JOURNAL OF COMBINATORIAL THEORY, Series A **74**, 1–13 (1996)
ARTICLE NO. 0033

New Flag-Transitive Affine Planes of Even Order

WILLIAM M. KANTOR* AND MICHAEL E. WILLIAMS*

Department of Mathematics, University of Oregon, Eugene, Oregon 97403-1222

Communicated by W. M. Kantor

Received September 23, 1994

Large numbers of new flag-transitive affine planes of even order are constructed.

1. INTRODUCTION

In this note we will prove the following:

THEOREM 1.1. *Let q be a power of 2. Let m be an odd integer such that $q^m > 8$, and let $m, m_1, ..., m_n$ be any sequence of $n+1 \geqslant 2$ distinct divisors of m such that each is divisible by the next. Then there are more than $[\Pi_1^n(q^{m_i}+1)]/2m_1 \log_2 q$ pairwise nonisomorphic nondesarguesian flag-transitive affine planes of order q^m with kernel containing $GF(q)$.*

At least $[\Pi_1^{n-1}(q^{m_i}+1)]\, q^{m_n}/2m_1 \log_2 q$ of these planes have kernel $GF(q)$. Moreover, we construct $\Sigma_{(m_i)} \Pi_i q^{m_i}$ planes, where the sum is over all sequences (m_i) behaving as in the theorem; and then we settle the isomorphism problem for these planes (Theorem 5.2).

The proof combines methods in [Wi] and [Ka]: these planes arise from symplectic and orthogonal spreads combined with changing from fields to proper subfields, and methods in [Wi] are used to keep track of these field changes. The latter is the difficult aspect of the construction, since it is just such repeated field changes that could not be handled at all in [Ka] (and hence restricted that paper to at most $q^{m_1}/2$ flag-transitive planes of order q^m, in the notation of the theorem). Nonisomorphism testing involves an elementary Sylow argument.

* The preparation of this paper was supported in part by an NSF grant.

0097-3165/96 $18.00

We note that these planes are the only known nondesarguesian flag-transitive affine planes of even order admitting solvable flag-transitive groups. Their orders comprise all integers of the form $2^{2^a b} > 8$ with b odd and not 1. Moreover, each of the planes admits a sharply flag-transitive group that induces a $q^m + 1$-cycle on the line at infinity.

All of these planes arise from symplectic spreads. Coding-theoretic aspects of this property are discussed in [Ka, Wi].

2. Ups and Downs: From Symplectic to Orthogonal and Back

We will briefly review some of the background required from [Ka]. Throughout this paper, all fields have characteristic 2. Consider a $2k$-dimensional vector space V over $GF(q)$, equipped with a nonsingular quadratic form Q of maximal Witt index. This means that there are k-spaces that are *totally singular* (i.e., on which Q vanishes). Then V has $(q^k - 1)(q^{k-1} + 1)$ nonzero singular vectors. An *orthogonal spread* of V is a family Σ of $q^{k-1} + 1$ totally singular k-spaces such that each nonzero singular vector is in exactly one of them. We recall that there are two *types* of totally singular k-spaces such that two totally singular k-spaces X and Y have the same type if and only if $\dim X \cap Y \equiv k \pmod 2$ [Ta, pp. 170–172].

There is also a symplectic structure on V, defined by the nonsingular alternating bilinear form $(u, v) = Q(u+v) - Q(u) - Q(v)$. If z is *any* nonsingular point of V, then $z^\perp/z$ inherits the nonsingular alternating bilinear form defined by $(u+z, v+z) = (u, v)$ for $u, v \in z^\perp$. If $X \in \Sigma$ then $\langle X \cap z^\perp, z\rangle/z$ is a $k-1$-dimensional *totally isotropic* subspace (i.e., (,) vanishes on it). Moreover,

$$\Sigma_z := \{\langle X \cap z^\perp, z\rangle/z \mid X \in \Sigma\} \tag{2.1}$$

is a *symplectic spread* of $z^\perp/z$: a family of $q^{k-1} + 1$ totally isotropic $k-1$-spaces such that each nonzero vector is in exactly one of them.

This process can be reversed: any symplectic spread $\mathscr{S}$ of $z^\perp/z$ can be "lifted" to an orthogonal spread $\Sigma_{\mathscr{S}}$ of V such that $(\Sigma_{\mathscr{S}})_z = \mathscr{S}$. We will exhibit such a lifting explicitly in the next section.

Given a vector space V' over a field K, with associated nonsingular alternating form (,), if L is a subfield of K and T: $K \to L$ is the trace map, then T(,) defines a nonsingular alternating form on the L-space V'. If $\mathscr{S}$ is a symplectic spread of the K-space V' then $\mathscr{S}$ is also a symplectic spread of the L-space V'.

Definition 2.2 [Wi]. Let $\mathscr{S}$ be a symplectic spread. Suppose that $\mathscr{S}'$ is another symplectic spread arising via a (repeated) up and down process of passing from symplectic to orthogonal geometries and back, or passing to subfields, as above. Then we call $\mathcal{S}'$ a *scion* of $\mathcal{S}$.

Corresponding to any symplectic spread $\mathcal{S}$ of any vector space there is an affine translation plane $\mathbf{A}(\mathcal{S})$ defined in the usual manner [De, p. 219]. Its collineation group will be denoted Aut $\mathbf{A}(\mathcal{S})$. If $\mathcal{S}'$ is a scion of $\mathcal{S}$ then $\mathbf{A}(\mathcal{S}')$ will be called a scion of $\mathbf{A}(\mathcal{S})$.

3. Construction of Orthogonal and Symplectic Spreads

For any field F let $F^{(2)}$ denote an extension of F of degree 2; if K is any subfield of F we assume that $F^{(2)} \supseteq K^{(2)}$. Consider a subfield K such that $[F: K]$ is odd, with associated trace map $T_K: F \to K$. The involutory automorphism $x \mapsto \bar{x}$ of $F^{(2)}$ restricts to the involutory automorphism of $K^{(2)}$. Define a nonsingular alternating K-bilinear form on $F^{(2)}$ by $(x, y)_K := T_K(x\bar{y} + \bar{x}y)$. Since $[F: K]$ is odd, $T_K(k) = k$ for $k \in K$, so that $T_K(x + T_K(x)) = 0$ for all $x \in F$ and hence

$$F = \ker T_K \oplus K.$$

This elementary observation will be a fundamental part of our use of the parity of $[F: K]$.

Write $C := \{\zeta \mid \zeta \in F^{(2)}, \zeta\bar{\zeta} = 1\}$, so that $F^{(2)*} = F^* \times C$. *The letters θ, γ and ζ will always denote elements of C.* If $\theta \in C$ then $\tilde{\theta}: x \mapsto \theta x$ defines an isometry of the symplectic space $F^{(2)}$; let $\tilde{C}$ be denote the group of these isometries.

For fixed $F^{(2)}$ we will study the following compatibility hypothesis for a triple (W, γ, K), where $\gamma \in C$ and W is a K-subspace of $F^{(2)}$:

Hypothesis 3.1.

(i) $W + K\gamma = W \oplus K\gamma$ *has dimension* $[F: K]$.

(ii) $T_K(w\bar{w}) = 0$ *for all* $w \in W$.

(iii) $(W, K^{(2)}\gamma)_K = 0$.

(iv) $\mathcal{S} := \{\theta(W + K\gamma) \mid \theta \in C\} = (W + K\gamma)\,\tilde{C}$ *is a spread of* $F^{(2)}$.

Since $\tilde{C}$ is transitive on $\mathcal{S}$, $\mathbf{A}(\mathcal{S})$ is a flag-transitive affine plane. Also, (ii) and (iii) imply that $(W, W)_K = 0 = (W, K\gamma)_K$, so that $W + \gamma K$ is totally isotropic and $\mathcal{S}$ is a symplectic spread. Note that we have not yet required the full force of (iii). However we are about to exhibit an orthogonal spread arising from $\mathcal{S}$, and for this we will use (iii).

First we note that the conditions in (3.1) can, indeed, be met: if $\gamma = 1$ and $W = \ker T_K$, then we just saw that $F = W \oplus K\gamma$; (iii) is obvious, $T_K(w\bar{w}) = T_K(w)^2 = 0$ in (ii), and (iv) defines a desarguesian spread in $F^{(2)}$.

Hypothesis 3.1 is, in fact, based on the only examples of flag-transitive planes known to arise within $F^{(2)}$ (although we expect that there are large numbers of others), and (iii) holds in these examples. In fact, using our original spread as a starter, the following theorem inductively allows us to construct large numbers of symplectic spreads that also arise from triples satisfying Hypothesis 3.1.

Let L be a proper subfield of K with $[F\colon L]$ odd, and equip the L-space $F^{(2)} \oplus L^{(2)}$ with the quadratic form $Q_L((x, \lambda)) := T_L(x\bar{x}) + \lambda\bar{\lambda}$ for $(x, \lambda) \in F^{(2)} \oplus L^{(2)}$. As we are about to see, the quadratic form Q_L has maximal Witt index. Note that $(\tilde{\theta}, 1)$ is an isometry whenever $\theta \in C$; let $(\tilde{C}, 1)$ denote the group of these isometries. Write $W_{L|K} := \ker T_L|_K$, and let $\Sigma_{\mathscr{S}}$ consist of the following subspaces of $F^{(2)} \oplus L^{(2)}$:

$$\Sigma_{\mathscr{S}}[\theta] := (\theta(W + W_{L|K}\gamma), 0) + \{(\lambda\gamma\theta, \lambda) \mid \lambda \in L^{(2)}\} \qquad \text{for } \theta \in C. \tag{3.2}$$

THEOREM 3.3. *If Hypothesis* 3.1 *is satisfied by the triple* (W, γ, K), *then the following hold.*

(i) $\Sigma_{\mathscr{S}}$ *is an orthogonal spread of* $F^{(2)} \oplus L^{(2)}$.

(ii) *If* $z = \langle 0, \zeta \rangle$ *with* $\zeta \in C \cap L^{(2)}$, *then* $(\Sigma_{\mathscr{S}})_z$ *is a symplectic spread of the L-space* $z^{\perp}/z$ (*cf.* (2.1)) *that is equivalent to the symplectic spread*

$$\mathscr{S}(z) := \{\theta(W' + L\gamma\zeta) \mid \theta \in C\}$$

of the L-space $F^{(2)}$, *where* $W' := W + W_{L|K}\gamma$. *Moreover*, $\tilde{C}$ *is transitive on* $\mathscr{S}(z)$ *and Hypothesis* 3.1 *is satisfied by the triple* $(W', \gamma\zeta, L)$.

(iii) $(\Sigma_{\mathscr{S}})_{\langle 0, 1 \rangle}$ *is equivalent to* $\mathscr{S}$.

Proof. (i) Certainly $(\tilde{C}, 1)$ acts transitively on $\Sigma_{\mathscr{S}}$. In order to check that each member of $\Sigma_{\mathscr{S}}$ is totally singular of dimension $[F\colon L] + 1$, by transitivity it suffices to show this for $\Sigma_{\mathscr{S}}[1]$. Here, note that $\dim_L(W + W_{L|K}\gamma) = [F\colon L] - 1$ (since $\dim_L(W + K\gamma) = [F\colon K][K\colon L] = [F\colon L]$ and $W_{L|K}$ is an L-hyperplane of K), $\dim_L L^{(2)} = 2$, and $(W + W_{L|K}\gamma, 0) \cap \{(\lambda\gamma, \lambda) \mid \lambda \in L^{(2)}\} = 0$, so that $\dim_L \Sigma_{\mathscr{S}}[1] = [F\colon L] + 1$. Moreover, if $w \in W$, $v \in W_{L|K}$ and $\lambda \in L^{(2)}$, then

$$\begin{aligned} &Q_L([w + v\gamma] + \lambda\gamma, \lambda) \\ &\quad = T_L([w + (v + \lambda)\gamma]\,\overline{[w + (v + \lambda)\gamma]}) + \lambda\bar{\lambda} \\ &\quad = T_L(w\bar{w} + (v + \lambda)\gamma\bar{w} + \overline{(v + \lambda)\gamma}\, w + [v^2 + \lambda v + \bar{\lambda} v + \lambda\bar{\lambda}]\,\gamma\bar{\gamma}) + \lambda\bar{\lambda} \\ &\quad = T_L(w\bar{w}) + ((v + \lambda)\gamma, w)_L + T_L(v)^2 + (\lambda + \bar{\lambda})\, T_L(v) \\ &\quad = 0 \end{aligned}$$

(by (3.1ii, iii), since $v+\lambda \in K^{(2)}$), so that $\Sigma_{\mathscr{S}}[1]$ is totally singular. (Note that we just applied the full force of (3.1iii).)

Finally, in order to show that $\Sigma_{\mathscr{S}}$ is an orthogonal spread it suffices to prove that $\Sigma_{\mathscr{S}}[\theta] \cap \Sigma_{\mathscr{S}}[1] = 0$ whenever $\theta \in C - \{1\}$. As $(\tilde{C}, 1)$ is a group of odd order, none of its elements can interchange the two types of totally singular $([F:L]+1)$-spaces of $F^{(2)} \oplus L^{(2)}$ (cf. Section 2), so the members of $\Sigma_{\mathscr{S}}$ are all of the same type. Consequently, if $\Sigma_{\mathscr{S}}[\theta] \cap \Sigma_{\mathscr{S}}[1] \neq 0$, then this intersection must have even L-dimension. Then $\Sigma_{\mathscr{S}}[\theta] \cap \Sigma_{\mathscr{S}}[1] \cap (F^{(2)} \oplus L) \neq 0$ since $F^{(2)} \oplus L$ is a hyperplane of $F^{(2)} \oplus L^{(2)}$, so there exist $w, w' \in W$, $u, u' \in W_{L|K}$ and $l, l' \in L$ such that

$$(\theta(w+u\gamma+l\gamma), l) = (w'+u'\gamma+l'\gamma, l') \neq 0$$

(cf. (3.2)). Since $u+l,\ u'+l' \in K$, it follows that $\theta(w+[u+l]\gamma) = w'+[u'+l']\gamma \in \theta(W+K\gamma) \cap (W+K\gamma)$, so that $\theta(w+[u+l]\gamma)=0$ by (3.1iv). By (3.1i), $[u+l]\gamma \in W \cap K\gamma = 0$, so that $0 = T_L(u) = l$ (since $[F\colon L]$ is odd) and hence $(\theta(w+[u+l]\gamma, l) = 0$. This contradiction completes the proof of (i).

(ii) By Section 2, $(\Sigma_{\mathscr{S}})_z$ is a symplectic spread of $z^{\perp}/z$. Here, $z^{\perp} = F^{(2)} \oplus L\zeta$, so that

$$\begin{aligned}\Sigma_{\mathscr{S}}[\theta] \cap z^{\perp} &= \{(\theta(W+W_{L|K}\gamma), 0) + \{(l\zeta\gamma\theta, l\zeta) \mid l \in L\}\}\\ &\equiv (\theta(W+W_{L|K}\gamma + L\gamma\zeta), 0) \qquad (\mathrm{mod}\ z)\end{aligned}$$

by (3.2). Thus, $\langle z, \Sigma_{\mathscr{S}}[\theta] \cap z^{\perp}\rangle/z$ may be identified with the subspace $\theta(W+W_{L|K}\gamma+L\gamma\zeta)$ of $F^{(2)}$. Note that the alternating bilinear form on $z^{\perp}$ is $T_L((x, l\zeta), (x', l'\zeta)) = T_L(x\overline{x'} + \bar{x}x')$, so that $\mathscr{S}(z)$ is indeed, a symplectic spread of $F^{(2)}$. Clearly $\tilde{C}$ is transitive on $\mathscr{S}(z)$.

We now prove that $(W', \gamma\zeta, L)$ satisfies Hypothesis 3.1. Since $\mathscr{S}(z)$ is a spread, (i) and (iv) are clear. Next, $T_L(w'\overline{w'}) = 0$ whenever $w' \in W' = W + W_{L|K}\gamma$: if $w \in W$ and $v \in W_{L|K}$, then

$$T_L((w+v\gamma)\,\overline{(w+v\gamma)}) = T_L(w\bar{w}) + T_L(\overline{v\gamma}w + v\gamma\bar{w}) + T_L(v)^2 = 0$$

using conditions (3.1ii, iii) for (W, γ, K). Lastly, $(W', L^{(2)}\gamma\zeta)_L = 0$: if $w \in W$, $v \in W_{L|K}$ and $\lambda \in L^{(2)}$, then

$$\begin{aligned}(w+v\gamma, \lambda\gamma\zeta)_L &= (w, \lambda\gamma\zeta)_L + (v\gamma, \lambda\gamma\zeta)_L\\ &= 0 + (\lambda\zeta + \overline{\lambda\zeta})\, T_L(v)\\ &= 0\end{aligned}$$

(using (3.1ii) and $\lambda\zeta \in K^{(2)}$, $\lambda\zeta + \overline{\lambda\zeta} \in L$ and $T_L(v) = 0$). Consequently, Hypothesis 3.1 is satisfied by our new triple, and (ii) holds.

(iii) $W' + L\gamma = W + W_{L|K}\gamma + L\gamma = W + K\gamma$. ▮

Theorem 3.3 provides a method to produce flag-transitive scions of the desarguesian plane. We now exhibit these scions explicitly.

4. Flag-Transitive Scions of the Desarguesian Plane

Let $F = F_0 \supset \cdots \supset F_n$ be a tower of fields with $[F: F_i]$ odd for each i and corresponding trace maps $T_i: F \to F_i$. Write $W_i := \ker T_{i+1}|_{F_i}$. For each i, let $F_i^{(2)}$ be a subfield of $F^{(2)}$ of degree 2 over F_i; view $F^{(2)}$ as a symplectic space over F_i with the associated alternating form defined by $(x, y)_i := T_i(x\bar{y} + \bar{x}y)$; and let $\zeta_i \in F_i^{(2)} \cap C$, where $\zeta_0 = 1$. Write $\gamma_i := \Pi_0^i \zeta_l$ and

$$\mathscr{S}((F_i)_0^n, (\zeta_i)_0^n) := \left\{ \theta \left(\sum_0^{n-1} W_i\gamma_i + F_n\gamma_n \right) \middle| \, \theta \in C \right\}. \tag{4.1}$$

This should be compared to the following direct sum decomposition of F:

$$F = W_0 \oplus \cdots \oplus W_{n-1} \oplus F_n, \tag{4.2}$$

which is an inductive consequence of the fact that $F_i = W_i \oplus F_{i+1}$ (since $[F_i: F_{i+1}]$ is odd). Of course, the images of F under $\tilde{C}$ form a desarguesian spread in $F^{(2)}$. Thus, (4.1) amounts to "perturbing" that spread, as well as the summands in (4.2), by suitable members γ_i of C. In fact, *the sum* $\sum_0^{n-1} W_i\gamma_i + F_n\gamma_n$ *in* (4.1) *is direct*; this is easily proved directly, but also follows immediately from (4.2) together with the next theorem.

Our perturbation behaves as follows:

Theorem 4.3. *$\mathscr{S}((F_i)_0^n, (\zeta_i)_0^n)$ is a symplectic spread of the F_n-space $F^{(2)}$, and $\tilde{C}$ acts transitively on this spread.*

Proof. We will use Theorem 3.3 and induction on n in order to show that $(\sum_0^{n-1} W_i\gamma_i, \gamma_n, F_n)$ satisfies Hypothesis 3.1. For the base case $n = 0$, $\mathscr{S}((F_0), (1)) = F_0\tilde{C}$ is a desarguesian spread and the triple $(0, 1, F_0)$ trivially satisfies Hypothesis 3.1.

Now assume that the triple $(\sum_0^{j-1} W_i\gamma_i, \gamma_j, F_j)$ satisfies Hypothesis 3.1 for some $j \geqslant 0$. As $\zeta_{j+1} \in F_{j+1}^{(2)} \cap C$, the spread $\mathscr{S}((F_i)_0^{j+1}, (\zeta_i)_0^{j+1})$ is obtained as in Theorem 3.3(ii), since $(\sum_0^{j-1} W_i\gamma_i) + W_j\gamma_j + F_{j+1}\gamma_j\zeta_{j+1} = \sum_0^j W_i\gamma_i + F_{j+1}\gamma_{j+1}$. This completes the induction. ▮

Note that each plane $\mathbf{A}(\mathscr{S}((F_i)_0^n, (\zeta_i)_0^n))$ is a flag-transitive scion of the desarguesian plane of order $|F_0|$. Conversely, every flag-transitive scion of that desarguesian plane is (isomorphic to) one of the planes just constructed (cf. Section 6, Remark 1).

DEFINITION 4.4. Call $((F_i)_0^n, (\zeta_i)_0^n)$ a *defining pair* for the symplectic spread $\mathscr{S}((F_i)_0^n, (\zeta_i)_0^n)$, and a *reduced* defining pair if, in addition, $\zeta_i \neq 1$ for all $i \geqslant 1$.

COROLLARY 4.5. *Modify a defining pair $((F_i)_0^n, (\zeta_i)_0^n)$ by deleting some or all entries F_i and ζ_i for which $i \geqslant 1$ and $\zeta_i = 1$. Then the resulting pair $((F'_i)_0^{n'}, (\zeta'_i)_0^{n'})$ is a defining pair for a spread $\mathscr{S}((F'_i)_0^{n'}, (\zeta'_i)_0^{n'})$, and $\mathscr{S}((F_i)_0^n, (\zeta_i)_0^n) = \mathscr{S}((F'_i)_0^{n'}, (\zeta'_i)_0^{n'})$. Furthermore, if all $\zeta_i = 1$ then $\mathscr{S}((F_i)_0^n, (\zeta_i)_0^n)$ is desarguesian.*

Proof. First assume that $j < n$ and $\zeta_j = 1$. Then $\gamma_{j-1} = \gamma_j$ and $W_{j-1}\gamma_{j-1} + W_j\gamma_j = W'_{j-1}\gamma_{j-1}$, where $W'_{j=1} = \ker T_{j+1}|_{F_{j-1}}$ (by (4.2)). Thus, by (4.1), $((F_i)_0^n, (\zeta_i)_0^n)$ and $((F_0, ..., F_{j-1}, \hat{F}_j, F_{j+1}, ..., F_n), (1, ..., \zeta_{j-1}, \hat{1}, \zeta_{j+1}, ..., \zeta_n))$ define the same spread (where "hats" denote deletions). A similar argument works in case $\zeta_n = 1$, as then $W_{n-1}\gamma_{n-1} + F_n\gamma_n = F_{n-1}\gamma_{n-1}$. ▌

Corollary 4.5 implies that we may restrict consideration to reduced defining pairs when we study the scions arising from Theorem 4.3. However, when we count planes we will fix one tower $(F_i)_0^n$, in which case non-reduced pairs account for subtowers.

5. ISOMORPHISMS BETWEEN FLAG-TRANSITIVE SCIONS

The following elementary but general result permits us to decrease the amount of calculation used in the proof of Theorem 1.1. Let F, $F^{(2)}$, and $\tilde{C}$ be as before, let $\phi\colon F \to \mathrm{GF}(2)$ be any nonzero additive map, and consider the $\tilde{C}$-invariant nonsingular alternating GF(2)-bilinear form $(x, y) := \phi(x\bar{y} + \bar{x}y)$.

PROPOSITION 5.1. *Let $\mathscr{S}$ and $\mathscr{S}'$ be symplectic spreads in the* GF(2)-*space $F^{(2)}$ such that $\tilde{C}$ is transitive on each of them. If $\mathbf{A}(\mathscr{S})$ and $\mathbf{A}(\mathscr{S}')$ are isomorphic, and if $|F| > 8$, then $\mathscr{S}' = \mathscr{S}^\sigma$ for some $\sigma \in \operatorname{Aut} F^{(2)}$.*

Proof. By [Ka I (3.5)], we may assume that the given isomorphism is induced by a symplectic transformation g of the GF(2)-space $F^{(2)}$. By Zsigmondy's Theorem [Zs], there is a prime p such that $\tilde{C}$ contains a Sylow p-subgroup P of $Sp(F^{(2)})$ and such that P is irreducible on $F^{(2)}$. Then P and P^g are Sylow subgroups of $\operatorname{Aut} \mathbf{A}(\mathscr{S}') \cap Sp(F^{(2)})$, so that $P^{gh} = P$ for some $h \in \operatorname{Aut} \mathbf{A}(\mathscr{S}') \cap Sp(F^{(2)})$. Now $gh \in Sp(F^{(2)})$ is an isomorphism $\mathbf{A}(\mathscr{S}) \to \mathbf{A}(\mathscr{S}')$, and normalizes P.

However, by Schur's Lemma the normalizer of P in $GL(F^{(2)})$ is $\{x \mapsto ax^{\sigma} \mid a \in F^{(2)*}, \sigma \in \operatorname{Aut} F^{(2)}\}$ (cf. [Hu, p. 187]), and the intersection of this with $Sp(F^{(2)})$ is just $\{x \mapsto ax^{\sigma} \mid a \in C, \sigma \in \operatorname{Aut} F^{(2)}\}$. (Namely, if $x \mapsto ax$ preserves our form, then $\phi(x\bar{y} + \bar{x}y) = \phi(ax\,\overline{ay} + \overline{ax}\,ay)$ and consequently $\phi((x\bar{y} + \bar{x}y)(a\bar{a} + 1)) = 0$ for all $x, y \in F^{(2)}$, so that $a\bar{a} + 1 = 0$ and hence $a \in C$, as asserted.) Since $\tilde{C}$ leaves $\mathcal{S}$ invariant, it follows that gh has the same effect on $\mathcal{S}$ as some element of Aut $F^{(2)}$. ▌

We can now give a complete solution to the isomorphism problem for the planes we have been studying:

THEOREM 5.2. *Let $\mathcal{S}$ and $\mathcal{S}'$ be scions of the desarguesian spread in $F^{(2)}$ with respective reduced defining pairs $((F_i)_0^n, (\zeta_i)_0^n)$ and $((F_i')_0^{n'}, (\zeta_i')_0^{n'})$. If $|F_0| > 8$, and if $\mathbf{A}(\mathcal{S})$ and $\mathbf{A}(\mathcal{S}')$ are isomorphic, then $n = n'$, $F_i = F_i'$ and $\zeta_i' = \zeta_i^{\sigma}$ for some $\sigma \in$ Aut $F^{(2)}$ and all i.*

Proof. Here $F^{(2)}$ is equipped with two alternating bilinear forms: $\mathcal{S}$ is symplectic with respect to $(x, y)_{F_n} := T_{F_n}(x\bar{y} + \bar{x}y)$, and $\mathcal{S}'$ is symplectic with respect to $(x, y)_{F'_{n'}} := T_{F'_{n'}}(x\bar{y} + \bar{x}y)$. We introduce a third alternating bilinear form on $F^{(2)}$, namely $(x, y) := T(x\bar{y} + \bar{x}y)$, where $T\colon F \to \mathrm{GF}(2)$ is the trace map.

Note that $T(T_{F_n}(x)) = T(x)$ for all $x \in F$: if we abbreviate $L = F_n$ and $K = \mathrm{GF}(2)$, then

$$T(T_L(x)) = \sum_{\substack{\lambda \in \mathrm{Gal}(F/L) \\ \sigma \in \mathrm{Gal}(F/K)}} x^{\lambda\sigma}$$

$$= \sum_{\rho \in \mathrm{Gal}(F/K)} (\#(\lambda, \sigma) \in \mathrm{Gal}(F/L) \times \mathrm{Gal}(F/K) \colon \rho = \lambda\sigma)\, x^{\rho},$$

where the indicated number is the odd integer $[F\colon L]$ (since, for any ρ and λ, we must choose $\sigma = \lambda^{-1}\rho$). This proves that $T(T_{F_n}(x)) = T(x)$, and similarly $T(T_{F'_{n'}}(x)) = T(x)$.

Thus, our new form refines the other two: $(x, y) = T((x, y)_{F_n}) = T((x, y)_{F'_{n'}})$, so that $\mathcal{S}$ and $\mathcal{S}'$ are symplectic with respect to the new form. In view of Proposition 5.1, all we now need to know is when two of our spreads coincide. While the required result offers no surprises, proving it appears to be less straightforward than one might expect:

LEMMA 5.3. *Let $\mathcal{S}$ and $\mathcal{S}'$ be scions of the desarguesian spread in $F^{(2)}$ with respective reduced defining pairs $((F_i)_0^n, (\zeta_i)_0^n)$ and $((F_i')_0^{n'}, (\zeta_i')_0^{n'})$. If $\mathcal{S} = \mathcal{S}'$ then $n = n'$, $F_i = F_i'$ and $\zeta_i = \zeta_i'$ for all i.*

Proof. We may assume that $n \leqslant n'$. We will prove by induction on j that, for $0 \leqslant j \leqslant n$, we have $F_i = F'_i$ for $0 \leqslant i \leqslant j$, $\zeta_i = \zeta'_i$ for $0 \leqslant i < j$, and

$$\sum_{i=j}^{n-1} W_i(\gamma_i/\gamma_{j-1}) + F_n(\gamma_n/\gamma_{j-1}) = \theta_0 \left(\sum_{i=j}^{n'-1} W'_i(\gamma'_i/\gamma'_{j-1}) + F'_{n'}(\gamma'_{n'}/\gamma'_{j-1}) \right), \tag{5.4}$$

where θ_0 is an element of C that is independent of j, $\gamma_{-1} = \gamma'_{-1} = 1$, and empty sums are deleted. By (4.1), $F_0 = F = F'_0$ and $\mathscr{S}[1] = \mathscr{S}'[\theta_0]$ for some $\theta_0 \in C$, so the base case holds.

Now assume that our induction hypothesis holds for some $0 \leqslant j < n$. As already noted, since $\mathscr{S}$ is a spread the sum in (4.1) is direct. In particular, both sides of (5.4) have size $|F_j| = |F'_j|$.

As $[F_j : F_{j+1}] \geqslant 3$, we have $\dim_{F_{j+1}} W_j = \dim F_{j+1} \geqslant (2/3)[F_j : F_{j+1}]$. In particular, $\dim_{\mathrm{GF}(2)} W_j \geqslant (2/3) \dim_{\mathrm{GF}(2)} F_j$; similarly, $\dim_{\mathrm{GF}(2)} W'_j \geqslant (2/3) \dim_{\mathrm{GF}(2)} F_j$. Since the left side of (5.4) has a summand $W_j(\gamma_j/\gamma_{j-1}) = W_j \zeta_j$, while the right side has a summand $W'_j \theta_0 (\gamma'_j/\gamma'_{j-1}) = W'_j \theta_0 \zeta'_j$, it follows that $0 \neq W_j \cap W'_j \theta_0 \zeta'_j \zeta_j^{-1} \subseteq F_j$, so that $\theta_0 \zeta'_j \zeta_j^{-1} \in F_j \cap C = \{1\}$. Thus, $\theta_0 \zeta_j = \zeta'_j$. Then in case $j = 0$ we see that $\theta_0 = 1$, and so in any case we have $\zeta_j = \zeta'_j$.

Divide both sides of (5.4) by ζ_j in order to obtain $W_j + X = W'_j + Y$, where $X := \sum_{i=j+1}^{n-1} W_i(\gamma_i/\gamma_j) + F_n(\gamma_n/\gamma_j)$ and $Y := \sum_{i=j+1}^{n'-1} W'_i(\gamma'_i/\gamma'_j) + F'_{n'}(\gamma'_{n'}/\gamma'_j)$. Here, $X \subseteq F_{j+1}^{(2)}$ since $\gamma_i/\gamma_j = \Pi_{l=j+1}^{i} \zeta_l \in F_{j+1}^{(2)}$; similarly, $Y \subseteq F'^{(2)}_{j+1}$.

First we show that $F_{j+1} = F'_{j+1}$. Consider the trace map $t : F^{(2)} \to F$ given by $z \mapsto z + \bar{z}$. Since $1 \neq \zeta_{i+1} = \gamma_{j+1}/\gamma_j \in C$ we see that $\zeta_{j+1} \notin F_0$ and $t(W_j + X) = t(X)$ contains the nonzero subset $W_{j+1}(\zeta_{j+1} + \overline{\zeta_{j+1}})$ (or $F_n(\zeta_n + \overline{\zeta_n})$ when $j = n - 1$). Here, $\zeta_{j+1} + \overline{\zeta_{j+1}} \in F_{j+1}$, while $|W_{j+1}| \geqslant |F_{j+1}|^{2/3}$ as seen above. Consequently, the subfield of F generated by $t(W_j + X)$ is F_{j+1}. Similarly, the subfield generated by $t(W'_j + Y)$ is F'_{j+1}. Thus, $F_{j+1} = F'_{j+1}$, and hence $W_j = W'_j$.

Next we show that $X = Y$, which is exactly the required condition (5.4) with j in place of $j - 1$. By symmetry, it suffices to prove that $X \subseteq Y$. If $0 \neq x \in X$, then $x = w + y$ for some $w \in W_j$ and $y \in Y$, and it suffices to prove that $w = 0$. We have $x\bar{x} = w^2 + w(y + \bar{y}) + y\bar{y}$, where $x \in F_{j+1}^{(2)}$ and hence $x\bar{x} \in F_{j+1}$; also $y\bar{y}$, $y + \bar{y} \in F_{j+1}$. Consequently,

$$x\bar{x} = T_{j+1}(x\bar{x}) = T_{j+1}(w)^2 + T_{j+1}(w(y + \bar{y})) + y\bar{y} = y\bar{y}.$$

Thus, $0 = w^2 + w(y + \bar{y})$. If $w \neq 0$, then $0 = w + y + \bar{y} = T_{j+1}(w + (y + \bar{y})) = y + \bar{y} = w$. Consequently, $w = 0$ and $X \subseteq Y$, as claimed.

Finally, when the induction terminates, $F_n = F'_n$ and

$$F'_n \zeta_n = F_n(\gamma_n/\gamma_{n-1}) = \sum_{i=n}^{n'-1} W'_i(\gamma'_i/\gamma'_{n-1}) + F'_{n'}(\gamma'_{n'}/\gamma'_{n-1}).$$

Suppose that $n' > n$. Then $\gamma'_{n'}/\gamma'_{n-1} \in F'_n \zeta_n$ and $W'_{n'-1}(\gamma'_{n'-1}/\gamma'_{n-1}) \subseteq F'_n \zeta_n$, where $W'_{n'-1} \subseteq F'_{n'-1} \subseteq F'_n$. Then $\gamma'_{n'}/\gamma'_{n-1}\zeta_n, \gamma'_{n'-1}/\gamma'_{n-1}\zeta_n \in C \cap F'_n = \{1\}$ and hence $\zeta'_{n'} = \gamma'_{n'}/\gamma'_{n'-1} = 1$, which contradicts the fact that we are dealing with reduced pairs.

Consequently, $n' = n$, $F'_n \zeta_n = F'_n(\gamma'_n/\gamma'_{n-1}) = F'_n \zeta'_n$, and $\zeta_n^{-1}\zeta'_n \in C \cap F'_n = \{1\}$. ▮

Corollary 5.5. *If $|F_0| > 8$, and if two defining pairs $((F_i)_0^n, (\zeta_i)_0^n)$ and $((F_i)_0^n, (\zeta'_i)_0^n)$ produce isomorphic planes, then $\zeta'_i = \zeta_i^\sigma$ for some $\sigma \in \operatorname{Aut} F^{(2)}$ and all i.*

Proof of Theorem 1.1. There are exactly $\Pi_1^n(q^{m_i}+1)$ defining pairs using a given tower $(F_i)_0^n$ of fields. By (4.1), any element of the Galois group of $F_0^{(2)}$ over $F_1^{(2)}$ stabilizes all spreads defined using the tower $(F_i)_0^n$. Thus, Corollary 5.5 implies the result. ▮

6. Kernels and Equivalence of Orthogonal Spreads

We now calculate the kernels (cf. [De, pp. 132–133]) of our planes:

Theorem 6.1. *If $((F_i)_0^n, (\zeta_i)_0^n)$ is a reduced defining pair, and if $|F_0| > 8$, then the kernel of the associated plane $\mathbf{A}(\mathscr{S}((F_i)_0^n, (\zeta_i)_0^n))$ is isomorphic to F_n.*

Proof. We can view F_n^* as a subgroup of the full group H of homologies of $\mathbf{A}(\mathscr{S}((F_i)_0^n, (\zeta_i)_0^n))$ with center 0. We will show that these groups are equal. By Zsigmondy's Theorem [Zs], there is a prime p such that $p \mid q^{2m}-1$ and $p \nmid q^k - 1$ for $1 \leqslant k < 2m$. Then $\tilde{C}$ contains a Sylow p-subgroup P of $GL(F^{(2)})$ (where $F^{(2)}$ is viewed as a $GF(2)$-space), and P is irreducible on $F^{(2)}$. Moreover, P normalizes H, and hence it even centralizes H since p is relatively prime to $q^{2m}-1$.

On the other hand, by Schur's Lemma $C_{\mathrm{GL}(F^{(2)})}(P)$ is the multiplicative group of a field, and hence is isomorphic to $F^{(2)*}$. Thus, each $h \in H$ has the form $x \mapsto ax$ for some $a \in F^{(2)}$. The following Lemma completes the proof of the theorem.

Lemma 6.2. *If $a \in F^{(2)*}$ and $x \mapsto ax$ induces the identity on $\mathscr{S}((F_i)_0^n, (\zeta_i)_0^n)$, where $((F_i)_0^n, (\zeta_i)_0^n)$ is reduced, then $a \in F_n^*$.*

Proof. We will prove by induction on j that, for $0 \leqslant j \leqslant n$, we have $a \in F_j$ and

$$a\left(\sum_{i=j}^{n-1} W_i \gamma_i + F_n \gamma_n\right) = \sum_{i=j}^{n-1} W_i \gamma_i + F_n \gamma_n \tag{6.3}$$

(as usual, empty sums are ignored).

For the base case note that $\dim_{\mathrm{GF}(2)} W_0 \geqslant (2/3) \dim_{\mathrm{GF}(2)} F_0$, so $0 \neq aW_0 \cap W_0$ and hence $a \in F_0$ (compare the proof of Proposition 5.3.). Assume that (6.3) holds for some j with $0 \leqslant j < n$, divide (6.3) by γ_j, and obtain $a(W_j + X) = W_j + X$ where $X := \sum_{i=j+1}^{n-1} W_i(\gamma_i/\gamma_j) + F_n(\gamma_n/\gamma_j)$.

We first show that $a \in F_{j+1}$. For, as $((F_i)_0^n, (\zeta_i)_0^n)$ is reduced, $W_{j+1}(\gamma_{j+1}/\gamma_j)$ (or $F_n(\gamma_n/\gamma_{n-1})$ if $j = n-1$) contains an element $x \notin F_0$. Since $x \in X$ we have $ax = w + y$ for some $w \in W_j$, $y \in X$. "Barring" this equation and adding yields $a(x + \bar{x}) = y + \bar{y}$, so that $a = (y + \bar{y})/(x + \bar{x}) \in F_{j+1}$.

Next, $X = aX$, which is just (6.3) with j replaced by $j+1$. The proof of this exactly the one given in the next to last paragraph of the proof of Proposition 5.3 (since $W_j + X = W_j + Y$ with $Y = aX$), and hence is omitted.

Finally, when the induction terminates at $j = n$ we see that $a \in F_n$, as required. ▌

The preceding theorem can be used to discuss the equivalence of orthogonal spreads:

Proposition 6.4. *Write $\mathscr{S} = \mathscr{S}((F_i)_0^n, (\zeta_i)_0^n)$ and $\mathscr{S}' = \mathscr{S}'((F'_i)_0^{n'}, (\zeta'_i)_0^{n'})$ for defining pairs $((F_i)_0^n, (\zeta_i)_0^n)$ and $((F'_i)_0^{n'}, (\zeta'_i)_0^{n'})$, and let L be a proper subfield of both F_n and $F'_{n'}$ such that $[F{:}\ L]$ is odd. Then the orthogonal spreads $\Sigma_{\mathscr{S}}$ and $\Sigma_{\mathscr{S}'}$ of the L-space $F^{(2)} \oplus L^{(2)}$ (cf. Theorem* 3.3) *are equivalent under $\Gamma O^+(F^{(2)} \oplus L^{(2)})$ if and only if the affine places $\mathbf{A}(\mathscr{S})$ and $\mathbf{A}(\mathscr{S}')$ are isomorphic.*

Proof. According to [Ka I (3.6)], if $\mathbf{A}(\mathscr{S}) \cong \mathbf{A}(\mathscr{S}')$ then $\Sigma_{\mathscr{S}}$ and $\Sigma_{\mathscr{S}'}$ are equivalent by an element of $\Gamma O^+(F^{(2)} \oplus L^{(2)})$. So only the converse remains.

By Theorem 3.3(iii), $\mathbf{A}((\Sigma_{\mathscr{S}})_{\langle 0, 1\rangle}) \cong \mathbf{A}(\mathscr{S})$ and $\mathbf{A}((\Sigma_{\mathscr{S}'})_{\langle 0, 1\rangle}) \cong \mathbf{A}(\mathscr{S}')$.

As in the proof of Proposition 5.1, if $\Sigma_{\mathscr{S}}$ and $\Sigma_{\mathscr{S}'}$ are equivalent under $\Gamma O^+(F^{(2)} \oplus L^{(2)})$ then they are equivalent via an element g normalizing $(\tilde{C}, 1)$. Then $0 \oplus L^{(2)}$ is an invariant subspace of g, and hence $\langle 0, 1\rangle^g = \langle 0, \zeta\rangle$ for some $\zeta \in L^{(2)*} = L^* \times (C \cap L^{(2)*})$; we may assume that $\zeta \in C \cap L^{(2)}$.

Now $\mathbf{A}(\mathscr{S}) \cong \mathbf{A}((\Sigma_{\mathscr{S}})^g_{\langle 0, 1\rangle^g}) = \mathbf{A}((\Sigma_{\mathscr{S}'})_{\langle 0, \zeta\rangle})$. By (the proof of) Theorem 4.3, $\mathbf{A}((\Sigma_{\mathscr{S}'})_{\langle 0, \zeta\rangle})$ has associated defining pair $((F'_i)_0^{n'+1}, (\zeta'_i)_0^{n'+1})$, where $F'_{n'+1} = L$ and $\zeta'_{n'+1} = \zeta$.

The kernel $\mathbf{A}(\mathscr{S})$, and so also of $\mathbf{A}((\Sigma_{\mathscr{S}'})_{\langle 0, \zeta \rangle})$, contains F_n and hence properly contains L. On the other hand, Theorem 6.1 implies that, for fixed $((F'_i)_0^{n'}, (\zeta'_i)_0^{n'})$, among all of the planes with defining pairs $((F'_i)_0^{n'+1}, (\zeta'_i)_0^{n'+1})$, where $F'_{n'+1} = L$ and $\zeta'_{n+1} \in L^{(2)}$, the only one whose kernel is larger than $F'_{n'+1}$ has $\zeta'_{n'+1} = 1$ and hence is $\mathbf{A}((\Sigma_{\mathscr{S}'})_{\langle 0, 1 \rangle}) \cong \mathbf{A}(\mathscr{S}')$. Thus $\mathbf{A}(\mathscr{S}) \cong \mathbf{A}(\mathscr{S}^g) \cong \mathbf{A}(\mathscr{S}')$, as required. ▮

THEOREM 6.5. *Let m an odd composite integer, and let $m, m_1, ..., m_{n-1}, 1$ be any sequence of $n+1 \geqslant 3$ distinct divisors of m such that each is divisible by the next. If $|F| = q^m$ and $|L| = q$, then there are at least $\prod_1^{n-1} (q^{m_i}+1)/2m_1 \log_2 q$ pairwise inequivalent orthogonal spreads of $F^{(2)} \oplus L^{(2)}$ each invariant under a transitive cyclic group of orthogonal transformations.*

Proof. This is immediate from Proposition 6.4 and Theorem 1.1. ▮

Remark 6.6. *The planes $\mathbf{A}(\mathscr{S}((F_i)_0^n, (\zeta_i)_0^n))$ are precisely the flag-transitive scions of the desarguesian plane of order $q^m = |F_0|$.* For, we know that each of these planes is such a scion. Conversely, any flag-transitive scion of the desarguesian plane is isomorphic to one of our planes. For, let $\mathbf{A}$ be such a flag transitive scion. Then the proof of Proposition 6.4 shows that any cyclic subgroup of $\Gamma O^+(F^{(2)} \oplus L^{(2)})$ of order q^m+1 is conjugate to $(\tilde{C}, 1)$. Thus, inductively we may assume that $\mathbf{A}$ is isomorphic to $\mathbf{A}((\Sigma_{\mathscr{S}})_z)$ for one of the spreads $\mathscr{S}$ in Theorem 4.3 and some nonsingular point z. Then $z = \langle 0, \zeta \rangle$ for some $\zeta \in C$, and hence $\mathbf{A}((\Sigma_{\mathscr{S}})_z)$ also arises in Theorem 4.3.

Remark 6.7. Proposition 6.4 is based on ideas in [Wi], where the sizes of fields play a crucial role in the proofs of equivalence of other types of planes (including semifield scions of desarguesian planes) and orthogonal spreads, as well as of certain codes. Moreover, the arguments in [Wi] are much more complicated than those used here. For example in our Theorem 6.1, Zsigmondy's Theorem was a standard type of crutch for us, but is not available in much of [Wi].

Remark 6.8. We have seen that each of our planes, $\mathbf{A}(\mathscr{S}((F_i)_0^n, (\gamma_i)_0^n)$, is naturally associated with all of the others, $\mathbf{A}(\mathscr{S}((F_i)_0^n, (\gamma'_i)_0^n))$, defined using a fixed tower, $(F_i)_0^n$, of fields. On the other hand, implicit in the proof of Proposition 5.3 there are *subplanes*, $\mathbf{A}(\mathscr{S}((F_i)_j^n, (\gamma_i)_j^n))$, arising from suitable subsets, $(F_i)_j^n$, of our original tower, $(F_i)_0^n$. In fact, each such subplane, $\mathbf{A}(\mathscr{S}((F_i)_j^n, (\gamma_i)_j^n))$, is the set of fixed points of an automorphism, $x \mapsto x^{|F_j|}$, of $F^{(2)}$. Thus, we also see that scions of the original desarguesian plane, $AG(2, |F_0|)$, breed scions of its subplanes, $AG(2, |F_j|)$.

Remark 6.9. In the proof of Theorem 1.1 we used an elementary Sylow argument in order to sidestep knowledge of the full automorphism groups of our planes. According to a result announced by Hering in 1973 [He], assuming the classification of finite simple groups the full collineation group of each of our planes is solvable, and hence lies in the 1-dimensional affine group $A\Gamma L(1, F^{(2)})$. However, it would be of interest to have a direct and more geometric proof of this fact.

References

[De] P. Dembowski, "Finite Geometries," Springer, Berlin/Heildelberg/New York, 1968.

[He] C. Hering, On linear groups which contain an irreducible subgroup of prime order, *in* "Proceedings Internat. Conference on Projective Planes, 1973," pp. 99–105, Washington State Univ. Press, Pullman, 1973.

[Hu] B. Huppert, "Endliche Gruppen," Springer, Berlin/Göttingen/Heidelberg, 1967.

[Ka] W. M. Kantor, Spreads, translation planes and Kerdock sets, I, II, *SIAM J. Alg. Discrete Meth.* **3** (1982), 151–165, 308–318.

[Ta] D. E. Taylor, "The Geometry of the Classical Groups," Heldermann, Berlin, 1992.

[Wi] M. E. Williams, "$\mathbb{Z}_4$-Linear Kerdock Codes, Orthogonal Geometries and Nonassociative Division Algebras," Ph.D. thesis, University of Oregon, 1995.

[Zs] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. Math. Phys.* **3** (1892), 265–284.