AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **66(2)** (2016), Pages 205–210

Cyclic elliptic spreads

William M. Kantor

Brookline
MA 02445
U.S.A.
kantor@uoregon.edu

Abstract

Moderately large numbers of transitive elliptic spreads are constructed in characteristic 2 and dimension $\equiv 2 \pmod 4$.

1 Introduction

If V is an orthogonal vector space, an *orthogonal spread* is a set of maximal totally singular subspaces such that every nonzero singular vector is in a unique member of the set. Throughout this note q will denote a power of 2. Dillon [4], and later also Dye [5], showed that $O^-(2m,q)$-spaces and $O(2m-1,q)$-spaces have orthogonal spreads for all $m \geq 2$, and that $O^+(2m,q)$-spaces have orthogonal spreads if and only if m is even. Moreover, the $O^+(2m,q)$-spreads and $O(2m-1,q)$-spreads constructed in [4, 5] are permuted 3-transitively by isometry groups isomorphic to $\mathrm{PSL}(2,q^{m-1})$, which is not the case for the $O^-(2m,q)$-spreads in [4, 5] when $m > 2$ (see Example 3.1 below). The fact that the various orthogonal spreads in those papers admit transitive cyclic groups of isometries is implicit in their constructions (see [7, 8] and Example 3.1). Much of the small literature on elliptic spreads (i. e., $O^-(2m,q)$-spreads) has focused on existence in large dimensions (citing [5]; cf. Example 3.2 below) or examples in dimension 6 behaving "nicely" (as in [3, 2]).

This note is concerned with large-dimensional examples, requiring information from [8] to obtain many $O^-(2m,q)$-spreads admitting transitive cyclic groups of isometries when $m > 1$ is odd (although "many" is rather small compared to the numbers obtained in related research on semifields [9]). Equivalence of elliptic spreads is defined at the end of the next section.

Theorem 1.1. *Let $m > 1$ be odd and let q be a power of 2. Let $m, m_1, \ldots, m_{n-1}$ be any sequence of $n \geq 1$ distinct divisors > 1 of m with each divisible by the next. Then there are at least $\big(\prod_1^{n-1}(q^{m_i}+1)\big)/2m_1\log_2 q$ pairwise inequivalent $O^-(2m,q)$-spreads each of which is permuted transitively by a cyclic group of isometries.*

We will see that this result is closely tied to results in [8]. Such a sequence (m_i) can be obtained from the prime factorization $m = \prod_1^n p_j$ of m by setting $m_i = \prod_{i+1}^n p_j$.

In particular, we obtain at least $q^{m/p}/2(m/p)\log_2 q$ inequivalent elliptic spreads when p is the smallest prime dividing m.

The desirability of having examples of transitive orthogonal spreads can be seen from [1]. There are analogous results in [8] producing many $O^+(2m,q)$-spreads and $O(2m-1,q)$-spreads.

2 Background

We refer to [12] for the standard properties of the orthogonal and symplectic 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. In characteristic 2, an orthogonal vector space is also a symplectic space, and t.s. subspaces are also t.i. subspaces.

Orthogonal spreads were defined earlier. For the $O^-(2m,q)$-spaces considered here, an orthogonal spread consists of q^m+1 t.s. $m-1$-spaces, and is also called an *elliptic spread.* A *symplectic spread* is a set of maximal t.i. subspaces of a symplectic space such that every nonzero vector is in a unique member of the set.

Two orthogonal or symplectic spreads are *equivalent* if there is an isomorphism of the underlying orthogonal or symplectic geometries sending one spread to the other. The automorphism group of an orthogonal or symplectic spread is the group of such isomorphisms of the spread with itself.

3 Examples

Let $F^{(2)}=\mathbb{F}_{q^{2m}}\supset F=\mathbb{F}_{q^m}\supset K=\mathbb{F}_q$ for $m\ge 2$, with involutory field automorphism $x\mapsto\bar{x}$. Let $W:=\ker T$ for the trace map $T\colon F\to K$.

The quadratic form $Q(x):=T(x\bar{x})$ turns $F^{(2)}$ into an orthogonal K-space with associated alternating bilinear form $(x,y):=T(x\bar{y}+\bar{x}y)$. The subspace W is t.s.: if $w\in W$ then $Q(w)=T(w\bar{w})=T(w)^2=0$.

Write $\mathrm{C}:=\{\theta\in F^{(2)}\mid\theta\bar{\theta}=1\}$, so that $F^{(2)*}=F^*\times\mathrm{C}$. If $\theta\in\mathrm{C}$ then $\widetilde{\theta}\colon x\mapsto x\theta$ defines an isometry of the orthogonal space $F^{(2)}$ (since $T(\theta x\overline{\theta x})=T(\theta\bar{\theta}x\bar{x})=T(x\bar{x})$). The occurrence of a group $\widetilde{\mathrm{C}}$ of these q^m+1 isometries makes it clear that $F^{(2)}$ is an $O^-(2m,q)$-space: its singular points form an elliptic quadric. Moreover, W is a maximal t.s. subspace since $\dim W=m-1$.

Example 3.1. The set $F^{\widetilde{\mathrm{C}}}$ is the usual desarguesian spread. Moreover, $W^{\widetilde{\mathrm{C}}}$ is an elliptic spread (as in [4] and [5]) permuted transitively by the cyclic isometry group $\widetilde{\mathrm{C}}$: the members of $W^{\widetilde{\mathrm{C}}}$ intersect pairwise in 0, and its union has size $1+(q^m+1)(q^{m-1}-1)$, which is the number of singular vectors. In view of [1, Theorem 1.1], if $m>2$ then the automorphism group of $W^{\widetilde{\mathrm{C}}}$ normalizes $\widetilde{\mathrm{C}}$.

In dimension $2m = 6$ the Klein correspondence produces an ovoid from $W^{\widetilde{\mathrm{C}}}$ that is constructed in an entirely different manner and studied in detail in [3]. These examples are equivalent by [3, Theorem 1.1], and the automorphism group appears in [3, Theorem 3.1].

Example 3.2. Let Σ be any symplectic spread in an $\mathrm{Sp}(2m, q)$-space V. There are many different ways that V can be equipped with the structure of an $O^-(2m, q)$-space producing the given symplectic structure. Choose one of them. We emphasize that this orthogonal structure is not related to Σ.

If $X \in \Sigma$ let X' be the set of singular vectors in X. Then X' is a t.s. $(m-1)$-space (since the quadratic form $Q|_X : X \to K$ is semilinear on the t.i. subspace X), and $\{X' \mid X \in \Sigma\}$ is an orthogonal spread of the orthogonal space V.

This presumably produces reasonably large numbers of inequivalent elliptic spreads starting from a single symplectic spread. However, in the next section we will proceed differently, using inequivalent symplectic spreads. Most of the *known* symplectic spreads in characteristic 2 are the ones in Example 3.1 or are obtained by a process described in [7, 8, 9]; examples are in the next section. The only other known types arise from the Suzuki groups [10], are in $\mathrm{Sp}(4m, 2^e)$-spaces for odd m and e, and again produce elliptic spreads.

4 Moderately large numbers of elliptic spreads

The following notation is based on [8]. Let $F^{(2)} \supset F = F_0 \supset \cdots \supset F_n = \mathbb{F}_q$ be a tower of fields with $m := [F : F_n]$ odd and corresponding trace maps $T_i : F \to F_i$. Write $W_i := \ker(T_{i+1}\big|_{F_i})$. Since m is odd, $T_n(1) = 1$ and $T_n T_i(x) = T_n(x)$ for all i and all $x \in F$. For each i let $F_i^{(2)}$ be the subfield of $F^{(2)}$ of degree 2 over F_i.

View $V := F^{(2)}$ as an $O^-(2m, q)$-space with associated quadratic form $Q_n(x) := T_n(x\overline{x})$. Then V is also a symplectic space, with alternating bilinear form $(x, y)_n := T_n(x\overline{y} + \overline{x}y)$. Let C and $\widetilde{\mathrm{C}}$ be as before.

Let $\zeta_0 = 1$ and $1 \neq \zeta_i \in \mathrm{C} \cap F_i^{(2)}$ for $i \geq 1$. Write $\gamma_i := \prod_0^i \zeta_j$, $0 \leq i \leq m-1$, and

$$\mathcal{S}\big((F_i)_0^n, (\zeta_i)_0^n\big) := \big\{ \big(\sum_0^{n-1} W_i \gamma_i + F_n \gamma_n \big)\theta \mid \theta \in \mathrm{C} \big\}. \tag{4.1}$$

By [8, Theorems 4.3 and 5.2] (cf. [6, pp. 565–617]),

(a) *$\mathcal{S}\big((F_i)_0^n, (\zeta_i)_0^n\big)$ is a symplectic spread of the F_n-space V, and $\widetilde{\mathrm{C}}$ acts transitively on this spread*; and

(b) *For $\big((F_i)_0^n, (\zeta_i)_0^n\big)$ and $\big((F_i')_0^{n'}, (\zeta_i')_0^{n'}\big)$ as above, if the associated symplectic spreads are equivalent then $n' = n$, $F_i' = F_i$ and $\zeta_i' = \zeta_i^\sigma$ for some $\sigma \in \mathrm{Aut}F^{(2)}$ and all i.*

We use (a), and parts of the proof of (b) in [8], to prove the following result, which implies Theorem 1.1:

Theorem 4.2. *For odd $m > 1$, even $q^m > 8$ and $\big((F_i)_0^n, (\zeta_i)_0^{n-1}\big)$ as above,*

(i) $\Sigma\big((F_i)_0^n, (\zeta_i)_0^{n-1}\big) := \big\{\big(\sum_0^{n-1} W_i\gamma_i\big)\theta \mid \theta \in \mathrm{C}\big\}$ *is an $O^-(2m,q)$-spread of the F_n-space V equipped with the quadratic form Q_n, and $\widetilde{\mathrm{C}}$ is a group of isometries acting transitively on this elliptic spread, and*

(ii) $\Sigma\big((F_i)_0^n, (\zeta_i)_0^{n-1}\big)$ *and* $\Sigma\big((F'_i)_0^{n'}, (\zeta'_i)_0^{n'-1}\big)$ *are equivalent if and only if $n' = n$, $F'_i = F_i$ and $\zeta'_i = \zeta_i^\sigma$ for some $\sigma \in \mathrm{Aut}F^{(2)}$ and all i.*

Proof. (i) By Example 3.2 together with theorem (a) stated above, it suffices to verify that $\sum_0^{n-1} W_i\gamma_i$ is a t.s. F_n-space. This subspace is a hyperplane of the t.i. F_n-space $\sum_0^{n-1} W_i\gamma_i + F_n\gamma_n$; we will show that it is the set of Q_n-singular vectors of that F_n-space. If $w_i \in W_i$, $0 \le i \le m-1$, then $Q_n(w_i\gamma_i) = T_n(w_i\gamma_i\overline{w_i\gamma_i}) = T_n(w_i^2) = T_nT_{i+1}(w_i)^2 = T_n(0)$. Thus, $\sum_0^{n-1} W_i\gamma_i$ is t.s. since it is a t.i. subspace spanned by singular vectors.

(ii) Assume that $\Sigma\big((F_i)_0^n, (\zeta_i)_0^{n-1}\big)$ and $\Sigma\big((F'_i)_0^{n'}, (\zeta'_i)_0^{n'-1}\big)$ are equivalent by a semilinear map of $F^{(2)}$ preserving the orthogonal geometry. Then that map is a semilinear isomorphism of $F^{(2)}$ as a vector space over F_n with $F^{(2)}$ as a vector space over $F_{n'}$, so that $F_n = F_{n'}$ and we have only one quadratic form Q_n to consider. (This avoids the additional trace map $F^{(2)} \to \mathbb{F}_2$ used in [8, p. 8].)

The cyclic group $\widetilde{\mathrm{C}}$ is transitive on both $\Sigma\big((F'_i)_0^{n'}, (\zeta'_i)_0^{n'-1}\big)$ and $\Sigma\big((F_i)_0^n, (\zeta_i)_0^{n-1}\big)$, so that $\Sigma\big((F'_i)_0^{n'}, (\zeta'_i)_0^{n'-1}\big) = \Sigma\big((F_i)_0^n, (\zeta_i)_0^{n-1}\big)^\sigma$ for some $\sigma \in \mathrm{Aut}F^{(2)}$ by the exact same Sylow argument as in [8, proof of Theorem 5.2]. This equality of sets implies that $n' = n$ and $\zeta'_i = \zeta_i^\sigma$ for some $\sigma \in \mathrm{Aut}F^{(2)}$ and all i as in [8, Lemma 5.3]. (More precisely, what is needed is the bookkeeping proof of that lemma but with all references to γ_n and $\gamma'_{n'}$ deleted.)

The converse is trivial. □

Remark 4.3. As in [8], the classification of the finite simple groups was not needed for dealing with elliptic spread equivalence. However, in view of [1] the automorphism group of $\Sigma\big((F_i)_0^n, (\zeta_i)_0^{n-1}\big)$ is a 1-dimensional semilinear group: the semidirect product of $\widetilde{\mathrm{C}} \times F_n^*$ with the stabilizer in $\mathrm{Aut}F^{(2)}$ of all ζ_i.

Remarks 4.4. A symplectic spread in an $O^-(2n,q)$-space produces an elliptic spread (Example 3.2). However, comparing (4.1) and the results following it with Theorem 4.2 shows that the same elliptic spread can arise from many inequivalent symplectic spreads by using different choices for ζ_n.

This observation should be compared with [7] and various sequels (such as [8, 9]). Those papers are based on the fact that a symplectic spread in an $\mathrm{Sp}(2m,q)$-space (with m odd and q even) produces an essentially unique orthogonal spread in an

$O^+(2m+2,q)$-space, while an orthogonal spread in an $O^+(2m+2,q)$-space produces many inequivalent symplectic spreads and hence many affine planes.

Remark 4.5. Is there any way to decide whether or not a given elliptic spread Σ in an $O^-(2n,q)$-space "extends" to a symplectic spread? In other words, is there a way to know from properties of Σ that, for each $X \in \Sigma$, it is possible to choose a t.i. subspace $\hat{X} \supset X$ so that the set of these $\hat{X}$ is a symplectic spread?

We used the cyclic group $\widetilde{\mathrm{C}}$ as a crutch for this purpose. Such choices presumably do not arise for the large numbers of $O^-(6,q)$-spreads obtained from a "derivation" process [3, 2]. Moreover, although we deal with large dimensions, the number of elliptic spreads we obtain in an orthogonal space of fixed dimension is tiny compared to the number obtained by derivation in an $O^-(6,q)$-space.

Corrections. 1. Alan Prince has observed that [8, Theorem 1.1] needs to be modified slightly by deleting the word "nondesarguesian". As it stands, that theorem states that there are more than 5/4 nondesarguesian flag-transitive planes of order 64, whereas there is only one such plane [11] (constructed in [8]).

2. In [8, Remark 6.6] it states that the affine planes obtained in that paper are *precisely the flag-transitive scions of the desarguesian plane of order* q^m; here "scions" refer to planes obtained by a recursive "up and down process" described in [8, 9]. That remark should have continued with the assumption that these scions were *obtained by retaining flag-transitivity throughout the up and down process.* Retaining flag-transitivity is needed for the inductive argument in that remark. Otherwise, however unlikely it may seem, this up and down process could magically produce a spread having unexpected automorphisms.

Acknowledgements

This research was supported in part by a grant from the Simons Foundation through Northeastern University.

References

[1] J. Bamberg and T. Penttila, A classification of transitive ovoids, spreads, and m-systems of polar spaces, *Forum Math.* 21 (2009), 181–216.

[2] A. Cossidente and G. L. Ebert, Permutable polarities and a class of ovoids of the Hermitian surface, *Europ. J. Combin.* 25 (2004), 1059–1066.

[3] A. Cossidente and G. Korchmáros, Transitive ovoids of the Hermitian surface of $\mathrm{PG}(3,q^2)$, q even, *J. Combin. Theory Ser. A* 101 (2003), 117–130.

[4] J. F. Dillon, *Elementary Hadamard difference sets.* Ph.D. Thesis, University of Maryland, 1974.

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

[6] N. L. Johnson, V. Jha and M. Biliotti, *Handbook of finite translation planes*, Chapman & Hall/CRC, Boca Raton, FL 2007.

[7] W. M. Kantor, Spreads, translation planes and Kerdock sets I, *SIAM J. Algebraic and Discrete Methods* 3 (1982), 151–165.

[8] W. M. Kantor and M. E. Williams, New flag-transitive affine planes of even order, *J. Combin. Theory Ser. A* 74 (1996), 1–13.

[9] W. M. Kantor and M. E. Williams, Symplectic semifield planes and $\mathbb{Z}_4$-linear codes, *Trans. AMS* 356 (2004), 895–938.

[10] H. Lüneburg, *Die Suzukigruppen und ihre Geometrien*, Springer, Berlin-New York 1965.

[11] A. R. Prince, Flag-transitive affine planes of order 64, *Des. Codes Crypto.* 18 (1999), 217–221.

[12] D. E. Taylor, *The geometry of the classical groups*, Heldermann, Berlin, 1992.

(Received 4 Dec 2015)