

SPREADS, TRANSLATION PLANES AND KERDOCK SETS. II*

W. M. KANTOR†

Abstract. New Kerdock sets of q^{2n-1} skew-symmetric $2n \times 2n$ matrices over $GF(q)$ are constructed for even q whenever $2n-1$ is composite. Related affine translation planes are studied in detail. In both cases, explicit coordinate descriptions are given.

1. Introduction. This paper is a continuation of [6], hereafter called [STK]. In that paper, the relationship between spreads, translation planes and Kerdock sets was described. Nondesarguesian examples were given, arising either from slices of desarguesian spreads or from certain spreads in $\Omega^+(8, q)$ spaces. In this paper we will study these slices more closely, and construct new Kerdock sets in higher dimensional spaces.

When an $\Omega^+(2m, q^e)$ space is turned into an $\Omega^+(2em, q)$ space by following the quadratic form with the trace map, new singular vectors are introduced. Thus, it is not possible to directly change the dimension of the space in which an orthogonal spread lies in order to obtain a new spread. However, when an $Sp(2m, q^e)$ space is turned into an $Sp(2em, q)$ space, this difficulty does not arise. This produces the following construction (§ 2): take an orthogonal spread, slice in order to obtain a symplectic spread, change fields, and then embed the resulting symplectic spread as a slice of a new orthogonal spread.

This procedure provides us with a machine for grinding out large numbers of new spreads and new translation planes. These do not seem to have new properties: from the point of view of their groups, they have fewer properties than the original spreads and planes. On the other hand, the procedure requires a great deal of interesting interplay between orthogonal spreads and translation planes. It is not at all clear how one can directly pass from an orthogonal spread to one of the many new ones it spawns; it seems even less likely that one could directly pass from a Kerdock set over $GF(q^e)$ to one of the many new ones over $GF(q)$.

The spreads and Kerdock sets obtained in this manner from the unitary spreads of [STK, § 6] are new for trivial reasons (§ 3), but are difficult to compute with.

Most of the paper is devoted to spreads obtained by starting with the desarguesian plane $AG(2, (q^e)^m)$, passing to one of its "cousins", and then changing fields. The resulting orthogonal spreads and Kerdock sets are studied in §§ 8 and 9. In order to show that these are new, we must study the aforementioned cousins rather carefully. This is done by using their coordinatizing quasifields in §§ 5 and 6.

The spreads of $\Omega^+(2m, 2)$ spaces obtained here produce partial geometries as in DeClerck, Dye and Thas [2], having the same parameters as their partial geometries but not isomorphic to their "desarguesian" ones.

2. Expanding spreads: definition. Let q be a power of 2, let m be odd with $m > 1$, and let Σ be a spread of an $\Omega^+(2m+2, q^e)$ space V . If e is odd, then many spreads can be constructed in $\Omega^+(2em+2, q)$ spaces, as follows.

Let y be any nonsingular point of V , and form the spread

$$\Sigma(y) = (y^\perp \cap \Sigma)/y = \{\langle y, y^\perp \cap F \rangle / y \mid F \in \Sigma\}$$

* Received by the editors July 14, 1981.

† Bell Laboratories, Murray Hill, New Jersey 07974. Permanent address: Mathematics Department, University of Oregon, Eugene, Oregon 97403.

in the $Sp(2m, q^e)$ space y^\perp/y [STK, (3.1)]. If (\cdot, \cdot) is the symplectic form on y^\perp/y , and $T: GF(q^e) \rightarrow GF(q)$ is the trace map, then $T(\cdot, \cdot)$ turns y^\perp/y into an $Sp(2em, q)$ space. Totally isotropic spaces remain totally isotropic. Thus, $\Sigma(y)$ produces a spread $\Sigma(y)^e$ of totally isotropic em -spaces of y^\perp/y . (Of course, $\Sigma(y)$ and $\Sigma(y)^e$ determine the same translation plane $\mathbf{A}(\Sigma(y))$.) Finally, form the spread $\mathbf{S}(\Sigma(y)^e)$ of an $\Omega^+(2em+2, q)$ space, as in [STK, (3.2)]. Note that e must be odd here, in order to have $2em+2 \equiv 0 \pmod{4}$.

The procedure described above will be called *expanding* the spread $\Sigma(y)$ into $2em+2$ dimensions.

In view of [STK, § 3], $\mathbf{S}(\Sigma(y)^e)$ determines many translation planes defined by symplectic spreads $(z^\perp \cap \mathbf{S}(\Sigma(y)^e))/z$, where z is any nonsingular point of the various $\Omega^+(2em+2, q)$ spaces. $\mathbf{S}(\Sigma(y)^e)$ also determines many Kerdock sets of $(em+1) \times (em+1)$ skew-symmetric matrices over $GF(q)$, as in [STK, § 5].

The remainder of this paper will be concerned with examples of such expanded spreads, planes and Kerdock sets are new.

Of crucial importance are the following trivial observations.

LEMMA 2.1. *Let Σ , y and $\Sigma^* = \mathbf{S}(\Sigma(y)^e)$ be as above.*

(i) *There is a nonsingular point y^* of the underlying $\Omega^+(2em+2, q)$ space such that $\Sigma(y)^e = \Sigma^*(y^*)$.*

(ii) *$\Gamma O^+(2m+2, q^e)_{\Sigma, y}$ induces a subgroup of $\Gamma O^+(2em+2, q)_{\Sigma^*, y^*}$ in such a way that the permutation representations on Σ and Σ^* are equivalent.*

3. Unitary spreads. The expanded examples which are most easily shown to be new arise from the unitary spreads constructed in [STK, § 6]. Such a spread Σ arises in an $\Omega^+(8, q^e)$ space, where $\log_2 q^e$ is odd and $q^e > 2$. Define N and M as in [STK, Thm. 7.1, Example 7.5]. Assume that $e > 1$.

THEOREM 3.1. *The expanded spreads $\mathbf{S}(\Sigma(\langle N \rangle)^e)$ and $\mathbf{S}(\Sigma(\langle M \rangle)^e)$ are nondesarguesian spreads in $\Omega^+(6e+2, q)$ space.*

Proof. There is a subgroup $G = PGU(3, q^3)$ of $\Gamma O^+(8, q^e)_\Sigma$. By [STK, § 7], $G_N = GU(2, q^e)$ has a cyclic normal subgroup of order q^e+1 fixing q^e+1 members of Σ . That cyclic group acts on $\mathbf{S}(\Sigma(\langle M \rangle)^e)$ by Lemma 2.1. However, the subgroup of $\Gamma O^+(6e+2, q)$ preserving a desarguesian spread induces $PGL(2, q^{3e})$ on that spread [STK, (4.1)], and hence cannot have a cyclic subgroup acting as above. Consequently, $\mathbf{S}(\Sigma(\langle N \rangle)^e)$ is nondesarguesian, and the same argument shows that $\mathbf{S}(\Sigma(\langle M \rangle)^e)$ also is.

THEOREM 3.2. *$\mathbf{S}(\Sigma(\langle N \rangle)^e)$ and $\mathbf{S}(\Sigma(\langle M \rangle)^e)$ are not equivalent under the action of $\Gamma O^+(6e+2, q)$.*

Proof. This requires some group theory, and will only be briefly sketched. Assume that these expanded spreads are equivalent. Call either of them Σ^* . Then $H = \Gamma O^+(6e+2, q)_{\Sigma^*}$ contains subgroups acting on Σ^* as G_N and G_M do on their respective symplectic spreads. It follows that H acts transitively on Σ^* . A detailed analysis yields that H acts 2-transitively on Σ^* . However, this is impossible in view of the following lemma. \square

LEMMA 3.3. *Let Σ be a spread in an $\Omega^+(2n+2, q)$ space V , where q is even, n is odd and $n > 3$. Assume that $\Gamma O^+(2n+2, q)_\Sigma$ is 2-transitive on Σ . Then Σ is desarguesian.*

Proof. First note that q^n+1 is not a prime power. Then $\Gamma O^+(2n+2, q)_\Sigma$ has a subgroup G inducing $PSL(2, q^n)$ or $PSU(3, q^{n/3})$ on Σ (Holt [5, Thm. 2]). Here, G has a $GF(2)$ -representation on our space of size q^{2n+2} . It follows that G cannot act irreducibly on V , and fixes some 1-space z (Fong and Seitz [4, (4A), (4B), (4D)]). Clearly, z cannot be singular. Thus, G acts on the translation plane $\mathbf{A}(\Sigma(z))$, inducing

$PSL(2, q^n)$ or $PSU(3, q^{n/3})$ on the line at infinity. Consequently, $\Sigma(z)$ is desarguesian (Lüneburg [7, pp. 178–179]), and hence so is Σ (by definition [STK, § 4]). \square

There are many translation planes arising from the spreads in Theorem 3.1 [STK, § 3], but none seems manageable or interesting.

4. Desarguesian spreads. In order to deal with the expanded cousins of desarguesian spreads, we will need to study these cousins using their coordinatizing quasifields. This in turn requires a description of the corresponding spreads, and hence of desarguesian spreads of $\Omega^+(2m + 2, q)$ spaces.

Let q be even and m be odd. Set $F = GF(q^m)$ and $K = GF(q)$ throughout §§ 4–7. Let $T: F \rightarrow K$ be the trace map. Then T is K -linear, and satisfies

$$(4.1) \quad T(\alpha)^2 = T(\alpha^2) \quad \text{for all } \alpha \in F, \quad T(a) = a \quad \text{if } a \in K.$$

Let V_0 be the F -space with basis e, f , view V_0 as a $2m$ -dimensional K -space, and form the $(2m + 2)$ -dimensional space $V = V_0 \oplus \langle u, w \rangle$. Define a quadratic form Q on V by

$$Q(\alpha e + \beta f + cu + dw) = T(\alpha\beta) + c^2 + cd.$$

This turns V into an $\Omega^+(2m + 2, q)$ space.

Set

$$(4.2) \quad \begin{aligned} \Sigma[\infty] &= Ff + K(u + w), \\ \Sigma[s] &= \{\alpha e + (s^2\alpha + sa)f + T(s\alpha)u + aw \mid \alpha \in F, a \in K\} \end{aligned}$$

for $s \in F$. Then

$$\Sigma = \{\Sigma[s] \mid s \in F \cup \{\infty\}\}$$

is a desarguesian spread in V .

Define linear transformations j and $[t]$ as follows (where $t \in F$).

$$(4.3) \quad j: \begin{cases} \alpha e \leftrightarrow \alpha f \\ u \rightarrow u \\ w \rightarrow w + u \end{cases} \quad [t]: \begin{cases} \alpha e \rightarrow \alpha e + \alpha t^2 f + T(\alpha t)u \\ f \rightarrow f \\ u \rightarrow u \\ w \rightarrow w + tf \end{cases}$$

Then j and $[t]$ preserve Q , and act on Σ as follows: $\Sigma[s]^j = \Sigma[s^{-1}]$ and $\Sigma[s]^{[t]} = \Sigma[s + t]$. Thus, $G = \langle j, [t] \mid t \in F \rangle$ induces $SL(2, q^m)$ on Σ , and is, in fact, isomorphic to $SL(2, q^m)$. The action of G (and even of $PGL(2, q^m)$) on Σ is used in [STK, § 4] in order to distinguish between the various cousins of $AG(2, q^m)$.

Every cousin has the form $\Sigma(y)$, with $y = \langle u \rangle, \langle f + u \rangle, \langle u + kw \rangle$ with $k \in K - GF(2)$, or $\langle ku + w + r(e + f) \rangle$ with $k \in K, r \in K$ and $x^2 + x + r$ irreducible. These cousins are, respectively, the first, second, third and fourth cousins of $AG(2, q^m)$ [STK, Thm. 4.2].

$\Sigma(\langle u \rangle)$ produces $AG(2, q^m)$.

Second cousin.

$$(4.4) \quad \begin{aligned} \Sigma(\langle f + u \rangle)[\infty] &= Ff, \\ \Sigma(\langle f + u \rangle)[s] &= \{\alpha e + (s^2\alpha + sT(\alpha) + T(s\alpha))f \mid \alpha \in F\}, \end{aligned}$$

Third cousins.

$$(4.5) \quad \begin{aligned} \Sigma(\langle u + kw \rangle)[\infty] &= Ff, \\ \Sigma(\langle u + kw \rangle)[s] &= \{\alpha e + (s^2\alpha + ksT(s\alpha))f \mid \alpha \in F\}. \end{aligned}$$

In the above spreads, we have projected onto V_0 in order to obtain these relatively simple descriptions. Note that (4.4) and (4.5) are both symplectic relative to the natural symplectic form $(\alpha e + \beta f, \alpha' e + \beta' f) = T(\alpha\beta' + \alpha'\beta)$ on V_0 .

Fourth cousins are also easily computed as $\Sigma(\langle ku + r(e + f) \rangle)$. However, the resulting spreads and quasifields seem difficult to compute with. An alternative description of fourth cousins will be used in § 7.

5. Second cousins. The next two sections consist of coordinate calculations with second and third cousins of desarguesian planes. These calculations are needed for Lemma 7.1, which is a crucial step in our proof (in Theorem 8.1) that expansions of these cousins are new. For completeness, we will provide an alternative verification of the fact that these cousins are nondesarguesian [STK, Thm. 4.2].

Let F, K and T be as in § 4. The spread (4.4) yields a semifield, which we now proceed to describe.

For $x, y \in F$, write

$$x * y = x^2y + xT(y) + T(xy).$$

LEMMA 5.1. *If $x * y = 0$ then $x = 0$ or $y = 0$.*

Proof. Write $z = xy$. Then $z^2 + zT(y) + yT(z) = 0$. Apply T and obtain $T(z)^2 + T(z)T(y) + T(y)T(z) = 0$. Then $T(z) = 0$ and $z^2 = zT(y)$. If $z \neq 0$ then $z = T(y)$, so that $0 = T(z) = T(y)$ (by (4.1)). Thus, $z = 0$. \square

DEFINITION 1. \bar{x} is the unique solution to

$$(5.2) \quad \bar{x}^2 + \bar{x} + T(\bar{x}) = x.$$

Thus, $x \rightarrow \bar{x}$ is the inverse of the map $x \rightarrow x * 1$. Note that $\bar{a} = a^{1/2}$ if $a \in K$, while $T(\bar{x})^2 = T(x)$ by (4.1).

DEFINITION 2. $x \circ y = \bar{x} * y = \bar{x}^2y + \bar{x}T(y) + T(\bar{x}y)$.

THEOREM 5.3. (F, \circ) is a semifield. It is not a field if $q^m > 8$.

Proof. If $a \in K$ then $a \circ x = ax = x \circ a$. Also, $x \rightarrow \bar{x}$ is additive. By Lemma 5.1, (F, \circ) is a semifield. The second part of Theorem 5.3 follows from the next two lemmas.

LEMMA 5.4. $GF(2) = \{a \in K \mid (a \circ u) \circ v = a \circ (u \circ v) \text{ for all } u, v \in F\}$.

Proof. Assume that $(a \circ u) \circ v = a \circ (u \circ v)$ for all $u, v \in F$, where $a \in K - GF(2)$. Since $(a \circ u) \circ v = (au) \circ v$ and $a \circ (u \circ v) = a(u \circ v)$, we have

$$\overline{au}^2v + \overline{au}T(v) + T(\overline{au}v) = a(\bar{u}^2v + \bar{u}T(v) + T(\bar{u}v)),$$

$$(\overline{au}^2 + a\bar{u}^2)v = (\overline{au} + a\bar{u})T(v) + (T(\overline{au}v) + aT(\bar{u}v)).$$

If $\overline{au}^2 + a\bar{u}^2 \neq 0$ for some u , we can divide in order to obtain $\dim_K F \leq 2$. Thus, $\overline{au}^2 + a\bar{u}^2 = 0$ for all u .

From (5.2) it now follows that

$$\overline{au} + au + T(\overline{au}) = a(\bar{u} + u + T(\bar{u}))$$

or

$$\overline{au} + a\bar{u} = T(\overline{au} + a\bar{u})$$

for all $u \in F$. Since $\overline{au}^2 = a\bar{u}^2$, $a^{1/2}\bar{u} + a\bar{u} \in K$ for all $u \in F$. However, $a^{1/2} + a \neq 0$, so this is impossible. \square

LEMMA 5.5. *If $q^m > 8$ then $K = \{z \in F \mid (u \circ v) \circ z = u \circ (v \circ z) \text{ for all } u, v \in F\}$.*

Proof. Call the indicated set L . If $a \in K$ then, by definition, $(u \circ v) \circ a = (u \circ v)a$ and $u \circ (v \circ a) = \bar{u}^2(va) + \bar{u}T(va) + T(\bar{u}(va))$. Thus, $L \supseteq K$.

Note that (L, \circ) is a field. The maps $u \rightarrow u \circ z$ for $z \in L^*$ form a group acting semiregularly on F^* . If L is $GF(q^l)$, then $q^l - 1 \mid q^m - 1$, so $l \mid m$. Assume that $l > 1$. Since m is odd, $l \geq 3$. Let $a \in K - GF(2)$. Then $(a \circ u) \circ v = a \circ (u \circ v)$ for all u, v in the field L . The argument in Lemma 5.4 can now be repeated (with u and v always in L) in order to obtain a contradiction. This completes the proof of both Lemma 5.5 and Theorem 5.3. \square

6. Third cousins. Let F, K and T be as in § 4, with $q > 2$. Fix $k \in K - GF(2)$. Using (4.5), we will again define $x * y, \bar{x}$ and $x \circ y$; however, these expressions will have nothing to do with those of the preceding section (except, of course, for the fact that the corresponding planes are cousins).

For $x, y \in F$ write

$$x * y = x^2y + kxT(xy).$$

LEMMA 6.1. *If $u * y - v * y = 0$ then $u = v$ or $y = 0$.*

Proof. If $(u * y - v * y)y = 0$ then

$$u^2y^2 + kuyT(uy) = v^2y^2 + kvyT(vy).$$

Set $\alpha = uy$ and $\beta = vy$. Then

$$\alpha^2 + k\alpha T(\alpha) = \beta^2 + k\beta T(\beta).$$

Apply T , and use (4.1):

$$T(\alpha)^2 + kT(\alpha)T(\alpha) = T(\beta)^2 + kT(\beta)T(\beta).$$

Thus, $T(\alpha) = T(\beta)$, so $\alpha^2 + \beta^2 = k(\alpha + \beta)T(\alpha)$. If $\alpha = \beta$, the lemma is clear. If $\alpha \neq \beta$ then $\alpha + \beta = kT(\alpha)$, so $0 = T(\alpha) + T(\beta) = kT(\alpha)$ and $\alpha + \beta = 0$. Thus, $\alpha = \beta$, as required. \square

DEFINITION 3. Let $x \rightarrow \bar{x}$ be the inverse of the map $x \rightarrow (x * 1)/(k + 1)$. Thus,

$$(6.2) \quad x = \frac{\bar{x}^2 + k\bar{x}T(\bar{x})}{k + 1}.$$

Apply T and obtain $T(x) = T(\bar{x})^2$. Also, $\bar{a} = a^{1/2}$ if $a \in K$.

DEFINITION 4. Let $y \rightarrow y'$ be the inverse of $y \rightarrow (1 * y)/(k + 1)$. Thus,

$$y = \frac{y' + kT(y')}{k + 1}.$$

This time, $T(y) = T(y')$, and we can solve for y' :

$$y' = (k + 1)y + kT(y).$$

Then $a' = a$ if $a \in K$.

DEFINITION 5. $x \circ y = (\bar{x} * y')/(k + 1)$.

THEOREM 6.3. (F, \circ) is a quasifield. It is never a field.

Proof. If $a \in K$ then $a \circ y = (\bar{a} * y')/(k + 1) = (a^{1/2} * y')/(k + 1) = (ay' + kaT(y'))/(k + 1) = y$ and $x \circ a = (\bar{x} * a')/(k + 1) = (\bar{x} * a)/(k + 1) = a(\bar{x} * 1)/(k + 1) = ax$. By Lemma 6.1, (F, \circ) is thus a quasifield. The theorem is then a consequence of the next result.

LEMMA 6.4. $K = \{y \in F \mid (u + v) \circ y = u \circ y + v \circ y \text{ for all } u, v \in F\}$.

Proof. Let L denote the right-hand set. If $a \in K$ then $u \circ a = ua = a \circ u$, so that $(u + v) \circ a = u \circ a + v \circ a$ and $K \subseteq L$. Note that $y \in L$ if and only if $\bar{u} + \bar{v} * y' = \bar{u} * y' + \bar{v} * y'$ for all $u, v \in F$. Set $L' = \{y' \mid y \in L\}$. Then L' consists of all $\zeta \in F$ such

that the following holds for all $u, v \in F$:

$$(6.5) \quad \overline{u+v}^2 \zeta + k\overline{u+v}T(\overline{u+v}\zeta) = \bar{u}^2 \zeta + k\bar{u}T(\bar{u}\zeta) + \bar{v}^2 \zeta + k\bar{v}T(\bar{v}\zeta).$$

Thus, L' is a vector space over K , and $L' \supseteq K$. We must show that $L' = K$.

Assume that $\dim L' \geq 2$. Define a nonsingular symmetric K -bilinear form on F by setting $(x, y) = T(xy)$. Then 1^\perp is the space of trace 0 elements F , and $1^\perp \supset L'^\perp$. From now on, \bar{u} and \bar{v} will be chosen from 1^\perp . Since $T(\alpha) = T(\bar{\alpha})^2$, this amounts to choosing $u, v \in 1^\perp$. Then $u+v$ and $\overline{u+v}$ also belong to 1^\perp .

By (6.2), $\bar{u}^2 = (k+1)u$. Thus, (6.5) reduces to

$$(u+v)T((u+v)\zeta^2) = uT(u\zeta^2) + vT(v\zeta^2)$$

for all $u, v \in 1^\perp$ and $\zeta \in L'$. Then $uT(v\zeta^2) = vT(u\zeta^2)$. Since $\dim 1^\perp > \dim L'^\perp$ we can find $v \in 1^\perp$ and $\zeta \in L'$ such that $T(v\zeta^2) = (v, \zeta^2) \neq 0$. Then each $u \in 1^\perp$ lies in the 1-space Kv . Since $\dim 1^\perp = m-1 \geq 2$, this is ridiculous. This completes the proof of both Lemma 6.4 and Theorem 6.3. \square

By definition, the plane over (F, \circ) has a very nice collineation of order $q^m - 1$ [STK, Thm. 4.2(iii)]. For completeness, we will exhibit this collineation.

PROPOSITION 6.6. *There is a collineation g of order $q^m - 1$ which fixes 0 and two points x_∞ and y_∞ at infinity, such that $\langle g \rangle$ has orbits of length $q^m - 1$ on the lines $0x_\infty$, $0y_\infty$ and $x_\infty y_\infty$.*

Proof. The lines through the origin of the plane over (F, \circ) are $x = 0$ and $y = n \circ x$. Define g by

$$(x, y)^g = ([1^*(\zeta^{-1}x')]/(k+1), \zeta y),$$

where $\langle \zeta \rangle = GF(q^m)^*$. Clearly, $x = 0$ and $y = 0$ are fixed lines. We will show that g sends $y = n \circ x$ to $y = r \circ x$, where $\bar{n} = \bar{r}\zeta$.

By definition, $(x, n \circ x)^g = (u, \zeta(n \circ x))$, where $u = [1^*(\zeta^{-1}x')]/(k+1)$. The definition of u' shows that $u' = \zeta^{-1}x'$, so $x' = \zeta u'$. Now

$$\begin{aligned} \zeta(m \circ x) &= \zeta(\bar{m} * (\zeta u')) / (k+1) \\ &= \zeta[\bar{m}^2 \zeta u' + k\bar{m}T(\bar{m}\zeta u')] / (k+1) \\ &= (\bar{r} * u') / (k+1) = r \circ u. \end{aligned}$$

Thus, g sends points of the form $(x, m \circ x)$ to points of the form $(u, r \circ u)$.

Since both $x \rightarrow (x * 1)/(k+1)$ and its inverse $x \rightarrow x'$ are additive (in fact, K -linear), g is a collineation. Moreover, the relations $\bar{r} = \bar{n}\zeta$ and $u' = x'\zeta^{-1}$ prove the desired transitivity on the line $y = 0$ and the line at infinity; on the line $x = 0$, this transitivity is obvious. This proves the result. \square

Remarks. 1. Let $F(k)$ denote the quasifield in Theorem 6.3. Clearly, $\text{Gal}(GF(q^m)/GF(q))$ lies in $\text{Aut } F(k)$, while $\text{Aut } GF(q^m)$ does not.

If $q = p^2$ is a square, and $k^p = k$, then the involutory field automorphism θ defined by $x^\theta = x^{p^m}$ is in $\text{Aut } F(k)$. If $x^\theta = x$ then $T(x)$ is also obtained from the trace map $GF(p^m) \rightarrow GF(p)$, and we obtain a Baer subplane which can be coordinatized by a quasifield obtained in the same manner as $F(k)$ was. In particular, this subplane is non-desarguesian.

2. In the notation of (4.5), $F(k)$ arises from the nonsingular point $\langle u + kw \rangle$. By (4.3), $\langle u + kw \rangle^j = \langle u + k_1 w \rangle$ with $k_1 = k/(k+1)$, so the planes over $F(k)$ and $F(k_1)$ are

isomorphic. This accounts for the 2 in the denominator occurring in [STK, Thm. 4.2(iii)].

3. By [STK, Thm. 4.2(iii)], the plane over $F(k)$ is not a semifield plane. It seems to be difficult to prove this directly from the definition of $F(k)$.

7. Homologies. Let \mathbf{A} be a second, third or fourth cousin of $AG(2, q^m)$. The group induced by $\text{Aut}(\mathbf{A})$ on the line at infinity is described in [STK, Thm. 4.2]. In order to deal with expansions of these planes, we will need information concerning the groups of homologies with center 0. This amounts to an easy application of parts of the last two sections when \mathbf{A} is a second or third cousin; however, a different approach is required in order to prove the corresponding result for fourth cousins.

LEMMA 7.1. *Let \mathbf{A} be a second, third or fourth cousin of $AG(2, q^m)$, where $q^m > 8$. Let H denote the group of all homologies with center 0. Then $H \cong GF(q)^*$.*

Proof. If (F, \circ) is one of the quasifields in §§ 5 or 6, then H is isomorphic to the group of all $x \in F^*$ such that $(u + v) \circ x = u \circ x + v \circ x$ and $(u \circ v) \circ x = u \circ (v \circ x)$ for all $u, v \in F$ (Dembowski [3, p. 132]). Now apply Lemmas 5.5 and 6.4.

The remainder of this section will be devoted to the case of fourth cousins. In order to prove Lemma 7.1 in this case, we will need a description of their spreads. This will be obtained from a description of desarguesian spreads different from that of § 4.

Let K, F and T be as usual. Let $F' = GF(q^{2m})$ and $K' = GF(q^2)$. We will depart from the notation in § 4 by writing $V = F' \oplus K'$ and

$$Q(\alpha, r) = T(\alpha\bar{\alpha}) + r\bar{r}$$

for $\alpha \in F'$ and $r \in K'$; here, $\bar{\alpha} = \alpha^{q^m}$. Note that $K' \not\subseteq F$.

Let W denote the kernel of T . Set

$$\Sigma[\theta] = \{(\theta w + \theta r, r) \mid w \in W, r \in K'\}$$

whenever $\theta\bar{\theta} = 1$, and

$$\Sigma = \{\Sigma[\theta] \mid \theta\bar{\theta} = 1\}.$$

Then $\Sigma[\theta]$ is a totally singular $m + 1$ -space (so that V is an $\Omega^+(2m + 2, q)$ space), and Σ is a spread.

If $r \neq 0$ then $(0, r)$ is nonsingular. Set $\Sigma' = \Sigma(\{(0, r)\})$. Then Σ' is a symplectic spread, which can be identified with the set of all K -subspaces

$$(7.2) \quad \Sigma'[\theta] = \theta W + \theta r K$$

of F' , where $\theta\bar{\theta} = 1$.

If $r \in K$ then (7.2) states that $\Sigma'[\theta] = \theta F$. Thus, Σ' is desarguesian in this case, and hence so is Σ .

Every $r \in K' - K$ determines a fourth cousin of $AG(2, q^m)$. Clearly, r and ar determine the same cousin if $a \in K^*$. Note that r and \bar{r} determine isomorphic cousins (compare [STK, Thm. 4.2(iv)]).

If $\phi\bar{\phi} = 1$, then $x \rightarrow \phi x$ sends $\Sigma'[\theta]$ to $\Sigma'[\phi\theta]$. This produces the cyclic collineation group appearing in [STK, Thm. 4.2(iv)].

We are now in a position to complete the proof of Lemma 7.1. Fix $r \in K' - K$. The group H of homologies of $\mathbf{A}(\Sigma')$ with center 0 consists of those invertible semilinear transformations of the K -space F' which induce the identity on Σ' .

Assume that $|H| > q - 1$. Clearly, H is normalized by the above cyclic collineation group of order $q^m + 1$. It follows that there is an irreducible collineation group $\langle g \rangle$

centralizing some $h \in H$ such that $|h| \nmid q-1$. By Schur's lemma, $C_{\Gamma L(F)}(g) \cong F^{**}$. Consequently, h has the form $x \rightarrow lx$ for some $l \in F' - K$.

Now $l\Sigma'[1] = \Sigma'[1]$. Since $\dim W = m-1 \geq 2$, $lW \cap W \neq 0$. Then $l \in F$, so that $lW \subseteq F \cap \Sigma'[1] = W$ (since $r \in K' - K$). Consequently, $|l|$ divides both $|F|-1$ and $|W|-1$. However, $|l| \nmid q-1$, so this is ridiculous.

This completes the proof of Lemma 7.1. \square

Note that the above argument provides a direct verification of the fact that fourth cousins are nondesarguesian.

8. Expanded cousins of desarguesian spreads. We are finally ready to deal with the spreads $S(\Sigma(y)^e)$ obtained from a desarguesian spread Σ of an $\Omega^+(2m+2, q^e)$ space, where e and m are odd.

THEOREM 8.1. *If $\Sigma(y)$ is a second, third or fourth cousin of the $AG(2, (q^e)^m)$ spread, where $e > 1$, $m > 1$ and em is odd, then $S(\Sigma(y)^e)$ is a nondesarguesian spread in an $\Omega^+(2em+2, q)$ space.*

Proof. Assume that $\Sigma^* = S(\Sigma(y)^e)$ is desarguesian. Let y^* be as in Lemma 2.1. Then $\Sigma^*(y^*)$ must be a cousin of $AG(2, q^{em})$, while $\Sigma^*(y^*) = \Sigma(y)^e$. Thus, $\Sigma^*(y^*)$ is nondesarguesian. Now two applications of Lemma 7.1 produce a contradiction. \square

THEOREM 8.2. (i) *The nondesarguesian spreads in Theorem 8.1 are not equivalent to the nondesarguesian spreads in Theorem 3.1.*

(ii) *The expanded fourth cousins in Theorem 8.1 are not equivalent to the expanded second or third cousins.*

Proof. (i) Assume that one of the spreads Σ^* in Theorem 3.1 is equivalent to one of those in Theorem 8.1. Then $H = \Gamma O^+(6e+2, q)_{\Sigma^*}$ has a subgroup G_N or G_M as in Theorem 3.1, as well as a subgroup with an orbit of length $|\Sigma^*|-1$ or $|\Sigma^*|-2$. Thus, H is at least 2-transitive on Σ^* . This contradicts Lemma 3.3.

(ii) Once again this follows from Lemma 3.3. \square

An explicit description of expanded third cousins is given in (9.10).

9. New Kerdock sets. In [STK, § 10], new Kerdock sets were shown to exist. Similarly, by [STK, § 5], the spreads in §§ 3 and 8 also yield new Kerdock sets over any field of characteristic 2, involving matrices of an arbitrarily large size. In this section we will provide explicit examples, using expanded third cousins of desarguesian planes. Instead of starting from a spread, we will begin with a direct construction, later verifying that it arises from such a cousin.

Let $F = GF(q^{em})$, $K = GF(q^e)$ and $K' = GF(q)$, where q is even, em is odd, and $e, m \neq 1$. Let $T: F \rightarrow K$ and $T': F \rightarrow K'$ be the trace maps.

LEMMA 9.1. *If $z \in F$ and $k \in K$ then*

(i) $T'(T(z)) = T'(z)$ and

(ii) $T'(kzT(z)) = T'(kz^2)$.

Proof. (i) $L(z) = T'(T(z)) - T'(z)$ defines a K' -linear map $F \rightarrow K'$ such that $L(1) = 0$ and $L(z^q) = L(z)$. Then $L[\sum_{i=1}^{em} x^{q^i}] = emL(x) = L(x)$, while $\sum_{i=1}^{em} x^{q^i} \in K'$, so $L(x) = 0$.

(ii) By (i), $T'(kzT(z)) = T'(T(kzT(z))) = T'(kT(z)T(z)) = T'(kT(z)^2) = T'(T(k^{1/2}z))^2 = T'(k^{1/2}z)^2 = T'(kz^2)$, as required. \square

Next, form the K' -space $F \oplus K'$. This has a natural inner product defined by $(\alpha, a) \cdot (\beta, b) = T'(\alpha\beta) + ab$. This is a nonsingular symmetric bilinear form, and admits an orthonormal basis. Fix any such basis, and use it to identify matrices and linear transformations.

Now fix $k \in K - GF(2)$, and set $k^* = 1 + k^{1/2}$.

For $s \in F$, define M_s by

$$(\alpha, a)M_s = (s^2\alpha + ksT(s\alpha) + k^*sT'(k^*s\alpha) + ak^*s, T'(k^*s\alpha)).$$

THEOREM 9.2. $\{M_s | s \in F\}$ is a Kerdock set of $(em + 1) \times (em + 1)$ skew-symmetric matrices.

Proof. Since

$$\begin{aligned} (\alpha, a)M_s \cdot (\alpha, a) &= T'(\alpha[s^2\alpha + ksT(s\alpha) + k^*sT'(k^*s\alpha) + ak^*s]) + aT'(k^*s\alpha) \\ &= T'(\alpha^2s^2) + T'(\alpha ksT(s\alpha)) + T'(\alpha k^*s)T'(k^*s\alpha) \\ &\quad + T'(\alpha ak^*s) + aT'(k^*s\alpha) \\ &= T'(\alpha^2s^2(1 + k^{*2})) + T'(kasT(\alpha s)) = 0 \end{aligned}$$

by Lemma 9.1(ii) (with $z = \alpha s$), each M_s is skew-symmetric.

Assume that

$$(9.3) \quad (\alpha, a)(M_r + M_s) = 0$$

with $r \neq s$. Then

$$(9.4) \quad T'(k^*r\alpha) = T'(k^*s\alpha)$$

and

$$(9.5) \quad r^2\alpha + krT(r\alpha) + k^*rT(k^*r\alpha) + ak^*r = s^2\alpha + ksT(s\alpha) + k^*sT(k^*s\alpha) + ak^*s.$$

Multiply (9.5) by α , and set $x = r\alpha$ and $y = s\alpha$:

$$(9.6) \quad x^2 + kxT(x) + k^*xT'(k^*x) + ak^*x = y^2 + kyT(y) + k^*yT'(k^*y) + ak^*y.$$

Apply T :

$$\begin{aligned} T(x)^2 + kT(x)^2 + k^*T(x)T'(k^*x) + T(ak^*x) \\ = T(y)^2 + kT(y)^2 + k^*T(y)T'(k^*y) + T(ak^*y). \end{aligned}$$

By (9.4), $T'(k^*x) = T'(k^*y)$, so this reduces to

$$(T(x) + T(y))^2(1 + k) = k^*(T(x) + T(y))T'(k^*x).$$

Now $T(x) + T(y)$ is 0 or $T'(k^*x)/k^*$. If $k^*(T(x) + T(y)) = T'(k^*x)$, apply T' :

$$\begin{aligned} T'(k^*x) &= T'(T(k^*T(x) + k^*T(y))) = T'(T(k^*x + k^*y)) \\ &= T'(k^*x) + T'(k^*y) = 0 \end{aligned}$$

by Lemma 9.1(i) and (9.4). Thus, $T(x) + T(y) = T'(k^*x)/k^* = 0$.

This leaves us with the case $T(x) + T(y) = 0$. By (9.6) and (9.4),

$$(x + y)^2 + k(x + y)T(x) + k^*(x + y)T'(k^*x) + ak^*(x + y) = 0.$$

If $\alpha = 0$ then $a = 0$ by (9.5). Assume that $a \neq 0$, so $\alpha \neq 0$ and $x + y \neq 0$. Then

$$x + y + kT(x) + k^*T'(k^*x) + ak^* = 0.$$

Consequently, $x + y \in K$, so that $x + y = T(x) + T(y) = 0$, which is not the case. This contradiction completes the proof of Theorem 9.2. \square

Remark 9.7. Let A_s be the matrix defined by $(\alpha, a)A_s = (s\alpha, a)$. Then $M_s = A_s M_1 A_s$. Also, A_s is a symmetric matrix, since $(\alpha, a)A_s \cdot (\beta, b) = T(\alpha s\beta) + ab = (\alpha, a) \cdot (\beta, b)A_s$. Clearly, the matrices $\{A_s | s \in F^*\}$ form a cyclic automorphism group of the Kerdock set in Theorem 9.2 which is transitive on the nonzero members. Of course, Kerdock sets need not have such a cyclic automorphism group: none of the ones arising from Theorem 3.1 does.

Remark 9.8. In the same notation, the usual Kerdock set on $F \oplus K'$ consists of the matrices $N_s, s \in F$, defined by

$$(\alpha, a)N_s = (s^2\alpha + sT'(s\alpha) + as, T'(s\alpha)).$$

Once again, $N_s = A_s N_1 A_s$. The corresponding spread is the desarguesian one in (4.2).

Remark 9.9. The Kerdock set corresponding to the spread in [STK, § 8] can be described in a similar manner. Let $F = GF(q^3), K = GF(q)$, and define $(\alpha, a) \cdot (\beta, b)$ as usual. This time,

$$(\alpha, a)N_s = (as^{q+q^2} + \alpha^q s^{q^2} + \alpha^{q^2} s^q, T(\alpha s^{q+q^2})).$$

It is an amusing exercise to verify directly that this does, indeed, yield a Kerdock set.

We now turn to the spread from which the Kerdock set of Theorem 9.2 arises.

Let F, K, K', T, T', k and k^* be as before. Let V_0 denote the F -space with basis e, f , regard V_0 as a K' -space, and form the $(2em + 2)$ -dimensional vector space $V' = V_0 \oplus \langle u', w' \rangle$. Define $Q': V' \rightarrow K'$ by

$$Q'(\alpha e + \beta f + cu' + dw') = T'(\alpha\beta) + c^2 + cd.$$

This yields an $\Omega^+(2em + 2, q)$ space. Set

$$(9.10) \quad \begin{aligned} \Sigma^*[\infty] &= Ff + K'(u' + w'), \\ \Sigma^*[s] &= \{\alpha e + (s^2\alpha + ksT'(s\alpha) + k^*sa)f + T'(k^*s\alpha)u' + aw' \mid \alpha \in F, a \in K\} \end{aligned}$$

and $\Sigma^* = \{\Sigma^*[s] \mid s \in F \cup \{\infty\}\}$.

THEOREM 9.11. (i) Σ^* is an expanded third cousin of $AG(2, (q^e)^m)$.

(ii) The Kerdock set defined by the pair $(\Sigma^*, \Sigma^*[\infty])$ is the Kerdock set in Theorem 9.2.

(iii) The Kerdock set in Theorem 9.2 is not equivalent to the desarguesian one in Remark 9.8.

Proof. $\Sigma^* - \{\Sigma^*[\infty]\}$ can be obtained as follows. Identify $\Sigma^*[0]$ with $F \oplus K'$ in the natural manner. Let $\pi: \Sigma^*[0] \rightarrow \Sigma^*[\infty]$ be defined by $(\alpha e + aw')\pi = \alpha f + a(u' + w')$. If $s \in F$ let M_s be as in (9.2). Then

$$(9.12) \quad \Sigma^*[s] = \{\alpha e + aw' + (\alpha e + aw')M_s\pi \mid \alpha \in F, a \in K'\}.$$

Since M_s is skew-symmetric, $(\alpha e + aw', (\alpha e + aw')M_s\pi) = (\alpha e + aw')M_s \cdot (\alpha e + aw) = 0$. Thus, $\Sigma^*[s]$ is a totally singular $(em + 1)$ -space.

In order to compute $\langle u' \rangle^\perp \cap \Sigma^*/\langle u' \rangle$, set $a = 0$ and $u = 0$ in (9.10) and obtain (4.5) (with K' replacing K in (4.5)). By definition (§ 2 and [STK, § 3]), Σ^* is obtained as required in (i). Then (ii) also follows by definition [STK, § 5]. Finally, (iii) is an immediate consequence of Theorem 8.1 and [STK, Lemma 5.4]. \square

THEOREM 9.13. Let q be a power of 2, and let $2n - 1$ be composite.

(i) There are at least two inequivalent nondesarguesian spreads in an $\Omega^+(4n, q)$ space.

(ii) There are at least three inequivalent nondesarguesian Kerdock sets of $2n \times 2n$ matrices over $GF(q)$.

Proof. (i) Write $2n - 1 = em$ with $e > 1$ and $m > 1$. If $q^{em} \neq 2^9$ we can apply Theorem 8.1 (for a suitable choice of e and m). If $q^{em} = 2^9$, use Theorem 3.1.

(ii) If Σ is one of the spreads in Theorem 9.11, then $\Gamma O^+(4n, q)_\Sigma$ is not transitive on Σ . Consequently, the result follows from [STK, Lemma 5.4]. \square

10. Concluding remarks. The reader will have noticed that we have left at least as many questions unanswered as we have answered. Here is a sample of some of these questions.

(1) Prove that all of the spreads in Theorem 8.1 are inequivalent. This will require a much more geometric approach to inequivalence questions.

(2) The expansion process can be repeated indefinitely. Do new spreads always arise? Prove that they do in the case of cousins of desarguesian spreads.

In particular, the fourth cousins of desarguesian planes can be expanded and sliced over and over in such a way that each resulting translation plane has a collineation transitively permuting the points at infinity. Presumably, this produces enormous numbers of flag-transitive translation planes. (Of course, we already know at least $q/2 \log_2 q$ flag-transitive planes of order q^{2n-1} [STK, Thm. 4.2iv]. In particular, if $2n-1$ is composite, then there are more than $2^{\sqrt{n}}/2\sqrt{n}$ flag-transitive planes of order 2^{2n-1} .)

Similarly, third cousins of desarguesian planes can be expanded over and over while retaining the existence of a collineation behaving as in Proposition 6.6. (However, there are already known to be more than $2^{\sqrt{n}}/2\sqrt{n}$ planes of order 2^{2n-1} behaving this way whenever $2n-1$ is composite.)

(3) The orthogonal spreads in Theorem 8.1 do not have transitive groups, and hence produce large numbers of nonisomorphic translation planes [STK, (3.6)]. Do any of them have interesting properties? Some have the rather perverse property that no collineation acts nontrivially on the line at infinity; when expanded, these undoubtedly produce large numbers of inequivalent Kerdock sets.

(4) If Σ is as in Theorem 8.1, and if W is an $\Omega^-(2em, q)$ subspace, then $W \cap \Sigma$ is a spread of W . Show that the resulting spreads are not equivalent to spreads obtained from desarguesian $\Omega^+(2em+2, q)$ spreads.

(5) Find an internal criterion for a translation plane to be symplectic.

REFERENCES

- [1] A. M. COHEN AND H. A. WILBRINK, *The stabilizer of Dye's spread on a hyperbolic quadric in $PG(4n-1, 2)$ within the orthogonal group*, to appear.
- [2] 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), pp. 323-326.
- [3] P. DEMBOWSKI, *Finite Geometries*, Springer, Berlin-Göttingen-Heidelberg, 1968.
- [4] P. FONG AND G. M. SEITZ, *Groups with a (B, N) -pair of rank 2.I*, *Invent. Math.*, 21 (1973), pp. 1-57.
- [5] D. F. HOLT, *Transitive permutation groups in which an involution central in a Sylow 2-subgroup fixes a unique point*, *Proc. LMS* (3), 37 (1978), pp. 165-192.
- [6] W. M. KANTOR, *Spreads, translation planes and Kerdock sets. I*, this Journal, 3 (1982), pp. 151-165.
- [7] H. LÜNEBURG, *Translation Planes*, Springer, New York, 1980.