^2})}{N(\pi)}\right), \tag{B.12}$$

which proves (ii). □

Example B.13. (i) If $\mathcal{S} \subseteq \{\langle(0, 0, \pi, 0)\rangle, \langle(0, a\pi + \pi^q, a^2\pi + a\pi^q, 0)\rangle \mid a \in K, a^2 + a + 1 \neq 0\}$, then

$$\left|\bigcap_{p\in\mathcal{S}} p^\perp \cap \Omega\right| = \begin{cases} q^2 + 1 & \text{if} \quad |\mathcal{S}| = 1 \\ 2q & \text{if} \quad |\mathcal{S}| = 2 \\ q + 2 & \text{if} \quad |\mathcal{S}| \geq 3. \end{cases}$$

(ii) If $\mathcal{S} \subseteq \{\langle(0, 0, \pi, 0)\rangle, \langle(0, \pi^q, 0, 0)\rangle, \langle(0, \pi + \pi^q, \pi + \pi^q, 0)\rangle, \langle(0, a\pi + \pi^q, a^3\pi + a^2\pi^q, 0)\rangle\}$ for an arbitrary $a \in K - \{0, 1\}$ such that $a^2 + a + 1 \neq 0$, then

$$\left|\bigcap_{p\in\mathcal{S}} p^\perp \cap \Omega\right| = \begin{cases} q^2 + 1 & \text{if} \quad |\mathcal{S}| = 1 \\ 2q & \text{if} \quad |\mathcal{S}| = 2 \\ q + 2 & \text{if} \quad |\mathcal{S}| = 3 \\ q + 1 & \text{if} \quad |\mathcal{S}| = 4. \end{cases}$$

Proof. All of the stated points are ordinary. Since $|p^\perp \cap \Omega| = q^2 + 1$ [15, p. 1204], we will assume that $|\mathcal{S}| \geq 2$.

(i) In (B.10), $k = a$ for all listed points other than $\langle(0, 0, \pi, 0)\rangle$. By (B.12), $t = \frac{T(\pi^{2q+q^2})}{N(\pi)} + \frac{T(\pi^{1+q})}{N(\pi)}\pi$ is in every intersection (which is easily checked directly); so is Ω_0, so that every intersection has size $\geq q + 2$. Since any intersection of three sets $p^\perp \cap \Omega$ has size $q + 2$ (by Lemma B.8(ii)), so does any intersection of at least four such sets.

(ii) The last three of these four ordinary points correspond to the pairs $(a, k) = (0, 0), (1, 1), (a, a^2)$ in (B.10). Then (B.12) and different 3-sets in $\mathcal{S}$ produce different values of v, so that $|\bigcap_{p\in\mathcal{S}} p^\perp \cap \Omega| = q + 1$ if $|\mathcal{S}| = 4$. The remaining sizes are given in Lemma B.8. □

C Suzuki–Tits ovoids: background

We will need information concerning a Suzuki–Tits ovoid Ω in an $O(5,q)$-space U with radical r, where $q = 2^{2e+1}$. The standard view of these ovoids is in symplectic space. For our purposes, the view from an $O(5,q)$-space has advantages, such as lying in an $O^+(8,q)$-space.

Let $\bar{\Omega}$ denote a standard Suzuki–Tits ovoid in the symplectic 4-space U/r [31]. If $\langle x, r\rangle/r \in \bar{\Omega}$ then the line $\langle x, r\rangle$ has a unique singular point. Thus, there is a set Ω of q^2+1 singular points of U that projects onto $\bar{\Omega}$. The group $Sz(q)$ lifts from a subgroup of $Sp(4,q)$ to a group $G < O(5,q)$ preserving Ω.

See [10, Section 6.4] for information concerning the inversive plane $\mathfrak{I}(\Omega)$ produced by Ω.

We will assume that $q > 2$. Then $U = \langle\Omega\rangle$ since G does not act on an $O^{\pm}(4,q)$-space. (If $q = 2$ then Ω spans an $O^-(4,2)$-space.)

Lemma C.1. *Every hyperplane meets Ω. More precisely, there are exactly five G-orbits of hyperplanes H of U:*

(i) *Tangent hyperplanes $H = p^\perp$ for $p \in \Omega$, with $r \in H$ and $H \cap \Omega = \{p\}$;*

(ii) *Secant hyperplanes $H = x^\perp$ containing r, where x is a singular point not in Ω, $x^\perp \cap \Omega$ is a circle of $\mathfrak{I}(\Omega)$ and $\langle x^\perp \cap \Omega\rangle = x^\perp$;*

(iii) *$O^-(4,q)$-hyperplanes H for which $H \cap \Omega$ is an orbit of a cyclic subgroup of G of order $|H \cap \Omega| = q \pm \sqrt{2q} + 1$ acting irreducibly on U/r; and*

(iv) *$O^+(4,q)$-hyperplanes H for which $H \cap \Omega$ contains an orbit of a cyclic subgroup of G of order $|H \cap \Omega| - 2 = q - 1$ that fixes two points of $H \cap \Omega$. Moreover, $H \cap \Omega$ is not one of the circles in* (ii).

Proof. (i) Projecting mod r shows that each point of Ω behaves as stated.

(ii) If x is a singular point not in Ω then each of the $q+1$ t.s. lines on x meets Ω since Ω is an ovoid, so that $|x^\perp \cap \Omega| = q+1$. Also, $\dim\langle x^\perp \cap \Omega\rangle = 4$, as otherwise $x^\perp \cap \Omega$ would project into a plane of U/r, and hence be contained in a conic, which is not the case since $q > 2$ [30, pp. 51–52]. Since $\langle x^\perp \cap \Omega\rangle$ lies in the 4-space $x^\perp$, these subspaces coincide.

(iii) This is [2, Theorem 1(a)].

(iv) The set of singular points of H is partitioned by $q+1$ t.s. lines, and each t.s. line of U meets Ω since Ω is an ovoid. Thus, $|H \cap \Omega| = q+1$.

We use the orbits of G to find G_H. There are exactly two point-orbits on U/r: $\bar{\Omega}$ and the remaining $q(q^2+1)$ points. There is a subgroup of G of order $q-1$ that fixes four points of U/r and induces all scalars on each of these 1-spaces [14, p. 183]. Since each line containing r has a unique singular point, the two point-orbits on U/r produce four point-orbits on $U - \{r\}$.

Since G has five point-orbits it also has five hyperplane-orbits, so that all $q^2(q^2+1)/2$ hyperplanes H in (iv) lie in an orbit. Then $|G_H| = |G|/[q^2(q^2+1)/2] = 2(q-1)$, so that G_H is dihedral of order $2(q-1)$, with orbits of size 2 and $q-1$ on Ω [25, Theorem 9].

For the final assertion, if $H \cap \Omega$ lies in two hyperplanes then it is in a plane, and hence is a conic, whereas in (ii) we already saw that $\langle x^\perp \cap \Omega\rangle = x^\perp$. □

Remarks C.2. Finally, we collect elementary properties of the group T appearing in Lemma C.1(iv). Consider the action of $G = Sz(q)$ on Ω.

(i) The stabilizer of a circle has order $q(q-1)$ [25, Theorem 9] and fixes a unique point c. Here G_c is a Frobenius group of order $q^2(q-1)$.

(ii) A subgroup T of order $q-1$ fixes two points $c, d \in \Omega$ and has $q+1$ other orbits on Ω of size $q-1$.

If $1 \neq t \in T$ then t fixes exactly two circles: it lies in a unique subgroup of order $q(q-1)$ of the Frobenius group G_c (or G_d). If C is either of these circles then T is transitive on $C - \{c, d\}$.

References

[1] B. Bagchi, N. S. Narasimha Sastry, Even order inversive planes, generalized quadrangles and codes. *Geom. Dedicata* **22** (1987), 137–147. MR877206 Zbl 0609.51011

[2] B. Bagchi, N. S. Narasimha Sastry, Intersection pattern of the classical ovoids in symplectic 3-space of even order. *J. Algebra* **126** (1989), 147–160. MR1023290 Zbl 0685.51006

[3] S. Ball, On ovoids of O(5, q). *Adv. Geom.* **4** (2004), 1–7. MR2155360 Zbl 1039.51004

[4] A. R. Calderbank, P. J. Cameron, W. M. Kantor, J. J. Seidel, Z_4-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets. *Proc. London Math. Soc.* (3) **75** (1997), 436–480. MR1455862 Zbl 0916.94014

[5] M. Cimráková, S. De Winter, V. Fack, L. Storme, On the smallest maximal partial ovoids and spreads of the generalized quadrangles $W(q)$ and $Q(4, q)$. *European J. Combin.* **28** (2007), 1934–1942. MR2344978 Zbl 1126.51005

[6] K. Coolsaet, J. De Beule, A. Siciliano, The known maximal partial ovoids of size $q^2 - 1$ of $Q(4, q)$. *J. Combin. Des.* **21** (2013), 89–100. MR3011983 Zbl 1273.05024

[7] B. N. Cooperstein, Hyperplane sections of Kantor's unitary ovoids. *Des. Codes Cryptogr.* **23** (2001), 185–195. MR1830940 Zbl 0986.51004

[8] A. Cossidente, On twisted tensor product group embeddings and the spin representation of symplectic groups: The case q odd. International Scholarly Research Notices Geometry (2011), Article 694605.

[9] W. v. Dam, M. Howard, Bipartite entangled stabilizer mutually unbiased bases as maximum cliques of Cayley graphs. *Phys. Rev. A* **84** (2011) 012117.

[10] P. Dembowski, *Finite geometries*. Springer 1968. MR0233275 Zbl 0159.50001

[11] J. F. Dillon, *Elementary Hadamard Difference-Sets*. PhD thesis, Univ. of Maryland 1974. MR2624542 Zbl 0346.05003

[12] R. H. Dye, Partitions and their stabilizers for line complexes and quadrics. *Ann. Mat. Pura Appl.* (4) **114** (1977), 173–194. MR0493729 Zbl 0369.50012

[13] M. Grassl, Unextendible sets of mutually unbiased bases (MUBs). Talk at "Systems of Lines, Applications of Algebraic Combinatorics", Conference at Worcester Polytechnic Institute, August 10–14, 2015.

[14] B. Huppert, N. Blackburn, *Finite groups. III*. Springer 1982. MR662826 Zbl 0514.20002

[15] W. M. Kantor, Ovoids and translation planes. *Canad. J. Math.* **34** (1982), 1195–1207. MR675685 Zbl 0467.51004

[16] W. M. Kantor, Codes, quadratic forms and finite geometries. In: *Different aspects of coding theory* (*San Francisco, CA,* 1995), volume 50 of *Proc. Sympos. Appl. Math.*, 153–177, Amer. Math. Soc. 1995. MR1368640 Zbl 0867.94036

[17] W. M. Kantor, MUBs inequivalence and affine planes. *J. Math. Phys.* **53** (2012), 032204. MR2798212 Zbl 1274.46059

[18] W. M. Kantor, M. E. Williams, Symplectic semifield planes and $\mathbb{Z}_4$-linear codes. *Trans. Amer. Math. Soc.* **356** (2004), 895–938. MR1984461 Zbl 1038.51003

[19] G. Lunardon, Partial ovoids and generalized hexagons. In: *Finite geometry and combinatorics* (*Deinze,* 1992), volume 191 of *London Math. Soc. Lecture Note Ser.*, 233–248, Cambridge Univ. Press 1993. MR1256280 Zbl 0792.51005

[20] P. Mandayam, S. Bandyopadhyay, M. Grassl, W. K. Wootters, Unextendible mutually unbiased bases from Pauli classes. *Quantum Inf. Comput.* **14** (2014), 823–844. MR3242270

[21] T. Penttila (unpublished).

[22] T. Penttila, B. Williams, Ovoids of parabolic spaces. *Geom. Dedicata* **82** (2000), 1–19. MR1789057 Zbl 0969.51008

[23] V. Pepe, C. Röβing, L. Storme, A spectrum result on maximal partial ovoids of the generalized quadrangle $\mathcal{Q}(4, q)$, q odd. In: *Finite fields: theory and applications*, volume 518 of *Contemp. Math.*, 349–362, Amer. Math. Soc. 2010. MR2648559 Zbl 1235.51014

[24] C. Röβing, L. Storme, A spectrum result on maximal partial ovoids of the generalized quadrangle $Q(4, q)$, q even. *European J. Combin.* **31** (2010), 349–361. MR2552614 Zbl 1190.51005

[25] M. Suzuki, On a class of doubly transitive groups. *Ann. of Math.* (2) **75** (1962), 105–145. MR0136646 Zbl 0106.24702

[26] D. E. Taylor, *The geometry of the classical groups*. Heldermann 1992. MR1189139 Zbl 0767.20001

[27] J. A. Thas, Old and new results on spreads and ovoids of finite classical polar spaces. In: *Combinatorics '90* (*Gaeta,* 1990), volume 52 of *Ann. Discrete Math.*, 529–544, North-Holland 1992. MR1195834 Zbl 0767.51004

[28] K. Thas, Unextendible mutually unbiased bases (after Mandayam, Bandyopadhyay, Grassl and Wootters). *Entropy* **18** (2016), 395. arXiv:1402.2778v1 [quant-ph]

[29] J. Tits, Sur la trialité et certains groupes qui s'en déduisent. *Inst. Hautes Études Sci. Publ. Math.* no. **2** (1959), 13–60. MR1557095 Zbl 0088.37204

[30] J. Tits, Ovoïdes à translations. *Rend. Mat. e Appl.* (5) **21** (1962), 37–59. MR0143086 Zbl 0107.38103

[31] J. Tits, Ovoïdes et groupes de Suzuki. *Arch. Math.* **13** (1962), 187–198. MR0140572 Zbl 0109.39402