Discrete Mathematics 106/107 (1992) 297–302
North-Holland

Kerdock codes and related planes

William M. Kantor*
University of Oregon, Eugene, OR 97403, USA

Received 12 January 1992
Revised 9 February 1992

Abstract

Kantor, W.M., Kerdock codes and related planes, Discrete Mathematics 106/107 (1992) 297–302.

Among the many aspects of coding theory Jack van Lint has studied intensively are some generalizations of Preparata and Kerdock codes (see Baker et al. (1983), Cameron and Van Lint (1991) and Van Lint (1983)). There are still many open problems concerning these. This note is a brief discussion of problems and new results involving orthogonal spreads, translation planes and associated generalized Kerdock codes.

1. Orthogonal spreads

Let V be a vector space of dimension $4m$ over a finite field L of characteristic 2, where $m \geq 2$. Assume that V is equipped with a quadratic form Q of Witt index $2m$; the associated bilinear form is denoted (u, v). Then the pair V, Q is equivalent to the pair L^{4m}, Q_{4m}, where

$$Q_{4m}((x_i)) = \sum_{1}^{2m} x_i x_{2m+i}.$$

Write the standard ordered basis of L^{4m} as $e_1, \ldots, e_{2m}, f_1, \ldots, f_{2m}$, so that $Q_{4m}(e_i) = Q_{4m}(f_i) = (e_i, e_j) = (f_i, f_j) = 0$ and $(e_i, f_j) = \delta_{ij}$ for $1 \leq i, j \leq 2m$. We will be concerned with totally singular $2m$-spaces. Examples of these are $E = \langle e_1, \ldots, e_{2m} \rangle$ and $F = \langle f_1, \ldots, f_{2m} \rangle$. Each totally singular $2m$-space having only 0 in common with E looks like

$$F\begin{pmatrix} I & O \\ M & I \end{pmatrix} \quad \text{with } M \text{ a skew-symmetric } 2m \times 2m \text{ matrix} \tag{1.1}$$

Correspondence to: W.M. Kantor, Department of Mathematics, University of Oregon, Eugene, OR 97403, USA.

* Supported in part by NSF and NSA grants.

(where skew-symmetric matrices are always assumed to have zero diagonal). Note that the $4m \times 4m$ matrix in (1.1) preserves the form Q_{4m}. Two subspaces (1.1), arising from matrices M and M', have only 0 in common if and only if $M - M'$ is nonsingular.

A *Kerdock set* $\boldsymbol{K}$ is a family of $|L|^{2m-1}$ skew-symmetric $2m \times 2m$ matrices the difference of any two of which is nonsingular. When $L = \mathrm{GF}(2)$, $\boldsymbol{K}$ produces a *generalized Kerdock code* $\mathscr{C}(\boldsymbol{K})$ consisting of the zeros of the following functions $L^{2m} \to L$:

$$xM^{\square}x^t + l(x) + c$$

where $M^{\square}$ denotes the matrix obtained from M by replacing all below-diagonal entries with 0 (so that $M = M^{\square} + M^{\triangledown}$), l ranges through all linear functionals on L^{2m}, and $c \in L$. Then $\mathscr{C}(\boldsymbol{K})$ is a code having length 2^{2m}, minimum distance $2^{2m-1} - 2^m$, and size 2^{4m}, just as in the case of classical Kerdock codes.

If V and L are as at the beginning of this section then a *spread* in the orthogonal space V is a family Σ of $|L|^{2m-1} + 1$ totally singular $2m$-spaces such that every nonzero singular vector is in a unique member of Σ. A Kerdock set $\boldsymbol{K}$ of $2m \times 2m$ matrices produces an orthogonal spread of L^{4m} via (1.1), namely,

$$\Sigma(\boldsymbol{K}) = \{E\} \cup \left\{ F\begin{pmatrix} I & O \\ M & I \end{pmatrix} \;\middle|\; M \in \boldsymbol{K} \right\}. \tag{1.2}$$

Conversely, each orthogonal spread of L^{4m} that contains E and F produces a Kerdock set via (1.1) and (1.2).

All of the above can be found in [2]. That book also discusses some of the other combinatorial objects arising from Kerdock sets: partial geometries and linked square designs. Strongly regular graphs also arise [7]. The remainder of this note focuses on the fact that orthogonal spreads produce many translation planes.

Let Σ be a spread in the orthogonal space V. If y is any nonsingular point of V, write

$$\Sigma_y = \{\langle y^{\perp} \cap X, y\rangle / y \mid X \in \Sigma\}.$$

Then Σ_y partitions the nonzero vectors in $y^{\perp}/y$: it is a spread in the classical sense of the term [3, p. 219]. Moreover, it is even a *symplectic spread*: each of its members is a totally isotropic $2m - 1$-space of the symplectic space $y^{\perp}/y$ (with respect to the alternating form $(u + y, v + y) = (u, v)$, $u, v \in y^{\perp}$). The translation plane $\mathscr{A}(\Sigma_y)$ determined by Σ and y has $y^{\perp}/y$ as its set of points, the lines being the cosets of the members of Σ_y.

Conversely, any symplectic spread in $y^{\perp}/y$ arises as Σ_y for an orthogonal spread Σ in V—and Σ is essentially unique [4]. In [4, (3.5), (3.6), (3.7)] it was shown that two planes arising in this manner from orthogonal spreads Σ, Σ' of V and nonsingular points y, y', are isomorphic if and only if there is an automorphism of the underlying orthogonal space V sending Σ to Σ' and y to y'; and every

collineation of $\mathscr{A}(\Sigma_y)$ is the product of a translation, a homology, and a semilinear transformation preserving the symplectic structure of $y^\perp/y$. The determination of the collineation group of a plane $\mathscr{A}(\Sigma_y)$ can be achieved in three stages: determine the group $G(\Sigma)$ of all semilinear transformations of V that send Σ to itself and preserve Q up to scalars (i.e., projectively); determine the stabilizer $G(\Sigma)_y$; and determine the group of homologies of $\mathscr{A}(\Sigma_y)$ fixing 0.

2. Examples

Let $F = \mathrm{GF}(2^{2m-1})$ and K be fields such that $F \supset K \supset \mathrm{GF}(2)$. Let $T: F \to K$ and $T': F \to \mathrm{GF}(2)$ be the corresponding trace maps.

Example 1 (*'Desarguesian spreads'*)**.** Consider the K-space $F \times K \times F \times K$, equipped with the quadratic form Q defined by

$$Q(\alpha, a, \beta, b) = T(\alpha\beta) + ab;$$

the corresponding bilinear form is $((\alpha, a, \beta, b), (\alpha', a', \beta', b')) = T(\alpha\beta' + \alpha'\beta) + ab' + a'b$. The desarguesian spread in $F \times F$ 'lifts' to the orthogonal spread Σ consisting of the totally singular subspaces

$$0 \times 0 \times F \times K$$

and

$$\{(\alpha, a, s^2\alpha + sT(s\alpha) + sa, T(s\alpha)) \mid \alpha \in F, a \in K\} \quad \text{for } s \in F. \tag{2.1}$$

Note that $\Sigma_{\langle 0,1,0,1\rangle}$ consists of the subspaces

$$0 \times 0 \times F \times 0 + \langle 0, 1, 0, 1\rangle \quad \text{and} \quad \{(\alpha, 0, s^2\alpha, 0) + \langle 0, 1, 0, 1\rangle \mid \alpha \in F\} \text{ for } s \in F,$$

and this evidently is the usual desarguesian spread producing the desarguesian plane $\mathscr{A}(\Sigma_{\langle 0,1,0,1\rangle}) = \mathrm{AG}(2, 2^{2m-1})$. The orthogonal spread (2.1) is called the *desarguesian spread* in [5].

Example 2 (*called in* [4, 5] *the 'third cousins of the desarguesian spread'*)**.** Fix $k \in K - \mathrm{GF}(2)$, and consider the nonsingular point $y_k = \langle 0, k+1, 0, 1\rangle$ in the space $F \times K \times F \times K$ appearing in Example 1. This produces a symplectic spread Σ_{y_k} in the symplectic space $y_k^\perp/y_k$, consisting of the following subspaces:

$$\begin{aligned} &0 \times 0 \times F \times 0 + y_k, \\ &\{(\alpha, 0, s^2\alpha + ksT(s\alpha), 0) + y_k \mid \alpha \in F\} \quad \text{for } s \in F. \end{aligned} \tag{2.2}$$

Example 2'. The symplectic space $y_k^\perp/y_k$ over K can also be viewed as a symplectic space over GF(2) by using the bilinear form $(u, v)' = T'((u, v))$ for $u, v \in y_k^\perp/y_k$. Then (2.2) also is a symplectic spread of this space.

Example 3. Now consider the GF(2)-space $V = F \times \mathrm{GF}(2) \times F \times \mathrm{GF}(2)$, equipped with the quadratic form Q' defined by

$$Q'(\alpha, a, \beta, b) = T'(\alpha\beta) + ab.$$

The subspaces $F \times \mathrm{GF}(2) \times 0 \times 0$ and $0 \times 0 \times F \times \mathrm{GF}(2)$ are totally singular. The spread (2.2), viewed as in Example 2′, lifts to the following orthogonal spread Σ^k (where we have written $k^* = 1 + \sqrt{k}$):

$$\begin{aligned} &0 \times 0 \times F \times \mathrm{GF}(2), \\ &\{(\alpha, a, s^2\alpha + ksT(s\alpha) + k^*sT'(k^*s\alpha) \\ &\quad + k^*sa, T'(k^*s\alpha)) \mid \alpha \in F, a \in \mathrm{GF}(2)\} \quad \text{for } s \in F. \end{aligned} \tag{2.3}$$

Namely, the members of Σ^k are totally singular subspaces intersecting pairwise only in 0, and the spread $\Sigma^k_{\langle 0,1,0,1\rangle}$ consists of the subspaces

$$\begin{aligned} &0 \times 0 \times F \times 0 + \langle 0, 1, 0, 1\rangle, \\ &\{(\alpha, 0, s^2\alpha + ksT(s\alpha), 0) + \langle 0, 1, 0, 1\rangle \mid \alpha \in F\} \quad \text{for } s \in F, \end{aligned}$$

as in (2.2). The question of equivalence among the orthogonal spreads Σ^k was studied in [6].

3. Some planes and Kerdock sets

There are many possibilities for the behavior of the full collineation groups of planes of the form $\mathscr{A}(\Sigma_y)$. The collineation group of any translation plane of order q must have order at least q^2: there are always q^2 translations present. This lower bound can be achieved:

Theorem 3.1. *If $2m-1$ is composite and >9, then there is a translation plane of order 2^{2m-1} whose full collineation group consists only of the 2^{4m-2} translations of the underlying vector space.*

In particular, every point of each of these affine planes has the 'boring' property that its stabilizer in the full collineation group is the trivial group. There does not appear to be any published example of a finite projective plane having a point whose stabilizer in the full collineation group is trivial.

More than $2^{2m-1} \cdot 2^{\sqrt{2m-1}}/4(2m-1)^2$ pairwise non-isomorphic planes of order 2^{2m-1} arise in (3.1). These planes are constructed as follows. Let $2m-1$ be composite and >9; let $F = \mathrm{GF}(2^{2m-1}) \supset K \supset \mathrm{GF}(2)$, as above. Let Ψ be a generator of F such that $T'(\Psi) = 1$; there are more than $2^{2m-2} - 2^{(2m-1)/3}$ choices for Ψ. Choose $k \in K - \mathrm{GF}(2)$. Consider the space V and form Q' defined in Example 3. The point $\langle \Psi, 0, 1, 0\rangle$ is nonsingular since $Q'(\Psi, 0, 1, 0\rangle = 1$, and it produces a symplectic spread $\Sigma^k_{\langle \Psi,0,1,0\rangle}$ in the symplectic GF(2)-space $\langle \Psi, 0, 1, 0\rangle^\perp / \langle \Psi, 0, 1, 0\rangle$. Then *the full collineation group of the affine plane $\mathscr{A}(\Sigma^k_{\langle \Psi,0,1,0\rangle})$ has order 2^{4m-2}.*

The proof [8] more or less follows the pattern indicated at the end of Section 1. Significant use is made of the isometries of V defined by $(\alpha, a, \beta, b) \mapsto$

$(\zeta\alpha, a, \zeta^{-1}\beta, b)$, where $\zeta \in F - \{0, 1\}$. Each of these lies in the group $G(\Sigma^k)$, fixes $z = \langle 0, 1, 0, 1\rangle$ and hence acts on the plane $\mathscr{A}(\Sigma_z^k)$, but moves $y = \langle \Psi, 0, 1, 0\rangle$ and hence does not act on the plane $\mathscr{A}(\Sigma_y^k)$. This is a somewhat surprising aspect of the proof of (3.1): the fact that a group $G(\Sigma^k)$ that is *not* a collineation group of a plane is somewhat large allows information to be obtained showing that the collineation group itself is small. Namely, it is easy to show that $G(\Sigma^k)_{yz} = 1$ by using the translation plane $\mathscr{A}(\Sigma_z^k)$. The crucial step consists of employing properties of the above isometries in order to deduce that $G(\Sigma^k)_y = 1$. Some group theory is used, but from the late 1960s rather than detailed information concerning simple groups. In addition, there is a final, highly computational step showing that the collineation group of $\mathscr{A}(\Sigma_y^k)$ contains no nontrivial homologies.

Theorem 3.2. *If $2m - 1$ is composite and >9, then there is a Kerdock set $\boldsymbol{K}$ of $2m \times 2m$ matrices such that* Aut $\mathscr{C}(\boldsymbol{K}) = 1$.

Such Kerdock sets $\boldsymbol{K}$ can be obtained as follows. Let s be a generator of F over GF(2), and let X_s be the corresponding member of Σ^k in (2.3). Use an orthogonal transformation to move the pair Σ^k, X_s to a pair Σ', E with Σ' an orthogonal spread containing E and F. Then $\boldsymbol{K}$ is the Kerdock set produced by Σ', E, F via (1.1). More than 2^{3m} pairwise inequivalent codes arise in this manner.

4. Open problems

After more than ten years there are still not many ways orthogonal or symplectic spreads have been constructed. Additional approaches seem essential in order to attempt to understand the nature of the projective planes and Kerdock sets arising from these spreads.

Problem 1. Construct symplectic spreads admitting a transitive group. Such spreads will produce flag-transitive affine planes. Only one type of construction is known, very closely tied to desarguesian spreads [4, §4; 5, §5].

Problem 2. Construct symplectic spreads such that the corresponding planes are semifield planes (i.e., planes coordinatized by non-associative division algebras). Once again, only one type of construction is known, very closely tied to desarguesian spreads [4, §4; 5, §7].

Problem 3. All orthogonal spreads are known for which $G(\Sigma)$ acts 2-transitively on Σ [5, (3.1); 9]. Determine all orthogonal spreads such that $G(\Sigma)$ fixes one member of Σ and acts sharply 2-transitively on the remaining ones. This occurs in the classical case, and corresponds to the fact that the classical Kerdock code

admits the 1-dimensional affine group. It may be that there are other examples of this phenomenon.

Problem 4. The planes in (3.1) have the property that no nontrivial linear transformation of the underlying GF(2)-space preserves their spreads. Undoubtedly there are large numbers of orthogonal spreads Σ such that $G(\Sigma) = 1$, but no examples presently are known. They would produce large numbers of Kerdock codes having trivial automorphism group.

Problem 5. What are the restrictions on the structure of automorphism groups of orthogonal spreads? Involutions are rather restricted. However, what are the restrictions on odd order groups acting on orthogonal spreads?

Problem 6. What *purely geometric* properties of the planes $\mathscr{A}(\Sigma_y)$ reflect that fact that they arise from *symplectic* spreads? This is the most intriguing, and the most important, question concerning these planes.

References

[1] R.D. Baker, J.H. van Lint and R.M. Wilson, On the Preparata and Goethals codes, IEEE Trans. Inform. Theory 29 (1983) 342–345.
[2] P.J. Cameron and J.H. van Lint, Designs, graphs, codes and their links (Cambridge Univ. Press, Cambridge, 1991).
[3] P. Dembowski, Finite Geometries (Springer, Berlin–Heidelberg–New York, 1968).
[4] W.M. Kantor, Spreads, translation planes and Kerdock sets. I, SIAM J. Algebraic Discrete Methods 3 (1982) 151–165.
[5] W.M. Kantor, Spreads, translation planes and Kerdock sets. II, SIAM J. Algebraic Discrete Methods 3 (1982) 308–318.
[6] W.M. Kantor, An exponential number of generalized Kerdock codes, Inform. Control 53 (1982) 74–80.
[7] W.M. Kantor, Strongly regular graphs defined by spreads, Israel J. Math. 41 (1982) 298–312.
[8] W.M. Kantor, Projective planes of order q whose collineation groups have order q^2, in preparation.
[9] P.B. Kleidman, The finite 2-transitive spreads and translation planes, manuscript.
[10] J.H. van Lint, Kerdock and Preparata codes, Proc. 14th Southeast Conf. Boca Raton, Congr. Numer. 39 (1983) 25–41.