

More Translation Planes and Semifields from Dembowski Ostrom Polynomials

Ulrich Dempwolff

Abstract

In this article we use pairs of Dembowski Ostrom polynomials with special properties (see (1)-(3) in the introduction below) to construct translation planes of order q^n which admit cyclic groups of order $q^n - 1$ having orbits of lengths $1, 1, (q^n - 1)/2, (q^n - 1)/2$ on the line at infinity. The same pairs also define semifields of order q^{2n} . We discuss the properties of these translation planes and semifields. These constructions extend the related construction in [7].

1 Introduction

Let q a prime power of the odd prime p , n an odd number, and $F = \text{GF}(q^n)$. Let ζ be a non-square in K . In [7] P. Müller and the author considered Dembowski Ostrom polynomials of the form $P(X) = L(X)X$, $L(X) = \sum_{i=0}^{n-1} a_i X^{q^i}$ such that (1) $F \ni x \mapsto L(x) \in F$ is bijective, (2) $|P(F^*)| = \frac{q^n - 1}{2}$, and (3) $P(F^*) \cap \zeta P(F^*) = \emptyset$. It was shown that such polynomials define translation planes of order q^n which admit a collineation group having orbits of lengths $1, 1, q^n - 1$ on the line at infinity.

The purpose of this article is to exploit these polynomials further. We will show (see Theorem 3.2) that *pairs* of polynomials with the above properties define in the same simple way as in [7] translation planes. This leads to a *uniform description* of some twisted field planes, the planes of [7], the planes of Suetake [18], and two new classes of planes (Theorem 3.7).

We also will show that such pairs of polynomials can be used to define semifield planes of order q^{2n} . One class can be viewed as quadratic extensions of twisted fields. It should be noted that our definition of semifields has nothing to do with the definition of commutative semifields by planar Dembowski Ostrom polynomials although our polynomials are planar too (see [7, Lemma 5.1]).

In the next section we will prove some preliminary results and introduce some notation. In the third section the family of translation planes of order q^n containing the planes of [7] and [18] will be introduced and isomorphism (Theorem 3.7) and automorphism problems (Theorem 3.13) will be discussed. The most important properties of the new classes are collected in:

Theorem A *Let $q > 3$ be a power of the odd prime p , n an odd number, $0 < r < n$ a number coprime to n , and $0, \pm 1 \neq \alpha \in \text{GF}(q)$. Then one can associate with the quadruple (q, n, r, α) two translation planes \mathbf{A}_1 and \mathbf{A}_2 of order q^n such that the following holds.*

- (a) *The kernel of \mathbf{A}_1 and \mathbf{A}_2 has order q .*
- (b) *Let G_i be a translation complement of the plane \mathbf{A}_i , $i = 1, 2$. Then G_1 has orbits of lengths 2 and $q^n - 1$ on the line at infinity while G_2 has orbits of lengths 1, 1, $(q^n - 1)/2$ and $(q^n - 1)/2$.*
- (c) *Each group G_i , $i = 1, 2$ has a normal subgroup \mathcal{G} such that \mathcal{G} has normal subgroups \mathcal{H} and Z with $\mathcal{G}/\mathcal{H} \simeq \text{Gal}(\text{GF}(q) : \text{GF}(p)[\alpha])$, $\mathcal{H}/Z \simeq C_n$, and $Z \simeq C_{q^n-1} \times C_{(q-1)/2}$. Moreover $|G_1 : \mathcal{G}| = 4$ or $= 2$ according as to whether or not there exists $\sigma \in \text{Aut}(\text{GF}(q))$ with $\alpha^\sigma = -\alpha$. Finally $G_2 = \mathcal{G}$.*
- (d) *Both types of planes define new families of translation planes.*

In the last section we construct with the help of our polynomials semifields of order q^{2n} and we compute their nuclei (Theorems 4.3, 4.9). The multiplication in these planes are given by (see Theorems 4.1 and 4.4):

Theorem B *Let q be a power of the odd prime p , n an odd number, $F = \text{GF}(q^n)$ and denote by ζ a non-square in $\text{GF}(q)$.*

- (a) *Let $P_1(X) = L_1(X)X$ and $P_2(X) = L_2(X)X$ two permutation polynomials satisfying (1)-(3) and assume $P_1(F^*) = P_2(F^*)$. Define a multiplication on F^2 by*

$$(u, v) * (x, y) = (ux + vL_1(y), uy + \zeta vL_2(x)).$$

*Then $(F^2, +, *)$ is a pre-semifield.*

- (b) *Let $0 < r < n$ and $a \in F^*$ such that $a^{(q^n-1)/(q^{(n,r)}-1)} \neq 1$. Assume further $0 \leq s, t < n$, $s \neq t$, and $t \equiv s \pmod{(n, r)}$. Define a multiplication on F^2 by*

$$(u, v) * (x, y) = (ux + v^{q^s} y^{q^r} - av^{q^t} y^{q^{-r}}, uy + \zeta(v^{q^s} x^{q^r} - av^{q^t} x^{q^{-r}})).$$

*Then $(F^2, +, *)$ is a pre-semifield.*

The major part of the last section is devoted to the computation of the nuclei of the semifields.

2 Preliminaries

For the remainder of this note q will be a power of the odd prime p and n will be a positive odd integer. We set

$$K = \text{GF}(q), \quad F = \text{GF}(q^n), \quad \text{with prime field } K_0 = \text{GF}(p),$$

and $no : F \rightarrow K$ will be the norm. By V we denote an n -dimensional K -space.

Spreads and translation planes We assume that the reader is familiar with the basics of finite translation planes (see [1], [5], [16] or [12]). For convenience we recall the description of translation planes by spreads. Let $W = V \times V$. A *spread* \mathcal{S} in W is a set of n -dimensional K -spaces such that

$$W = \bigcup_{X \in \mathcal{S}} X, \quad X \cap Y = 0, \text{ for } X, Y \in \mathcal{S}, X \neq Y.$$

Then $|\mathcal{S}| = q^n + 1$. The corresponding affine plane $\mathbf{A} = \mathbf{A}(\mathcal{S})$ has as points the vectors of W and as lines the cosets of the fibers of \mathcal{S} . Sometimes it is convenient to consider such a plane as a projective plane, i.e. as the *projective extension*. The points of the extension are the elements of W together with symbols (X) , $X \in \mathcal{S}$ and the lines are the *line at infinity*

$$L_\infty = \{(X) \mid X \in \mathcal{S}\}$$

and lines of the form $(X+w) \cup \{(X)\}$, $X \in \mathcal{S}$, $w \in W$ (i.e. $X+w$ is the "affine part" of this line).

Spread sets. Concrete coordinatizations of spreads lead to spread sets. A set $0 \in \Sigma \subseteq \text{GL}(V) \cup 0$ is called a *spread set* iff $\det(T - T') \neq 0$ for $T, T' \in \Sigma$, $T \neq T'$ and $|\Sigma| = q^n$. Then

$$\mathcal{S} = \mathcal{S}(\Sigma) = \{V(\infty)\} \cup \{V(T) \mid T \in \Sigma\}$$

is a spread where

$$V(\infty) = 0 \times V \quad \text{and} \quad V(T) = \{(v, vT) \mid v \in V\}.$$

Vice versa: using a suitable basis of W any spread can be described by a spread set.

Suppose that two spreads defined by Σ and Σ' share the fibers $V(0)$ and $V(\infty)$ and let D be a semilinear transformation mapping the first spread onto the second. If D fixes both $V(0)$ and $V(\infty)$ we write $D = \text{diag}(A, B)$ where $A = D_{V(0)}$, $B = D_{V(\infty)}$, and both fibers are identified in an obvious way with V . A fiber represented by $X \in \Sigma$ is then mapped to the fiber of the second spread represented by $A^{-1}XB$. If D interchanges $V(0)$ and $V(\infty)$ we write

$$D = \begin{pmatrix} \mathbf{0} & B \\ A & \mathbf{0} \end{pmatrix}.$$

Since $(v, vX)D = (w, wA^{-1}X^{-1}B)$, $w = vXA$, a fiber represented by X is then mapped to the fiber represented by $A^{-1}X^{-1}B$.

Translation complements. Denote by $\Gamma\text{L}(W)$ the group of invertible semilinear operators on W . Then

$$G = \{T \in \Gamma\text{L}(W) \mid ST = \mathcal{S}\}$$

is called the *translation complement* of \mathbf{A} . It induces in the obvious way a group of collineations and the full automorphism group of \mathbf{A} is the semidirect product of W (identified with the group of translations) with G . In particular the automorphism group is determined completely by the translation complement.

It will be convenient to identify an n -dimensional K -space V with F . For $a \in F$ and $0 \leq k < n$ we define a K -linear mapping $T_k(a)$ by

$$xT_k(a) = ax^{q^k}.$$

The basic multiplication rule for such maps is

$$T_k(a)T_\ell(b) = T_{k+\ell}(a^{q^\ell}b)$$

where $k + \ell$ is read modulo n . A K -endomorphism T of V has a unique representation

$$T = \sum_{i=0}^{n-1} T_i(a_i), \quad a_i \in F.$$

Let γ be an automorphism of F and $T \in \text{End}_K(V)$. Denote by $[\gamma, T]$ the operator on V defined by

$$[\gamma, T] : v \mapsto v^\gamma T.$$

Then $[\gamma, T]$ is a semilinear operator, i.e. semilinear with respect to the automorphism γ_K . There is some ambiguity in this representation: γ and $\gamma\tau$ induce the same automorphism on K for $\tau \in \text{Gal}(F : K)$. In fact the K -linear map $(v) \mapsto (v^q)$ is the same as $T_1(1)$. We remove this ambiguity by requiring $\gamma \in \Gamma$ where

Γ is a set of coset representatives of $\text{Gal}(F : K_0)/\text{Gal}(F : K)$.

Note that the latter group is isomorphic to $\text{Gal}(K : K_0)$. Using this convention the description of semilinear operators is now unique.

Definition (a) For $P(X) \in F[X]$ we denote by the letter P the polynomial map $P : F \rightarrow F$, $x \mapsto P(x)$. If the map P is invertible we denote by $P^{-1}(X)$ the unique polynomial of degree $\leq |F| - 1$ which induces the inverse of this mapping. Assume $|F| = p^m$. A polynomial $P(X)$ is called *Dembowski-Ostrom polynomial* or short *DO polynomial* if it has the form

$$P(X) = \sum_{i,j=0}^{m-1} a_{ij} X^{p^i+p^j}, \quad a_{ij} \in F.$$

(b) We call a polynomial $L(X) \in F[X]$ a *K-linear polynomial* if L is a K -linear. We call $P_L(X) = L(X)X$ the *associated DO polynomial*.

(c) Assume now that ζ is a non-square in K (hence a non-square in F too). We say that $L(X)$ has *property (P)* (see the introduction) if the following holds:

(P1) L is bijective.

(P2) $|P_L(F^*)| = \frac{q^n - 1}{2}$.

(P3) $P_L(F^*) \cap \zeta P_L(F^*) = \emptyset$.

Proposition 2.1 *Let q, n, F and $K = \text{GF}(q)$ be chosen as usual.*

(a) *Let $L(X) \in F[X]$ have property (P). Then $L^{-1}(X) \in F[X]$ has property (P) too and $P_L(F^*) = P_{L^{-1}}(F^*)$.*

(b) *Let $0 < r < n$ and $a \in F^*$ such that $a^{(q^n - 1)/(q^{(n,r)} - 1)} \neq 1$. Set $A_{a,r}(X) = X^{q^r} - aX^{q^{-r}}$. Then $A_{a,r}$ has property (P).*

(c) *Let $0 < r < n$ and $b \in F^*$ such that $b^{(q^n - 1)/(q^{(n,r)} - 1)} \neq \pm 1$. Set $B_{b,r}(X) = 2A^{-1}(X) - X$ where $A(X) = X - bX^{q^r}$. Then $B_{b,r}$ has property (P).*

Proof. (a) As $L(x)x = yL^{-1}(y)$ for $x = L(y)$ the assertion follows.

(c) was proved in [7]. We show assertion (b). Set $A = A_{a,r}$ and $P = P_A$. Suppose $A(x) = x^{q^r} - ax^{q^{-r}} = 0$ for some $x \in F^*$. Then

$$a = \frac{x^{q^r}}{x^{q^{-r}}} = \frac{x^{q^r}}{(x^{q^r})^{q^{-2r}}}$$

and hence $a^{(q^n - 1)/(q^{(n,r)} - 1)} = 1$, a contradiction. So (P1) holds. To prove (P2) we first observe $P(x) = P(-x)$. Assume $P(x) = P(y)$ for $x, y \neq 0$ and $y \neq \pm x$. This implies

$$x^{q^r+1} - y^{q^r+1} = a(x^{q^{-r}+1} - y^{q^{-r}+1}).$$

Since $(q^n - 1, q^r + 1) = 2$ the equation $x^{q^r+1} = y^{q^r+1}$ leads to $y = \pm x$, a contradiction. Hence

$$a = \frac{x^{q^r+1} - y^{q^r+1}}{x^{q^{-r}+1} - y^{q^{-r}+1}} = \frac{x^{q^r+1} - y^{q^r+1}}{(x^{q^r+1} - y^{q^r+1})^{q^{-r}}}$$

giving the same contradiction as before. Finally assume

$$x^{q^r+1} - ax^{q^{-r}+1} = P(x) = \zeta P(y) = \zeta(y^{q^r+1} - ay^{q^{-r}+1})$$

for $x, y \neq 0$. Then we get

$$a = \frac{x^{q^r+1} - \zeta y^{q^r+1}}{(x^{q^r+1} - \zeta y^{q^r+1})^{q^{-r}}},$$

again a contradiction. This shows property (P3). \square

Proposition 2.2 *With the notation of Proposition 2.1 the following holds:*

(a) *Assume $b^{(q^n - 1)/(q^{(n,r)} - 1)} \neq \pm 1$. Then $A'((F^*)^2) = P_{B_{b,r}}(F^*)$ where $A'(X) = X - b^2X^{q^r}$.*

(b) Assume $a = b^2$ and $b^{(q^n-1)/(q^{(n,r)}-1)} \neq \pm 1$. Then $P_{A_{a,r}}(F^*) = P_{B_{b,-r}}(F^*)$.

Proof. (a) Set $P = P_{B_{b,r}}$. A typical element in $P(F^*)$ has the form $w = (2A^{-1}(x) - x)x$ where $A(X) = X - bX^{q^r}$. Write $x = A(y)$. Then

$$w = (2y - A(y))A(y) = (y + by^{q^r})(y - by^{q^r}) = A'(y^2).$$

(b) Set $P(X) = P_{A_{a,r}}(X)$ and $P'(X) = P_{B_{b,r}}(X)$. A typical element in $P(F^*)$ has the form $x^{q^r+1} - ax^{q^{-r}+1}$ and a typical element in $P'(F^*)$ has by (a) the form $z^2 - az^{2q^{-r}}$. Writing $z = x^{(q^r+1)/2}$ we see that both elements are equal. \square

3 Translation planes of order q^n defined by DO polynomials

We assume that q, p, n, K, K_0 , and F have the same meaning as in the previous section. By ζ we denote a non-square from K and $no : F \rightarrow K$ denotes the norm.

Lemma 3.1 *Let $L(X) \in F[X]$ satisfy property (P). Define for $y \in F$ a K -linear Operator $N_y = N_y^L : F \rightarrow F$ by $xN_y = L(xy)y$. The following holds.*

(a) *The operator N_y is invertible for $0 \neq y \in F$.*

(b) *$N_y = N_z$ iff $z = \pm y$.*

(c) *Let $y, z \in F$ such that $z \neq \pm y$. Then $N_y - N_z$ is invertible.*

Proof. (a) From $0 = xN_y = L(xy)y$ we deduce $P_L(xy) = 0$. This implies $xy = 0$, i.e. $x = 0$ and hence N_y is invertible.

(b) Clearly, $N_y = N_{-y}$. The rest of the assertion follows once we verified part (c).

(c) Let $y, z \in F^*$, $z \neq \pm y$. Assume $0 = x(N_y - N_z)$, i.e. $L(xy)y = L(xz)z$. Multiply both sides of this equation by x . We obtain $P_L(xy) = P_L(xz)$, i.e. $xz = \pm xy$ by property (P). But this can only hold if $x = 0$. Thus $N_y - N_z$ is invertible. \square

Theorem 3.2 *Let $L_1(X), L_2(X) \in F[X]$ be polynomials with property (P) such that $P_{L_1}(F^*) = P_{L_2}(F^*)$. Then*

$$\{N_y^{L_1}, \zeta N_y^{L_2} \mid y \in F\}$$

is a spread set of K -linear operators on F .

Proof. By Lemma 3.1 we already know that $\Sigma_1 = \{N_y^{L_1} \mid y \in F\}$ and $\Sigma_2 = \{\zeta N_y^{L_2} \mid y \in F\}$ are partial spread sets. It remains to show that $T - S$ is invertible for $0 \neq T = N_y^{L_1} \in \Sigma_1$ and $0 \neq S = \zeta N_z^{L_2} \in \Sigma_2$. So assume $xN_y^{L_1} = \zeta xN_z^{L_2}$ with $x, y, z \in F$, $y, z \neq 0$. Multiplying this equation with x we

get $P_{L_1}(xy) = \zeta P_{L_1}(xz)$. By assumption this implies $P_{L_1}(xy) = \zeta P_{L_1}(xz) = 0$ from which we deduce $xy = xz = 0$, i.e. $x = 0$. \square

Notation Let $L_1(X), L_2(X) \in F[X]$ be polynomials with property (P) such that $P_{L_1}(F^*) = P_{L_2}(F^*)$. We denote the spread set from Theorem 3.2 by

$$\Sigma(L_1, L_2) = \{N_y^{L_1}, \zeta N_y^{L_2} \mid y \in F\}.$$

Lemma 3.3 *The spread sets $\Sigma(L_1, L_2)$, $\Sigma(L_2, L_1)$, $\Sigma(L_1^{-1}, L_2^{-1})$, and $\Sigma(L_2^{-1}, L_1^{-1})$ define isomorphic planes.*

Proof. Note that $(K^*)^2 \Sigma(L_1, L_2) = \Sigma(L_1, L_2)$. This implies that the mapping $W \ni (x, y) \mapsto (x, \zeta y)$ maps $\Sigma(L_1, L_2)$ onto $\Sigma(L_2, L_1)$. Moreover $\Sigma(L_1, L_2)^{-1} = \{X^{-1} \mid X \in \Sigma(L_1, L_2) - 0\} \cup 0 = \Sigma(L_1^{-1}, L_2^{-1})$. \square

Definition The spread set $\Sigma(L_2, L_1)$ (the associated spread, the associated translation plane) has *type I* if $L_1 = L_2$, *type II* if $L_1^{-1} = L_2$, and *type III* if $L_1^{\pm 1} \neq L_2$.

For the construction of the planes we use the polynomials $A_{a,r}(X)$ and $B_{b,r}(X)$ of Proposition 2.1 with $a^{(q^n-1)/(q^{(n,r)}-1)} \neq 1$, $b^{(q^n-1)/(q^{(n,r)}-1)} \neq \pm 1$ (and $b^2 = a$ if both types are used simultaneously (see Proposition 2.2)). According to the preceding lemma it suffices to consider for types I or II the subcases I.A and II.A where $L(X) = A_{a,r}(X)$, I.B and II.B where $L(X) = B_{b,r}(X)$ and for type III we take $L_1(X) = A_{a,r}(X)$, $L_2(X) = B_{b,-r}(X)$. Note that in the cases I.B, II.B and III we have

$$q > 3.$$

Remark If $(n, r) = e > 1$ we set $K' = GF(q^e)$, $q' = q^e$, and $n' = n/e$. Then the polynomials $L_1(X)$ and $L_2(X)$ are even K' -linear. Considering $V = F$ as a K' -space and replacing our construction the pair (n, q) by (n', q') we obtain the same spread set. So by assuming $(n, r) = 1$ we do not lose any spread sets. Therefore we will assume for the remainder of this section

$$(n, r) = 1.$$

Notation We will denote by G the translation complement of a plane of type I, II or III. The symbol

$$G_0, \quad G_{0,\infty}, \quad G_{\{0,\infty\}}, \quad G_y, \quad \text{etc.}$$

will denote in G the stabilizer of the fiber $V(0)$, the stabilizer of the fibers $V(0), V(\infty)$, the stabilizer of the set $\{V(0), V(\infty)\}$, the stabilizer of the fiber $V(N_y)$ respectively. The following technical lemma will be used repeatedly.

Lemma 3.4 *Let $u, v \in F^*$ and $\sigma \in \text{Aut}(F)$. Write $\sigma = \gamma \circ \tau$ where $\gamma \in \Gamma$ and τ is the k -th power of q . Also G denotes the translation complement of a plane of type I, II, or III. Then the following holds.*

(a) Let $y \in F$ and $0 \leq \ell < n$. Then

$$[\gamma, T_k(u)]^{-1} T_\ell(y) [\gamma, T_k(v)] = T_\ell(u^{-q^\ell} v y^\sigma).$$

(b) Assume that $L(X)$ has property (P). Then

$$T_0(u) N_y^L T_0(u) = N_{uy}^L.$$

In particular $\mu_u = \text{diag}(u^{-1}, u)$ lies in $G_{0,\infty}$.

(c) Assume that $L(X)$ has property (P) and $u \in K^*$. Then

$$T_0(u) N_y^L T_0(u) = u^2 N_y^L = N_y^L T_0(u^2).$$

In particular $\lambda_u = \text{diag}(\mathbf{1}, u^2)$ lies in $G_{0,\infty}$.

(d) Assume $L(X) = A_{a,r}(X)$ and that there are $u, v, z \in F^*$ such that $z^{q^r+1} = u^{-q^r} v$. Then

$$[\gamma, T_k(u)]^{-1} N_y^L [\gamma, T_k(v)] = N_{y'}^{L'}$$

with $L'(X) = A_{u^{1-q^r} v^{1-q^r} a^\sigma, r}(X)$ and $y' = z y^\sigma$.

(e) Assume $L(X) = B_{b,r}(X)$. Then

$$[\gamma, T_k(u)]^{-1} N_y^L [\gamma, T_k(u)] = N_{y'}^{L'}$$

with $L'(X) = B_{u^{1-q^r} b^\sigma, r}(X)$ and $y' = y^\sigma$.

Proof. (a) A straightforward computation shows $T_\ell(y) [\gamma, T_k(v)] = [\gamma, T_k(u)] T_\ell(u^{-q^\ell} v y^\sigma)$. Moreover (b) follows from $x T_0(u) N_y^L T_0(u) = L(xuy) y T_0(u) = x N_{uy}^L$.

(c) As L is a K -linear map we get

$$x T_0(u) N_y^L T_0(u) = L(xuy) uy = u^2 L(xy) y = x N_y^L T_0(u^2).$$

(d) Obviously $N_1^L = T_r(1) - T_{-r}(a)$ and from (b) we deduce $N_y^L = T_r(y^{q^r+1}) - T_{-r}(a y^{q^r+1})$. Using (a) we see

$$[\gamma, T_k(u)]^{-1} N_y^L [\gamma, T_k(u)] = T_r(u^{-q^r} v (y^\sigma)^{q^r+1}) - T_{-r}(a^\sigma u^{-q^r} v (y^\sigma)^{q^r+1}).$$

Substituting $u^{-q^r} v$ by z^{q^r+1} we see $z^{q^r+1} = (z^{q^r+1})^{q^r}$ and get the expression $T_r((z y^\sigma)^{q^r+1}) - T_{-r}(a^\sigma u^{1-q^r} v^{1-q^r} (z y^\sigma)^{q^r+1})$ which shows the assertion.

(e) Clearly, $N_1^L = 2(T_0(1) - T_r(b))^{-1} - \mathbf{1}$. This implies by (a)

$$[\gamma, T_k(u)]^{-1} N_1^L [\gamma, T_k(u)] = 2(T_0(1) - T_r(u^{-q^r+1} b^\sigma))^{-1} - \mathbf{1} = N_1^{L'}.$$

As $[\gamma, T_k(u)]^{-1} T_0(y) [\gamma, T_k(u)] = T_0(u^\sigma)$ we deduce from (b) $[\gamma, T_k(u)]^{-1} N_y^L [\gamma, T_k(u)] = N_{y'}^{L'}$. \square

Some automorphisms Again G shall denote the translation complement of a plane of type I, II, or III. Set

$$Z_1 = \{\mu_u = \text{diag}(T_0(u^{-1}), T_0(u)) \mid u \in F^*\}, \quad Z_0 = \{\lambda_u = \text{diag}(\mathbf{1}, T_0(u)) \mid u \in K^*\}$$

and

$$Z = \begin{cases} Z_1 \times Z_0, & \text{for type I,} \\ Z_1 \times Z_0^2, & \text{else.} \end{cases}$$

Then by Lemma 3.4 $Z \leq G_{0,\infty}$. Set

$$\Lambda = \begin{pmatrix} \mathbf{0} & \mathbf{1} \\ \zeta\mathbf{1} & \mathbf{0} \end{pmatrix}.$$

Then $\Lambda \in \text{GL}(W)$ is a collineation of a plane of type II which interchanges $V(0)$ and $V(\infty)$. For $b \in F^*$ set

$$\mathcal{A}_b = \{\sigma \in \text{Aut}(F) \mid b^\sigma \equiv b \pmod{(F^*)^{q-1}}\}.$$

and

$$\mathcal{A}_b^* = \{\sigma \in \text{Aut}(F) \mid b^\sigma \equiv \pm b \pmod{(F^*)^{q-1}}\}.$$

Clearly, $|\mathcal{A}_b^* : \mathcal{A}_b| \leq 2$.

For $\sigma \in \mathcal{A}_b$ choose $\gamma \in \Gamma$ and $\tau \in \text{Gal}(F : K)$, $x^\tau = x^{q^k}$, such that $\sigma = \gamma \circ \tau$. It follows from Lemma 3.4 that there exists some $x = x_\sigma \in F^*$ such that $\nu_\sigma = \text{diag}([\gamma, T_k(x)], [\gamma, T_k(x)]) \in G_{0,\infty}$. We set

$$\mathcal{G} = Z\{\nu_\sigma \mid \sigma \in \mathcal{A}_b\} \leq G_{0,\infty}.$$

We denote by \mathcal{H} the intersection of \mathcal{G} with $\text{GL}(W)$. It follows from [7]

$$\mathcal{G}/\mathcal{H} \simeq \text{Gal}(K : K_0[\alpha]), \quad \mathcal{H}/Z \simeq C_n, \quad Z \simeq C_{(q^n-1)/2} \times C_{q-1}$$

where $\alpha = no(a)$ (types I.A, II.A) and $\alpha = no(b)$ otherwise, a and b as usual. Note that the group \mathcal{G} has on the line at infinity orbits of lengths $1, 1, q^n - 1$ for type I and orbits of lengths $1, 1, (q^n - 1)/2, (q^n - 1)/2$ for types II and III. For Type II the group $\mathcal{G}\langle\Lambda\rangle$ has orbits of lengths $2, q^n - 1$.

Lemma 3.5 *The group $\mathcal{K} = K^*\mathbf{1}_W$ is the group of kern homologies. In particular the kernel of a translation plane of type I, II or III is isomorphic to K .*

Proof. The proof is the same as of [7, Lemma 4.5]. □

Lemma 3.6 (a) *Let \bar{p} be a p -primitive divisor of $q^n - 1$ and $S \in \text{Syl}_{\bar{p}}(Z)$. Then $S \neq 1$ and $S \in \text{Syl}_{\bar{p}}(G)$.*

(b) *Let $T \in \text{GL}(W)$ be of the form $\text{diag}([\gamma, T_s(a)], [\gamma' T_t(b)])$ and assume that T normalizes S . Then $s = t$ and $\gamma = \gamma'$.*

Proof. (a) First $S \neq 1$ by Zsigmondy's theorem [19]. Clearly, Z restricted to a fiber $X = V(0)$ or $V(\infty)$ is a Singer group in $\text{GL}(X)$, i.e. this restriction contains a Sylow \bar{p} -subgroup of $\text{GL}(X)$. So if S would be a proper subgroup of a Sylow \bar{p} -subgroup of $G_{0,\infty}$ this group would contain a subgroup isomorphic to $C_{\bar{p}} \times C_{\bar{p}}$ centralizing Z , i.e. an element of the form $\text{diag}(\mathbf{1}, c)$ of order \bar{p} . Since this prime is odd there exist $y, z \in F^*$ such that $N_y^L L T_0(c) = N_z^L$. Therefore $L(xy)yc = L(xz)z$ for all $x \in F$. It is easy to see that the relation $L(xu) = L(u)w$ for all $x \in F$ implies $u = w \in K$. Hence $yz^{-1}c = y^{-1}z \in K$, or $c \in K$, a contradiction.

Hence $S \in \text{Syl}_{\bar{p}}(G_{0,\infty})$. Let \widehat{S} be a Sylow \bar{p} -subgroup of G containing S . Then \widehat{S} is abelian as a Sylow \bar{p} -subgroup of $\text{GL}(W)$ has the form $C_{\bar{p}^k} \times C_{\bar{p}^k}$ where $\bar{p}^k = (q^n - 1)_{\bar{p}}$. Thus \widehat{S} leaves invariant the set $\{V(0), V(\infty)\}$ of fixed fibers of S . As $\bar{p} \neq 2$ even $\widehat{S} \in \text{Syl}_{\bar{p}}(G_{0,\infty})$ and the assertion follows.

(b) This is Lemma 5.3 of [8]. Note that the representation of semilinear operators differs slightly from the notation we use here. \square

Theorem 3.7 *Translation planes of different types are not isomorphic. Moreover:*

- (a) *A plane of type I.A is a twisted field plane. A plane of type I.B belongs to [7].*
- (b) *A plane of type II.A is a plane of Suetake [18]. Planes of type II.B are new.*
- (c) *Planes of type III are new.*

The term "new" should be read with some caution. We will show that the planes of type II.B or III are not nearfield planes, not semifield planes, nor generalized André planes. Besides the known planes of type I and II these are the natural candidates for possible isomorphisms. See also Chapter 70.1 [1]. To the best of our knowledge these planes are all known planes which admit a cyclic automorphism group of order $q^n - 1$. We prove this theorem by a series of lemmas. We first observe that planes of type I can be defined by permutation polynomials in the sense of [8]. For a group element x of a finite group denote by $x_2 (x_{2'})$ the 2-part ($2'$ -part) of this element.

Lemma 3.8 *Let $L(X)$ be a polynomial with property (P). Choose a multiple N of $(q^n - 1)/(q - 1)$ such that $x^N = x_2$ for $x \in F^*$. Then $L(X)X^{1+N}$ is a permutation polynomial on F .*

Proof. Let $\mathcal{O} = F^* - (F^*)^N$ be the set of elements of odd order in F^* . Then P_L is injective on \mathcal{O} . Let w generate a Sylow 2-subgroup of F^* and assume $(q - 1)_2 = 2^s$. Then

$$P_L(F^*) = \bigcup_{i=1}^{2^s} P_L(\mathcal{O}w^i) = \bigcup_{i=1}^{2^{s-1}} P_L(\mathcal{O})w^i$$

is a partition as $P_L(\mathcal{O})w^i = P_L(\mathcal{O}w^i) = P_L(\mathcal{O}w^{i+2^{s-1}})$ and $|\mathcal{O}| = (q^n - 1)/2^s$. Set $\widehat{P}(X) = L(X)X^{1+N}$ and assume $\widehat{P}(x) = \widehat{P}(y)$ for $x, y \in F^*$. Writing $x = x_2x_{2'}$ and $y = y_2y_{2'}$ and using that L is K -linear and $x_2, y_2 \in K$ we get

$$P_L(x_{2'}) = P_L(y_{2'})(y_2/x_2)^{2+N}.$$

By property (P) we conclude that $(y_2/x_2)^{2+N} \in \langle w \rangle$ is a square. Looking at our partition we see that $(y_2/x_2)^{2+N} = 1$ and $x_2 = y_2$ follows. Hence $P_L(x_{2'}) = P_L(y_{2'})$ which implies $x_{2'} = y_{2'}$ too. \square

Lemma 3.9 *Planes of type I.A are twisted field planes.*

Proof. A typical non-trivial element of $\Sigma = \Sigma(A_{a,r}, A_{a,r})$ has the form $N_y = T_r(y^{q^r+1}) + T_{-r}(-ay^{q^{-r}+1})$ or ζN_y , $y \in F^*$. As $(y^{q^r+1})^{q^{-r}} = y^{q^{-r}+1}$ and since $\zeta^{q^{-r}} = \zeta$ we see that the entries in the T_{-r} component are obtained from the entries of the T_r component via the additive map $x \mapsto -ax^{q^{-r}}$. Hence Σ is closed under addition. The assertion follows from (b) of Lemma 3.8, (1) and (2) of [8], and the main result of [6]. \square

Lemma 3.10 *A planes of type I.B, II or III is not semifield plane.*

Proof. That follows from [7, Lemma 3.3]. \square

Represent $T \in \text{GL}(V)$ as $T = \sum_{i=0}^{n-1} T_i(a_i)$. The notation

$$\text{spi}(T) = \{i \mid a_i \neq 0\}$$

will be used frequently. The following observation which has an obvious verification will be useful.

Lemma 3.11 *Let $a, b \in F^*$, $\gamma \in \Gamma$ and $0 \leq t < n$. Then PolPlane2.ps*

$$\text{spi}([\gamma, T_t(a)]^{-1}T[\gamma, T_t(b)]) = \text{spi}(T).$$

Lemma 3.12 *Two planes of type I.A, I.B, II.A, II.B or III are non-isomorphic if they have different types.*

Proof. By Lemma 3.9 and Lemma 3.10 only the planes of type I.A are semifield planes. So we can assume that the two planes have type I.B, II.A, II.B or III. Let $\Sigma = \Sigma(L_1, L_2)$ and $\Sigma' = \Sigma(L'_1, L'_2)$ represent the two planes and let $\phi \in \text{GL}(W)$ be an isomorphism which maps $\mathcal{S}(\Sigma)$ onto $\mathcal{S}(\Sigma')$. Since S is a Sylow \bar{p} -subgroup in the translation complement of both planes we may assume that ϕ normalizes S . This shows that ϕ fixes the set $\{V(0), V(\infty)\}$ of fixed fibers of S . In particular either $\phi = \text{diag}(A, B)$, ϕ fixes both fibers, and $\Sigma' = A^{-1}\Sigma B$ or $\phi = \begin{pmatrix} \mathbf{0} & B \\ A & \mathbf{0} \end{pmatrix}$, ϕ interchanges both fibers, $\Sigma' = A^{-1}\Sigma^{-1}B$ (see the introduction of Section 2).

The second case can be reduced to the first case: Note that the type does not change if we replace Σ by $\Sigma^{-1} = \Sigma(L_1^{-1}, L_2^{-1})$. Then $\text{diag}(A, B)$ is an isomorphism of the two planes which maps $\mathcal{S}(\Sigma^{-1})$ onto $\mathcal{S}(\Sigma')$ and the assertion follows from Lemma 3.3. So we assume $\phi = \text{diag}(A, B)$.

Assume first that Σ has type II.A. As ϕ normalizes S we have

$$\phi = \text{diag}([\gamma, T_t(a)], [\gamma, T_t(b)])$$

by Lemma 3.6. One has precisely for $(q^n - 1)/2$ elements $T \in \Sigma$ with $|\text{spi}(T)| = n$ and $|\text{spi}(T)| = 2$ for the other $(q^n - 1)/2$ nontrivial elements in Σ (see [18]). Assume that Σ' has type I.B or II.B then $|\text{spi}(T)| = n$ for all $0 \neq T \in \Sigma'$ (see [7, Lemma 4.1]). But then $\Sigma' = [\gamma, T_t(a)]^{-1}\Sigma[\gamma T_t(b)]$ is in conflict with Lemma 3.11. If Σ' has type III we can replace Σ' by $(\Sigma')^{-1}$. Then by [18] and [7] again $|\text{spi}(T)| = n$ for all $0 \neq T \in (\Sigma')^{-1}$. We get the same contradiction as before. Similarly possible isomorphisms between planes of type I.B or II.B with planes of type III are ruled out.

Finally one knows from [7, Lemma 4.9] that a plane of type I.B has no collineation in $\text{GL}(W)$ which interchanges $V(0)$ and $V(\infty)$. But planes of type II.B have such a collineation (denoted by Λ above). So planes of type I.B and II.B can not be isomorphic either. \square

Proof of Theorem 3.7 Lemma 3.9 and the definition of the planes of type I.B together with [7] show assertion (a).

The definition of planes of type II.A and of the planes of Suetake [18] coincide showing one half of assertion (b).

It remains to show that the classes II.B and III are new. By Lemma 3.12 these planes are not of types I.A, I.B or II.A. They are not generalized André planes or nearfield planes either: By [16], Thm. 11.7 or [9] the homology group with axis $V(\infty)$ and center (0) contains in both cases a cyclic group of order \bar{p} . We deduce from Lemma 3.6 that a plane of type II.B or III is not generalized André plane or nearfield plane. \square

The automorphism groups of twisted field planes (panes of type I.A) [2], of the planes of Suetake (panes of type II.A) [18] and of type I.B [7] have been described in detail. It remains to determine the automorphism groups of planes of type II.B and III.

Theorem 3.13 *Let G be the translation complement of a plane of type II.B or III. Then $G = G_{\{0, \infty\}}$. Moreover the following holds:*

- (a) *Assume type II.B. Then $|G : G_{0, \infty}| = 2$ and $G_{0, \infty} = \mathcal{G}$ if $\mathcal{A}_b^* = \mathcal{A}_b$ and $|G_{0, \infty} : \mathcal{G}| = 2$ if $\mathcal{A}_b^* > \mathcal{A}_b$.*
- (b) *Assume type III. Then $G = \mathcal{G}$.*

We prove the theorem by a series of lemmas.

Lemma 3.14 Let $L(X) = B_{b,r}(X)$. Assume that we have (with $N_1 = N_1^L$)

$$[\gamma, T_t(x)]^{-1} N_1 [\gamma, T_t(y)] = \zeta N_1^{-1}.$$

Denote by σ the automorphism of F which is the composition of γ and the automorphism $x \mapsto x^{q^t}$. Then the following holds.

(a) $\sigma \in \mathcal{A}_b^*$, more precisely $b^\sigma = -bx^{q^r-1}$.

(b) $y = \zeta x$.

(c) $[\gamma, T_t(x)]^{-1} \zeta N_1^{-1} [\gamma, T_t(y)] = \zeta \zeta^\sigma N_1$.

Proof. Write $N_1 = \sum_{i=0}^{n-1} T_i(b_i)$ and $N_1^{-1} = \sum_{i=0}^{n-1} T_i(\bar{b}_i)$. Then

$$b_0 = \frac{1 + no(b)}{1 - no(b)} \text{ and } b_{jr} = \frac{2}{1 - no(b)} b^{1+q^r+\dots+q^{(j-1)r}} \text{ for } j > 0.$$

and the \bar{b}_i 's are obtained from the b_i 's if we replace b by $-b$ (see equation (5) and Lemma 4.1 in [7]). A computation shows

$$[\gamma, T_t(x)]^{-1} \sum_{i=0}^{n-1} T_i(b_i) [\gamma, T_t(y)] = \sum_{i=0}^{n-1} T_i(b_i^\sigma x^{-q^i} y).$$

Since $no(-b) = -no(b)$ we obtain the equations

$$\frac{1 + no(b)^\sigma}{1 - no(b)^\sigma} y = \zeta \frac{1 - no(b)}{1 + no(b)} x$$

and for $j > 0$

$$\frac{2}{1 - no(b)^\sigma} (b^{1+q^r+\dots+q^{(j-1)r}})^\sigma y = \frac{2}{1 + no(b)} (-b)^{1+q^r+\dots+q^{(j-1)r}} x^{q^{jr}}.$$

Divide the equation for $j = 2$ by the equation for $j = 1$. We get

$$(b^{q^r})^\sigma = (-b)^{q^r} x^{q^{2r}-q^r} \text{ or } b^\sigma = -bx^{q^r-1}.$$

This implies assertion (a) and $no(b)^\sigma = -no(b)$. The first equation therefore implies $y = \zeta x$, i.e. (b) holds.

Our computation shows also

$$[\gamma, T_t(x)]^{-1} \zeta N_1^{-1} [\gamma, T_t(y)] = \zeta^\sigma \sum_{i=0}^{n-1} T_i(\bar{b}_i^\sigma x^{-q^i} y).$$

It follows from our (simplified) equations that $\zeta^\sigma \bar{b}_i^\sigma x^{-q^i} y = \zeta \zeta^\sigma b_i$ for all $0 \leq i < n$. Thus (c) holds too. \square

Remark Let $\sigma \in \mathcal{A}_b^*$ and x be as in (a). Then we deduce from Lemma 3.4 that $\text{diag}([\gamma, T_t(x)], [\gamma, T_t(\zeta x)]) \in G_{0,\infty}$ for type II.B.

The following lemma has a similar proof as Lemma 3.14.

Lemma 3.15 Assume $L(X) = B_{b,r}(X)$ and (with $N_1 = N_1^L$) that

$$[\gamma, T_t(x)]^{-1}N_1[\gamma, T_t(y)] = N_1.$$

Denote by σ the automorphism of F which is the composition of γ and the automorphism $x \mapsto x^{q^t}$. Then $b^\sigma \equiv b \pmod{(F^*)^{q-1}}$.

Lemma 3.16 Let G be the translation complement of a plane of type II.B defined by the polynomial $L(X) = B_{b,r}(X)$. The following holds:

- (a) $|G_{\{0,\infty\}} : G_{0,\infty}| = 2$ and $G_{\{0,\infty\}} = G_{0,\infty}\langle \Lambda \rangle$.
- (b) Assume that S is normal in $G_{0,\infty}$. Then $G_{0,\infty} = \mathcal{G}$ if $\mathcal{A}_b^* = \mathcal{A}_b$ and $|G_{0,\infty} : \mathcal{G}| = 2$ if $\mathcal{A}_b^* > \mathcal{A}_b$.

Proof. Assertion (a) follows from the existence of the collineation Λ .

(b) Let T be a collineation in $G_{0,\infty}$. By assumption and Lemma 3.6 we have $T = \text{diag}([\gamma, T_t(x)], [\gamma, T_t(y)])$. Since the nontrivial Z orbits on the spread are represented by the fibers $V(N_1)$ and $V(\zeta N_1^{-1})$ we can adjust T by an element from Z such that either $[\gamma, T_t(x)]^{-1}N_1[\gamma, T_t(y)] = N_1$ or $[\gamma, T_t(x)]^{-1}N_1[\gamma, T_t(y)] = \zeta N_1^{-1}$ holds. In the first case we define σ as in Lemma 3.15. Then $\sigma \in \mathcal{A}_b$. We can adjust T further by an element of the form ν_σ so that $\sigma = \mathbf{1}$ and $T_0(x)^{-1}N_1T_0(y) = N_1$. The computation of the proof of [7, Lemma 4.5] shows then that $T \in \mathcal{K}$.

So assume now that we are in the second case. By Lemma 3.14 and the succeeding remark we see that $\sigma \in \mathcal{A}_b^* - \mathcal{A}_b$ and that T is a collineation which interchanges the two nontrivial Z orbits on the spread. In fact we know by this remark that $|\mathcal{A}_b^* : \mathcal{A}_b| = 2$ guarantees the existence of such a collineation. \square

Lemma 3.17 Let G be the translation complement of a plane of type III. The following holds:

- (a) $G_{\{0,\infty\}} = G_{0,\infty}$.
- (b) Assume that S is normal in $G_{0,\infty}$. Then $G_{0,\infty} = \mathcal{G}$.

Proof. (a) Set $\Sigma = \Sigma(L_1, L_2)$. A Frattini argument shows $G_{\{0,\infty\}} = G_{0,\infty}N_{G_{\{0,\infty\}}}(S)$.

Assume $G_{\{0,\infty\}} > G_{0,\infty}$. Then there exists a $T \in N_{G_{\{0,\infty\}}}(S) - G_{0,\infty}$. By Lemma 3.6 (c) (note that the transformation $(x, y) \mapsto (y, x)$ lies in $N_{\text{GL}(W)}(S)$) T has the form

$$T = \begin{pmatrix} \mathbf{0} & B \\ A & \mathbf{0} \end{pmatrix}, \quad A = [\gamma, T_k(x)], \quad B = [\gamma, T_k(y)],$$

which implies

$$[\gamma, T_k(x)]^{-1}\Sigma^{-1}[\gamma, T_k(y)] = \Sigma.$$

But $|spi(S)| = n$ for all $S \in \Sigma^{-1} - \{0\}$ while Σ contains transformations S' with $|spi(S')| = 2$. This contradicts Lemma 3.11.

(b) We know by Lemma 3.6 that any transformation in $G_{0,\infty}$ has the form $T = \text{diag}([\gamma, T_k(x)], [\gamma, T_k(y)])$ and again by Lemma 3.11 we then see that the transformation $X \mapsto [\gamma, T_k(x)]^{-1} X [\gamma, T_k(y)]$ must fix the subsets $\{N_y^{L_1} \mid y \in F\}$ and $\{\zeta N_y^{L_2} \mid y \in F\}$ of Σ invariant. By Lemma 3.15 $\sigma \in \mathcal{A}_b$ where σ is defined as usual. We can adjust T by an element from \mathcal{G} and assume $\sigma = \mathbf{1}$ and $T_0(x)^{-1} N_1^{L_1} T_0(y) = N_1^{L_1}$. As usual we deduce $T \in Z$. \square

Lemma 3.18 *Let G be the translation complement of a plane of type II.B or III. The following holds:*

- (a) *The group S is normal in $G_{0,\infty}$.*
- (b) *$G = G_{\{0,\infty\}}$.*

Before we start with the proof we record an observation on the stabilizer of a partial spread whose proof is similar as the proof of the analogous statement on kernels of spreads.

Lemma 3.19 *Let \mathcal{U} be a partial spread on $W = V(2n, q)$, $n \geq 2$, of size $> q^{n-1} + 1$. Let $H \leq \text{GL}(W)$ fix all fibers of \mathcal{U} . Then H is a cyclic group whose order divides $q^n - 1$.*

Proof of Lemma 3.18. The proof follows the lines of the proofs of [7, Lemma 4.6] and [8, Proposition 4.6]. We refer to these proofs if the arguments can be carried over and give the details if the present situation needs modifications. We set $\mathcal{M} = N_{G_{0,\infty}}(S)$. This group is known by Lemmas 3.16 and 3.17.

(1) Let $T \in G_{0,\infty}$ such that $T_{V(0)} \in \mathcal{M}_{V(0)}$ and $T_{V(\infty)} \in \mathcal{M}_{V(\infty)}$. Then $T \in \mathcal{M}$.

This is proved as (1) in the proof of [7, Lemma 4.6].

(2) Assertion (a) holds, in particular $\mathcal{M} = G_{0,\infty}$.

Assume the converse. By (1) one has $\mathcal{M}_{V(0)} < (G_{0,\infty})_{V(0)}$ or $\mathcal{M}_{V(\infty)} < (G_{0,\infty})_{V(\infty)}$. Suppose for instance that the first case holds. From the classification of 2-transitive affine groups (see [15]) it follows that $(G_{0,\infty})_{V(0)}$ will contain a subgroup of the form $\text{GL}(m, q^t)$, $m > 1$, $mt = n$. As shown in [7] such a group can not act on **A**.

We are now in the position to prove assertion (b) in the case II.B. We already know from Lemma 3.16 that $|G_{\{0,\infty\}} : G_{0,\infty}| = 2$ and that $G_{\{0,\infty\}}$ has on L_∞ orbits of size 2 and $q^n - 1$.

Assume $G > G_{\{0,\infty\}}$. Then G is transitive on L_∞ and thus G acts flag transitive on the associated plane (note that Z acts transitively on $V(0) - 0$). We apply the classification of flag transitive linear spaces [3, Theorem]. Let \hat{p} be a p -primitive divisor of $q^{2n} - 1$. If case (II) of this theorem holds we see that

$G \leq N_{\Gamma L(W)}(\mathcal{T})$ where \mathcal{T} is a Sylow \widehat{p} -subgroup of $\text{GL}(W)$. But then S would centralize \mathcal{T} and \mathcal{T} would therefore fix the set $\text{Fix}_{L_\infty}(S) = \{(0), (\infty)\}$. But \mathcal{T} acts semiregularly on L_∞ and $\widehat{p} > 2$, a contradiction.

If case (I) of this theorem would hold then our plane would be an example in [3, Section 3] which is false.

So from now on we assume that our plane has type III. We know by Lemma 3.17 that $G_{\{0, \infty\}} = \mathcal{M}$ has orbits of sizes $1, 1, (q^n - 1)/2, (q^n - 1)/2$ on L_∞ .

Assume $G > \mathcal{M}$. If G would be transitive on L_∞ we can argue as in the case of typ II.B and we would reach a contradiction. So we assume that G is not transitive on L_∞ and note that by Lemma 3.17 G has no orbit of length 2. The following possibilities for the orbit lengths can occur: (i) $1, q^n$, (ii) $1, (q^n - 1)/2, (q^n + 1)/2$, (iii) $(q^n + 1)/2, (q^n + 1)/2$, or (iv) $(q^n - 1)/2, (q^n + 3)/2$.

CASE (i) This case is eliminated in the same way as in the proof of [7, Lemma 4.6] steps (2) and (3).

CASE (ii) In this case G fixes a fiber $X \in \{V(0), V(\infty)\}$ and G contains a Sylow \widehat{p} -subgroup \mathcal{T} of $\text{GL}(W)$. But this is in conflict with the irreducible action of \mathcal{T} on W .

CASE (iii) In this case G has orbits of lengths $1, (q^{2n} - 1)/2, (q^{2n} - 1)/2$ on W and contains a Sylow \widehat{p} -subgroup \mathcal{T} of $\text{GL}(W)$. We now apply the classification of affine rank 3 groups by Liebeck [15, Theorem]. Again we can rule out the case $G \leq N_{\Gamma L(W)}(\mathcal{T})$ as before, i.e. (A.1) of this theorem is impossible. Also any of the cases (A.2)-(A.11) is impossible: either the orbit lengths are not of the form $1, (q^{2n} - 1)/2, (q^{2n} - 1)/2$ (for instance (A.2)) or \widehat{p} does not divide the group order (for instance (A.3)).

The extraspecial case (B) of this theorem does not occur since q^n has not the form p^b of the Table 1 in [15].

By the same reason (using Table 2) all exceptional cases (C) can not occur with the only possible exception of $q^{2n} = 5^6$ and $G^{(\infty)}/Z(G^{(\infty)}) \simeq J_2$. But $\overline{p} = 31$ does not divide the order of J_2 .

CASE (iv) Now G is an irreducible subgroup of $\Gamma L(W)$ of order $|\mathcal{M}| \cdot (q^n + 3)/2$. Moreover G has on L_∞ orbits $\mathcal{O}_1, \mathcal{O}_2$ of length $(q^n + 3)/2$ and $(q^n - 1)/2$ respectively.

Assume there is a $T \in G$ such that $V(0)T = V(\infty)$. Then $T^{-1}ZT$ and $T^{-1}ST$ lie in $G_\infty = G_{0, \infty}$ (Lemma 3.17). But S is a characteristic Sylow \overline{p} -subgroup of $G_{0, \infty}$. Hence $S = T^{-1}ST$ and $T^{-1}ZT = C_{G_{0, \infty}}(S) = Z$. Clearly, $V(0)$ and $V(\infty)$ are the only proper Z -invariant spaces in W . We conclude $T \in G_{\{0, \infty\}} - G_{0, \infty}$ which contradicts Lemma 3.17. Therefore the set $\Delta = \{(0), (\infty)\}$ is a block for the action of G on \mathcal{O}_1 . Then G induces a 2-transitive action on $\Omega = \{\Delta T \mid T \in G\}$ of degree $(q^n + 3)/4$ and by Lemma 3.17 the kernel of this action is \mathcal{K} .

Denote by U/\mathcal{K} the socle of G/\mathcal{K} and assume first that U/\mathcal{K} is simple. We inspect the list of possible examples [4].

If U/\mathcal{K} is a sporadic case the degree is 11, 12, 15, 22, 23, 24, 28, 176, or 276. But none of these numbers has the shape $(q^n + 3)/4$.

Assume $U/\mathcal{K} \simeq \text{Alt}(m)$, $m = (q^n + 3)/4$. Since $m \geq 31$ the minimal degree of a non-trivial projective representation of $\text{Alt}(m)$ over $\text{GF}(q)$ is $\geq m - 2$ (see [10]). We get $(q^n - 5)/4 \leq 2n$ which is impossible.

Assume $U/\mathcal{K} \simeq \text{PSL}(d, \bar{q})$, $d \geq 2$. Then $(q^n + 3)/4 = (\bar{q}^d - 1)/(\bar{q} - 1)$ and U/\mathcal{K} has a projective representation of degree $\leq 2n$ over $\text{GF}(q)$. Inspecting the order of G we see that $(q, \bar{q}) = 1$. By [10] a lower bound m for a projective representation of U/\mathcal{K} over $\text{GF}(q)$ is

$$m = \begin{cases} \frac{\bar{q}^d - 1}{\bar{q} - 1} - 1, & d \geq 3, \\ \frac{\bar{q} - 1}{2}, & d = 2. \end{cases}$$

We get a contradiction as before.

The cases $(U/\mathcal{K}, |\Omega|) = (\text{U}_3(q), q^3 + 1)$, $(\text{Suz}(q), q^2 + 1)$, $(\text{Re}(q), q^3 + 1)$, or $(\text{Psp}(2d, 2), 2^{2d-1} \pm 2^{d-1})$ are ruled out in a similar fashion.

Assume that U/\mathcal{K} is an elementary abelian \tilde{p} -group of order $\tilde{p}^m = (q^n + 3)/4$. Act with U/\mathcal{K} on the orbit \mathcal{O}_2 of length $(q^n - 1)/2$. As $((q^n + 3)/2, (q^n - 1)/2) = 2$ we see that U/\mathcal{K} fixes at least one point in \mathcal{O}_2 if $\tilde{p} > 2$. As U/\mathcal{K} is a minimal normal subgroup in G/\mathcal{K} we see that U/\mathcal{K} acts trivially on \mathcal{O}_2 , i.e. the pre-image U fixes all the fibers which correspond to the points in \mathcal{O}_2 . From Lemma 3.19 we deduce that U is cyclic and $|U|$ divides $q^n - 1$. This is impossible.

Assume finally $\tilde{p} = 2$. Then $(q^n - 1)/2 \equiv 2 \pmod{4}$. If U/\mathcal{K} would act nontrivially on \mathcal{O}_2 all U/\mathcal{K} -orbits on \mathcal{O}_2 would have length 2^m since U/\mathcal{K} is a minimal normal subgroup. That is impossible. Hence U/\mathcal{K} acts trivially on \mathcal{O}_2 and we reach the same contradiction as before. \square

Proof of Theorem 3.13 and Theorem A. Theorem 3.13 follows from Lemmas 3.14 to 3.18 and Theorem A follows Theorems 3.7 and 3.13. \square

Remarks (a) One can show as in [7, Lemma 4.10] using Lemma 3.4 that the number of planes of type II.B and III and order q^n is in each case $\varphi(n)M_q/2$ where φ is the Euler function and M_q the number of orbits of $\text{Aut}(K)$ on $K - \{0, \pm 1\}$.

(b) The translation complement of a plane of type II.B acts transitively on the set of non-vertices of each side of the triangle $L_\infty, V(0), V(\infty)$. This adds another class of planes to the family of translation planes which are called *triangle transitive* in [13] and *nearly flag-transitive* in [14].

(c) Assume $q = q_0^2$ and denote by τ the involution in $\text{Aut}(F)$. Let $L(X) = B_{b, \tau}(X)$ define a plane of type II.B and order q^n . Assume further $b^\tau = -b$. Then ι defined by $(x, y) = (v^\tau, x^\tau)$ is a Baer involution. One can now apply [7,

Proposition 5.5] and one observes that the subplane $C_W(\iota)$ is the same kind of flag transitive plane of Kantor-Suetake type as in this proposition.

4 Semifields of order q^{2n} and their nuclei

We assume that q, p, n, K, K_0 , and F have the same meaning as in Section 2. By ζ we denote a non-square from K . We will use again pairs of polynomials $L_1(X), L_2(X)$ with property (P) to define (pre)-semifields of order q^{2n} . We will take F^2 as the additive group of the semifield. The multiplication will have the form

$$(u, v) * (x, y) = (ux + v \circ y, uy + \zeta(v \bullet x))$$

where the semifield multiplications \circ and \bullet are derived from the polynomials with property (P). In the simplest version the multiplications have the shape $v \circ y = vL_1(y)$ and $v \bullet x = vL_2(x)$. Namely:

Theorem 4.1 *Let $L_1, L_2 \in F[X]$ be K -linear polynomials which have property (P). Moreover assume $P_{L_1}(F^*) = P_{L_2}(F^*)$. Define*

$$\Sigma = \Sigma_{L_1, L_2} = \left\{ M(x, y) = \begin{pmatrix} x & y \\ L_1(y) & \zeta L_2(x) \end{pmatrix} \mid x, y \in F \right\} \subseteq F^{2 \times 2}.$$

Then Σ is an additively closed spread set.

Notation and Remark From the theorem we deduce that the multiplication

$$(u, v) * (x, y) = (u, v)M(x, y) = (ux + vL_1(y), uy + \zeta vL_2(x))$$

turns F^2 into a pre-semifield. The pre-semifield determined by Σ_{L_1, L_2} will be denoted by

$$\mathbf{S} = \mathbf{S}(L_1, L_2).$$

Proof. Clearly, Σ is closed under addition. Moreover $\det M(x, y) = P_{L_2}(x) - \zeta P_{L_1}(y)$. The assertion follows from the assumption. \square

Note that the spread $\Sigma_{L_1^{-1}, L_2^{-1}}$ is equivalent to Σ_{L_1, L_2} and that the spread $\Sigma_{L_1^{-1}, L_2}$ is obtained from Σ_{L_1, L_2} by transposition. Because of Theorem 4.1 and Proposition 2.1 we consider spread sets $\Sigma = \Sigma_{L_1, L_2}$ with:

- (a) $L_1 = L_2$ has the form $A_{a,r}(X)$ or $B_{b,r}(X)$.
- (b) $L_i(X) = A_{b^2, r}(X)$ and $L_j(X) = B_{b, -r}(X)$ for $\{i, j\} = \{1, 2\}$.

If $(r, n) = d > 1$ we set $r' = r/d$. Then $A_{a,r}(X)$ ($B_{b,r}(X)$) can be considered as a polynomial of the form $A_{a,r'}(X)$ ($B_{b,r'}(X)$) with $K' = \text{GF}(q^d)$ in the role of K . We therefore make the assumption

$$(r, n) = 1.$$

In this way we do not lose any semifield but avoid some double counting. The associated pre-semifield

$\mathbf{S} = \mathbf{S}(L_1, L_2)$ will be called of *type (a)* if $L_1 = L_2$
and of *type (b)* if $L_1 \neq L_2$.

Lemma 4.2 *Let $L(X) = A_{a,r}(X)$ or $B_{b,r}(X)$. The following holds:*

- (a) *Assume $c, d \in F^*$ such that $cL(x) = L(dx)$ for $x \in F$. Then $c = d \in K$.*
- (b) *There is no pair $c, d \in F^*$ such that $cL(x) = L^{-1}(dx)$ for $x \in F$.*
- (c) *Let $L(X) = A_{a,r}(X)$ and $L' = B_{b,r}^{\pm 1}(X)$. There is no pair $c, d \in F^*$ such that $cL'(x) = L(dx)$ for $x \in F$.*

Proof. We consider only the case $L(X) = B_{b,r}(X) = 2A(X)^{-1} - X$, $A(X) = X - bX^{q^r}$. The case $A_{a,r}$ is similar. We know by [7] that $L(X) = \sum_{i=0}^{n-1} a_i X^{q^i}$ with $a_i \neq 0$ for all i .

(a) The equation $cL(x) = L(dx)$ implies $c = d^{q^i}$ for all i and the assertion follows.

(b) Using [7, (3.4)] and the remark after [7, (3.5)] we see that $L^{-1}(X) = \sum_{i=0}^{n-1} a'_i X^{q^i}$ with $a'_0 = a_0^{-1}$, $a'_{jr} = (-1)^j a_0^{-1} a_{jr}$ for $j > 0$. Assuming $cL(x) = L^{-1}(dx)$ for $x \in F$ we get $d^{q^{2r}} = d = -d^{q^r}$, a contradiction.

Assertion (c) is verified in a similar fashion. \square

Theorem 4.3 *Set $\mathbf{S} = \mathbf{S}(L_1, L_2)$. The following holds.*

- (a) *The middle nucleus of the pre-semifield \mathbf{S} is isomorphic to K .*
- (b) *The left nucleus (i.e. the kernel) of \mathbf{S} is isomorphic to F .*
- (c) *The right nucleus is isomorphic to K for type (b) and isomorphic to $\text{GF}(q^2)$ for type (a).*

Proof. We use the connection between the nuclei and certain homology groups as described in [1, Result 12.4], [12, Theorem 8.2].

(a) A nontrivial element from the middle nucleus corresponds to a $A \in \text{GL}(2, F)$ with $\Sigma = A\Sigma$. Let $A = (a_{ij})$ then

$$AM(x, 0) = \begin{pmatrix} a_{11}x & a_{12}\zeta L_2(x) \\ a_{21}x & a_{22}\zeta L_2(x) \end{pmatrix}.$$

We get the equations $L_2(a_{11}x) = a_{22}L_2(x)$ and $L_1(a_{12}\zeta L_2(x)) = a_{21}x$ for $x \in F$. Write the second equation as $a_{12}\zeta L_2(x) = L_1^{-1}(a_{21}x)$. We deduce from Lemma 4.2 that $a_{11} = a_{22} \in K^*$ and $a_{12} = a_{21} = 0$.

(b) Clearly, by (a) Σ is not desarguesian. Since the left nucleus contains F the second assertion follows.

(c) Let $A = (a_{ij}) \in \text{GL}(2, F)$ correspond to an element of the right nucleus, i.e. $\Sigma A = \Sigma$. Then

$$M(x, 0)A = \begin{pmatrix} a_{11}x & a_{12}x \\ a_{21}\zeta L_2(x) & a_{22}\zeta L_2(x) \end{pmatrix}$$

lies in Σ . We conclude $L_2(a_{11}x) = a_{22}L_2(x)$ and $L_1(a_{12}x) = a_{21}\zeta L_2(x)$ for $x \in F$. From Lemma 4.2 we conclude $a_{12} = a_{21} = 0$ in the case $L_1 \neq L_2$ and $a_{11} = a_{22} \in K$. This shows the first assertion.

Assume now $L = L_1 = L_2$. Again Lemma 4.2 implies $a_{11} = a_{22}$ and $a_{12} = a_{21}\zeta$ and both elements lie in K . Obviously

$$K_1 = \left\{ \begin{pmatrix} c & \zeta d \\ d & c \end{pmatrix} \mid c, d \in K \right\} \simeq \text{GF}(q^2)$$

and it is easy to see that $\Sigma A \subseteq \Sigma$ for $A \in K_1$. The proof is complete. \square

We now consider a semifield multiplication of the form

$$(u, v) * (x, y) = (ux + v \circ y, uy + \zeta(v \circ x))$$

where \circ defines a pre-semifield $(F, +, \circ)$ isotopic to a twisted field.

Theorem 4.4 *Let q be an odd prime power, $0 < n \in \mathbb{N}$ odd, $F = \text{GF}(p^n)$ and $K = \text{GF}(q)$. Let $0 < r < n$ and $a \in F^*$ such that $a^{(q^n-1)/(q^{(n,r)}-1)} \neq 1$. Assume further $0 \leq s, t < n$, $s \neq t$, and $t \equiv s \pmod{(n, r)}$. Define a multiplication on F^2 by*

$$(u, v) * (x, y) = (ux + v^{q^s} y^{q^r} - av^{q^t} y^{q^{-r}}, uy + \zeta(v^{q^s} x^{q^r} - av^{q^t} x^{q^{-r}})).$$

Then $(F, +, *)$ is a pre-semifield.

Notation and Remark The pre-semifield defined in this lemma will be denoted by

$$\mathbf{S} = \mathbf{S}(a, r, s, t).$$

Note that the multiplication $v \circ y = v^{q^s} y^{q^r} - av^{q^t} y^{q^{-r}}$ is isotopic to the multiplication $v \circ y = vy - av^{q^{t-s}} y^{q^{-2r}}$ which is the multiplication of a twisted field of order q^n . Moreover note that if

$$2r + t \equiv s \pmod{n}$$

the multiplication \circ is isotopic to the multiplication of a field.

Proof. Let $(x, y) \neq (0, 0)$. We have to show that $(u, v) * (x, y) = (0, 0)$ implies $(u, v) = (0, 0)$. If $x = 0$ we get $u = 0$ and then even $v^{q^s} y^{q^r} - av^{q^t} y^{q^{-r}} = 0$, i.e.

$$a = \frac{v^{q^s} y^{q^r}}{v^{q^t} y^{q^{-r}}}$$

contradicting the choice of a . Similarly the case $y = 0$ is ruled out. So assume $x \neq 0 \neq y$. The equations $u = -x^{-1}(v^{q^s} y^{q^r} - av^{q^t} y^{q^{-r}})$ and $u = -y^{-1}\zeta(v^{q^s} x^{q^r} - av^{q^t} x^{q^{-r}})$ imply

$$a = \frac{v^{q^s}}{v^{q^t}} \left(\frac{y^{q^r+1} - \zeta x^{q^r+1}}{y^{q^{-r}+1} - \zeta x^{q^{-r}+1}} \right)$$

leading to the same contradiction as in the proof of Proposition 2.1. \square

Remark Set

$$S(x) = T_s(x^{q^r}) - T_t(ax^{q^{-r}}), \quad x \in F.$$

A spread set associated to the above multiplication has the form

$$\Sigma = \Sigma_{a,r,s,t} = \left\{ M(x, y) = \begin{pmatrix} T_0(x) & T_0(y) \\ S(y) & \zeta S(x) \end{pmatrix} \mid x, y \in F \right\}.$$

Lemma 4.5 *Let $M = \sum_{i=0}^{n-1} T_i(m_i)$, $b \in F^*$ and assume $S(x)M = S(bx)$ for all $x \in F$. If $2r + t \not\equiv s \pmod{n}$ then $b \in \text{GF}(q^{(n,r)})$ and $M = T_0(b)$. If $2r + t \equiv s \pmod{n}$ then $M = S(1)^{-1}T_0(b^{q^{-t-r}})S(1)$.*

Proof. Assume first $2r + t \not\equiv s \pmod{n}$. We compute

$$\begin{aligned} S(x)M &= \sum_i T_{s+i}(x^{q^{r+i}} m_i) - \sum_j T_{t+j}(a^{q^j} x^{q^{-r+j}} m_j) \\ &= \sum_i T_{s+i}(m_i x^{q^{r+i}} - a^{q^{i+s-t}} m_{i+s-t} x^{q^{i+s-t-r}}). \end{aligned}$$

For $i \neq 0, t-s$ we deduce $m_i = m_{i+s-t} = 0$ as $r+i \not\equiv i+s-t-r \pmod{n}$. Considering the terms $T_s(*)$ and $T_t(*)$ we see that the only m_0, m_{s-t} or m_{t-s} can be non-trivial. Also if $i = 2(t-s)$ then $i \neq 0, t-s$. Hence $m_{2(t-s)} = m_{t-s} = 0$. Similarly, as $s-t \neq 0, t-s$ we obtain $m_{s-t} = 0$. This shows $m_i = 0$ for $i > 0$ and

$$S(x)M = T_s(m_0 x^{q^r}) - T_t(am_0 x^{q^{-r}})$$

which implies by assumption $m_0 x^{q^r} = (bx)^{q^r}$ and $m_0 x^{q^{-r}} = (bx)^{q^{-r}}$ for $x \in F$. We conclude $b = b^{q^{2r}}$ showing $b \in \text{GF}(q^{(n,r)})$.

Assume now $2r + t \equiv s \pmod{n}$. Then $S(x) = T_0(x^{q^{-t-r}})S(1)$. Therefore the equation $S(bx) = S(x)M$ implies $M = S(1)^{-1}T_0(b^{q^{-t-r}})S(1)$. \square

Lemma 4.6 *Let $M = \sum_{i=0}^{n-1} T_i(m_i)$, $b \in F^*$ and assume $MS(x) = S(bx)$ for all $x \in F$. Then $b \in \text{GF}(q^d)$, $d = (n, 2r + t - s)$, and $M = T_0(b)$.*

Proof. We compute

$$\begin{aligned} MS(x) &= \sum_i T_{s+i}(m_i^{q^s} x^{q^r}) - \sum_j T_{t+j}(am_j^q x^{q^{-r}}) \\ &= \sum_i T_{s+i}(m_i^{q^s} x^{q^r} - am_{i+s-t}^q x^{q^{-r}}). \end{aligned}$$

Also if $i = 2(t-s)$ then $i \neq 0, t-s$. Hence $m_{2(t-s)} = m_{t-s} = 0$. Similarly, as $s-t \neq 0, t-s$ we obtain $m_{s-t} = 0$. This shows $m_i = 0$ for $i > 0$ and

$$MS(x) = T_s(m_0^{q^s} x^{q^r}) - T_t(am_0^q x^{q^{-r}}).$$

We conclude $m_0^{q^s} x^{q^r} = (bx)^{q^r}$ and $m_0^q x^{q^{-r}} = (bx)^{q^{-r}}$. Thus $m_0^{q^s} = b^{q^r}$ or $m_0 = b^{q^{r-s}}$ so that $b^{q^{r+t-s}} = b^{q^{-r}}$ implying $b = b^{q^{2r+t-s}}$. \square

Lemma 4.7 Let $M = \sum_{i=0}^{n-1} T_i(m_i)$, and assume $MS(x) \subseteq T_0(F)$ for all $x \in F$. Then $M = 0$.

Proof. We have seen before

$$MS(x) = \sum_i T_{s+i}(m_i^{q^s} x^{q^r} - am_{i+s-t}^{q^t} x^{q^{-r}}).$$

For $i \neq -s$ we have $m_i = m_{i+s-t} = 0$. The only possible nontrivial m_i 's are m_{-s} and m_{-t} . Since $t - 2s \neq -s$ we get $m_{-s} = 0$ and as $s \neq t$ also $m_{-t} = 0$. \square

Lemma 4.8 Let $A = \sum_{i=0}^{n-1} T_i(a_i)$ and $B = \sum_{i=0}^{n-1} T_i(b_i)$. The following holds:

- (a) Assume $AT_0(x) = T_0(x)B$ for all $x \in F$. Then $A = B \in T_0(F)$.
- (b) Assume $AS(x) = S(x)T_0(b)$, $b \neq 0$ for all $x \in F$. Then $A = T_0(b)$ and $b \in \text{GF}(q^e)$ where $e = (n, t - s)$.
- (c) Assume $AT_0(x) = S(x)B$ for all $x \in F$. Then $A = B = 0$.

Proof. (a) Since $AT_0(x) = \sum_{i=0}^{n-1} T_i(a_i x)$ and $T_0(x)B = \sum_{i=0}^{n-1} T_i(b_i x^{q^i})$ the assertion follows.

(b) We already know $AS(x) = \sum_i T_{s+i}(a_i^{q^s} x^{q^r} - aa_{i+s-t}^{q^t} x^{q^{-r}})$ and $S(x)T_0(b) = T_s(bx^{q^r}) - T_t(abx^{q^{-r}})$. Therefore the LHS must have the form

$$T_s(a_0^{q^s} x^{q^r} - aa_{s-t}^{q^t} x^{q^{-r}}) + T_t(a_{t-s}^{q^s} x^{q^r} - aa_0^{q^t} x^{q^{-r}}).$$

We deduce $a_i = 0$ for $i > 0$ and $a_0^{q^s} = b = a_0^{q^t}$. Hence $A = T_0(b)$ and $b \in \text{GF}(q^e)$.

(c) We already know $S(x)B = \sum_i T_{s+i}(b_i x^{q^{r+i}} - a^{q^{i+s-t}} b_{i+s-t} x^{q^{i+s-t-r}})$ and $AT_0(x) = \sum_i T_i(a_i x)$. Since the terms on the RHS must be of the form $T_*(x)$ we conclude $B = T_r(b_r) + T_{-r}(b_{-r})$. Then $S(x)B$ has the form

$$T_{s+r}(b_r x^{q^{2r}}) - T_{t+r}(a^{q^r} b_r x) + T_{s-r}(b_{-r} x) - T_{t-r}(a^{q^{-r}} b_{-r} x^{q^{-2r}}).$$

As $s \neq t$ and $2r \neq 0 \neq 4r$ we deduce $b_r = b_{-r} = 0$, i.e. $A = B = 0$. \square

Theorem 4.9 Set $\mathbf{S} = \mathbf{S}(a, r, s, t)$. The following holds:

- (a) The middle nucleus of \mathbf{S} is isomorphic to $\text{GF}(q^d)$, $d = (n, 2r + t - s)$.
- (b) The right nucleus of \mathbf{S} is isomorphic to $\text{GF}(q^f)$, $f = 2(n, r)$.
- (c) The left nucleus of \mathbf{S} is isomorphic to $\text{GF}(q^e)$, $e = (n, t - s)$.

Proof. Again we use [1, Result 12.4], [12, Theorem 8.2].

(a) Suppose $A = (A_{ij})_{1 \leq i, j \leq 2} \in \text{GL}(F^2)$ such that $A\Sigma = \Sigma$ where $\Sigma = \Sigma_{a, r, s, t}$. Then there exist (additive) functions $x \mapsto x'$ and $x \mapsto y'$ such that $AM(x, 0) = M(x', y')$. Using the block decomposition of A we obtain

$$A_{11}T_0(x) = T_0(x'), \quad \zeta A_{12}S(x) = T_0(y'), \quad A_{21}T_0(x) = S(y'), \quad \zeta A_{22}S(x) = \zeta S(y').$$

From Lemma 4.7 we deduce $A_{12} = 0$ and thus $A_{21} = 0$. Hence $A_{11} \neq 0$. Therefore $A_{11} = T_0(b)$, $b \neq 0$. We deduce that $x \mapsto x' = bx$. From Lemma 4.6 we get $A_{22} = T_0(b)$ and $b \in \text{GF}(q^d)$. On the other hand if A has this shape it is easy to see that $A\Sigma = \Sigma$.

(b) Assume now $\Sigma A = \Sigma$ and write A as in (a). Writing $M(x, 0)A = M(x', y')$ obtain similarly as before

$$T_0(x)A_{11} = T_0(x'), \quad T_0(x)A_{12} = T_0(y'), \quad \zeta S(x)A_{21} = S(y'), \quad \zeta S(x)A_{22} = \zeta S(x')$$

for all $x \in F$ and functions $x \mapsto x'$ and $x \mapsto y'$.

Assume first $2r+t \not\equiv s \pmod{n}$. Suppose $A_{11} \neq 0$. Then $A_{11} = T_0(b)$, $b \neq 0$ and hence $S(x)A_{22} = S(bx)$ for $x \in F$. From Lemma 4.5 we obtain $A_{22} = T_0(b)$, $b \in \text{GF}(q^{(n,r)})$.

Suppose next $A_{12} \neq 0$. Then $A_{12} = T_0(c)$, $c \neq 0$ and hence $\zeta S(x)A_{21} = S(cx)$ for $x \in F$. Again by Lemma 4.5 $A_{21} = T_0(\zeta^{-1}c)$ and $c \in \text{GF}(q^{(n,r)})$.

Assume now $2r+t \equiv s \pmod{n}$. This time Lemma 4.5 shows $A_{11} = T_0(b)$, $A_{12} = T_0(c)$, $\zeta A_{21} = S(1)^{-1}T_0(c^{q^{-t-r}})S(1)$, and $A_{22} = S(1)^{-1}T_0(b^{q^{-t-r}})S(1)$. We also have an equation $M(0, x)A = M(x'', y'')$ for all $x \in F$ and functions $x \mapsto x''$ and $x \mapsto y''$ which shows $A_{21} = T_0(d)$ and $A_{22} = T_0(e)$. Thus $S(1)T_0(d) = T_0(c^{q^{-t-r}})S(1)$ and $S(1)T_0(e) = T_0(b^{q^{-t-r}})S(1)$. This implies again $b, c, d, e \in \text{GF}(q^{(n,r)})$. On the other hand if

$$A = \begin{pmatrix} T_0(b) & T_0(\zeta c) \\ T_0(c) & T_0(b) \end{pmatrix}, \quad b, c \in \text{GF}(q^{(n,r)})$$

then a calculation shows $\Sigma A \subseteq \Sigma$. Clearly, the matrices of this shape form a field isomorphic to $\text{GF}(q^{2(n,r)})$.

(c) In order to compute the left nucleus we consider pairs $A = (A_{ij})_{1 \leq i, j \leq 2}$, $B = (B_{ij})_{1 \leq i, j \leq 2} \in \text{GL}(F^2)$ such that $AM(x, y) = M(x, y)B$ for all $x, y \in F$. Specializing $(x, y) = (x, 0)$ we obtain

$$A_{11}T_0(x) = T_0(x)B_{11}, \quad \zeta A_{12}S(x) = T_0(x)B_{12}, \quad A_{21}T_0(x) = \zeta S(x)B_{21}, \quad A_{22}S(x) = S(x)B_{22}$$

for $x \in F$. By Lemma 4.8 $A_{11} = B_{11} = T_0(b)$ and $A_{21} = B_{21} = 0$. Specializing $(x, y) = (0, x)$ we obtain

$$A_{12}S(x) = T_0(x)B_{21}, \quad A_{11}T_0(x) = T_0(x)B_{22}, \quad A_{22}S(x) = S(x)B_{11}, \quad A_{21}T_0(x) = S(x)B_{12}.$$

Hence $A_{12} = B_{12} = 0$ and $B_{22} = T_0(b)$, $b \neq 0$. The equation $A_{22}S(x) = S(x)T_0(b)$ shows by Lemma 4.8 that $A_{22} = T_0(b)$, $b \in \text{GF}(q^e)$. \square

Remark Our semifield multiplications have some resemblance to semifield multiplications introduced by Pott and Zhou [17]. Let F, K, ζ as before. These authors define semifield multiplications on F^2 of the form:

$$(u, v) * (x, y) = (ux + vy, u \circ y + \zeta(v \bullet x))$$

where \circ and \bullet are suitable semifield multiplications. In fact these multiplications can be chosen as multiplications of twisted fields [17, Theorem 2.1] producing again quadratic extensions of the twisted fields.

References

- [1] M. Biliotti, V. Jha, N. Johnson: *Handbook of Finite Translation Planes*, CRC, 2007.
- [2] M. Biliotti, V. Jha, N. Johnson: The collineation groups of generalized twisted field planes, *Geom. Dedicata* 76(1999), 97-126.
- [3] F. Buekenhout, A. Delandtsheer, J. Doyen, P. Kleidman, M. Liebeck, J. Saxl: Linear spaces with flag-transitive automorphism groups, *Geom. Ded.* 36(1990), 89-94.
- [4] P. Cameron: Finite permutation groups and finite simple groups, *Bull. London Math. Soc.* 13(1981), 1-22.
- [5] P. Dembowski: *Finite Geometries*, Springer, 1968.
- [6] U. Dempwolff: A characterization of the generalized twisted field planes, *Archiv Math.* 50(1988), 477-480.
- [7] U. Dempwolff, P. Müller: Translation planes of odd order via Dembowski-Ostrom Polynomials, to appear in *Osaka J. Math.*.
- [8] U. Dempwolff, P. Müller: Permutation Polynomials and Translation Planes of Even Order submitted *Advances in Geom.*.
- [9] D. Foulser: A generalization of André's systems, *Math. Z.* 100(1967), 380-395.
- [10] R. Guralnik, T. Penttila, C. Praeger, J. Saxl: Linear groups with orders having certain large prime divisors, *Proc. Lond. Math. Soc. III Ser.* 78(1999), 167-214.
- [11] B. Huppert: *Endliche Gruppen I*, Springer 1967.
- [12] D. Hughes, F. Piper: *Projective Planes*, Springer 1973.
- [13] V. Jha, N. Johnson: The planes of Suetake, *J. Geom.* 94(2009), 89-105.
- [14] W. Kantor, M. Williams: Nearly flag-transitive affine planes, *Advances in Geometry*, 10(2010), 161-183.
- [15] M. Liebeck: The affine permutation groups of rank three, *Proc. Lond. Math. Soc.* (3)54(1987), 477-516.
- [16] H. Lüneburg: *Translation Planes*, Springer 1980.
- [17] A. Pott, Y. Zhou: A family of semifields with 2 parameters, submitted for publication.
- [18] C. Suetake: A family of translation planes of order q^{2m+1} with two orbits of length 2 and $q^{2m+1} - 1$ on ℓ_∞ , *Geom. Dedicata*, 42(1992), 773-786.

- [19] K. Zsigmondy: Zur Theorie der Potenzreste, Monatshefte Math. Phys. 3(1892), 163-185.