Orthogonal spreads and translation planes

William M. Kantor[*]
University of Oregon

Abstract

There have been a number of striking new results concerning translation planes of characteristic 2, obtained using orthogonal and symplectic spreads. The impetus for this came from coding theory. This paper surveys the geometric advances, while providing a hint of their coding–theoretic connections.

1. Introduction

Spreads are familiar in finite geometry since they produce translation planes (cf. Section 3.1 below). Orthogonal and symplectic spreads are less familiar. They have an underlying additional structure, produced by a quadratic form or an alternating bilinear form on the vector space. When the field is $\mathbb{Z}_2$ they also produce Kerdock codes over $\mathbb{Z}_2$ and $\mathbb{Z}_4$. This note summarizes results that are more than 10 years old, while setting the stage for a discussion of new advances.

2. Orthogonal spreads

Let $V = \mathrm{GF}(q)^{2n} = X \oplus Y$ for subspaces X and Y both of which are identified with $\mathrm{GF}(q)^n$. Equip V with the quadratic form Q defined by $Q(x, y) = x \cdot y$ (using the usual dot product on $\mathrm{GF}(q)^n$); this form is nonsingular, with isometry group $\mathrm{O}^+(2m, q)$ and associated symmetric bilinear form (,). Then V has $(q^n - 1)(q^{n-1} + 1)$ nonzero singular vectors and each totally singular n–space (such as X and Y) contains $q^n - 1$ nonzero singular vectors. This suggests that there might be families of $q^{n-1} + 1$ totally singular n–spaces that partition the set of all nonzero singular vectors; such a family is called an *orthogonal spread. We will assume that q is even* and see that such a family cannot exist unless n is even, in which case there is always at least one orthogonal spread.

2.1. Matrices

Fix a basis $x_1, \ldots, x_n$ of X and let $y_1, \ldots, y_n$ be the dual basis of Y: $(x_i, y_j) = \delta_{ij}$. Write matrices with respect to the basis $x_1, \ldots, x_n, y_1, \ldots, y_n$. It is easy to check that the group $\mathrm{O}^+(2n, q)_{(Y)}$ of isometries of V that fix every vector of Y consists of those linear transformations whose matrices are $\begin{pmatrix} I & M \\ O & I \end{pmatrix}$ for some skew–symmetric $n \times n$ matrix M over $GF(q)$

[*] This paper was written during a visit to RIMS in Kyoto University, whose hospitality is gratefully acknowledged.

(in characteristic 2, "skew–symmetric" means "symmetric with 0 diagonal"); $\mathrm{O}^+(2n,q)_{(Y)}$ is isomorphic to the vector space of all skew–symmetric $n \times n$ matrices over $GF(q)$, and is regular on the set of totally singular n–spaces Z such that $Y \cap Z = 0$.

Note that $\dim X\left(\begin{smallmatrix} I & M \\ O & I \end{smallmatrix}\right) \cap X\left(\begin{smallmatrix} I & N \\ O & I \end{smallmatrix}\right) = n - \mathrm{rank}(M - N)$. In particular, if two such totally singular n–spaces meet only at 0, then n must be even (since $M - N$ is skew–symmetric). There is another view of this parity remark: the totally singular n–spaces fall into two families such that two such subspaces are in the same family if and only if the dimension of their intersection has the same parity as n, so that there can be three such subspaces pairwise having only 0 in common only if n is even.

It is now straightforward to prove

Proposition 2.1. (i) *If Σ is an orthogonal spread of V that contains both X and Y, then*

$$\Sigma \colon = \{Y\} \bigcup \left\{ X\begin{pmatrix} I & M \\ O & I \end{pmatrix} \;\middle|\; M \in \mathcal{K} \right\}$$

for a set $\mathcal{K}$ of $n \times n$ skew–symmetric matrices, containing O, and such that the difference of any two is nonsingular (a **Kerdock set** *of matrices).*

(ii) *Conversely, if $\mathcal{K}$ is a Kerdock set of $n \times n$ skew–symmetric matrices, then the set Σ defined in* (i) *is an orthogonal spread of V that contains both X and Y.*

Of course, since $\mathrm{O}^+(2n,q)$ is transitive on the ordered pairs of totally singular n–spaces having intersection 0, the restriction in (i) is insignificant.

Definition 2.2. Kerdock sets $\mathcal{K}_1$ and $\mathcal{K}_2$ are *equivalent* if $A^t\mathcal{K}_1^\tau A + M = \mathcal{K}_2$ for some $A \in \mathrm{GL}(n,q)$, some skew–symmetric matrix M, and some field automorphism τ. Orthogonal spreads Σ_1 and Σ_2 are *equivalent* if there is an element of $\Gamma\mathrm{O}(V)$ sending Σ_1 to Σ_2. (Here, $\Gamma\mathrm{O}(V)$ is the set of semilinear maps g on V that preserve Q projectively: $Q(vg) = aQ(v)^\tau$ for some $a \in K^*$, some $\tau \in \mathrm{Aut}K$ and all $v \in V$.)

Evidently, in Proposition 2.1(ii), Σ depends on $\mathcal{K}$. It turns out that it is straightforward to determine more about the interdependence of Σ and $\mathcal{K}$:

Proposition 2.3. *Let $\mathcal{K}_1$ and $\mathcal{K}_2$ be Kerdock sets of $n \times n$ matrices over* $\mathrm{GF}(q)$. *Then the following are equivalent:*

(i) *$\mathcal{K}_1$ and $\mathcal{K}_2$ are equivalent;*

(ii) *The orthogonal spreads Σ_1 and Σ_2 of V, determined by $\mathcal{K}_1$ and $\mathcal{K}_2$ via* Proposition 2.1, *are equivalent by an element of $\Gamma\mathrm{O}(V)$ sending Y to itself.*

It is easy to deduce that there are many choices of inequivalent Kerdock sets that produce equivalent orthogonal spreads.

2.2. To symplectic spreads

Let z denote any nonsingular point (1–space) of V: $Q(z) \neq 0$. If Σ is any orthogonal spread of V, then n is even and

$$\{\, Z \cap z^\perp \mid Z \in \Sigma \,\}$$

is a family of totally singular $n-1$–spaces of $z^\perp$ that partitions the set of nonzero singular vectors.

Since the characteristic is 2, z is contained in the hyperplane $z^\perp$. The $2n-2$–space $z^\perp/z$ is turned into a symplectic space using the inherited alternating bilinear form $(u+z, v+z) := (u, v)$ (for $u, v \in z^\perp$). Then

$$\Sigma_z := \{\langle Z \cap z^\perp, z\rangle/z \mid Z \in \Sigma\}$$

is a family of $|\Sigma| = q^{n-1}+1$ *totally isotropic* $n-1$*–spaces of* $z^\perp/z$ *that partitions the set of nonzero singular vectors.* Such a family is called a *symplectic spread* of the symplectic space $z^\perp/z$. (N.B.—There is no quadratic form inherited by $z^\perp/z$.)

2.3. From symplectic spreads

The preceding construction can be reversed, proceeding from symplectic spreads to orthogonal ones.

Namely, let m be odd, and start with a symplectic space V' of dimension $2m$ over $GF(q)$ together with a symplectic spread Σ' in it. If $m = n-1$ then we can identify V' with the symplectic space $z^\perp/z$ arising, as above, from the orthogonal space V and one of its nonsingular points z. Each totally isotropic subspace of V' is the projection, mod z, of a unique totally singular subspace of $z^\perp/z$. In particular, Σ' arises from a family

$$\Sigma'^{\uparrow} := \{U \mid \langle U, z\rangle/z \in \Sigma'\}$$

of totally singular $n-1$–spaces of $z^\perp$ such that each nonzero vector of $z^\perp/z$ lies in just one of its members.

Finally, each totally singular $n-1$–space of $z^\perp$ lies in exactly two totally singular n–spaces of V, one from each family. Pick a family $\mathcal{M}$ of such n–spaces, and let

$$\Sigma := \{Z \mid Z \in \mathcal{M} \text{ and } Z \text{ contains a member of } \Sigma'^{\uparrow}\}.$$

Then Σ *is an orthogonal spread of* V*, and* $\Sigma_z = \Sigma'$. Note that this passage from symplectic to orthogonal spreads is essentially unique: it only depends on the choice of the family $\mathcal{M}$. (Moreover, the nontrivial orthogonal transvection with center z interchanges $\mathcal{M}$ with the other family while leaving Σ' unchanged.)

2.4. Back and forth

Starting with a symplectic spread Σ' in a $2m$–dimensional symplectic space over GF(q) with m odd, Section 2.3 produces an orthogonal spread in a $2m+2$–dimensional orthogonal space, in such a way that there is a nonsingular point z for which Σ_z is Σ'. Once we have Σ, Section 2.2 can be used to form a *different* symplectic spread Σ_{z^*} using a *different* nonsingular point z^*.

2.5. Changing fields: up and down

Iterating the procedure in Section 2.4 never produces a "new" orthogonal spread. There is a simple way to modify that procedure in order to get large numbers of new orthogonal and symplectic spreads.

Start with a symplectic spread Σ' in a $2m$–dimensional vector space V' over $K = \mathrm{GF}(q)$. Let L be any proper subfield of K over which K has odd degree, and let $T: K \to L$ be the trace map. Then $T(u,v)$ defines a nonsingular alternating L-bilinear from on the L–space V'. We can view Σ' as a family of subspaces of this L–space. It is still a spread, and each of its members is still totally isotropic with respect to the new form. Thus, *Σ' is a symplectic spread of the L–space V'*. Here, $\dim_L V' = m[K:L]$.

Now Section 2.3 can be applied, producing an orthogonal spread of a $(2m[K:L]+2)$–dimensional orthogonal L–space. In fact, Section 2.4 now gives us "new" symplectic spreads. It is a difficult problem to decide, in general, whether these spreads are actually new: conceivably some are equivalent to ones already obtained.

Up and down process. This process of *repeatedly* going from a symplectic spread over some field, changing fields, going up to an orthogonal spread and then back down to a symplectic spread, is called the *up and down process*. It is difficult to keep control over properties of these spreads. However, in important special cases control can be maintained, a surprising discovery of Williams [Wi] that will be discussed shortly (Sections 3.5–3.9).

3. Projective planes

An entirely different type of geometric view of symplectic spreads is provided by projective planes, and provides one of the principal motivations for their study. For this purpose we begin by ignoring the symplectic structure.

3.1. From spreads to projective planes

Let V' be a $2m$–dimensional vector space over $\mathrm{GF}(q)$ (no restriction is placed even on the parity of q and m).

Spreads A *spread* of V' is a family Σ' of q^m+1 subspaces of dimension m whose union is all of V'. This means that every nonzero vector is in a unique member of Σ'. *Any family of q^m+1 m–spaces in a $2m$–space, any two of which have only* 0 *in common, is a spread.* (N.B.—An orthogonal spread is not a spread in this sense, but a symplectic spread is.)

Example 3.1. If V' is a 2–dimensional vector space over a finite field E, its set Σ' of 1–spaces is a *desarguesian (or "regular") spread.* Note that this spread is symplectic with respect to any alternating bilinear form on V'. It is also symplectic when V' is viewed as a vector space over any subfield of E (cf. Section 2.5).

Translation planes Any spread of V' determines a *translation plane* $\mathbf{A}(\Sigma')$, an affine plane of order q^m whose points are vectors and whose lines are the cosets $W+v$ with $W\in\Sigma', v\in V'$. The plane $\mathbf{A}(\Sigma')$ corresponding to a desarguesian spread Σ' is a desarguesian plane.

Any isomorphism between two translation planes is induced by a semilinear transformation of the underlying vector spaces. See [De] for more background concerning translation planes. The transition to *projective planes* is standard: introduce a line at infinity whose points are all parallel classes of lines, in order to obtain a projective plane of order q^m.

3.2. Symplectic translation planes

Example 3.2. (Example 3.1 *continued.*) Starting with a desarguesian spread Σ' in $\mathrm{GF}(q)^{2m}$, where m is odd, by Section 2.3 we obtain an orthogonal spread Σ in $\mathrm{GF}(q)^{2m+2}$, and hence a

Kerdock set. This latter Kerdock set is the one first discovered by Kerdock [Ke] when $q = 2$ (cf. [Di] and [MS, Ch. 15 §5], among many other references).

Each orthogonal spread appears to produce large numbers of symplectic spreads Σ_z. This leads us to the isomorphism question: when are two planes $\mathbf{A}(\Sigma_z)$ obtained in this manner isomorphic? If there is a symplectic transformation sending one spread to the other, the planes are certainly isomorphic. It seems surprising that the converse is (essentially) true:

Theorem 3.3. *For $i = 1, 2$, let Σ_i be a symplectic spread in a $2m$–dimensional symplectic space V_i over $\mathrm{GF}(q)$. Let $g\colon \mathbf{A}(\Sigma_1) \to \mathbf{A}(\Sigma_2)$ be an isomorphism that sends the point 0 to the point 0. Then there is an invertible semilinear transformation $h\colon V_1 \to V_2$ such that the following hold:*

(i) $(\Sigma_1)h = \Sigma_2$,

(ii) *There is a field automorphism τ, and a nonzero scalar a, such that $(uh, vh) = a(u, v)^\tau$ $\forall u, v \in V_1$, and*

(iii) *$g^{-1}h$ fixes every member of Σ_2.*

The elementary proof is in [Ka1, I (3.5)]. The set of all nonsingular linear transformations fixing every member of Σ_2 (as in (iii)), together with 0, is a field, the *kernel* of the translation plane. It is the largest field over which the spread consists of subspaces.

The preceding theorem implies that isomorphic planes can only arise from equivalent orthogonal spreads (Definition 2.2). Moreover:

Corollary 3.4. *Two translation planes $\mathbf{A}(\Sigma_{z_1})$ and $\mathbf{A}(\Sigma_{z_2})$ arising from the same orthogonal spread Σ are isomorphic if and only if z_1 and z_2 are in the same orbit of the group $G(\Sigma)$ of all elements of $\Gamma\mathrm{O}(V)$ that preserve Σ.*

Theorem 3.3 also permits the determination of the full automorphism groups of many of these planes. The construction techniques for planes, using Kerdock sets and orthogonal and symplectic spreads, are very flexible. They have produced planes with relatively large collineation groups (Sections 3.5–3.7) as well as planes with unexpectedly small collineation groups (Section 3.8).

3.3. Prequasifields

A translation plane is usually coordinatized by an algebraic system called a *quasifield* [De]. Here it will be convenient to consider a weaker, but geometrically equivalent system, called a *prequasifield*.

Definition 3.5. Consider a binary operation $*$ on $F = \mathrm{GF}(q^m)$ related to field addition by the following conditions (for all $x, y, z \in F$):

- $(x + y) * z = x * z + y * z$, and
- $x * y = x * z \Longrightarrow x = 0$ or $y = z$.
- $x * y = 0 \iff x = 0$ or $y = 0$.

Then $(F,+,*)$ will be called a *prequasifield*. It is a *quasifield* if it has an identity element; for use with (3.6), it is preferable to delete this condition even though an identity element is readily introduced. $(F,+,*)$ is a *presemifield* if both distributive laws hold, and a *semifield* if, in addition, there is an identity element.

A translation plane is obtained by using $F \oplus F$ as point–set and letting the lines have the familiar appearance

$$\text{“}x = c\text{''} \quad \textit{and} \quad \text{“}y = x * s + b\text{''} \qquad \forall b, c, s \in F.$$

If we view F and $F \oplus F$ as vector spaces over $K = \mathrm{GF}(q)$, then the spread $\Sigma(*)$ of $F \oplus F$ associated with $(F,+,*)$ consists of the lines "$y = x * s$" through 0. We will assume that our quasifield associates with K in the following manner:

$$(kx) * s = k(x * s) \;\; \forall k \in K; \;\; x, s \in F,$$

so that $x \mapsto x * s$ is a K–linear map for each $y \in F$. Thus, K is contained in the kernel of the plane, since $(x,y) \mapsto (kx, ky)$ fixes each member "$y = x * s$" of $\Sigma(*)$ whenever $k \in K^*$.

In order to consider symplectic translation planes, we use a substitute for the dot product. The trace map $T\colon F \to K$ determines an inner product $T(xy)$ on F having an orthonormal basis that lets us identify F, equipped with this inner product, and K^m, equipped with its usual dot product.

Finally, we assume in addition that m is *odd* and that $*$ satisfies the following condition:

$$T(x(x * y)) = T(xy)^2 \;\; \forall x, y \in F. \tag{3.6}$$

One example of such a binary operation is $x * y = xy^2$; the corresponding plane is desarguesian. Soon we will present many more examples. Note that, if we had required that our prequasifield have an identity element, then we would have had to use a more complicated version of the inner product. Thus, for example, it is more convenient in the present context to use the preceding inconvenient–looking modification xy^2 of ordinary multiplication in F.

Replacing x in turn by x, z, $x + z$ in (3.6) and subtracting, we find that

$$T(x(z * y)) = T(z(x * y)) \;\; \forall x, y, z \in F\,. \tag{3.7}$$

By a simple calculation:

Proposition 3.8. *Equip $F \oplus F$ with the alternating bilinear form*

$$((x_1, y_1), (x_2, y_2))\colon = T(x_1 y_2 - x_2 y_1). \tag{3.9}$$

Then the spread $\Sigma(*)$ of $F \oplus F$ associated with a prequasifield $(F,+,*)$ is symplectic if and only if $(F,+,*)$ satisfies (3.7).

In view of this result, it may seem as if condition (3.6) is unnecessarily restrictive. When searching for examples, this may be so, but in fact it is no serious restriction at all:

Proposition 3.10. *If $(F,+,*)$ is a symplectic prequasifield, then there is a permutation μ of F such that $x \circ y\colon = x * y^\mu$ defines a prequasifield $(F,+,\circ)$ that is symplectic with respect to the same form* (3.9)*, defines the same plane, and behaves as in* (3.6).

Namely, by (3.7) for each $y \in F$ the map $x \mapsto T(x(x*y))^{1/2}$ is K–linear, so $T(x(x*y)) = T(xy^\pi)^2$ for some map $\pi: F \to F$ with $0^\pi = 0$. If π is bijective, let μ denote its inverse and note that $T(x(x*y^\mu)) = T(xy)^2$ for all x, y, in which case $x \circ y: = x * y^\mu$ behaves as required.

Suppose that π is not bijective, and let $y, z \in F$, $y \neq z$, with $y^\pi = z^\pi$. If g denotes the K–linear map $x \mapsto x*y - x*z$, then $T(xx^g) = T(x(x*y)) - T(x(x*z)) = 0\ \forall x \in F$. Then the K-bilinear map $(u,v): = T(uv^g)$ on F satisfies $(u,u) = 0\ \forall u \in F$, and hence is an alternating bilinear form. It is nonsingular since g is (i.e., $T(Fy^g) = 0 \implies y^g = 0 \implies y = 0$). Since $[F:K] = m$ is odd, this is impossible.

3.4. Up to Kerdock sets and orthogonal spreads, and down again

Now equip $F \oplus K$ with the inner product

$$((x,a),(y,b)): = T(xy) + ab.$$

Proposition 3.11. *The linear maps*

$$M_s: (x,a) \mapsto (x*s + sT(sx) + as, T(sx)),\ \ s \in F\,,$$

form a Kerdock set of $(m+1)\times(m+1)$ *skew–symmetric matrices over* K*. If the above inner product is used, then every Kerdock set is equivalent to one arising in this manner.*

The proof is straightforward. Corresponding to this Kerdock set is the orthogonal spread $\Sigma[*]$ in $F \oplus K \oplus F \oplus K$ consisting of $0 \oplus 0 \oplus F \oplus K$ together with the subspaces

$$\Big\{(x, k, x*s + T(xs)s + ks, T(xs)\ \Big|\ x \in F,\ k \in K\Big\} \text{ for } s \in F; \tag{3.12}$$

here, the quadratic form is $Q(x,a,y,b) = T(xy) + ab$.

For some choices of a nonsingular point z it is easy to write down the symplectic spread $\Sigma[*]_z$. Namely, if $z = \langle(0, a, \zeta, 1)\rangle$ with $a \in K^*, \zeta \in F$, then a straightforward calculation shows that the following symplectic prequasifield multiplication $\circ$ gives rise to an equivalent copy of $\Sigma[*]_z$ lying inside $F \oplus F$, where the alternating form is (3.9):

$$x \circ s = [x*s + (1+a)T(xs)s + T(xs)\zeta + T(x\zeta)s]/a. \tag{3.13}$$

(Division by a in (3.13) is only included so that (3.6) will hold for $\circ$. Namely, $T(x[x*s + (1+a)T(xs)s + T(xs)\zeta + T(x\zeta)s]) = T(xs)^2 + (1+a)T(xs)T(xs) + T(xs)T(x\zeta) + T(x\zeta)T(xs) = aT(xs)^2$.)

3.5. Semifield planes

Let F and K be as before, with $K \supset GF(2)$, and let T denote the trace map $F \to K$. The presemifield

$$x * y: = xy^2 + T_1(x)y + T_1(xy)$$

was introduced and studied in [Ka1, II]. The corresponding spread arises by starting with the desarguesian spread, going up and down once (cf. Section 2.5) while preserving the group of $|F|$ elations with axis $0 \oplus F$. This produces a nondesarguesian semifield plane.

This approach was greatly generalized in [Wi]. The presemifields studied there arise by the up and down process (Section 3.4), carefully retaining elations having a finite axis. In fact, by iterating (3.13) but always using $a = 1$, these presemifields can be described explicitly as follows. Let $F = F_0 \supset F_1 \supset \cdots \supset F_n = K$ be a sequence of fields with $n \geq 3$, let $T_i: F \to F_i$ be the trace map, and choose $\zeta_i \in F_i$ for each $i \geq 1$. Then

$$x * y = xy^2 + \sum_1^n \Big(T_i(\zeta_i x)y + \zeta_i T_i(xy)\Big) \tag{3.14}$$

defines a 2–sided distributive binary operation on F that produces a symplectic semifield plane.

Theorem 3.15. [Wi] *Assume that a sequence $F = F_0 \supset F_1 \supset \cdots \supset F_n = K$ is given as above with $[F_0 : F_1] \geq 7$ and $[F{:}K]$ odd. If (ζ_i) and (ζ_i') are sequences as above, then they define isomorphic planes if and only if $\zeta_i' = a\zeta_i^\tau$ for some $a \in F^*$, some $\tau \in \mathrm{Aut}F$, and all i.*

When all ζ_i are 0, the plane is desarguesian. The theorem implies, for example, that *there are at least $|F|^{n-2}/(|F|-1)\log_2|F|$ pairwise nonisomorphic symplectic semifield planes defined by* (3.14)—provided that $m = [F : K]$ has at least $n \geq 3$ (not necessarily distinct) prime factors, at least one of which is ≥ 7. Stronger versions of this result appear in [Wi].

3.6. Nearly flag–transitive planes

If F and K are as before, and if $a \in K - \mathrm{GF}(2)$, then the prequasifield

$$x * y{:} = xy^2 + aT(xy)y$$

was introduced and studied in [Ka1, II]. As in Section 3.5, this spread (and those in Section 3.7 below) arises by starting with the desarguesian spread, going up to the orthogonal spread in Example 3.2, and then coming down in a different manner (cf. Section 2.2). This time the group preserved is isomorphic to F^*: it has the form $(x, y) \mapsto (x\alpha, y/\alpha)$ with $\alpha \in F^*$, fixes two members of the symplectic spread, and cyclically permutes the remaining ones.

This approach was again generalized in [Wi] by iterating (3.13) but this time always using $\zeta = 0$. Let $F = F_0 \supset F_1 \supset \cdots \supset F_n = K \supset \mathrm{GF}(2)$ be a sequence of fields, where $[F : K]$ is odd. For each i, let $T_i: F \to F_i$ be the trace map, where $T_n = T$ in our earlier notation; and choose $c_i \in F^*$ such that $c_0 = 1$ and $c_i/c_{i-1} \in F_i$ for each i. Then

$$x * y{:} = xy^2 + \sum_1^n \Big(c_{i-1}yT_i(c_{i-1}xy) + c_i y T_i(c_i xy)\Big)$$

defines a prequasifield, the corresponding plane is nondesarguesian, and the maps $(x, y) \mapsto (x\alpha, y/\alpha)$, where $\alpha \in F^*$, form a cyclic collineation group of order $|F| - 1$. Isomorphisms among these planes are determined in [Wi].

This construction suggests the following general approach, for any characteristic and unrelated to symplectic spreads. Suppose that F is a finite field and $g: F \to F$ *is an additive map such that $x \mapsto xg(x)$ is bijective.* Then $(F, +, *)$ *is a prequasified, where*

$$x * y{:} = g(xy)y.$$

(Namely, left distributivity is clear, and $x * y = x * z \Rightarrow xg(xy)y = xg(xz)z \Rightarrow xy = xz$, as required.) Once again *the maps $(x, y) \mapsto (\alpha x, y/\alpha)$ with $\alpha \in F^*$ form a cyclic collineation group fixing the $x-$ and y–axes and transitively permuting the remaining lines through the origin.* (Namely, $(x, x * s)$ is sent to $(\alpha x, g(\alpha x s/\alpha)s/\alpha) = (\alpha x, (\alpha x) * (s/\alpha))$.)

Soon after I mentioned to Y. Hiramine this condition on a map g, he produced the following example: if $\omega \in \mathrm{GF}(2^6)$ and $\omega^6 = \omega + 1$, let $g(x) = x + \omega x^4 + \omega^{47} x^{16}$. However, the proof that this satisfies the required condition, and hence produces a plane of order 64, involves a long and ingenious case argument.

In the examples given earlier, $g(x) = x + \sum_1^n \Big(c_{i-1}T_i(c_{i-1}x) + c_iT_i(c_ix)\Big)$ (or, somewhat more precisely, $g(x/c_n)$ is the preceding right hand side in order to make (3.6) hold). That the resulting spread is symplectic comes from fact that g has following additional property:

$$T(xg(z)) = T(zg(x))\ \forall x, z \in F$$

(cf. (3.7)).

3.7. Flag–transitive planes

There is one further way to obtain planes from a desarguesian spread, while retaining a large collineation group [KW]. In the previous sections we preserved a group of order $|F|$ or $|F| - 1$, this time the group will have order $|F| + 1$. Once again, the planes are obtained by starting with the desarguesian spread and using the up and down process (Section 3.4). This time, in order to describe these planes we need to use the field $E = \mathrm{GF}(q^{2m})$ (where m is odd), and its multiplicative subgroup of order $q^m + 1$.

Let $E = E_0 \supset \cdots \supset E_n$ be a sequence of fields, where $[E : E_n]$ is odd and $|E|$ is a square; let "overbar" denote the involutory field automorphism of E. For each i let F_i be the subfield of E_i over which E_i has degree 2, let $T_i \colon F_0 \to F_i$ be the trace map, and write $W_i := \ker T_{i+1}|_{F_i}$. Pick any $\zeta_i \in E_i$, where $\zeta_i\bar{\zeta}_i = 1$ and $\zeta_0 = 1$, and write $\gamma_i := \Pi_0^i \zeta_l$. Then

$$\Big\{\theta(\sum_0^{n-1} W_i\gamma_i + F_n\gamma_n) \ \Big|\ \theta\bar{\theta} = 1\Big\} \tag{3.16}$$

is a symplectic spread in E, and $\{z \mapsto \theta z + w \mid \theta, w \in F,\ \theta\bar{\theta} = 1\}$ *is a sharply flag–transitive collineation group.*

This produces exponential numbers of flag–transitive affine planes of order q^m. In [KW] there is a complete determination of when two of them are isomorphic, as well as a discussion of the iteration involved in the construction. Once again, the simplest of these planes were first studied in [Ka1, II].

3.8. Orthogonal spreads and boring planes

The group $G(\Sigma)$ has been determined for various orthogonal spreads Σ [Ka1; Ka2; Ka4; KW; Wi]. For many of the ones in Sections 3.5–3.7, $G(\Sigma)$ is generated by the group preserved in the specific section (of order $|F|$ or $|F| \pm 1$) together with scalar transformations and some elements of Aut$F$. It is then possible to find nonsingular points z such that $G(\Sigma)_z$ consists only of scalars. In view of Theorem 3.3, this means that the collineation group of $\mathbf{A}(\Sigma_z)$ consists entirely of perspectivities. Showing that the stabilizer of 0 is (isomorphic to) K^* can be messy (as in [Ka4]) or partly pleasant (as in [Wi]), depending on the specific circumstances.

The most interesting case is that arising in Section 3.5. There, the orthogonal spread Σ occurs at the end of an iterative process. The last step of the iteration starts with an orthogonal spread $\widehat{\Sigma}$ in a smaller–dimensional space over a field properly between F and K, forms a symplectic semifield spread $\widehat{\Sigma}_{\hat{z}}$, and identifies this with a symplectic semifield spread Σ_z

arising from our orthogonal spread Σ over the smaller field K (so $\widehat{\Sigma}_{\widehat{z}} = \Sigma_z$. In [Wi], Williams proceeds as follows: he identifies all of the nonsingular points z' such that $\Sigma_{z'}$ is a semifield spread, and then shows that z is the only such z' for which the kernel of $\mathbf{A}(\Sigma_{z'})$ is larger than K. It follows that $G(\Sigma)$ must fix z, and hence is determined by $\mathrm{Aut}\mathbf{A}(\Sigma_z) = \mathrm{Aut}\mathbf{A}(\widehat{\Sigma}_{\widehat{z}})$. Then $G(\Sigma)$ is determined by $G(\widehat{\Sigma})$ (cf. Theorem 3.3), and induction can be used. This outline is the pleasant part of the argument. The difficult part is in the implementation: calculating the kernels of planes defined using the formula (3.14).

Boring planes. A *boring plane* is a translation plane $\mathbf{A}$ of order q^m with kernel $\mathrm{GF}(q)$ such that $|\mathrm{Aut}\mathbf{A}| = q^{2m}(q-1)$ is as small as possible. The reason for this name "boring" is that such planes are contrary to those usually studied in finite geometry, in which collineation groups are assumed to be in some sense "big". The only examples known in odd characteristic are two planes of order 17^2 [Ch]. By contrast, there are too many boring planes when the characteristic is 2 [Ka4; Wi]. These planes arise as follows: as already indicated, $G(\Sigma)$ is known for many orthogonal spreads Σ. For most of these there are nonsingular points z such that $G(\Sigma)_z = 1$. In view of Theorem 3.3, this means that $\mathrm{Aut}\mathbf{A}(\Sigma_z)$ consists of perspectivities. All that then remains is to show that the kernel of this plane is just K. This step involves calculations that are very different in the proofs for $q = 2$ [Ka4] or $q > 2$ [Wi]. (Neither proof extends to the situation in the other part of the theorem.) Clearly this theorem still leaves open the case of other values of m, as well as the entirely different case in which m is even—and of course, the case q odd also needs to be investigated. It is very likely that there large numbers of boring planes in all of these cases as well.

Similarly, a *boring semifield plane* is a semifield plane of order q^m with kernel $\mathrm{GF}(q)$ such that $|\mathrm{Aut}\mathbf{A}| = q^{3m}(q-1)$, which again is as small as possible. Once again large numbers of these are obtained in [Wi] using (3.14) and $G(\Sigma)$ for the corresponding orthogonal spread Σ.

3.9. The number of Kerdock sets and orthogonal spreads

In view of Proposition 2.3 and Theorem 3.3, the planes we have been discussing produce exponential numbers of inequivalent Kerdock sets and orthogonal spreads. We refer to [Wi] for estimates of the numbers of these, which significantly improve previous estimates in [Ka1; Ka2].

4. Additional uses of Kerdock sets

Symplectic and orthogonal spreads are also important for reasons quite different than the construction of planes. The basic constructions of the objects discussed presently depend on planes, which are involved in all present descriptions — with the exception of the original approach used in the construction of Kerdock codes [Ke] (and we have seen that this can be viewed as dealing with desarguesian spreads, albeit in a somewhat indirect manner).

The recent resurgence of interest in Kerdock codes (and hence of orthogonal spreads) stems from their versions over $\mathbb{Z}_4$ (Section 4.2) [CCKS; Wi].

4.1. Kerdock codes

Assume that the underlying field is $\mathbb{Z}_2$. Fix an ordering of the vectors in $\mathbb{Z}_2^n$, where n is even.

Each Kerdock set $\mathcal{K}$ determines a *Kerdock code*

$$C(\mathcal{K}) := \{\, (Q_B(v) + sv^t + \varepsilon)_{v \in \mathbb{Z}_2^n} \mid B \in \mathcal{K}, s \in \mathbb{Z}_2^n, \varepsilon \in \mathbb{Z}_2 \,\}, \tag{4.1}$$

where Q_B denotes any quadratic form whose associated bilinear form is uBv^t. The code $C(\mathcal{K})$ has length 2^n, consists of $2^{n-1}2^n2 = 2^{2n}$ codewords (i.e., vectors), and has minimum distance $2^{n-1} - 2^{(n-2)/2}$.

The resulting codes have interesting combinatorial properties, and were investigated starting in [Ke] and continuing in [Di; Ka1; Ka2; Wi]. See [MS, Ch. 15 §5; Li; CL] for further background concerning these codes.

Quasi-equivalence of codes Two binary codes of the same length will be called *quasi-equivalent* if there is an isometry of the underlying Hamming space sending one to the other. This means: permute the coordinates of the first code and then add a constant vector to all codewords in order to get the second code. The codes are called *equivalent* if only a permutation of coordinates is used. The latter is the more standard notion. However, we need the broader notion of quasi-equivalence in view of the following elementary fact: *Two Kerdock codes are quasi-equivalent if and only if they arise from equivalent Kerdock sets.*

Since we already know that there are large numbers of inequivalent Kerdock sets, it follows that the same is true for Kerdock codes.

4.2. $\mathbb{Z}_4$-codes

Each code $C(\mathcal{K})$ is nonlinear. In [CHKSS], unexpected relationships were discovered between codes over $\mathbb{Z}_4$ and binary codes, allowing the original Kerdock codes [Ke] to be viewed as codes over $\mathbb{Z}_4$ that are $\mathbb{Z}_4$–linear. This was generalized in [CCKS]: with each (binary) Kerdock code $C(\mathcal{K})$ of length 2^{m+1} is associated a $\mathbb{Z}_4$–code $C_4(\mathcal{K})$ of length 2^m that is *isometric* to $C(\mathcal{K})$, where a suitable natural metric is used on $\mathbb{Z}_4^{2^m}$: the *Lee metric* d_L. (This is defined by $d_L((a_i),(b_i)) = \sum |a_i - b_i|$, where $|a_i - b_i|$ is reduced mod 4 so as to be in $\{0,1,2\}$ and the sum is taken in $\mathbb{Z}$.)

We will define $C_4(\mathcal{K})$ using a binary operation as in Sections 3.3–3.4. By (3.7), for each $r \in F$ the map $P_r : x \mapsto x * r$ is self-adjoint with respect to the inner product $T(xy)$ on F. We fix an orthonormal basis for F, and view P_r as a matrix $\widehat{P}_r$ with entries 0 and 1 *in* $\mathbb{Z}_4$ *rather than* $\mathbb{Z}_2$. Similarly, we view each $x \in F$ as a row vector $\widehat{x}$ with entries $0, 1 \in \mathbb{Z}_4$. If $\mathcal{K}$ denotes the Kerdock set given in Proposition 3.11, then

$$C_4(\mathcal{K}) := \{\widehat{x}\widehat{P}_r\widehat{x}^t + 2\widehat{s}\cdot\widehat{x} + \varepsilon)_{x \in F} \mid r \in F, s \in F, \varepsilon \in \mathbb{Z}_4\}$$

is a $\mathbb{Z}_4$*–Kerdock code*. The similarity of this definition to (4.1) is evident.

Moreover, $C_4(\mathcal{K})$ *is* $\mathbb{Z}_4$*–linear if and only if* $*$ *is* 2*–sided distributive.* Part of this is easy to see: suppose that $*$ is 2–sided distributive. Then, for any $s, s' \in F$, $\widehat{P}_{s+s'} - \widehat{P}_s - \widehat{P}_{s'}$ is twice a symmetric matrix, and hence $x \mapsto \widehat{x}[\widehat{P}_{s+s'} - \widehat{P}_s - \widehat{P}_{s'}]\widehat{x}^t$ is additive from F to $2\mathbb{Z}_4$: it looks like $x \mapsto 2\widehat{r} \cdot \widehat{x}$ for some $r \in F$. Thus, semifields enter coding theory. These results, and a thorough discussion of equivalences among these $\mathbb{Z}_4$–codes, can be found in [CCKS; Wi].

If P is a symmetric binary $m \times m$ matrix then the map $x \mapsto \widehat{x}\widehat{P}\widehat{x}^t$ is called a $\mathbb{Z}_4$*–valued quadratic form* [Br]. In view of the above connection, it appears that the $\mathbb{Z}_4$–module of all of these needs to be investigated from a combinatorial point of view (cf. [Wo]).

4.3. Further topics

[CCKS] and [Wi] discuss relationships between Kerdock sets, extraspecial 2–groups, and extremal line–sets in real and complex vector spaces.

Symplectic and orthogonal spreads produce other types of combinatorial objects: partial geometries [DDT] or strongly regular graphs [Ka3].

Relationships of symplectic and orthogonal spreads with Lie algebras are surveyed in [Ka5].

Finally, Kerdock codes over $\mathbb{Z}_2$ and $\mathbb{Z}_4$ have suggested natural variations: codes over the quaternion group of order 8 [Ka6].

References

[Br] E. H. Brown, Generalizations of Kervaire's invariant, Annals of Math. 95 (1972), 368–383.

[CCKS] A. R. Calderbank, P. J. Cameron, W. M. Kantor and J. J. Seidel, $\mathbb{Z}_4$–Kerdock codes, orthogonal spreads, and extremal Euclidean line–sets (submitted).

[CHKSS] A. R. Calderbank, A. R. Hammons, Jr., P. V. Kumar, N. J. A. Sloane, and P. Solé, The $\mathbb{Z}_4$–linearity of Kerdock, Preparata, Goethals and related codes, IEEE Trans. Inform. Theory **40** (1994) 301–319.

[CL] P. J. Cameron and J. H. van Lint, Designs, Graphs, Codes and their Links, London Math. Soc. Student Texts 22, Cambridge Univ. Press, Cambridge, 1991.

[Ch] C. Charnes, A non–symmetric translation plane of order 17^2. J. Geometry 37 (1990), 77-83.

[DDT] F. DeClerck, R. H. Dye and J. A. Thas, An infinite class of partial geometries associated with the hyperbolic quadric in $PG(4n-1,2)$, Europ. J. Combinatorics 1 (1980) 323–326.

[De] P. Dembowski, Finite Geometries, Springer, Berlin-Heidelberg-New York, 1968.

[Di] J. F. Dillon, Elementary Hadamard Difference Sets. Ph.D. thesis, U. of Maryland, 1974.

[Ka1] W. M. Kantor, Spreads, translation planes and Kerdock sets. I,II, SIAM J. Alg. Discr. Math. 3 (1982), 151–165 and 308–318.

[Ka2] W. M. Kantor, An exponential number of generalized Kerdock codes, Inform. Control 53 (1982), 74–80.

[Ka3] W. M. Kantor, Strongly regular graphs defined by spreads, Israel J. Math 41 (1982) 298–312.

[Ka4] W. M. Kantor, Projective planes of order q whose collineation group has order q^2. J. Algebraic Combinatorics 3 (1994) 405–425.

[Ka5] W. M. Kantor, Note on Lie algebras, finite groups and finite geometries (to appear in: Proc. Ohio State U. Groups and Geometries Conference).

[Ka6] W. M. Kantor, Quaternionic line-sets and quaternionic Kerdock codes (submitted).

[KW] W. M. Kantor and M. E. Williams, New flag–transitive affine planes of even order (to appear in JCT(A)).

[Ke] A. M. Kerdock, A class of low–rate nonlinear binary codes, Inform. Control 20 (1972), 182–187.

[Li] J. H. van Lint, Kerdock and Preparata codes, Congressus Numerantium 39 (1983), 25–41.

[MS] F. J. MacWilliams and N. J. A. Sloane, The theory of error-correcting codes. North–Holland, Amsterdam 1977.

[Wi] M. E. Williams, $\mathbb{Z}_4$–linear Kerdock codes, orthogonal geometries, and non–associative division algebras, Ph.D. thesis, University of Oregon 1995 (in preparation).

[Wo] J. Wood, Witt's extension theorem for mod four valued quadratic forms, Trans. Amer. Math. Soc. 336 (1993), 445–461.