Journal of Algebraic Combinatorics 3 (1994), 405–425

Projective Planes of Order q whose Collineation Groups have Order q^2

WILLIAM M. KANTOR* kantor@math.uoregon.edu
Department of Mathematics, University of Oregon, Eugene, OR 97403

Received February 25, 1992; Revised January 10, 1994

IN MEMORY OF R.H. BRUCK

Abstract. Translation planes of order q are constructed whose full collineation groups have order q^2.

Keywords: collineation group, projective plane

1. Introduction

The most interesting finite projective planes are those having reasonably large collineation groups; such planes are the most amenable to characterizations. The present note concerns planes that are uninteresting according to the preceding criterion: ones with small groups. If a translation plane has order $q = p^n$, where p is prime, then its full collineation group has order at least $q^2(p-1)$: translations and homologies must be present. This minimal possible order can occur, even when $p = 2$:

Theorem 1.1 *If $q = 2^n$ with n is odd, composite and greater than 9, then there are translation planes of order q whose full collineation groups have order q^2. If n is neither 27 nor the product of 3 and a prime, then there are more than $q(2^{\sqrt{n}}/4n^2)$ pairwise nonisomorphic planes of this sort.*

In particular, every point of each of these "boring" affine planes has the 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. Moreover, it appears that the only published examples of translation planes of order $q = p^n$ whose full collineation groups have order exactly $q^2(p-1)$ are two planes of order $q = 17^2$ studied in [2].

How can one calculate the full collineation group of a plane? This is, in general, a difficult and apparently tedious task—and one that is especially hard when the plane has very large order. It is sometimes possible to replace calculations with group-theoretic considerations when the group is known to be relatively large (e.g., due to transitivity properties). Here we are dealing with the opposite situation: we want a (very!) small group. However, [6] provides a framework that allows us to have things both ways: the fact that a certain group *related* to the collineation group is somewhat large allows us to get enough information to

*Research supported in part by NSF and NSA grants.

show that the collineation group is small. On the other hand, the required group theory is that of the late-1960's: it does not involve information concerning simple groups.

Section 2 reviews the background needed from [6, 7]: orthogonal and symplectic spreads. Section 3 contains remarks concerning a more computational version of orthogonal spreads: "Kerdock sets". Section 4 constructs some translation planes and eliminates homologies. This appears to be a highly computational question; dealing with it is dull and tedious, somewhat resembling parts of [7] but noticeably more complicated. It would be very desirable to have a general framework in which the kernel of a translation plane could be calculated with much less pain. Section 5 identifies the planes in Section 4 with some of those in Section 2. The pleasant, noncomputational part of the proof of the Theorem appears in Section 6, where projective geometry and group theory are used (together with computational results from earlier sections) in order to limit and then determine the automorphism groups of some orthogonal spreads. Finally, Section 7 glues together the results of the previous sections in order to complete the proof of the Theorem.

The techniques in [6, 7] are very flexible. There they were used in order to obtain the only known nondesarguesian affine planes of even order admitting solvable flag-transitive groups, as well as translation planes of even order q whose collineation groups contain elements having a $q-1$-cycle on the line at infinity (cf. Example 2 in Section 2). In the present paper the same techniques are employed in the opposite direction, producing minimal groups. The possibility of achieving this minimality was mentioned in [9, p.154]. The examples studied in [6–8], as well as those in the Theorem, indicate an inherent difficulty in classifying all translation planes.

2. Orthogonal spreads

Throughout this paper, F, K and K' will be fields satisfying

$$F \supset K \supset K' = GF(2), [F : K'] \text{ is odd and greater than 9.} \tag{2.1}$$

Note that each integer q appearing in (1.1) occurs as $|F|$ for some fields satisfying (2.1). Let L denote either K or K'.

In this section we will review some of the required background from [6, 7]. Let V be a vector space of dimension $4m$ over L, $m \geq 2$, equipped with a quadratic form Q of Witt index $2m$; the associated bilinear form is $(u, v) = Q(u+v) - Q(u) - Q(v)$. 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. If y is any nonsingular point of V, write

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

Then $y^\perp/y$ is a symplectic space (with respect to the alternating form $(u+y, v+y) = (u, v)$ for $u, v \in y^\perp$), and Σ_y is a spread in the usual sense [3, p. 219]—but it is even a *symplectic spread*: each of its members is a totally isotropic $2m-1$-space. Let $\mathcal{A}(\Sigma_y)$ denote the translation plane determined by Σ and y; it 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 [6].

A crucial property of these planes is as follows:

Proposition 2.2 [6, (3.5), (3.6), (3.7)]. *Let Σ_i be a spread in the orthogonal space V_i over L (with associated quadratic form Q_i) for $i = 1, 2$, and let y_i be a nonsingular point of V_i. If g is any isomorphism $\mathcal{A}(\Sigma_{y_1}) \to \mathcal{A}(\Sigma_{y_2})$, then there is a semilinear transformation $h: V_1 \to V_2$ such that the following hold:*

(i) $y_1^h = y_2$;

(ii) $\Sigma_1^h = \Sigma_2$;

(iii) $Q_2(v^h) = aQ_1(v)^\tau$ *for some* $a \in L$, *some* $\tau \in \mathrm{Aut}L$, *and all* $v \in V$; *and*

(iv) *If $\tilde{h}$ denotes the map $y_1^\perp/y_1 \to y_2^\perp/y_2$ induced by h, then $\tilde{h}$ also induces an isomorphism $\mathcal{A}(\Sigma_{y_1}) \to \mathcal{A}(\Sigma_{y_2})$, and $g\tilde{h}^{-1}$ is an automorphism of the plane $\mathcal{A}(\Sigma_{y_1})$ that is the identity on the line at infinity; in particular, it is a homology if $0^g = 0$.*

In other words, two of these planes are isomorphic if and only if there is an isomorphism of the orthogonal spaces inducing an isomorphism of the planes; and every collineation of one of these planes is the product of a translation, a homology and a semilinear transformation preserving the symplectic structure of $y_1^\perp/y_1$. In particular, the determination of the collineation group of a plane $\mathcal{A}(\Sigma_y)$ can be achieved in three stages:

- determine the group $G(\Sigma)$ of all semilinear transformations of V that "preserve" Q as in (2.2iii) and send Σ to itself;
- determine the stabilizer $G(\Sigma)_y$; and
- determine the group of homologies of $\mathcal{A}(\Sigma)_y$ fixing 0.

This is essentially how Theorem 1.1 will be proved.

First we need to provide examples leading to the orthogonal spreads needed in Theorem 1.1.

Examples Let F, K and K' be as in (2.1). Let $T: F \to K$ and $T': F \to K'$ 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

$$\begin{aligned} &0 \times 0 \times F \times K \quad \text{and} \\ &\{(\alpha, a, s^2\alpha + sT(s\alpha) + sa, T(s\alpha)) \mid \alpha \in F, a \in K\} \quad \text{for } s \in F. \end{aligned} \tag{2.3}$$

Here, "lifts" refers to the fact that $\Sigma_{\langle 0,1,0,1\rangle}$ consists of the subspaces $0 \times 0 \times F \times 0 + \langle 0,1,0,1\rangle$ and $\{(\alpha, 0, s^2\alpha, 0) + \langle 0,1,0,1\rangle \mid \alpha \in F\}$, $s \in F$, and these evidently constitute the usual desarguesian spread in $\langle 0,1,0,1\rangle^\perp/\langle 0,1,0,1\rangle$, producing the desarguesian plane $\mathcal{A}(\Sigma_{\langle 0,1,0,1\rangle})$ of order $|F|$. The orthogonal spread (2.3) is called the *desarguesian spread* in [6]. Note that the $|F| - 1$ isometries

$$g_\zeta\colon (\alpha, a, \beta, b) \mapsto (\zeta\alpha, a, \zeta^{-1}\beta, b), \quad \text{where } \zeta \in F^*, \tag{2.4}$$

of $F \times K \times F \times K$ fix $\langle 0,1,0,1\rangle$, preserve Σ, and hence act on the plane $\mathcal{A}(\Sigma_{\langle 0,1,0,1\rangle})$. The points fixed by all of these isometries are just those of the 2-space $\langle (0,1,0,0), (0,0,0,1)\rangle$.

Example 2 (*called in* [6, 7] *the "third cousins of the desarguesian spread"*). Fix $k \in K - K'$, and consider the 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 is nonsingular (since $Q(0, k+1, 0, 1) = k+1$) and produces a symplectic spread Σ_{y_k} in the symplectic space $y_k^\perp/y_k$, consisting of the following subspaces:

$$\begin{aligned} &0 \times 0 \times F \times 0 + y_k, \\ &\{(\alpha, 0, s^2\alpha + ksT(s\alpha), 0) + y_k \mid \alpha \in F\} \quad \text{for } s \in F. \end{aligned} \tag{2.5}$$

Namely, $(\alpha, a, s^2\alpha + sT(s\alpha) + sa, T(s\alpha))$ is perpendicular to $\langle 0, k+1, 0, 1\rangle$ if and only if $a = (k+1)T(s\alpha)$, in which case $(\alpha, a, s^2\alpha + sT(s\alpha) + sa, T(s\alpha)) = (\alpha, 0, s^2\alpha + ksT(s\alpha), 0) + T(s\alpha)(0, k+1, 0, 1)$.

Since $y_k = \langle 0, k+1, 0, 1\rangle$ is fixed by the automorphisms g_ζ defined in (2.4), each g_ζ induces an automorphism of the translation plane $\mathcal{A}(\Sigma_{y_k})$.

Example 2′ The symplectic space $y_k^\perp/y_k$ over K can also be viewed as a symplectic space over K' by using the bilinear form $(u, v)' = T'((u, v))$ for $u, v \in y_k^\perp/y_k$. Then (2.5) also is a symplectic spread of this K'-space.

Example 3 Now consider the K'-space $V = F \times K' \times F \times K'$, equipped with the quadratic form Q' defined by

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

the corresponding bilinear form is again

$$((\alpha, a, \beta, b), (\alpha', a', \beta', b'))' = T'(\alpha\beta' + \alpha'\beta) + ab' + a'b. \tag{2.6}$$

The subspaces $F \times K' \times 0 \times 0$ and $0 \times 0 \times F \times K'$ are totally singular. The spread (2.5), viewed as in Example 2′, lifts to the following orthogonal spread Σ^k (where we have written $k^* = 1 + \sqrt{k}$):

$$\begin{aligned} &0 \times 0 \times F \times K', \\ &\left\{(\alpha, a, s^2\alpha + ksT(s\alpha) + k^*sT'(k^*s\alpha) + k^*sa, T'(k^*s\alpha)) \mid \alpha \in F, a \in K'\right\} \\ &\qquad\qquad \text{for } s \in F. \end{aligned} \tag{2.7}$$

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

$$0 \times 0 \times F \times 0 + \langle 0,1,0,1\rangle,$$
$$\left\{(\alpha, 0, s^2\alpha + ksT(s\alpha), 0) + \langle 0,1,0,1\rangle \mid \alpha \in F, a \in K'\right\} \quad \text{for } s \in F,$$

as in (2.5). (Note that $(\alpha, a, s^2\alpha+ksT(s\alpha)+k^*sT'(k^*s\alpha)+k^*sa, T'(k^*s\alpha))$ is perpendicular to $(0,1,0,1)$ if and only if $(\alpha, a, s^2\alpha+ksT(s\alpha)+k^*sT'(k^*s\alpha)+k^*sa, T'(k^*s\alpha)) = (\alpha, 0, s^2\alpha + sT(s\alpha) + sa, 0) + T'(k^*s\alpha)(0,1,0,1)$.)

Define linear transformations g'_ζ as in (2.4), but this time using the present orthogonal space. Then each g'_ζ is in $G(\Sigma^k)$, and these isometries form a cyclic group fixing the two members $F \times K' \times 0 \times 0$ and $0 \times 0 \times F \times K'$ of Σ^k while permuting the remainder of Σ^k in a single cycle. Note that $0 \times K' \times 0 \times K'$ is the set of vectors fixed by all of the transformations g'_ζ, and that $\langle 0,1,0,1\rangle$ *is the only nonsingular point fixed by all of these isometries* since $K' = GF(2)$. We will determine $G(\Sigma^k)$ in Section 3. For now, we note only that

$$\begin{aligned} &G(\Sigma^k)_{\langle 0,1,0,1\rangle} \text{ is generated by the isometries } g'_\zeta \text{ and some field automorphisms} \\ &(\alpha, a, \beta, b) \mapsto (\alpha^\tau, a^\tau, \beta^\tau, b^\tau), \tau \in \mathrm{Aut}F \text{ (cf. [7, (4.2iii)])}. \end{aligned} \tag{2.8}$$

Example 4 Let $\Psi \in F$ with $T'(\Psi) = 1$, so that the point $\langle \Psi, 0, 1, 0\rangle$ of V is nonsingular: $Q'(\Psi, 0, 1, 0) = 1$. If Σ^k is as in Example 3, then $(\Sigma^k)_{\langle \Psi,0,1,0\rangle}$ is a symplectic spread in the symplectic K'-space $\langle \Psi, 0, 1, 0\rangle^\perp / \langle \Psi, 0, 1, 0\rangle$. The planes occurring in (1.1) are just those of the form $\mathcal{A}\big((\Sigma^k)_{\langle \Psi,0,1,0\rangle}\big)$ such that Ψ generates F.

3. Kerdock sets

Assume that $F, K, K', T, T', k^*, k = k^{*2} + 1, V = F \times K' \times F \times K'$ and Q' are as in Section 2. Note that

$$\begin{aligned} &\text{(i) } T(1) = 1 = T'(1), \text{ (ii) } T'(kT(\gamma)) = T'(k\gamma), \\ &\text{and (iii) } T'(k\gamma T(\gamma)) = T'(k\gamma^2) \qquad \text{for all } \gamma \in F, k \in K \end{aligned} \tag{3.1}$$

[7, (9.1)]. (In (iii) we have $T'(k\gamma T(\gamma)) = T'(T(k\gamma T(\gamma))) = T'(kT(\gamma)T(\gamma)) = T'(kT(\gamma)^2) = T'(T(k\gamma^2)) = T'(k\gamma^2)$.)

Fix a basis $e_1, \ldots, e_{n+1}$ of $F \times K' \times 0 \times 0$, and let $f_1, \ldots, f_{n+1}$ be the corresponding dual basis of $0 \times 0 \times F \times K'$ (so $(e_i, f_j) = \delta_{ij}$ for all i, j). Temporarily use the basis $e_1, \ldots, e_{n+1}, f_1, \ldots, f_{n+1}$ of $F \times K' \times F \times K'$ in order to write vectors and matrices. If a subspace X of V satisfies $0 \times 0 \times F \times K' \cap X = 0$, then X has the form $\{(\alpha, a, 0, 0)\binom{IM}{OI} \mid (\alpha, a) \in F \times K'\}$ for an $(n+1) \times (n+1)$ matrix M. Here, X is totally singular if and only if M is skew-symmetric (i.e., symmetric with 0 diagonal). Letting X range over $\Sigma^k - \{0 \times 0 \times F \times K'\}$ produces a binary *Kerdock set* $\mathcal{K}$ of matrices M: a set of 2^n binary skew-symmetric $(n+1) \times (n+1)$ matrices such that the difference of any two is

nonsingular (cf. [6, 8]). We will not actually need to use matrices: linear transformations will suffice for our computational requirements.

For each $s \in F$ define (for all $\alpha \in F, a \in K'$)

$$(\alpha, a)M_s = (s^2\alpha + ksT(s\alpha) + k^*sT'(k^*s\alpha) + k^*sa, T'(k^*s\alpha)). \tag{3.2}$$

Then Σ^k consists of $0 \times 0 \times F \times K'$ and $\{(x, xM_s) \mid x \in F \times K'\}$ for $s \in F$; or, alternatively, of $0 \times 0 \times F \times K', F \times K' \times 0 \times 0$ and $\{(xM_s^{-1}, x) \mid x \in F \times K'\}$ for $s \in F^*$. It is clear from (3.2) that M_s "depends quadratically" on s, in the sense that the map $M_{s+t} + M_s + M_t$ is additive in both s and t (we will use this sort of observation often in the next section). We will also need a similar formula for M_s^{-1}:

Lemma 3.3 *If $s \neq 0$ then*

$$(\beta, b)M_s^{-1} = (s^{-2}\beta + k^{*-1}s^{-1}b + kk^{*-2}s^{-1}T(s^{-1}\beta) + k^{*-1}s^{-1}T'(k^{*-1}s^{-1}\beta), T'(k^{*-1}s^{-1}\beta)).$$

Proof: If the right side of (3.3) is (α, a) then calculate as follows, using (3.1) and the fact that $k^* + kk^{*-1} + k^{*-1} = 0$:

$$\begin{aligned}
T'(k^*s\alpha) &= T'\Big(k^*s\big[s^{-2}\beta + k^{*-1}s^{-1}b + kk^{*-2}s^{-1}T(s^{-1}\beta) \\
&\qquad + k^{*-1}s^{-1}T'(k^{*-1}s^{-1}\beta)\big]\Big) \\
&= T'(k^*s^{-1}\beta) + T'(b) + T'\big(kk^{*-1}T(s^{-1}\beta)\big) + T'\big(T'(k^{*-1}s^{-1}\beta)\big) \\
&= b + T'(k^*s^{-1}\beta) + T'(kk^{*-1}s^{-1}\beta) + T'(k^{*-1}s^{-1}\beta) = b,
\end{aligned}$$

$$\begin{aligned}
&s^2\alpha + ksT(s\alpha) + k^*sT'(k^*s\alpha) + k^*sa \\
&\quad = s^2\big[s^{-2}\beta + k^{*-1}s^{-1}b + kk^{*-2}s^{-1}T(s^{-1}\beta) + k^{*-1}s^{-1}a\big] \\
&\qquad + ksT\Big(s\big[s^{-2}\beta + k^{*-1}s^{-1}b + kk^{*-2}s^{-1}T(s^{-1}\beta) + k^{*-1}s^{-1}a\big]\Big) \\
&\qquad + k^*sT'\Big(k^*s\big[s^{-2}\beta + k^{*-1}s^{-1}b + kk^{*-2}s^{-1}T(s^{-1}\beta) + k^{*-1}s^{-1}a\big]\Big) \\
&\qquad + k^*sa \\
&\quad = \beta + k^{*-1}sb + kk^{*-2}sT(s^{-1}\beta) + k^{*-1}sa \\
&\qquad + ksT(s^{-1}\beta) + ksk^{*-1}T'(b) + kskk^{*-2}T(T(s^{-1}\beta)) + ksk^{*-1}T'(a) \\
&\qquad + k^*sT'(k^*s^{-1}\beta) + k^*sT'(b) + k^*sT'(kk^{*-1}T(s^{-1}\beta)) + k^*sT'(a) \\
&\qquad + k^*sa \\
&\quad = \beta + k^{*-1}sb + ksk^{*-1}b + k^*sb \\
&\qquad + kk^{*-2}sT(s^{-1}\beta) + ksT(s^{-1}\beta) + kskk^{*-2}T(s^{-1}\beta) \\
&\qquad + k^{*-1}sa + ksk^{*-1}a + k^*sa \\
&\qquad + k^*sT'(k^*s^{-1}\beta) + k^*sT'(kk^{*-1}T(s^{-1}\beta)) + k^*sa \\
&\quad = \beta + [k^{*-1} + kk^{*-1} + k^*]sb + [kk^{*-2} + k + k^2k^{*-2}]sT(s^{-1}\beta) \\
&\qquad + [k^{*-1} + kk^{*-1} + k^*]sa + k^*sT'\big([k^* + kk^{*-1} + k^{*-1}]s^{-1}\beta\big) \\
&\quad = \beta.
\end{aligned}$$

□

Let $N_0 = 0$ and $N_s = (M_{s^{-1}})^{-1}$ if $s \in F^*$.

Corollary 3.4 *Σ^k consists of $F \times K' \times 0 \times 0$ and $\{(xN_s, x) \mid x \in F \times K'\}$ for $s \in F$. If $\ell = k/(k+1)$ then Σ^k and Σ^ℓ are orthogonally equivalent by an orthogonal transformation interchanging $0 \times 0 \times F \times K'$ and $F \times K' \times 0 \times 0$.*

Proof: The first statement was noted above. Let $\ell^* = \sqrt{\ell} + 1$, so $\ell^* = k^{*-1}$. By (3.3),

$$(\beta, b)N_s = (s^2\beta + \ell s T(s\beta) + \ell^* s T'(\ell^* s\beta) + \ell^* sb, T'(\ell^* s\beta)) \tag{3.5}$$

for all $s \in F$, which is the same as (3.2) with k replaced by ℓ. Thus, the orthogonal transformation $(\alpha, a, \beta, b) \mapsto (\beta, b, \alpha, a)$ produces the desired equivalence. □

Proposition 3.6

(i) *$\{M_s \mid s \in F\}$ is not closed under addition.*

(ii) *$\{0, M_s^{-1} \mid 0 \neq s \in F\}$ is not closed under addition.*

Proof: (i) Assume that this set is closed under addition. Let $r, s, t \in F$ with $M_r + M_s = M_t$. Since $(0, a)M_s = (k^* sa, 0)$, it follows that $r + s = t$. By (3.2), for all $\alpha \in F$,

$$\begin{aligned} &krT(r\alpha) + k^* rT'(k^* r\alpha) + ksT(s\alpha) + k^* sT'(k^* s\alpha) \\ &\quad = k(r+s)T((r+s)\alpha) + k^*(r+s)T'(k^*(r+s)\alpha), \end{aligned}$$

so that

$$\begin{aligned} &k\alpha rT(s\alpha) + k\alpha sT(r\alpha) = k^*\alpha rT'(k^* s\alpha) + k^* sT'(k^* r\alpha), \\ &0 = T(k\alpha r)T(s\alpha) + T(k\alpha s)T(r\alpha) = T(k^*\alpha r)T'(k^* s\alpha) \\ &\quad + T(k^*\alpha s)T'(k^* r\alpha), \end{aligned}$$

and hence $T(\gamma)T'(\delta) = T(\delta)T'(\gamma)$ for all $\gamma, \delta \in F$. When $\delta = 1$ this states that $T(\gamma) = T'(\gamma)$ for all $\gamma \in F$, which is ridiculous.

(ii) This follows from (i) and (3.5). □

More generally:

Proposition 3.7 *No binary Kerdock set is closed under addition.*

Proof: If a binary Kerdock set closed under addition, then the corresponding binary Kerdock code $\mathcal{C}$ also is closed under addition (cf. [6, §5, or 8]), and the weight distribution of the linear code $\mathcal{C}$ is uniquely determined. Then so is the weight distribution of the dual code $\mathcal{C}^\perp$. The latter weight distribution is that of a Preparata code [11, p. 466]. However, there is no *linear* code $\mathcal{C}^\perp$ having the weight distribution of a Preparata code [4, 7.2]. □

Much more generally:

Theorem 3.8 (P. J. Cameron). *If U is a subspace of the space of all skew-symmetric $2m \times 2m$ matrices over any finite field, and if all nonzero elements of U are nonsingular, then* $\dim U \leq m$.

Proof: If $(a_{ij}) \in U$ then $\det(a_{ij}) = \mathrm{Pf}(a_{ij})^2$, where $\mathrm{Pf}(a_{ij})$ is the Pfaffian of (a_{ij}) and is a polynomial of degree m in the a_{ij} [10, p. 373]. Let $A_1, \ldots, A_d$ be a basis of U. If $A = \Sigma_i x_i A_i$ for scalars x_i, then $\mathrm{Pf}(A) = f(x_1, \ldots, x_d)$ for a polynomial f of degree m. By the Chevalley-Warning Theorem [10, p. 140], f has more than one zero if $d > m$. □

4. Quasifields

In this section we will study a class of translation planes defined using a horrible-looking quasifield. In the next section we will see that these planes are exactly the same as some of those arising from the orthogonal spreads Σ^k.

Let $F, K, K' = GF(2), T$ and T' be as in Section 2. Choose k, k^* and Ψ follows:

$$k \in K - K', k^* = 1 + \sqrt{k}; \text{ and } \Psi \in F - K, T'(\Psi) = 1. \tag{4.1}$$

Define the following binary operation # on F:

$$s\#\gamma = B_{\gamma,s} + T'(B_{\gamma,s}\Psi) + T'\big(k^* s[\{\gamma + T'(\gamma)\} + J_{\gamma,s}\Psi]\big) \tag{4.2}$$

where

$$\begin{aligned} J_{\gamma,s} &:= T'\Big(\Big[s^2\{\gamma + T'(\gamma)\} + ksT\big(s\{\gamma + T'(\gamma)\}\big) \\ &\qquad + k^* sT'\big(k^* s\{\gamma + T'(\gamma)\}\big) + k^* sT'(\gamma)\Big]\Psi\Big) \in K' \quad \text{and} \\ B_{\gamma,s} &:= s^2\big[\{\gamma + T'(\gamma)\} + J_{\gamma,s}\Psi\big] + ksT\Big(s\big[\{\gamma + T'(\gamma)\} + J_{\gamma,s}\Psi\big]\Big) \\ &\qquad + k^* sT'\Big(k^* s\big[\{\gamma + T'(\gamma)\} + J_{\gamma,s}\Psi\big]\Big) + k^* sT'(\gamma) \end{aligned} \tag{4.3}$$

for all $\gamma, s \in F$. It is difficult to motivate these bizarre formulas: they are precisely what are needed in Section 7. However, recall that we are trying to prove Theorem 1.1, and hence the unpleasant appearance of (4.2, 4.3) may perhaps be forgiven. By (3.1ii, 4.1),

$$T'(\gamma + T'(\gamma)) = 0 \text{ and } T'\big(\{\gamma + T'(\gamma)\} + J_{\gamma,s}\Psi\big) = T'(\Psi)J_{\gamma,s} = J_{\gamma,s}. \tag{4.4}$$

Proposition 4.5

(i) *$(F, \#)$ determines a translation plane as follows: the points are the elements of $F \times F$, and the lines are the subsets with equations $x = c$ or $y = m\#x + b$ for some $c, m, b \in F$.*

(ii) *This plane has no nontrivial homologies with center* $(0, 0)$.

In other words, these translation planes have kernel $GF(2)$ [3, pp. 132–133].

Proof: (i) (A second proof of this is implicit in the next section. The present proof is included both for completeness and because some parts of it will be needed later in this section.) The binary operation # is right distributive, so we only need to show that, for all distinct $s, t \in F$, the map $\gamma \mapsto s\#\gamma - t\#\gamma$ is bijective. In other words, we must show that

$$\text{if } s\#\gamma = t\#\gamma \text{ and } s \neq t \text{ then } \gamma = 0. \tag{4.6}$$

By (4.2), we are assuming that

$$\begin{aligned} &B_{\gamma,s} + T'(B_{\gamma,s}\Psi) + T'(k^* s[\{\gamma + T'(\gamma)\} + J_{\gamma,s}\Psi]) \\ &\quad = B_{\gamma,t} + T'(B_{\gamma,t}\Psi) + T'(k^* t[\{\gamma + T'(\gamma)\} + J_{\gamma,t}\Psi]). \end{aligned}$$

If we write

$$\begin{aligned} &\alpha := \{\gamma + T'(\gamma)\} + J_{\gamma,s}\Psi,\ \alpha' := \{\gamma + T'(\gamma)\} + J_{\gamma,t}\Psi, \\ &\quad \beta := B_{\gamma,s}, \text{ and } \beta' := B_{\gamma,t}, \end{aligned} \tag{4.7}$$

then this becomes

$$\beta + T'(\beta\Psi) + T'(k^* s\alpha) = \beta' + T'(\beta'\Psi) + T'(k^* t\alpha'). \tag{4.8}$$

Multiply by Ψ and apply T':

$$\begin{aligned} &T'(\beta\Psi) + T'(\beta\Psi)T'(\Psi) + T'(k^* s\alpha)T'(\Psi) \\ &\quad = T'(\beta'\Psi) + T'(\beta'\Psi)T'(\Psi) + T'(k^* t\alpha')T'(\Psi). \end{aligned}$$

Since $T'(\Psi) = 1$ it follows that

$$T'(k^* s\alpha) = T'(k^* t\alpha') \text{ and } \beta + T'(\beta\Psi) = \beta' + T'(\beta'\Psi). \tag{4.9}$$

Next, $T'(\alpha) = J_{\gamma,s}$ by (4.4, 4.7), so that by (4.7, 4.9) we have

$$\alpha + T'(\alpha)\Psi = \gamma + T'(\gamma) \text{ and } \alpha' + T'(\alpha')\Psi = \gamma + T'(\gamma). \tag{4.10}$$

By (4.3, 4.7),

$$\beta = B_{\gamma,s} = s^2\alpha + ksT(s\alpha) + k^* sT'(k^* s\alpha) + k^* sT'(\gamma). \tag{4.11}$$

By (3.1iii, 4.4, 4.7), if $\theta := \gamma + T'(\gamma)$ then $\alpha = \theta + J_{\gamma,s}\Psi$ and

$$\begin{aligned} T'(\beta\Psi) &= T'(s^2\theta\Psi) + T'(s^2\Psi\Psi J_{\gamma,s}) \\ &\quad + T'(ks\Psi T(s\theta)) + T'(k \cdot s\Psi T(s\Psi J_{\gamma,s})) + T'(k^* s\Psi T'(\gamma)) \\ &\quad + T'(k^* s\Psi)T'(k^* s\theta) + T'(k^* s\Psi)T'(k^* s\Psi J_{\gamma,s}) \\ &= T'(s^2\theta\Psi) + T'(ks\Psi T(s\theta)) + T'(k^* s\Psi)T'(k^* s\theta) + T'(k^* s\Psi T'(\gamma)) \\ &\quad + \{T'(s^2\Psi\Psi) + T'(k \cdot s\Psi s\Psi) + T'(k^* s\Psi)T'(k^* s\Psi)\}J_{\gamma,s} \\ &= J_{\gamma,s} = T'(\alpha) \end{aligned}$$

since

$$T'(s^2\Psi^2) + T'(ks\Psi s\Psi) + T'(k^* s\Psi)T'(k^* s\Psi) = T'([1 + k + k^{*2}]s^2\Psi^2) = 0.$$

Again by (3.1iii, 4.11),

$$\begin{aligned}T'(\alpha\beta) &= T'\big(s^2\alpha^2 + k\cdot s\alpha T(s\alpha) + k^*s\alpha T'(k^*s\alpha) + k^*s\alpha T'(\gamma)\big)\\ &= T'(s^2\alpha^2) + T'(ks\alpha s\alpha) + T'(k^*s\alpha)^2 + T'(k^*s\alpha)T'(\gamma)\\ &= T'(k^*s\alpha)T'(\gamma).\end{aligned}$$

Thus,

$$\begin{aligned}&T'\big([\alpha + T'(\alpha)\Psi][\beta + T'(\beta\Psi)]\big)\\ &\quad= T'\big([\alpha + T'(\alpha)\Psi][\beta + T'(\alpha)]\big)\\ &\quad= T'(\alpha\beta) + T'(\alpha T'(\alpha)) + T'(T'(\alpha)\Psi\beta) + T'\big(T'(\alpha)\Psi T'(\alpha)\big)\\ &\quad= T'(k^*s\alpha)T'(\gamma) + T'(\alpha)^2 + T'(\alpha)T'(\Psi\beta) + T'(\alpha)^2\\ &\quad= T'(k^*s\alpha)T'(\gamma) + 3T'(\alpha)^2.\end{aligned}$$

By (4.9, 4.10), it follows that $3T'(\alpha)^2 = 3T'(\alpha')^2$, and hence $\alpha = \alpha'$ by (4.10). Then $T'(\beta\Psi) = T'(\alpha) = T(\beta'\Psi)$ by symmetry, so that $\beta = \beta'$ by (4.9).

Write $x := s\alpha$ and $y := t\alpha$. Since $\beta\alpha = \beta'\alpha'$, (4.11) yields

$$\begin{aligned}&x^2 + kxT(x) + k^*xT'(k^*x) + k^*xT'(\gamma)\\ &\quad= y^2 + kyT(y) + k^*yT'(k^*y) + k^*yT'(\gamma).\end{aligned} \tag{4.12}$$

Apply T:

$$\begin{aligned}&T(x)^2 + kT(x)T(x) + k^*T(x)T'(k^*x) + k^*T(x)T'(\gamma)\\ &\quad= T(y)^2 + kT(y)T(y) + k^*T(y)T'(k^*y) + k^*T(y)T'(\gamma),\end{aligned}$$

where $T'(k^*x) = T'(k^*y)$ by (4.9). Since $1 + k = k^{*2}$,

$$k^{*2}T(x+y)^2 + k^*T(x+y)T'(k^*x) + T(x+y)k^*T'(\gamma) = 0.$$

If $T(x) \neq T(y)$ then $k^*T(x+y) + T'(k^*x) + T'(\gamma) = 0$. Then

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

by (3.1ii), so that $k^*T(x+y) + 0 = 0$.

Thus, $T(x) = T(y)$, and (4.12) becomes

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

If $x \neq y$ then $x + y + kT(x) + k^*T'(k^*x) + k^*T'(\gamma) = 0$. Apply T and subtract in order to obtain $x + y = T(x+y) = 0$.

Thus, $x = y$, which says that $s\alpha = t\alpha$. Now $\alpha = 0$, and hence $\beta = k^*sT'(\gamma)$ by (4.11). By symmetry, $\beta' = k^*tT'(\gamma)$. Then $k^*sT'(\gamma) = k^*tT'(\gamma)$, so that $T'(\gamma) = 0$. Now (4.10) implies that $\gamma = 0$, as required.

Remark It should now be clear that methods using orthogonal spreads can not only make the discovery of unusual planes easier, they can also make it far simpler to prove that a given geometry is a plane.

(ii) We need two more consequences of definitions (4.2) and (4.3). By (3.1i),

$$J_{1,s} = T'(k^* s\Psi). \tag{4.13}$$

By (4.2), $T'((s\#1)\Psi) = T'(B_{1,s}\Psi)+T'(B_{1,s}\Psi)T'(\Psi)+T'(k^* sJ_{1,s}\Psi)T'(\Psi) = T'(k^* s\Psi)T'(k^* s\Psi)$, so that, since $K' = GF(2)$,

$$T'((s\#1)\Psi) = T'(k^* s\Psi). \tag{4.14}$$

Next, we need a quasifield for the plane in (i). Define a new operation $\circ$ on F by

$$(x\#1) \circ (1\#y) = x\#y \quad \text{for all } x, y \in F. \tag{4.15}$$

Then $(F, +, \circ)$ is a quasifield with identity element $1\#1$. The kernel of this quasifield is contained in

$$D := \{z \in F \mid (x + y) \circ z = x \circ z + y \circ z \text{ for all } x, y \in F\}$$

[3, p. 132]. Let $x \mapsto \overline{x}$ denote the permutation of F defined by the equation

$$x = \overline{x}\#1. \tag{4.16}$$

By (4.14),

$$T'(x\Psi) = T'(k^* \Psi \overline{x}) \quad \text{for all } x \in F. \tag{4.17}$$

Moreover, $x \circ (1\#\gamma) = \overline{x}\#\gamma$ by (4.15), and D consists of those elements $1\#\gamma$ such that

$$\overline{x + y}\#\gamma = \overline{x}\#\gamma + \overline{y}\#\gamma \quad \text{for all } x, y \in F. \tag{4.18}$$

We will show that (4.18) *implies that* $\gamma \in K'$, and hence $1\#\gamma \in \{1\#0, 1\#1\} = \{0, 1\#1\}$, so the kernel has size 2, as required in part (ii) of the proposition.

Since (4.18) asserts that $x + y = x + y$ in case $\gamma = 1$ (cf. (4.16)), (4.18) holds when γ is replaced by $T'(\gamma)$; and then by adding the two equations we find that

$$\text{We may assume that } T'(\gamma) = 0; \textit{ we must show that } \gamma = 0. \tag{4.19}$$

Let

$$U := \{s \in F \mid T'(k^* s\Psi) = 0\}, \tag{4.20}$$

so that $\dim_{K'} U = \dim_{K'} F - 1$. If $\overline{x} \in U$ then $J_{1,\overline{x}} = 0$ by (4.13), so that $B_{1,\overline{x}} = k^*\overline{x}$ by (4.3, 3.1i) and hence $\overline{x}\#1 = B_{1,\overline{x}} + T'(B_{1,\overline{x}}\Psi) + 0 = k^*\overline{x} + T'(k^*\overline{x}\Psi)$ by (4.2). Consequently, by (4.16, 4.20),

$$x = \overline{x}\#1 = k^*\overline{x} \quad \text{for all } \overline{x} \in U. \tag{4.21}$$

Equations (4.17) and (4.21) produce a significant simplification of (4.18): if $\overline{x}, \overline{y} \in U$ then

$$T'(k^*\Psi\overline{x+y}) = T'((x+y)\Psi) = T'(k^*\Psi\overline{x}) + T'(k^*\Psi\overline{y}) = 0+0$$

by (4.17), which means that $\overline{x+y} \in U$ by (4.20), so that $k^*\overline{x+y} = x+y = k^*\overline{x} + k^*\overline{y}$ by (4.21). Hence, if $s = \overline{x}$ and $t = \overline{y}$ then (4.18) implies that

$$(s+t)\#\gamma = s\#\gamma + t\#\gamma \quad \text{for all } s,t \in U. \tag{4.22}$$

From now on, *s and t will always denote elements of* U.

Next, by (4.3, 4.19, 4.20),

$$\begin{aligned} J_{\gamma,s} &= T'\Big(s^2\gamma\Psi + ksT(s\gamma)\Psi + k^*sT'(k^*s\gamma)\Psi\Big) + 0 \\ &= T'(s^2\gamma\Psi) + T'(ksT(s\gamma)\Psi) + 0 + 0 \\ B_{\gamma,s} &= s^2\gamma + s^2J_{\gamma,s}\Psi + ksT(s\gamma) \\ &\quad + ksT(sJ_{\gamma,s}\Psi) + k^*sT'(k^*s\gamma) + 0 + 0. \end{aligned} \tag{4.23}$$

By (4.20),

$$\begin{aligned} T'(B_{\gamma,s}\Psi) &= T'(s^2\gamma\Psi) + T'(s^2J_{\gamma,s}\Psi\Psi) + T'(ksT(s\gamma)\Psi) \\ &\quad + T'(ksT(sJ_{\gamma,s}\Psi)\Psi) + 0 \\ &= T'(s^2\gamma\Psi) + T'(s^2\Psi^2)J_{\gamma,s} + T'(ks\Psi T(s\gamma)) \\ &\quad + T'(k\cdot s\Psi T(s\Psi))J_{\gamma,s}. \end{aligned}$$

By (3.1iii, 4.1, 4.20),

$$\begin{aligned} T'(s^2\Psi^2) + T'(k\cdot s\Psi T(s\Psi)) &= T'(s^2\Psi^2) + T'(k\cdot s\Psi s\Psi) \\ &= T'(k^{*2}s^2\Psi^2) = T'(k^*s\Psi)^2 = 0, \end{aligned}$$

so that $T'(B_{\gamma,s}\Psi) = T'(s^2\gamma\Psi) + T'(ks\Psi T(s\gamma))$. Then, by (4.2, 4.19, 4.20, 4.23),

$$\begin{aligned} s\#\gamma = &\{s^2\gamma + s^2J_{\gamma,s}\Psi + ksT(s\gamma) + ksT(sJ_{\gamma,s}\Psi) + k^*sT'(k^*s\gamma)\} \\ &+ \{T'(s^2\gamma\Psi) + T'(ks\Psi T(s\gamma))\} + T'(k^*s\gamma) + 0. \end{aligned} \tag{4.24}$$

Three of the terms on the right side of (4.24) are visibly additive in s. By (4.22),

$$\begin{aligned} &(s+t)^2\Psi J_{\gamma,s+t} + s^2\Psi J_{\gamma,s} + t^2\Psi J_{\gamma,s} + t^2\Psi J_{\gamma,t} \\ &\quad + k(s+t)T((s+t)\gamma) + k(s+t)T((s+t)\Psi)J_{\gamma,s+t} \\ &\quad + ksT(s\gamma) + ksT(s\Psi)J_{\gamma,s} + ktT(t\gamma) + ktT(t\Psi)J_{\gamma,t} \\ &\quad + k^*(s+t)T'(k^*(s+t)\gamma) + k^*sT'(k^*s\gamma) + k^*tT'(k^*t\gamma) \\ &\quad + T'\big(k(s+t)\Psi T((s+t)\gamma)\big) + T'(ks\Psi T(s\gamma)) + T'(kt\Psi T(t\gamma)) = 0. \end{aligned} \tag{4.25}$$

This apparently unwieldy identity yields, for all $s,t \in U$, an inclusion relationship of the form

$$s^2\Psi\{J_{\gamma,s+t} + J_{\gamma,s}\} + t^2\Psi\{J_{\gamma,s+t} + J_{\gamma,t}\} \in Ks + Kt + K. \tag{4.26}$$

By (4.20) and (2.1), $|K \cap U| \geq \frac{1}{2}|K| > 2$. If we choose $s,t \in K \cap U$ then (4.26) states that

$$s^2\{J_{\gamma,s+t} + J_{\gamma,s}\} + t^2\Psi\{J_{\gamma,s+t} + J_{\gamma,t}\} \in K$$

with $J_{\gamma,s+t}+J_{\gamma,s}, J_{\gamma,s+t}+J_{\gamma,t} \in K' = \{0,1\}$. Fix $s \in (K\cap U)-\{0\}$. Since $\Psi \notin K$, for each of the $|K\cap U|-2$ choices of t in $(K\cap U)-\{0,s\}$ we see that $J_{\gamma,s} = J_{\gamma,s+t} = J_{\gamma,t}$. Since $s \in K$, (4.23) implies that $J_{\gamma,s} = T'(s^2\gamma\Psi)+T'(kssT(\gamma)\Psi)$ is additive in s. Thus,

$$J_{\gamma,s} = 0 \quad \text{for all } s \in K \cap U. \tag{4.27}$$

More generally:

Lemma 4.28 *$J_{\gamma,s} = 0$ for all $s \in U$.*

Proof: Let $0 \neq t \in K \cap U$, so that $J_{\gamma,t} = 0$ by (4.27). Whenever $s \in U - K$, (4.26) states that

$$s^2\Psi(J_{\gamma,s+t} + J_{\gamma,s}) + t^2\Psi J_{\gamma,s+t} \in K + Ks \tag{4.29}$$

where $J_{\gamma,s+t} + J_{\gamma,s}, J_{\gamma,s+t} \in \{0,1\}$.

Let $B := \{x \in U | J_{\gamma,x} = 1\}$. Then $B \cap (K \cap U) = \emptyset$ by (4.27). Consider an arbitrary $s \in B$. Then $\{J_{\gamma,s+t} + J_{\gamma,s}, J_{\gamma,s+t}\} = \{0,1\}$

Suppose that $J_{\gamma,s+t} + J_{\gamma,s} = 1$ and $J_{\gamma,s+t} = 0$. Then (4.29) becomes a quadratic equation of the form $s^2\Psi + \alpha s + \beta = 0$ with $\alpha, \beta \in K$ not both 0. There are fewer than $|K|^2$ equations of this sort, with fewer than $2|K|^2$ possibilities for roots s.

On the other hand, if $J_{\gamma,s+t} + J_{\gamma,s} = 0$ and $J_{\gamma,s+t} = 1$ then (4.29) states that Ψ, 1 and s are linearly dependent over K. This occurs for fewer than $|K + K\Psi| = |K|^2$ choices of s.

This shows that $|B| < 3|K|^2$.

Now *fix* $s \in U - B$. There are at most $|B|$ elements $u \in U - B$ such that $K's + K'u = \{0, s, u, s+u\}$ meets B, and so at least $|U|-|B|$ elements $u \in U-B$ such that $s+u \in U-B$. In view of the definition of B, since $s, u, s+u \in B$ we have $J_{\gamma,s} = J_{\gamma,u} = J_{\gamma,s+u} = 0$. By (4.23), the equation $J_{\gamma,s+u} + J_{\gamma,s} + J_{\gamma,u} = 0$ simplifies to

$$T'(ksT(u\gamma)\Psi) = T'(kuT(s\gamma)\Psi). \tag{4.30}$$

This identity holds for at least $|U| - |B| > \frac{1}{2}|F| - 3|K|^2 = |U| - 3|K|^2 \geq \frac{1}{2}|U|$ elements u of U (since $|F| \geq 8|K|^2$ by (2.1)), and hence these must span the K'-space U! Thus, (4.30) holds for all $u \in U$. Similarly, for each $u \in U$ we now know that (4.30) holds for at least $|U| - |B|$ choices of $s \in U$ and hence (4.30) *holds for all* $s, u \in U$.

Now consider any $b \in B$. There are at most $|B| - 1$ possible K'-subspaces of U of the form $K'b + K'c = \{0, b, c, b + c\}$ with $c \in B - K'b$. Then there are at most $|B| - 1$ elements $s \in U - B$ such that $b + s \in B$. Consequently, there are at least $|U|-|B|-(|B|-1) > 8|K|^2-3|K|^2-3|K|^2$ elements $s \in U-B$ such that $b+s \in U-B$. In particular, there is at least one such element $s \in U - B$. Write $u = b + s$. In view of (4.30) and the definition of B, (4.23) implies that

$$\begin{aligned} 1 = J_{\gamma,b} &= 0 + 0 + J_{\gamma,s+u} = J_{\gamma,s} + J_{\gamma,u} + J_{\gamma,s+u} \\ &= T'(ksT(u\gamma)\Psi) + T'(kuT(s\gamma)\Psi) = 0. \end{aligned}$$

This contradiction shows that $B = \emptyset$. □

We now return to the proof of (4.5ii). In view of (4.28), (4.25) states that

$$ksT(t\gamma) + ktT(s\gamma) + k^*sT'(k^*t\gamma) + k^*tT'(k^*s\gamma) + T'(ks\Psi T(t\gamma)) + T'(kt\Psi T(s\gamma)) = 0$$

for all $s, t \in U$. Then

$$s\{kT(t\gamma) + k^*T'(k^*t\gamma)\} \in Kt + K.$$

Let $t \in U - \{0\}$, and then choose any $s \in U - (Kt + K)$ (there is such an s by (2.1)) in order to deduce that

$$kT(t\gamma) = k^*T'(k^*t\gamma) \quad \text{for all } t \in U. \tag{4.31}$$

Again let $t \in U - \{0\}$. Since $|U \cap Kt| \geq \frac{1}{2}|Kt| > 2$, there is some $a \in K - K'$ such that $at \in U$. By two applications of (4.31), $T'(k^*at\gamma) = (k/k^*)T(at\gamma) = (k/k^*)aT(t\gamma) = aT'(k^*t\gamma)$. Since $a \notin K'$ it follows that $T'(k^*t\gamma) = 0 = T(t\gamma)$ for all $t \in U$. However, U has index 2 as a subgroup of F, and hence is not a vector space over K, so that $F = KU$. Consequently, $T(F\gamma) = T(KU\gamma) = KT(U\gamma) = 0$, so that $\gamma = 0$, as required in (4.19). This completes the proof of (4.5). □

We need one additional equally dull computation:

Lemma 4.32 *If $|F| > 2^5|K|^3$, then the affine plane in* (4.5) *has no nontrivial elation with axis $x = 0$.*

Proof: Suppose that there is such an elation. If the line $y = 0$ is sent to the line $y = a\#x$, then $a \neq 0$ and $(x, 0) \mapsto (x, a\#x)$ for all $x \in F$. Also $(0, y) \mapsto (0, y)$, so that $(x, y) \mapsto (x, y + a\#x)$ for all $x, y \in F$. Since the line $y = m\#x$ must be sent to a line, it follows that $m\#x + a\#x = m'\#x$ for a permutation $m \mapsto m'$ of F. We will change notation slightly in order to conform to (4.2) and (4.3):

$$s\#\gamma + a\#\gamma = s'\#\gamma \quad \text{for all } s, \gamma \in F.$$

From now on, choose γ so that $T'(\gamma) = 0$. Then (4.2) and (4.3) imply that

$$\begin{aligned} &s^2\gamma + a^2\gamma + s'^2\gamma + s^2\Psi J_{\gamma,s} + a^2\Psi J_{\gamma,a} + s'^2\Psi J_{\gamma,s'} \\ &\quad + ksT(s\gamma + s\Psi J_{\gamma,s}) + kaT(a\gamma + a\Psi J_{\gamma,a}) + ks'T(s'\gamma + s'\Psi J_{\gamma,s'}) \\ &\quad + k^*sT'(k^*s\gamma + J_{\gamma,s}k^*s\Psi) + k^*aT'(k^*a\gamma + J_{\gamma,a}k^*a\Psi) \\ &\quad + k^*s'T'(k^*s'\gamma + J_{\gamma,s'\gamma}k^*s'\Psi) \in K'. \end{aligned} \tag{4.33}$$

Then $(s + a + s')^2\gamma \in s^2\Psi K' + a^2\Psi K' + s'^2\Psi K' + sK + aK + s'K + K'$. The K'-subspace on the right has size $\leq 2^3|K|^32$, and this is less than $|F|/2$, by hypothesis. Since there are $|F|/2$ choices for γ, it follows that $s' = s + a$.

Now (4.33) states that

$$\begin{aligned} s^2\Psi(J_{\gamma,s}+J_{\gamma,s'})+a^2\Psi(J_{\gamma,a}+J_{\gamma,s'}) \\ +\ ksT(s\gamma+s\Psi J_{\gamma,s}+s'\gamma+s'\Psi J_{\gamma,s'}) \\ +\ kaT(a\gamma+a\Psi J_{\gamma,a}+s'\gamma+s'\Psi J_{\gamma,s'}) \\ +\ k^*sT'(k^*s\gamma+J_{\gamma,s}k^*s\Psi+k^*s'\gamma+J_{\gamma,s'}k^*s'\Psi) \\ +\ k^*aT'(k^*a\gamma+J_{\gamma,a}k^*a\Psi+k^*s'\gamma+J_{\gamma,s'}k^*s'\Psi)\in K'. \end{aligned}$$

This can be viewed as a polynomial equation in s of the form $\alpha_2 s^2\Psi+\alpha_1 s+\beta_2 a^2\Psi+\beta_1 a+\beta_0=0$ with $\alpha_2,\beta_2,\beta_0\in K'$ and $\alpha_1,\beta_1\in K$. There are at most $2^3|K|^2-1$ nonzero equations of this form, and each has at most 2 roots. Since $|F|>2\cdot 2^3|K|^2$ by hypothesis, there is an element s of F that satisfies no nonzero equation of this sort, and hence such that

$$\begin{aligned} J_{\gamma,s}+J_{\gamma,s'}=0 \text{ and } kT(a\gamma+s\Psi J_{\gamma,s}+s'\Psi J_{\gamma,s'}) \\ +\ k^*T'(k^*a\gamma+J_{\gamma,s}k^*s\Psi+J_{\gamma,s'}k^*s'\Psi)=0 \end{aligned}$$

whenever $T'(\gamma)=0$. In particular, $s\Psi J_{\gamma,s}+s'\Psi J_{\gamma,s'}=a\Psi J_{\gamma,s}$, and hence

$$\begin{aligned} T(a\gamma)=T(a\Psi)J_{\gamma,s}+(k^*/k)T'(k^*a\gamma+J_{\gamma,s}k^*s\Psi+J_{\gamma,s'}k^*s'\Psi) \\ \text{whenever } T'(\gamma)=0. \end{aligned} \tag{4.34}$$

The right side of (4.34) lies in the K'-space $T(a\Psi)K'+(k^*/k)K'$ of size at most 4, while the left side ranges over a K-subspace of F. It follows that $T(a\gamma)=0$ whenever $T'(\gamma)=0$. Then a hyperplane of the K'-space F is contained in a hyperplane of the K-space F, which is ridiculous. □

Remark The restriction on $|F|$ in (4.32) is unfortunate and unnecessary: it can be removed, but at the expense of a great deal more computation which we omit.

5. Identification

Now we consider some of the planes $\mathcal{A}\big((\Sigma^k)_{\langle\Psi,0,1,0\rangle}\big)$ arising in Example 4 of Section 2. Choose k and Ψ as in (4.1). The point $y=\langle\Psi,0,1,0\rangle$ of V is nonsingular: $Q'(\Psi,0,1,0)=1$.

Lemma 5.1 *$\mathcal{A}\big((\Sigma^k)_{\langle\Psi,0,1,0\rangle}\big)$ is one of the planes in* (4.5)*, and hence has kernel $K'=GF(2)$.*

Proof: By (2.6), $y^\perp$ consists of the vectors (α,a,β,b) such that $T'(\alpha)=T'(\beta\Psi)$. Define a linear transformation $\pi: y^\perp/y\to F\times F$ by

$$\pi:(\alpha,a,\beta,b)+y\mapsto(\alpha+T'(\alpha)\Psi+a,\beta+T'(\beta\Psi)+b);$$

this is well-defined since, for all $k\in K'$,

$$(\alpha+k\Psi)+T'(\alpha+k\Psi)\Psi=\alpha+k\Psi+T'(\alpha)\Psi+kT'(\Psi)\Psi=\alpha+T'(\alpha)\Psi$$

$$(\beta + k) + T'((\beta + k)\Psi) = \beta + k + T'(\beta\Psi) + kT'(\Psi) = \beta + T'(\beta\Psi).$$

We claim that π *is a bijection.* For this it suffices to show that its kernel is 0, so suppose that $((\alpha, a, \beta, b) + y)^\pi = 0$. Then $\beta = T'(\beta\Psi) + b \in K'$, so that $(\alpha, a, \beta, b) + y = (\alpha + \beta\Psi, a, 0, b) + y$ and hence we may assume that $\beta = 0$. Now $b = 0, T'(\alpha) = T'(\beta\Psi) = 0$ and $\alpha + a = 0$. It follows that $a = T'(\alpha + a) = 0$ and hence that $a = 0$, which proves the claim.

Thus, by (2.7), $\mathcal{A}\big((\Sigma^k)_{\langle\Psi,0,1,0\rangle}\big)^\pi$ consists of the following n-dimensional subspaces of $F \times F$:

$$\begin{aligned} &0 \times F, \text{ and, for } s \in F, \\ &\Big\{\big(\alpha + T'(\alpha)\Psi + a, \beta + T'(\beta\Psi) + T'(k^*s\alpha)\big)\Big|\alpha \in F, a \in K', \quad \text{and} \\ &\qquad\qquad T'(\beta\Psi) = T'(\alpha)\Big\}, \end{aligned} \tag{5.2}$$

where $\beta := s^2\alpha + ksT(s\alpha) + k^*sT'(k^*s\alpha) + k^*sa$ depends on s, α and a.

In order to identify these subspaces, we will construct a subspace of each of the second type of subspace in (6.2) that has K'-dimension equal to that of F. Fix $s, \gamma \in F$, and define elements of F as follows:

$$\theta := \gamma + T'(\gamma), \ a := T'(\gamma) \quad \text{and } \alpha := \theta + J_{\gamma,s}\Psi$$

in the notation of (4.3). By (3.1ii), $T'(\alpha) = T'(\gamma) + T'(T'(\gamma)) + J_{\gamma,s}T'(\Psi) = J_{\gamma,s}$. If we write $\beta = s^2\alpha + ksT(s\alpha) + k^*sT'(k^*s\alpha) + k^*sa$ as above then $\beta = B_{\gamma,s}$ in the notation of (4.3), and then the exact same calculation as that following (3.11) yields $T'(\beta\Psi) = J_{\gamma,s} = T'(\alpha)$.

Moreover,

$$\begin{aligned} &\alpha + T'(\alpha)\Psi + a = \theta + J_{\gamma,s}\Psi + T'(\alpha)\Psi + T'(\gamma) = \gamma \text{ and} \\ &\beta + T'(\beta\Psi) + T'(k^*s\alpha) = \beta + T'(\beta\Psi) + T'(k^*s[\theta + J_{\gamma,s}\Psi]) = s\#\gamma \end{aligned}$$

by (4.2). Then, for each $s \in F$, we have

$$\Big\{\big(\alpha + T'(\alpha)\Psi + a, \beta + T'(\beta\Psi) + T'(k^*s\alpha)\big)\Big|\alpha \in F, a \in F \text{ with } T'(\beta\Psi) = T'(\alpha)\Big\} \supseteq \{(\gamma, s\#\gamma)|\gamma \in F\}.$$

The preceding two subspaces of $F \times F$ have the same K'-dimension and hence coincide. Thus, (5.2) is the set of lines through (0, 0) of the plane appearing in (4.5). □

6. Groups

We now return to the study of the orthogonal spreads Σ^k appearing in Example 3 of Section 2. In this section we will determine the group $G(\Sigma^k)$. Since V is a vector space over $K' = GF(2)$, in (2.2iii) we have $a = 1$ and $\tau = 1$; moreover, we can identify a point with

Write $z = \langle 0, 1, 0, 1\rangle$, so that $(\Sigma^k)_z$ is the symplectic spread appearing in (2.5); see the discussion following (2.7). By (2.8), $G(\Sigma^k)_z$ has a normal subgroup $A \equiv F^*$. Moreover,

$$G(\Sigma^k)_z = G(\Sigma^k)_{WXz} \text{ is isomorphic to a subgroup of } A \rtimes \mathrm{Aut}F, \text{ and has odd order,} \tag{6.1}$$

where W is one member of $\{F \times K' \times 0 \times 0, 0 \times 0 \times F \times K'\}$ and X is the other one. In particular, $G(\Sigma^k)_z$ has no element interchanging W and X. Write $|F| = 2^n$, so that $\dim V = 2n + 2$.

Theorem 6.2 *If $|F| > 2^5|K|^3$, then $G(\Sigma^k) = G(\Sigma^k)_z \leq A \rtimes \mathrm{Aut}F$.*

Proof: Write $G = G(\Sigma^k), z = w + x$ with $w \in W, x \in X, W' = W \cap z^\perp$ and $X' = X \cap z^\perp$. Then $w \notin W'$ since $0 \neq Q'(z) = (w, x) = (w, z)$. Similarly, $x \notin X'$. Moreover, W', X', w and x are fixed by A, and A cyclically permutes the $2^n - 1$ points of W' (or of X') as well as the $2^n - 1$ points $\neq w$ of $W - W'$ (and the points $\neq x$ of $X - X'$). (Note that $\{W', X'\} = \{F \times 0 \times 0 \times 0, 0 \times 0 \times F \times 0\}$.)

The next three lemmas gradually restrict G.

Lemma 6.3 *$G_{WX} = G_z$, and z is the unique nonsingular point fixed by G_{WX}.*

Proof: Assume that G_{WX} moves z. Then it moves w or x, and we may assume that it moves w. The known orbits of the subgroup A of G_z and G_{WX} show that G_z fixes only one nonsingular point, and also that the orbit $\mathcal{O} := w^{G_{WX}}$ of G_{WX} is one of the following subsets of W: (i) w together with the points of W'; (ii) all points of $W - W'$; or (iii) all points of W.

(i) This is impossible since W' would be the only subspace of its size inside $\mathcal{O}$.

(ii) Here G_{WX} is 2-transitive on the set $W - W'$ of size 2^n. Moreover, G_{WX} fixes W' and hence fixes $W'^\perp \cap X = x$. Then the stabilizer $(G_{WX})_w = (G_{WXx})_w$ of the point w fixes z and hence is a group of odd order having a cyclic normal subgroup $A \cong F^*$ of composite order that is transitive on $\mathcal{O} - \{w\}$. By [1], it follows that the group induced by G_{WX} on $W - W'$ has an elementary abelian regular normal subgroup. Also, since $(G_{WX})_w$ fixes z we can use the known behavior of G_{WXz} (cf. (2.4, 2.8)) in order to conclude that that G_{WX} acts faithfully on $W - W'$ and hence on W. Thus, G_{WX} has an elementary abelian normal subgroup E of order 2^n, and A acts transitively on $E - \{1\}$.

Since EA also acts on $\Sigma^k - \{W, X\}$ and E fixes a member of this set, E must act trivially: E fixes each member of Σ^k. If $1 \neq e \in E$ then e is an involution, so that $\dim C_Y(e) \geq (\dim Y)/2 = (n + 1)/2$ for each of the $2^n + 1$ members Y of Σ^k. Then $\dim C_V(e) > n + 1$, so that $C_V(e)$ contains at least two nonsingular points y. It follows that e induces a collineation of $\mathcal{A}((\Sigma^k)_y)$ that fixes 0 while acting trivially on the line $(\Sigma^k)_y$ at infinity, and hence induces the identity on this plane of even order. Then e is a transvection of V with center y for at least two choices of y, which is ridiculous.

(iii) Since A is transitive on the lines of W through w, G_{WX} is line-transitive on W. By [5], it follows that G_{WX} is 2-transitive on W. Then $(G_{WX})_{W'} = G_{WXx}$ is transitive on

$W - W'$ (by an orbit count [3, p.78]), and this leads to the same contradiction as in (ii). □

Lemma 6.4 *G fixes W or X.*

Proof: First assume that some element $g \in G$ interchanges W and X. Then g normalizes G_{WX} and hence fixes the unique nonsingular point z fixed by G_{WX} (cf. (6.3)). This contradicts (6.1) since G_z fixes X and W.

Thus, G moves $\{W, X\}$. Since A is transitive on $\Sigma^k - \{W, X\}$ it follows that G is 2-transitive on Σ^k, which contradicts the preceding paragraph. □

Lemma 6.5 *W and X.*

Proof: Suppose that G fixes W and moves X. By (3.3) and (3.4), if $\ell = k/(k+1)$ then Σ^ℓ is orthogonally equivalent to Σ^k by an orthogonal transformation interchanging W and X. Hence, we can replace k by ℓ if necessary in order to have $W = 0 \times 0 \times F \times K'$. Then $w = (0, 0, 0, 1)$.

The transitivity of A on $\Sigma^k - \{W, X\}$ implies that G is 2-transitive on $\Sigma^k - \{W\}$. Since G is faithful on Σ^k (by (6.3) and (6.1)), and since the stabilizer of X has odd order, we can again apply [1] in order to conclude that G has an elementary abelian normal subgroup E that is regular on $\Sigma^k - \{W\}$.

Case 1 $E = 1$ *on* W. In the notation introduced following (3.1), E consists of matrices of the form $\left(\begin{smallmatrix} I & M \\ O & I \end{smallmatrix}\right)$ with M skew-symmetric. The set $\mathcal{K}$ of these matrices M is closed under addition, since E is a group. This contradicts (3.6) (or (3.7), or (3.8)).

Case 2 *E fixes W'.* Then E fixes some point of W', while A is transitive on the points of W', so that $E = 1$ on W'. If $1 \neq e \in E$ then e fixes only one member W of Σ^k, and hence fixes no singular point outside of W.

Since e is an involution, $\dim C_V(e) \geq n + 1$; and $C_V(e) \neq W$ by Case 1. Thus, $C_V(e)$ contains a nonsingular point. Since all singular points in $C_V(e)$ lie in the totally singular subspace W', the radical of $C_V(e)$ must contain W'. Consequently $C_V(e)/W'$ contains the unique nonsingular point $\langle W', z\rangle/W'$ of $W'^{\perp}/W'$, so that e lies in G_z. This contradicts the fact that G_z has odd order, by (6.1).

Case 3 *E moves W'.* Since E fixes some point of W, and A acts on the set S of such fixed points, S is a union of orbits of A. By Case 2, S is not contained in W'. If S contains a point $\neq w$ of $W - W'$ then it contains a spanning subset of W, whereas E is nontrivial on W. Thus, $S = \{w\}$. Now E fixes some hyperplane on w, while A is transitive on the

hyperplanes on w, so that E fixes every hyperplane on w. Consequently, E induces on W the group of all elations with center w.

If $1 \neq e \in E$ then e induces an elation of W whose axis $C_W(e)$ contains w. As in Case 2, $C_V(e)$ must contain a nonsingular point in $C_W(e)^\perp$. If $T'(\Psi) = 1$ then the point $y = \langle \Psi, 0, 1, 0 \rangle$ is perpendicular to $w = \langle 0, 0, 0, 1 \rangle$ by (2.6). In view of the transitivity of A on the hyperplanes of W we can conjugate e by an element of A in order to assume that $C_W(e) = y^\perp \cap W$. Then e acts on $\mathcal{A}\big((\Sigma^k)_y\big)$ as an elation with axis $\langle y^\perp \cap W, y \rangle / y$. This contradicts (4.32). □

Completion of the proof of (6.2) By (6.3) and (6.5), $G = G_z$. Now use (6.1). □

Theorem 6.2 produces a proof of a weak version of the main result in [8]:

Theorem 6.6 *Suppose that $n = ab > 9$ for odd integers $a, b > 1$.*

(i) *If $n > 5 + 3b$ then there are at least $(2^b - 2)/2n$ pairwise inequivalent orthogonal spreads Σ^k in an $\Omega^+(2n + 2, 2)$-space.*

(ii) *If n is neither 27 nor the product of 3 and a prime, then there are at least $(2^{\sqrt{n}} - 2)/2n$ such spreads.*

Proof: (i) Let $k, \ell \in K - K'$, and suppose that Σ^k and Σ^ℓ are equivalent by an orthogonal transformation g of V. By (6.2), z is the only nonsingular point fixed by $G(\Sigma^k)$, and g sends z to the nonsingular point z fixed by $G(\Sigma^\ell)$. Then g sends $\mathcal{A}\big((\Sigma^k)_z\big)$ to $\mathcal{A}\big((\Sigma^\ell)_z\big)$. In the notation of Examples 1 and 2 of Section 2, $(\Sigma^k)_z = \Sigma_{y_k}$. By (2.2), g lifts to an isometry g^* of $F \times K \times F \times K$ fixing Σ and sending y_k to y_ℓ. Then g^* conjugates $G(\Sigma)_{y_k}$ to $G(\Sigma)_{y_\ell}$, and hence normalizes the group C consisting of the transformations g_ζ defined in (2.4).

By [6, (4.1)], $G(\Sigma) \cong P\Gamma L(2, 2^n)$, so that $|N_{G(\Sigma)}(C)| = 2n|C|$. Since C fixes y_k it follows that y_k has at most $2n$ images under $N_{G(\Sigma)}(C)$. There are $|K| - 2$ choices for k in $K - K'$, so this proves (i).

(ii) Let a be the smallest factor of n greater than 3, let $K = GF(2^b)$, and observe that $n = ab > 5 + 3b$ and $2^b \geq 2^{\sqrt{n}}$. □

7. Proof of Theorem 1.1

Let $F = GF(2^n)$ with n odd, composite and > 9. Then there is always a choice for a factor m of n such that the subfield $K = GF(2^m)$ of F behaves as in (2.1) and (6.2). Fix such a choice of m.

Let k in $K - K'$. We will use the planes $\mathcal{A}\big((\Sigma^k)_{\langle \Psi, 0, 1, 0 \rangle}\big)$ arising in Example 4 of Section 2, with Ψ restricted as follows.

The number N of generators of F satisfies

$$2^n - N \leq 1 + \sum_{n \neq d | n} (2^d - 1) < 2^{1 + n/3}. \tag{7.1}$$

If Ψ is a generator then so is $\Psi + 1$, and either $T'(\Psi) = 1$ or $T'(\Psi + 1) = 1$. Thus, $N/2$ of the generators Ψ satisfy $T'(\Psi) = 1$; and *these are the elements* Ψ *we will use* in order to obtain the planes $\mathcal{A}\big((\Sigma^k)_{\langle\Psi,0,1,0\rangle}\big)$.

As in Section 6, let $z = \langle 0, 1, 0, 1\rangle$ and $\{W, X\} = \{F \times K' \times 0 \times 0, 0 \times 0 \times F \times K'\}$. As in Section 5, let $y = \langle\Psi, 0, 1, 0\rangle$. By (2.8), $G(\Sigma^k)_{yz} = 1$ since no nontrivial element of $\mathrm{Aut}F$ fixes the generator Ψ. Then $G(\Sigma^k)_y = 1$ by (6.2).

By (2.2iv), every collineation of $\mathcal{A}\big((\Sigma^k)_y\big)$ induces the identity on the line at infinity. By (5.1) and (4.5), the kernel of this plane is $GF(2)$, so every collineation of $\mathcal{A}\big((\Sigma^k)_y\big)$ must be a translation. This proves the main part of (1.1).

In order to count the number of planes obtained in this manner, recall from (6.2) that different choices, Ψ, Ψ' can yield isomorphic planes only if there is an element of $G(\Sigma^k) = G(\Sigma^k)_z$ sending $\langle\Psi, 0, 1, 0\rangle$ to $\langle\Psi', 0, 1, 0\rangle$. By (6.1) this occurs only if $\Psi' \in \Psi^{\mathrm{Aut}F}$. Thus, each choice of k produces at least $(N/2)/n$ different planes behaving as required in (1.1).

While this already proves that we have constructed many nonisomorphic planes, (6.6) provides a slightly improved lower bound on their number. Namely, while different choices of k in $K - K'$ can produce orthogonally equivalent spreads Σ^k, by (2.2) and (6.6) the total number of different planes obtained is at least $\{N/2n\}\{(|K| - 2)/n\}$.

Now assume that n is neither 27 nor the product of 3 and a prime. Then we may assume that K has been chosen so that $|K| \geq 2^{\sqrt{n}}$ in addition to the condition in (6.2). By (7.1), we have obtained more than $(2^{n-1}2^{n/3})(|K|-2)/n^2 > 2^{n+\sqrt{n}-2}/n^2$ planes. This completes the proof of (1.1). □

The number of planes is as stated in Theorem 1.1 even when the additional restriction on n is dropped, but then the analogue of (6.2) is significantly messier to prove.

The proof of the theorem begs an obvious question: Are there orthogonal spreads Σ such that $G(\Sigma) = 1$? The answer undoubdtedly is "Yes, and in great numbers". It is likely that such spreads can be constructed by another iteration of the field change method seen in Examples 2′ and 3 (cf. [7, Section 2]). However, proving that $G(\Sigma) = 1$ would require new ideas.

Acknowledgment

I am grateful to the referee and to Michael Williams for pointing out errors in versions of this paper.

References

1. Bender, H., "Endliche zweifach transitive Permutationsgruppen, deren Involutionen keine Fixpunkte haben," *Math. Z.* **104** (1968) 175–204.
2. Charnes, C., "A non-symmetric translation plane of order 17^2," *J. Geometry* **37** (1990), 77–83.
3. Dembowski, P., *Finite Geometries*. Springer, Berlin-Heidelberg-New York, 1968.
4. Goethals, J.-M., and Snover, S. L., "Nearly perfect binary codes," *Discrete Math.* **3** (1972), 65–68.
5. Kantor, W. M., "Line-transitive collineation groups of finite projective spaces," *Israel J. Math.* **14** (1973), 229–235.

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

7. Kantor, W. M., "Spreads, translation planes and Kerdock sets. II," *SIAM J. Algebraic and Discrete Methods* **3** (1982), 308–318.

8. Kantor, W. M., "An exponential number of generalized Kerdock codes," *Inform. and Control* **53** (1982), 74–80.

9. Kantor, W. M., "Expanded, sliced and spread spreads," pp. 251–261 in *Finite Geometries: Proc. Conf. in Honor of T. G. Ostrom*, Dekker, New York 1983.

10. Lang, S., *Algebra*, Addison-Wesley, Reading 1971.

11. MacWilliams, F. J., and Sloane, N. J. A., *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam 1977.