

Permutation Polynomials and Translation Planes of Even Order

Ulrich Dempwolff, Peter Müller

Abstract

We describe two classes of permutation polynomials over finite fields F in characteristic 2 of the shape $L(X)X^k$ where $L(X)$ is an additive polynomial. Such polynomials determine translation planes of order $|F|$. We show that our polynomials define new classes of translation planes and we compute the automorphisms of these planes.

1 Introduction

Let F be a finite field. In this paper we consider permutation polynomials of the form $L(X)X^k$ where $L(X)$ is an additive polynomial and k a positive integer. The motivation for a search of such polynomials is a simple connection with translation planes of order $|F|$ which admit a cyclic collineation group of order $|F| - 1$ fixing two points at the line of infinity and permuting the others transitively (see Proposition 2.1).

One class of permutation polynomials, presented in Theorem 3.2, is obtained in even characteristic and $L(X)$ is a truncated trace map in this case. These polynomials are of particular interest since they are related to the class of exceptional permutation polynomials, which are permutation polynomials in infinitely many fields. Implicitly contained in a paper of Kantor and Williams [18] is a large class of permutation polynomials of the special form $L(X)X$. Theorem 3.3 gives a twisted version of the polynomials of Kantor-Williams. The polynomials of 3.2 and 3.3 lead to new classes of translation planes in characteristic 2. We finally mention a very simple construction (Theorem 3.4) of permutation polynomials. However it turns out (Proposition 3.5) that this last class does not produce new translation planes.

Translation planes which admit a collineation group fixing two points at the line of infinity and permuting the others transitively have been studied before. In [17] they are called *triangle transitive* and in [18] nearly *flag-transitive*. Chapter 70 of [1] gives a survey of known planes with this property. Among such planes are nearfield planes, generalized twisted field planes, planes of Suetake [23] and some André planes. Particularly many planes of this type were found by Kantor and Williams [18] in even characteristic and by the authors [6] for odd characteristic.

In the next section we introduce some notation and give a preliminary discussion of the planes defined by permutation polynomials. Section 3 is concerned with the construction of permutation polynomials. In section 4 we compute automorphisms of the associated translation planes and in section 5 we are concerned with isomorphisms between such planes and other nearly flag transitive planes. In section 6 we show that our planes have – in contrast to the planes of [18] – no symplectic spreads.

2 Permutation polynomials and translation planes

Finite weak quasifields and translation planes. We assume that the reader is familiar with the fundamental notions of finite translation planes (see [1], [4], [22] or [16]). For convenience we repeat some basics and fix thereby some notation.

Let $(F, +)$ be a finite abelian group and $\cdot : F \times F \rightarrow F$ a binary operation with the following properties:

(WQ1) $x \cdot 0 = 0 \cdot x = 0$ for all $x \in F$.

(WQ2) $x \cdot (y + z) = x \cdot y + x \cdot z$ for all $x, y, z \in F$.

(WQ3) For all $0 \neq a \in F$ the mappings $x \mapsto x \cdot a$ and $x \mapsto a \cdot x$ are bijective.

Then $F = (F, +, \cdot)$ is called a *weak (left) quasifield* [16] or *(left) pre-quasifield* [1]. One knows that $(F, +)$ has to be an elementary abelian p -group, p a prime, i.e. F is a vector space over $\text{GF}(p)$. The associated *spread* of the weak quasifield is the set

$$\mathcal{S} = \{V(a) \mid a \in F \cup \infty\}$$

of $\text{GF}(p)$ -spaces of $W = F \times F$ where

$$V(\infty) = 0 \times F \quad \text{and} \quad V(a) = \{(x, a \cdot x) \mid x \in F\}.$$

The linear maps $N(y)$, $y \in F$, defined by $N(y)x = y \cdot x$ define a *spread set* $\Sigma = \{N(y) \mid y \in F\}$ associated to the spread. The spread in turn defines an affine plane $\mathbf{A} = \mathbf{A}_{\mathcal{S}}$ whose point set is W and whose lines have the form $w + X$, $w \in W$, $X \in \mathcal{S}$. For $w \in W$ the translation $x \mapsto x + w$ induces a collineation of \mathbf{A} , i.e. the plane is a translation plane with translation group $\simeq W$. The full collineation group is the semidirect product of the translation group with $\{T \in \text{GL}(W) \mid T\mathcal{S} = \mathcal{S}\}$, the *translation complement*. We usually consider collineations which either fix the fibers $V(0)$ and $V(\infty)$ or interchange both fibers. In the first case $T(x, y) = (T_1x, T_2y)$ with linear transformations T_i . A typical element in the fiber $V(y)$ has the form $(x, N(y)x)$. Since $T(x, N(y)x) = (z, T_2N(y)T_1^{-1}z)$ ($z = T_1x$) we see that T maps $V(y)$ onto the fiber $V(y')$ with $N(y') = T_2N(y)T_1^{-1}$. In the second case one has $T(x, y) = (T_1y, T_2x)$. A similar computation as before shows that $TV(y) = V(y')$ where $N(y') = T_2N(y)^{-1}T_1^{-1}$.

Consider translation planes satisfying the following hypothesis:

HYPOTHESIS (NF). Let $\mathbf{A} = \mathbf{A}_S$ be a translation plane of order p^n , p a prime. The translation complement contains a cyclic group Z of order $p^n - 1$ which fixes two fibers X, Y of S , acts faithfully on X , and permutes the remaining fibers of S transitively.

In our setup we may assume under hypothesis (NF) that $X = V(0)$ and $Y = V(\infty)$. Using suitable bases of X and Y we may identify F with $\text{GF}(p^n)$ and Z with the group of transformations $\mu_c, c \in F^*$, such that the action of the μ_c 's on W is given by

$$\mu_c(x, y) = (c^{-1}x, c^k y). \quad (\text{A}_k)$$

where k is an integer between 0 and $p^n - 2$. For $k = 0$ one sees immediately that the associated plane is desarguesian. The planes of [18] represent the case $k = 1$.

Permutation polynomials, additive polynomials. Let F be a finite field and $P(X) \in F[X]$. We denote by the symbol P the polynomial map $x \mapsto P(x)$ on F . The polynomial is called *permutation polynomial* if P is a bijection of F . The polynomial $L(X) \in F[X]$ is called *additive* if L is additive, i.e. linear over the prime field. We also write for polynomials $P(X) \equiv Q(X)$ if they induce the same polynomial maps.

Proposition 2.1 *Let p be a prime, $0 < n$ an integer and $F = \text{GF}(p^n)$.*

- (a) *Let $L(X) = a_0X + a_1X^p + \dots + a_{n-1}X^{p^{n-1}}$ be an additive polynomial, $0 \leq k < p^n - 1$, and assume that $L(X)X^k$ is a permutation polynomial. Then $L(X)$ is a permutation polynomial and*

$$x \cdot y = L(xy)x^k$$

defines the multiplication of a weak quasifield on F . The associated translation plane satisfies hypothesis (NF) and has action (A_k) .

- (b) *Let \mathbf{A} be a translation plane of order p^n satisfying hypothesis (NF) such that the cyclic group has action (A_k) . Then there exist an additive polynomial $L(X)$ such that a quasifield is associated with \mathbf{A} which has a multiplication as in (a).*

Proof. (a) Set $P(X) = L(X)X^k$. Assume $L(x) = 0$ for some $x \in F$. Multiplying with x^k we obtain $P(x) = 0$, i.e. $x = 0$ and L is bijective.

We now verify the properties of a weak quasifield. Clearly, (WQ1) and (WQ2) hold. We have to verify (WQ3). Assume first $x \cdot y = x_1 \cdot y$ for $y \neq 0$. We have to show $x = x_1$. Multiply this equation with y^k . We obtain $P(xy) = P(x_1y)$ and $x = x_1$ as P is bijective.

Assume now $x \cdot y = x \cdot y_1$ for $x \neq 0$. Multiply the equation with x^{-k} . We obtain $L(xy) = L(xy_1)$ and therefore $xy = xy_1$ as L is bijective. Hence $y = y_1$.

Define μ_c by action (A_k). A typical element in $V(b)$ has the form $(x, b \cdot x) = (x, L(xb)b^k)$. Set $y = c^{-1}x$. Then

$$\mu_c(x, b \cdot x) = (c^{-1}x, L(bx)b^k c^k) = (y, L(bcy)(bc)^k)$$

which is a typical element of $V(bc)$.

(b) We may assume that W and Z are represented as in the section about quasifields and translation planes. Let $X \neq V(0), V(\infty)$ be a fiber of the Z -invariant spread \mathcal{S} . Then X has the form $\{(x, L(x)) \mid x \in F\}$ where $L(X) = a_0X + a_1X^p + \cdots + a_{n-1}X^{p^{n-1}}$ is an additive permutation polynomial. By assumption $\mathcal{S} = \{V(0), V(\infty)\} \cup \{\mu_c X \mid c \in F^*\}$. A similar computation as in part (a) shows $X\mu_c = \{(x, L(xc)c^k) \mid x \in F\}$.

We claim that $P(X) = L(X)X^k$ is a permutation polynomial. Assume $P(b) = P(c)$ for $b, c \in F^*$. Then

$$(1, P(b)) = (1, P(c)) \in X\mu_b \cap X\mu_c$$

and $b = c$ by the basic properties of a spread. □

The preceding proof shows that the operators $N(y)$ of the spread set have the form $N(y) = L_y$ where L_y is defined by the additive polynomial

$$L_y(X) = \sum_{i=0}^{n-1} a_i y^{p^i+k} X^{p^i}.$$

The preceding lemma motivates:

PROBLEM. Find additive polynomials $L(X)$ on $\text{GF}(p^n)$ and integers k such that

$$L(X)X^k \text{ is a permutation polynomial.}$$

3 Permutation polynomials of the form $L(X)X^k$

In this section we study permutation polynomials on a finite field F of the form $P(X) = L(X)X^k$, where $L(X) \in F[X]$ is additive on F , and $k \in \mathbb{N}$.

To such a polynomial we relate another permutation polynomial of this form. The construction and the proof of the basic properties work in a more general context. Let F/K be a finite separable extension of fields, and let $T : F \rightarrow K$ be the trace form. The bilinear form on F defined by $(u, v) = T(uv)$ is nondegenerate. Thus, to any K -linear map $D : F \rightarrow F$ there exists the adjoint map D^* uniquely defined by $T(D(u)v) = T(uD^*(v))$ for all $u, v \in F$. Furthermore, D is invertible if and only if D^* is invertible.

Lemma 3.1 *Let $L : F \rightarrow F$ be K -linear, and let $M : F \rightarrow F$ be a multiplicative bijection. Then the map $x \mapsto L(x)M(x)$ is injective on F if and only if $x \mapsto L^*(x)M^{-1}(x)$ is injective.*

Proof. Associated to L, M and $y \in F$ we consider the K -linear map $\Delta_{L,M,y}$ defined by

$$\Delta_{L,M,y}(x) = L(xy)M(y).$$

Write $P(x) = L(x)M(x)$. Then

$$P(xy_1) - P(xy_2) = (\Delta_{L,M,y_1}(x) - \Delta_{L,M,y_2}(x))M(x).$$

Clearly, $x \mapsto P(x)$ is injective if and only if the linear maps $\Delta_{L,M,y_1} - \Delta_{L,M,y_2}$ are invertible for all distinct $y_1, y_2 \in F$, and this holds if and only if $\Delta_{L,M,y_1}^* - \Delta_{L,M,y_2}^*$ is invertible. The same reasoning shows that $x \mapsto L^*(x)M^{-1}(x)$ is injective if and only if $\Delta_{L^*,M^{-1},y_1} - \Delta_{L^*,M^{-1},y_2}$ is invertible for distinct y_1, y_2 . Since M is bijective, this latter condition is equivalent to $\Delta_{L^*,M^{-1},M(y_1)} - \Delta_{L^*,M^{-1},M(y_2)}$ being invertible. Thus we are done once we know that $\Delta_{L^*,M,y}^* = \Delta_{L^*,M^{-1},M(y)}$. For this we have to show that the following holds for all $u, v \in F$:

$$T(\Delta_{L,M,y}(u)v) = T(u\Delta_{L^*,M^{-1},M(y)}(v)).$$

In terms of L and L^* this is equivalent to

$$T(L(uy)M(y)v) = T(uL^*(vM(y))y).$$

But by definition, $T(L(w)z) = T(wL^*(z))$ for all $w, z \in F$, so the assertion follows from setting $w = uy$, $z = M(y)v$. \square

Theorem 3.2 *Let $F = \text{GF}(2^n)$ with n odd. Let m be odd with $1 < m < n$ and relatively prime to n . Let $L(X) = \sum_{i=0}^{m-1} X^{2^i}$ be a truncated trace map. Set $k = 2^{n-1} - 2^{m-1} - 1$, and choose $1 \leq k' \leq 2^n - 1$ with $kk' \equiv 2^{m-1} \pmod{2^n - 1}$. Then*

$$L(X)X^k \text{ and } L(X)X^{k'}$$

are permutation polynomials on F .

Proof. Note that

$$L^*(X)^{2^{m-1}} \equiv \left(\sum_{i=n-m+1}^n X^{2^i} \right)^{2^{m-1}} \equiv L(X).$$

We show that the bijectivity of $L(X)X^k$ implies the bijectivity of $L(X)X^{k'}$: Choose $\ell \in \mathbb{N}$ such that $k\ell \equiv 1 \pmod{2^n - 1}$, so $\ell 2^{m-1} \equiv k' \pmod{2^n - 1}$. By the previous lemma, $L^*(X)X^\ell$ is bijective, and hence so is $(L^*(X)X^\ell)^{2^{m-1}} \equiv L(X)X^{\ell 2^{m-1}} \equiv L(X)X^{k'}$.

Thus it remains to show that $L(X)X^k$ is a permutation polynomial on F .

We first note that 0 is the only root of $L(X)$ in F : Since exactly half of the elements of $\text{GF}(2^m)$ are in the kernel of the trace polynomial $L(X)$, and $L(X)$ has degree 2^{m-1} , we see that all roots of $L(X)$ are in $\text{GF}(2^m)$. But m and n are relatively prime, and $L(1) = 1$ since m is odd, so 0 is the only root in F .

Thus it suffices to show injectivity of $L(X)X^k$ on $F^* = F \setminus \{0\}$.

By assumption $2k \equiv -(2^m + 1) \pmod{2^n - 1}$, so $(L(X)X^k)^2$ gives the same map on F^* as the rational function $g(X) = \frac{L(X)^2}{X^{2^m+1}}$. Set $f(X) = g(\frac{1}{X})$. Then $f(X) = \sum_{i=1}^m X^{2^m+1-2^i}$ is a polynomial of degree $2^m - 1$. Clearly, we only need to show that $f(X)$ is injective on F^* .

For the moment, write $f_m(X)$ for this polynomial for any $m \in \mathbb{N}$. Then $f_m(X) = \frac{f_{m-1}(X)^2 + X^{2^m}}{X}$. Let Z be another variable. Then, using this recursion and induction, we get

$$f_m\left(Z + \frac{1}{Z}\right) = Z^{2^m-1} + \frac{1}{Z^{2^m-1}}.$$

But that is exactly the defining property of a Dickson polynomial, see e.g. [20] or [19]. The permutation behavior of these polynomials is well known (see e.g. [20, Theorem 7.16]) and easy to work out: Suppose that $f(x) = f(y)$. Pick u and v in a possibly quadratic extension of F with $x = u + \frac{1}{u}$, $y = v + \frac{1}{v}$. So

$$u^{2^m-1} + \frac{1}{u^{2^m-1}} = f\left(u + \frac{1}{u}\right) = f(x) = f(y) = f\left(v + \frac{1}{v}\right) = v^{2^m-1} + \frac{1}{v^{2^m-1}}.$$

This implies $u^{2^m-1} = v^{2^m-1}$ or $u^{2^m-1} = \frac{1}{v^{2^m-1}}$. Since $u, v \in \text{GF}(2^{2n})$ and $2^m - 1$ is prime to $2^{2n} - 1$, we get $u = v$ or $u = \frac{1}{v}$, hence $x = y$ in either case. \square

A connection to Cohen–Matthews polynomials. Despite the similar shape of the polynomials $L(X)X^k$ and $L(X)X^{k'}$ in Theorem 3.2, the latter polynomials have an interesting connection to a class of permutation polynomials for which the permutation property is more difficult to prove than for the Dickson polynomials in the previous section.

In [3], Cohen and Matthews define the following polynomials under the same assumptions on m and n as in Theorem 3.2: Let c, d be integers with $cd = 2^m + 1$. Then set

$$f_{m,d}(X) = \frac{L(X^c)^d}{X^{2^m}}.$$

Note that $f_{m,d}(X)$ is indeed a polynomial. See also [11, Theorem 4.3] for a deep Galois theoretic characterization of these polynomials.

The polynomials $f_{m,d}(X)$ are bijective on F by the main result [3, Theorem 3.15]. The proof, as well as some subsequent proofs like [24], use the fact that none of the irreducible factors of $(f_{m,d}(X) - f_{m,d}(Y))/(X - Y)$ over $\text{GF}(q)$ is absolutely irreducible. To the best of our knowledge, there is only one direct proof of the permutation behavior of these polynomials. In [7], Dillon and Dobbertin use discrete additive Fourier transforms to relate the permutation behavior of the Cohen–Matthew polynomials to that of the Dickson polynomials.

Theorem 3.2 gives an alternative and even more direct proof of the permutation property of the Cohen–Matthew polynomials $f_{m,d}(X)$: Set $P(X) = L(X)X^{k'}$. Since c and $2k$ are relatively prime to $2^n - 1$, the rational map

$$\left(\frac{1}{P(X^c)}\right)^{2k} = \frac{1}{L(X^c)^{2k} X^{2kk'/c}}$$

is injective on F^* . Using that $2k \equiv -2^m - 1 \pmod{2^n - 1}$, $2kk' \equiv 2^m \pmod{2^n - 1}$ and $cd = 2^m + 1$ shows, that this rational map induces the same map on F^* as the following rational function:

$$\frac{L(X^c)^{2^m+1}}{X^{2^m c}} = \frac{L(X^c)^{cd}}{X^{2^m c}} = \left(\frac{L(X^c)^d}{X^{2^m}} \right)^c = f_{m,d}(X)^c.$$

Thus $f_{m,d}(X)$ is injective on F^* and then also injective on F , since $L(X)$ has no root in F but 0.

Remark A polynomial $f(X) \in K[X]$ over a finite field K is called exceptional if it induces a bijection on infinitely many finite extensions of K . In contrast to permutation polynomials, exceptional polynomials are rare. Still, they are not fully classified. If we write an exceptional polynomial as a composition of polynomials, then each of the constituents is exceptional too. The converse holds as well, but that is less obvious. Thus one tries to classify the functionally indecomposable exceptional polynomials.

Using the classification of the finite simple groups and Weil's theorem about points on algebraic curves over finite fields, a thorough Galois theoretic investigation has begun, see e.g. [9], [10], [11], [12] and the references given there. It turns out that there are three types of candidates, distinguished by Galois theoretic properties:

Let \bar{K} be an algebraic closure of K , t a variable, and $G = \text{Gal}(f(X) - t / \bar{K}(t))$ the Galois group of $f(X) - t$, considered as a permutation group on the roots.

Dickson case. The easiest and best understood examples arise when the degree n of $f(X)$ is prime to the characteristic of K . Then G is cyclic or dihedral, and $f(X)$ is essentially a Dickson polynomial $D_{a,n}(X)$ ($a \in K$), which is related to the cyclic polynomial X^n by the twist $D_{a,n}(Z + \frac{a}{Z}) = Z^n + (\frac{a}{Z})^n$. Note that $D_{0,n}(X) = X^n$. In the proof of part (a) of our theorem, we have $f(X) = D_{1,2^m-1}(X)$.

Affine case. Other possibilities arise when G is an affine group, of degree which is a power of the characteristic of K . A prototype is an additive polynomial $L(X)$ which is bijective on K . Let the splitting field of $L(X)$ over K have degree r . Then $L(X)$ has no nonzero roots on each finite extension F of K whose degree is prime to r , thus $L(X)$ is bijective on these infinitely many fields. It is easy to see that G is elementary abelian. One can slightly twist $L(X)$ to obtain affine groups with cyclic point stabilizers. However, not all exceptional polynomials with affine G come from additive polynomials, see [10]. It is an open question if there are more affine examples beyond the additive polynomials and their twists and those in [10] (together with their characteristic 2 analogs which weren't studied there).

PSL-case. The remaining possibilities only arise in characteristic 2 and 3. In this case, q is an odd power of the characteristic of K , and $G = \text{PSL}_2(q)$ in

it action on $q(q-1)/2$ points. The rather peculiar possibilities were classified in [11] and [12]. The polynomial $f(X)$ in the proof of (b) corresponds to this case.

A computer search showed that for $n \in \{5, 7, 11, 13\}$ the examples in the theorem are the only ones where $L(X)X^a$ is bijective on $F = \text{GF}(2^n)$, where $L(X) \in \text{GF}(2)[X]$ is additive with at least 3 terms, and $1 \leq a < 2^n - 1$.

If n is not a prime, then different constructions are possible which are not related to the cases in the theorem:

Set $F_n = \text{GF}(2^n)$ and if d divides n denote by $T_{n:d} : F_n \rightarrow F_d$ the trace map. We now give a twisted version of permutation polynomials of the form $L(X)X$ which arise from the nearly flag transitive planes of [18]. Let d_1 be a divisor of n such that n/d_1 is odd. Assume $d_1|d_2|\dots|d_h|n$ and let $c_i \in F_{d_i}^*$, $1 \leq i \leq h$, such that $\sum_{j=1}^i c_j \neq 0$ for all i . Choose $1 \leq \ell < d_1$ with $(2^{d_1} - 1, 2^\ell + 1) = 1$ and $c_0 \in F_{d_1}^*$. Set

$$L(X) = \left(\sum_{i=1}^h c_i \right) X + \sum_{i=1}^h c_i T_{n:d_i}(X) + c_0 T_{n:d_1}(X)^{2^\ell}.$$

Then we have:

Theorem 3.3 *The polynomial $L(X)X$ is a permutation polynomial on F_n .*

Proof. Set $P(X) = L(X)X$ and assume $P(x) = P(y)$ for $x, y \in F_n$, $x \neq y$. We make induction on h .

Case $h = 1$. Apply $T_{n:d_1}$ to the equation $P(x) = P(y)$ and we obtain

$$c_0 T_{n:d_1}(x)^{2^\ell+1} = c_0 T_{n:d_1}(y)^{2^\ell+1}.$$

Since $(2^{d_1} - 1, 2^\ell + 1) = 1$ we have even $T_{n:d_1}(x) = T_{n:d_1}(y)$. This shows $c_1 x^2 + ax = c_1 y^2 + ay$ with $a = c_1 T_{n:d_1}(x) + c_0 T_{n:d_1}(x)^{2^\ell}$. Hence $y = x + \frac{a}{c_1}$. Since $\frac{a}{c_1} \in F_{d_1}$ we get

$$T_{n:d_1}(x) = T_{n:d_1}(y) = T_{n:d_1}(x) + \frac{a}{c_1}.$$

Therefore $a = 0$ which implies $x^2 = y^2$, a contradiction.

Case $h > 1$. Apply $T_{n:d_h}$ to the equation $P(x) = P(y)$. Using $T_{n:d_i}(z) = T_{d_h:d_i}(T_{n:d_h}(z))$ and writing $x_1 = T_{n:d_h}(x)$ and $y_1 = T_{n:d_h}(y)$ we obtain

$$\begin{aligned} & \left(\sum_{i=1}^{h-1} c_i \right) x_1^2 + \sum_{i=1}^{h-1} c_i T_{d_h:d_i}(x_1) x_1 + c_0 T_{d_h:d_1}(x_1)^{2^\ell} x_1 \\ &= \left(\sum_{i=1}^{h-1} c_i \right) y_1^2 + \sum_{i=1}^{h-1} c_i T_{d_h:d_i}(y_1) y_1 + c_0 T_{d_h:d_1}(y_1)^{2^\ell} y_1. \end{aligned}$$

Then $T_{n:d_n}(x) = x_1 = y_1 = T_{n:d_n}(y)$ by induction and hence $T_{n:d_i}(x) = T_{n:d_i}(y)$ for all i too. Therefore $P(x) = P(y)$ implies $cx^2+ax = cy^2+ay$ with $c = \sum_{i=1}^h c_i$ and $a = \sum_{i=1}^h c_i T_{n:d_i}(x) + c_0 T_{n:d_1}(x)^{2^\ell}$. So $y = x + \frac{a}{c}$ with $\frac{a}{c} \in F_{d_h}$. After applying $T_{n:d_h}$ we reach as in the case before the contradiction $x = y$. \square

We finally give a very simple construction which produces permutation polynomials of the form $L(X)X^{k+a}$ using permutation polynomials of the form $L(X)X^k$.

Theorem 3.4 *Let q be a prime power, n a positive integer, and $F = \text{GF}(q^n)$. Set $N = \frac{q^n-1}{q-1}$. Let $L(X) \in F[X]$ be a $\text{GF}(q)$ -linear polynomial on F such that $L(X)X^k$ is a permutation polynomial on F . Then $(k+1, q-1) = 1$. Let $(k+1)\ell \equiv 1 \pmod{q-1}$ and let b be a multiple of N such that $(b\ell+1, q-1) = 1$. Then $L(X)X^{k+b}$ is a permutation polynomial. In particular if $L(X)$ is a permutation polynomial and b a multiple of N such that $(b+1, q-1) = 1$ then $L(X)X^b$ is a permutation polynomial.*

Proof. Set $P(X) = L(X)X^k$ and $P'(X) = L(X)X^{k+b}$. If $d = (k+1, q-1)$ and $u \in \text{GF}(q)$ such that $u^d = 1$ we see $P(1) = P(u)$ which implies $d = 1$ and we can choose ℓ as desired. Now

$$P'(z) = L(z)z^{k+b} = L(z)z^{k+b(k+1)\ell} = L(z^{1+b\ell})(z^{1+b\ell})^k = P(z^{1+b\ell})$$

for $z \in F$. Assume $P'(x) = P'(y)$ for $x, y \in F^*$. Then $P(x^{1+b\ell}) = P(y^{1+b\ell})$ and $x^{1+b\ell} = y^{1+b\ell}$ follows. Now $x^{(1+b\ell)b\ell} = y^{(1+b\ell)b\ell}$ implies $x^{b\ell} = y^{b\ell}$ as $(b\ell+1, q-1) = 1$. Dividing the equation $x^{1+b\ell} = y^{1+b\ell}$ by $x^{b\ell}$ we reach $x = y$. The last assertion is obtained if we specialize $k = 0$. \square

Form the view point of translation planes however the last result is irrelevant:

Proposition 3.5 *The permutation polynomials $L(X)X^k$ and $L(X)X^{k+b}$ of Theorem 3.4 define the same translation plane.*

Proof. Define $P(X)$ and $P'(X)$ as in the proof of 3.4. The quasifield multiplication defined by $P(X)$ has the form $x \cdot y = L(xy)x^k$ and the quasifield multiplication defined by $P'(X)$ has the form $x \circ y = L(xy)x^{k+b}$. As we have seen in the proof of the preceding theorem we have $x \circ y = x^{1+b\ell} \cdot y$ which implies that both multiplications define the same spread sets, i.e. identical planes. \square

4 Automorphisms

In this section \mathbf{A} will denote a translation plane defined by a permutation polynomial of the form $L(X)X^k$ over a field $F = \text{GF}(p^n)$. We also do assume $(p^n-1, k) = 1$. By G we denote the translation complement of \mathbf{A} . The symbols $W = F \times F$ and $Z = \{\mu_c \mid c \in F^*\}$ will have the same meaning as in section

2 (i.e. Z has action (A_k) on W). We assume that a p -primitive prime divisor \bar{p} of $p^n - 1$ exists and denote by S a Sylow \bar{p} -subgroup of Z . Note that the existence of such a prime divisor is guaranteed (by Zsigmondy's theorem [25]) in the concrete cases which we will consider. We write the additive polynomial again as $L(X) = \sum_{i=0}^{n-1} a_i X^{p^i}$. We first prove some results in this general setting and specialize later to the case $p = 2$ and the polynomials of section 3.

For $a \in F = \text{GF}(p^n)$ and $0 \leq r < n$ we define the operator $T_r(a) \in \Gamma\text{L}(1, F)$ by

$$T_r(a)x = ax^{p^r}.$$

A cyclic group in $\text{GL}(n, p)$ is called a *Singer group* if it acts regularly on the nontrivial vectors of $V = \text{GF}(p)^n$. The following result about Singer groups [15, II.7.3] is useful.

Lemma 4.1 *Let $V = \text{GF}(p)^n$.*

- (a) *Identify V with $F = \text{GF}(p^n)$. Then $\mathcal{C} = \{T_0(a) \mid a \in F^*\}$ is a Singer group. Its normalizer in $\text{GL}(V)$ is $N_{\text{GL}(V)}(\mathcal{C}) = \{T_i(a) \mid a \in F^*, 0 \leq i < n\}$.*
- (b) *Any two Singer groups in $\text{GL}(V)$ are conjugate.*
- (c) *Let $T \in \text{GL}(V)$ be an irreducible operator. Then T lies in a unique Singer group which is the centralizer of T in $\text{GL}(V)$.*

The notation

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

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

Lemma 4.2 *Let $L(X)$ be an additive polynomial, $a, b \in F^*$ and $0 \leq s, t < n$. Then*

$$\text{spi}(T_s(a)LT_t(b)^{-1}) = \{i + r \mid i \in \text{spi}(L)\},$$

where $r = s - t$ and the numbers $i + r$ are read modulo n .

Lemma 4.3 *Set*

$$r = \gcd\{i - j \mid i, j \in \text{spi}(L)\}.$$

Then the kernel of \mathbf{A} is isomorphic to $\text{GF}(p^r)$.

Proof. The group S normalizes the group \mathcal{K} of kern homologies. It is easy to see that then S even centralizes \mathcal{K} (see the proof of [6, 4.4]). Therefore by Lemma 4.1 $\kappa \in \mathcal{K}$ has an action of the form $\kappa(x, y) = (T_0(a)x, T_0(b)y)$, $a, b \in F^*$, on W . Since $\kappa V(z) = V(z)$ (i.e. $T_0(b)L_z T_0(a)^{-1} = L_z$) for all $z \in F$ we obtain the identity

$$\sum_{i=0}^{n-1} a_i x^{p^i} z^{p^i+k} = \sum_{i=0}^{n-1} a_i a^{-p^i} b x^{p^i} z^{p^i+k}$$

for all $x \in F$. Hence $a^{p^i} = b$ if $a_i \neq 0$. In particular $a^{p^{i-j}} = a$ if $a_i \neq 0 \neq a_j$. This shows that $a, b \in \text{GF}(p^r)$. Since all arguments can be reversed the proof is complete. \square

For $a, b \in F^*$ and $\alpha \in \text{Aut}(F)$ define the operator $\tau_{a,b,\alpha}$ on W by $\tau_{a,b,\alpha}(x, y) = (ax^\alpha, by^\alpha)$. Note that $(ax^\alpha, by^\alpha) = (T_s(a)x, T_s(b)y)$ if $x^\alpha = x^{p^s}$.

Lemma 4.4 *The operator $\tau_{a,b,\alpha}$ lies in G if $a_i^\alpha a^{-p^i} b = a_i$ for $0 \leq i < n$.*

Proof. As similar computation as in Lemma 4.3 shows that under our assumptions we have $\tau_{a,b,\alpha}V(z) = V(z^\alpha)$, $z \in F$. \square

By Lemma 4.3 we see that the group of kern homologies has the form

$$\mathcal{K} = \{\tau_{a,a^{p^j},1} \mid a \in \text{GF}(p^r)^*\}$$

for any j with $a_j \neq 0$. By Lemma 4.4 the group

$$\mathcal{A} = \{\tau_{a,b,\alpha} \mid a_i^\alpha a^{-p^i} b = a_i \text{ for } 0 \leq i < n\}$$

lies in G . We set

$$\mathcal{G} = Z\mathcal{K}\mathcal{A}.$$

We will see that in the generic case \mathcal{G} is essentially equal to G . Denote the stabilizer of a fiber $V(z)$ in G by G_z .

Lemma 4.5 *Let \mathbf{A} be non-desarguesian. The following hold.*

- (a) S is a Sylow \bar{p} -subgroup of $G_{0,\infty}$.
- (b) Let $\gamma \in G_{0,\infty}$ normalize S . Then $\gamma = \tau_{a,b,\alpha}$ for some $a, b \in F^*$ and $\alpha \in \text{Aut}(F)$.
- (c) $\mathcal{G} = N_{G_{0,\infty}}(S)$.

Proof. (a) Obviously $S_{V(0)}$ ($S_{V(\infty)}$) is a Sylow \bar{p} -subgroup of $\text{GL}_{\text{GF}(p)}(V(0))$ ($\text{GL}_{\text{GF}(p)}(V(\infty))$). Assume that S is contained properly in a Sylow \bar{p} -subgroup of $G_{0,\infty}$. As such a group is certainly abelian it contains an element $\nu = \tau_{1,b,1}$ with b of order \bar{p} . Suppose $\nu V(1) = V(z)$ (i.e. $L_z = T_0(b)L_1$). Then we obtain the identity

$$\sum_{i=0}^{n-1} a_i b x^{p^i} = \sum_{i=0}^{n-1} a_i x^{p^i} z^{p^i+k}$$

for $x \in F$. This implies $b = z^{p^i+k}$ for $a_i \neq 0$ or $bz^{-k} = z^{p^i}$. As \mathbf{A} is non-desarguesian at least two a_i 's are nontrivial. Hence $z \in \text{GF}(p^r)$ and then $b \in \text{GF}(p^r)$ too which is impossible by the assumption on \bar{p} .

(b) Write $\gamma(x, y) = (\gamma_1 x, \gamma_2 y)$. There exists an m such that $\gamma \mu_c \gamma^{-1} = \mu_c^m$ for all $\mu_c \in S$. This implies $\gamma_i T_0(c) \gamma_i^{-1} = T_0(c^m)$. The assertion follows from

Lemma 4.1.

(c) Clearly, $\mathcal{G} \leq N_{G_{0,\infty}}(S)$. By (b) an element γ in $N_{G_{0,\infty}}(S)$ has the form $\gamma = \tau_{a,b,\alpha}$ if we adjust this element by an element from Z we may even assume $\gamma V(1) = V(1)$. We get the identity

$$\sum_{i=0}^{n-1} a_i^\alpha a^{-p^i} b x^{p^i} = \sum_{i=0}^{n-1} a_i x^{p^i}$$

for $x \in F$. Hence $\gamma \in \mathcal{A}$. □

The proof of the following proposition is purely group theoretic and essentially identical with the proof of [6, 4.6]. We will only outline the proof and refer the reader to [6] for details. The main ingredient of the proof is the classification of 2-transitive affine groups by Hering [13], [14] and Liebeck [21].

Proposition 4.6 *Assume that \mathbf{A} is not a semifield plane. The following hold.*

- (a) $G_{0,\infty} = \mathcal{G}$.
- (b) The group S is a normal Sylow \bar{p} -subgroup in G .
- (c) $G = G_{\{0,\infty\}}$, i.e. G fixes the set $\{V(0), V(\infty)\}$.

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

This is (1) in the proof of [6, 4.6]. An immediate consequence is that S is a Sylow \bar{p} -subgroup in G .

STEP 2. $G_{0,\infty} = \mathcal{G}$

Assume the converse. By step 1 one has $\mathcal{G}_{V(0)} < (G_{0,\infty})_{V(0)}$ or

$\mathcal{G}_{V(\infty)} < (G_{0,\infty})_{V(\infty)}$. Suppose for instance that the first case holds. From the classification of 2-transitive affine groups it follows that $(G_{0,\infty})_{V(0)}$ will contain a subgroup of the form $\text{GL}(m, p^t)$, $m > 1$, $mt = n$. As shown in [6] such a group can not act on \mathbf{A} .

STEP 3. $G_{0,\infty} = G_0 = G_\infty$.

Assume for instance $G_0 > G_{0,\infty}$. As \mathbf{A} is not a semifield plane one has $\mathcal{G}_{V(0)} < (G_{0,\infty})_{V(0)}$ or $\mathcal{G}_{W/V(0)} < (G_{0,\infty})_{W/V(0)}$. A similar argument as in step 2 leads to a contradiction.

STEP 3. $G = G_{\{0,\infty\}}$.

Assume $G > G_{\{0,\infty\}}$. Then by step 3 the group G is nonsolvable and acts transitively on the nontrivial elements of W . By the result of Hering and Liebeck

the group G is known. Again it can be shown that non of the resulting possibilities can act on \mathbf{A} (or use directly [2, Theorem]). \square

If \mathbf{A} is a semifield plane then the structure of the polynomial $L(X)$ is rather restricted:

Lemma 4.7 *Let \mathbf{A} be a non-desarguesian semifield plane and denote by $L^{-1}(X)$ the additive polynomial which defines the inverse of the transformation induced by $L(X)$. Then at most two coefficients of the polynomials $L(X)$ or $L^{-1}(X)$ are nontrivial.*

Proof. Clearly, $V(\infty)$ or $V(0)$ is the axis of the shears group. In the first case it follows from [5, (3.3)] that at most two coefficients of $L(X)$ are non-trivial. In the second case we observe that interchanging the roles of $V(\infty)$ and $V(0)$ means that the original spread set is replaced by the inverse spread set and $L^{-1}(X)$ takes the role of $L(X)$. \square

Remark We now turn to the case $p = 2$ and the polynomials of section 3. According to the preliminary results on automorphisms two main tasks are left: 1. Decide as to whether or not \mathbf{A} is a semifield plane and (which amounts to the investigation of L^{-1}). 2. Decide as to whether or not $G = G_{0,\infty}$ or $|G : G_{0,\infty}| = 2$.

Definition. We call \mathbf{A} of *type I* if \mathbf{A} is defined by a polynomial of Theorem 3.2 and \mathbf{A} is of *type II* if \mathbf{A} is defined by a polynomial of Theorem 3.3.

Theorem 4.8 *Let \mathbf{A} be a plane of type I. Then the kernel is isomorphic to $\text{GF}(2)$. Moreover*

$$G = G_{0,\infty} = Z\{\tau_{1,1,\alpha} \mid \alpha \in \text{Aut}(F)\} \simeq C_{2^{n-1}} \cdot C_n.$$

We use:

Lemma 4.9 *Let $L(X)$ be an additive polynomial of type I and $L^{-1}(X)$ the inverse additive polynomial. Then $L^{-1}(X) \in \text{GF}(2)[X]$. Moreover:*

- (a) $L^{-1}(X)$ is not the sum of one or two monomials.
- (b) For any $0 \leq r < n$ and any $1 < m' < n$, m' odd, $\text{spi}(L^{-1}) \neq \{i + r \mid 0 \leq i < m'\}$.

Proof. Since L (and the identity) commute with the Frobenius automorphism of F the polynomial $L^{-1}(X)$ has coefficients in $\text{GF}(2)$. An easy computation then shows that $L^{-1}(X)$ must have more than two nontrivial terms, assertion (a) follows.

To (b): Assume $\text{spi}(L) = \{i \mid 0 \leq i < m\}$. A matrix of L is the circulant matrix whose whose 0-th row is $L_{0*} = \sum_{i=0}^{m-1} e_{i+1-m}$ (e_i is a usual standard basis vector of the row space $\text{GF}(2)^n$ and we index rows and columns from 0 to

$n-1$). Suppose $\text{spi}(L^{-1}) = \{i+r \mid 0 \leq i < m'\}$. Then the matrix of L^{-1} is circulant and has the 0-th column $L_{*0}^{-1} = \sum_{j=0}^{m'-1} e_{r+j}^t$. The $m+r-1$ -th row of L is $L_{m+r-1*} = \sum_{i=0}^{m-1} e_{r+i}e$. We see that $(LL^{-1})_{m+r-1,0} = 1$. Moreover if $m \leq m'$ we have $(LL^{-1})_{m+r-2,0} = 1$ and if $m > m'$ one has $(LL^{-1})_{m+r-1,n-2} = 1$, a contradiction in either case. \square

Proof of Theorem 4.8. We recall that \mathbf{A} is determined by a polynomial of the form $L(X)X^k$ or $L(X)X^{k'}$ with $L(X) = \sum_{i=0}^{m-1} X^{2^i}$ and $1 < m < n$ and m, n are both odd. The assertion about the kernel follows from Lemma 4.3 and Lemma 4.4 shows the existence of the collineations $\tau_{1,1,\alpha}$. We now know $\mathcal{G} = N_{G_{\infty,0}}(S) = Z\{\tau_{1,1,\alpha} \mid \alpha \in \text{Aut}(F)\}$ by Lemma 4.5. By (a) of Lemma 4.9 and Lemma 4.7 \mathbf{A} is not a semifield plane. In view of Proposition 4.6 it remains to show that there exists no $T \in G$ interchanging $V(0)$ and $V(\infty)$.

Assume the converse. We may adjust T by an element from Z so that T fixes $V(1)$. As T normalizes S it has the form $T(x, y) = (T_s(a)y, T_t(b)x)$ and therefore $T_t(b)LT_s(a)^{-1} = L^{-1}$ contradicting Lemma 4.2 and Lemma 4.9 (b). \square

Using the notation of section 3 for polynomials of type II we have:

Theorem 4.10 *Let \mathbf{A} be a plane of type II and let $c_i, d_i, L(X), \ell$ have the meaning of Theorem 3.3. Then the kernel is isomorphic to $F_{(\ell, d_1)}$ and $\mathcal{K} = \{\tau_{a,a,1} \mid a \in F_{(\ell, d_1)}^*\}$ is the group of kern homologies. Moreover $G = G_{0,\infty}$ and $G/Z\mathcal{K}$ is isomorphic to the group of all $\alpha \in \text{Aut}(F)$ such that there exists an $a \in F_{d_1}$ with $c_i^{\alpha-1} = ab^{-1}$ for $b = a^{2^\ell} c_0^{1-\alpha}$ and all $1 \leq i \leq h$.*

We need two lemmas. Let d be a divisor of n . Use the notation of section 2 and define $\widehat{T}_{n:d}(x) = T_{n:d}(x) + x$. Then we have:

Lemma 4.11 *Let $e \mid d \mid n$ such that n/e is odd. Let $a \in F_d, b \in F_e$.*

$$(a) \widehat{T}_{n:d}(b\widehat{T}_{n:e}(x)) = b\widehat{T}_{n:d}(x)$$

$$(b) \widehat{T}_{n:e}(a\widehat{T}_{n:d}(x)) = a\widehat{T}_{n:d}(x)$$

Proof. (a) $\widehat{T}_{n:d}(b\widehat{T}_{n:e}(x)) = T_{n:d}(bT_{n:e}(x) + bx) + b\widehat{T}_{n:e}(x) = bT_{n:e}(x) + bT_{n:d}(x) + b\widehat{T}_{n:e}(x) = b\widehat{T}_{n:d}(x)$.

(b) As $T_{n:e}(ax) = T_{d:e}(aT_{n:d}(x))$ we have:

$$\begin{aligned} \widehat{T}_{n:e}(a\widehat{T}_{n:d}(x)) &= T_{n:e}(aT_{n:d}(x) + ax) + a\widehat{T}_{n:d}(x) \\ &= T_{d:e}(aT_{n:d}(x)) + T_{n:e}(ax) + a\widehat{T}_{n:d}(x) \\ &= a\widehat{T}_{n:d}(x) \end{aligned}$$

\square

Lemma 4.12 *Let $c_i, d_i, L(X), \ell$ have the meaning of Theorem 3.3. Then the operator defined by $L(X)$ can be written in the form $L(x) = \sum_{i=1}^h c_i \widehat{T}_{n:d_i}(x) + c_0 T_{n:d_1}(x)^{2^\ell}$. Let $L^{-1}(X)$ be the additive permutation polynomial defined by the inverse of L . Then L^{-1} acts as*

$$L^{-1}(x) = \sum_{i=1}^h f_i \widehat{T}_{n:d_i}(x) + f_0 T_{n:d_1}(x)^{2^{d_1-\ell}}$$

with $f_i \in F_{d_i}$ and $f_0 = c_0^{-1}, f_1 = c_1^{-1}$.

Proof. The first assertion is obvious. For the second assertion we induct on h .

Case $h = 1$. Set $L'(x) = c_1^{-1} \widehat{T}_{n:d_1}(x) + c_0^{-1} T_{n:d_1}(x)^{2^{d_1-\ell}}$. Then by Lemma 4.11

$$\begin{aligned} L(L'(x)) &= c_1 \widehat{T}_{n:d_1}(c_1^{-1} \widehat{T}_{n:d_1}(x) + c_0^{-1} T_{n:d_1}(x)^{2^{d_1-\ell}}) \\ &\quad + c_0 T_{n:d_1}(c_1^{-1} \widehat{T}_{n:d_1}(x) + c_0^{-1} T_{n:d_1}(x)^{2^{d_1-\ell}})^{2^\ell} \\ &= \widehat{T}_{n:d_1}(x) + 0 + 0 + T_{n:d_1}(x) = x \end{aligned}$$

Hence $L' = L^{-1}$.

Case $h > 1$. Set $L_1(x) = L(x) + c_h \widehat{T}_{n:d_h}(x)$. By induction there exist $f_0 = c_0^{-1}, f_1 = c_1^{-1}, f_2, \dots, f_{h-1}$, with $f_i \in F_{d_i}$, such that

$$L_1^{-1}(x) = \sum_{i=1}^{h-1} f_i \widehat{T}_{n:d_i}(x) + f_0 T_{n:d_1}(x)^{2^{d_1-\ell}}$$

We set $L'(x) = L_1^{-1}(x) + f_h \widehat{T}_{n:d_h}(x)$ with a $f_h \in F_{d_h}$ which will be determined later. Then

$$\begin{aligned} L(L'(x)) &= L_1(L_1^{-1}(x) + f_h \widehat{T}_{n:d_h}(x)) + c_h \widehat{T}_{n:d_h}(L_1^{-1}(x) + f_h \widehat{T}_{n:d_h}(x)) \\ &= x + L_1(f_h \widehat{T}_{n:d_h}(x)) + c_h \widehat{T}_{n:d_h}((L_1^{-1}(x)) + c_h f_h \widehat{T}_{n:d_h}(x)). \end{aligned}$$

By Lemma 4.11

$$\begin{aligned} L_1(f_h \widehat{T}_{n:d_h}(x)) &= \sum_{i=1}^{h-1} c_i \widehat{T}_{n:d_i}(f_h \widehat{T}_{n:d_h}(x)) + c_0 T_{n:d_1}(f_h \widehat{T}_{n:d_h}(x))^{2^\ell} \\ &= \sum_{i=1}^{h-1} c_i f_h \widehat{T}_{n:d_h}(x) \end{aligned}$$

as

$$T_{n:d_1}(f_h \widehat{T}_{n:d_h}(x))^{2^\ell} = \widehat{T}_{n:d_1}(f_h \widehat{T}_{n:d_h}(x))^{2^\ell} + f_h \widehat{T}_{n:d_h}(x)^{2^\ell} = 0.$$

Moreover

$$\begin{aligned} c_h \widehat{T}_{n:d_h}((L_1^{-1}(x))) &= c_h \sum_{i=1}^{h-1} \widehat{T}_{n:d_h}(f_i \widehat{T}_{n:d_i}(x)) + c_h \widehat{T}_{n:d_h}(f_0 T_{n:d_1}(x))^{2^{d_1-\ell}} \\ &= \sum_{i=1}^{h-1} c_h f_i \widehat{T}_{n:d_h}(x) \end{aligned}$$

as again $\widehat{T}_{n:d_h}(T_{n:d_1}(x)) = 0$. Therefore

$$L(L'(x)) = x + (f_h \sum_{i=1}^h c_i + c_h \sum_{i=1}^{h-1} f_i) \widehat{T}_{n:d_h}(x).$$

Define

$$f_h := \frac{c_h \sum_{i=1}^{h-1} f_i}{\sum_{i=1}^h c_i}.$$

Then $L^{-1} = L'$. □

Remark Using induction and the formula of the proof we see that all f_i 's are nontrivial and that $\sum_{j=1}^i f_j \neq 0$ for all $1 \leq i \leq h$.

Proof of Theorem 4.10. It follows immediately from the definition of the polynomials of type II that $L(X)$ can be written as $\sum_{i=0}^{n-1} a_i X^{2^i}$ with

$$a_i = \begin{cases} c_0, & i \equiv \ell \pmod{d_1}, \\ c_1 + \cdots + c_s, & 0 < i, d_s | i, d_{s+1} \nmid i, \\ 0, & \text{otherwise.} \end{cases}$$

From Lemma 4.3 we deduce that the kernel is isomorphic to $F_{(\ell, d_1)}$. It is then clear that the group \mathcal{K} are the kern homologies.

Claim. Equivalent are:

- (a) $\tau_{a,b,\alpha} \in \mathcal{A}$.
- (b) $a, b \in F_{d_1}$, $b = a^{2^\ell} c_0^{1-\alpha}$, and $c_i^{\alpha-1} = ab^{-1}$ for all $1 \leq i \leq h$.

Assume (a). By Lemma 4.4 and Lemma 4.5 we have $a_i^\alpha a^{-2^i} b = a_i$ for $0 \leq i < n$. In particular as $a_i = c_0$ for $i = d_1 j + \ell$, $0 \leq j < d_1$, we have

$$a^{2^{d_1 j + \ell}} b^{-1} = c_0^{\alpha-1}.$$

This shows $a \in F_{d_1}$ and $b = a^{2^\ell} c_0^{1-\alpha}$. As $a_{d_s} = c_1 + \cdots + c_s$ we get $c_1^\alpha + \cdots + c_s^\alpha = (c_1 + \cdots + c_s) a^{2^{d_s}} b^{-1} = (c_1 + \cdots + c_s) ab^{-1}$ and the last assertion of (b) follows by induction on s . Starting with (b) similar computations show that then $\tau_{a,b,\alpha}$ is a collineation of \mathbf{A} .

At this point we know by Lemma 4.5 and Proposition 4.6 that $G_{0,\infty}$ has the desired form. From Lemma 4.12 we deduce that \mathbf{A} is not a semifield plane. Finally if there exist $T \in G - G_{0,\infty}$ we can assume as usual that $T(x, y) = (T_t(b)y, T_s(a)x)$ which would imply by Lemma 4.2 that $\text{spi}(L^{-1}) = \{i + r \mid i \in \text{spi}(L)\}$, where $r = s - t$. But this contradicts Lemma 4.12. □

5 Isomorphisms

In this section we consider isomorphisms between planes defined by permutation polynomials of section 3 and we show that these planes are not isomorphic to previously known nearly flag transitive planes. Often an isomorphism between two planes can not occur as the automorphism groups differ. In the remaining case an isomorphism $\phi : \mathbf{A} \rightarrow \mathbf{A}'$ is a $\text{GF}(2)$ -linear map on W which maps the associated spread \mathcal{S} onto the spread \mathcal{S}' . Clearly, ϕ fixes the 2-set $\{V(0), V(\infty)\}$ and normalizes the Sylow \bar{p} -subgroup S . Using the action of the group Z we may assume in addition that $V(L)\phi = V(L')$, where the additive polynomials $L(X)$ and $L'(X)$ determine \mathbf{A} and \mathbf{A}' respectively.

We first consider polynomials (planes) of type I. We write $\mathbf{A} = \mathbf{A}_{n,m}$ if \mathbf{A} has order 2^n and \mathbf{A} is defined by $L(X)X^k$ with $L(X) = X + X^2 + \dots + X^{2^m-1}$ and $k = 2^{n-1} - 2^{m-1} - 1$. We write $\mathbf{A} = \mathbf{A}_{n,m}^*$ if \mathbf{A} is defined by $L(X)X^{k'}$.

Theorem 5.1 *For planes of type I the following hold.*

- (a) $\mathbf{A}_{n,m} \simeq \mathbf{A}_{n,m'}$ or $\mathbf{A}_{n,m}^* \simeq \mathbf{A}_{n,m'}^*$ iff $m = m'$.
- (b) $\mathbf{A}_{n,m} \not\simeq \mathbf{A}_{n,m'}^*$ for all m, m' .

Proof. As explained before we can assume that an isomorphism $\phi : \mathbf{A} \rightarrow \mathbf{A}'$ of planes of type I normalizes S . Thus it has the form $\phi(x, y) = (T_s(a)x, T_t(b)y)$ or $= (T_s(a)y, T_t(b)x)$, and we can assume $L' = T_t(b)LT_s(a)^{-1}$ or $L' = T_t(b)L^{-1}T_s(a)^{-1}$. Assertion (a) follows immediately from Lemma 4.2 and Lemma 4.9. If $\mathbf{A} = \mathbf{A}_{n,m} \simeq \mathbf{A}_{n,m'}^* = \mathbf{A}'$ then by Lemma 4.2 and Lemma 4.9 the isomorphism has the first type and $m = m'$. But then Z has at the same time action (A_k) as well as action $(A_{k'})$ which is impossible. \square

We turn now to planes of type II. Such a plane is determined by the following parameters: a number n , two sequences $\underline{c}_h = (c_0, \dots, c_h)$, $\underline{d}_h = (d_1, \dots, d_h)$, and a number $1 < \ell < d_1$ which satisfy the conditions of Theorem 3.3. We denote the associated plane by $\mathbf{A}_{n, \underline{c}_h, \underline{d}_h, \ell}$. By Lemma 4.12 and the remark afterwards the polynomial $L^{-1}(X)$ defines a plane with parameters $n, \underline{f}_h, \underline{d}_h, d_1 - \ell$. We call these parameters *inverse* to the parameters $n, \underline{c}_h, \underline{d}_h, \ell$. Interchanging the roles of $V(0)$ and $V(\infty)$ defines the same plane but $L^{-1}(X)$ takes the role of $L(X)$. Hence

$$\mathbf{A}_{n, \underline{c}_h, \underline{d}_h, \ell} \simeq \mathbf{A}_{n, \underline{f}_h, \underline{d}_h, d_1 - \ell}.$$

Using this notation we obtain.

Theorem 5.2 *Assume $\mathbf{A}_{n, \underline{c}_h, \underline{d}_h, \ell} \simeq \mathbf{A}_{n, \underline{c}'_h, \underline{d}'_h, \ell'}$ (for planes of type II). Then $h = h'$, $\underline{d}_h = \underline{d}'_h$ and there exist $\alpha \in \text{Aut}(F_n)$ and $a \in F_0^*$ such that one of the following hold.*

- (a) $\ell' = \ell$ and $c'_i = c_i^\alpha ab^{-1}$ for $b = a^{2^\ell} c'_0 c_0^{-\alpha}$ and $1 \leq i \leq h$.
- (b) $\ell' = d_1 - \ell$ and $c'_i = f_i^\alpha ab^{-1}$ for $b = a^{d_1 - 2^\ell} c'_0 f_0^{-\alpha}$ and $1 \leq i \leq h$ where $(\underline{f}_h, d_1 - \ell)$ is inverse to (\underline{c}_h, ℓ) .

We use

Lemma 5.3 *Let $T \in \text{GL}(W)$ be of the form $T(x, y) = (T_s(a)y, T_t(b)x)$ and assume that T normalizes S . Then $s = t$.*

Proof of Lemma 5.3. Assume $T\mu_c = \mu_c^m T$ for $\mu_c \in S$ and some number m . Since $k = 1$, $T\mu_c(x, y) = (ac^{2^s}y^{2^s}, bc^{-2^t}x^{2^t})$ and $\mu_c^m T(x, y) = (ac^{-m}y^{2^s}, bc^m x^{2^t})$ we see $c^{2^s} = c^{-m} = c^{2^t}$. \square

Proof of Theorem 5.2. Let $\phi : \mathbf{A} = \mathbf{A}_{n, \underline{c}_h, \underline{d}_h, \ell} \rightarrow \mathbf{A}' = \mathbf{A}_{n, \underline{c}'_{h'}, \underline{d}'_{h'}, \ell'}$ be an isomorphism. Again we can assume that ϕ normalizes S and maps $V(L)$ onto $V(L')$ (where $L(X)$ is associated with \mathbf{A} and $L'(X)$ is associated with \mathbf{A}'). By Lemma 5.3 ϕ has the form $\phi(x, y) = (T_s(a)x, T_s(b)y)$ or $(T_s(a)y, T_s(b)x)$, i.e. $L' = T_s(b)LT_s(a)^{-1}$ or $L' = T_s(b)L^{-1}T_s(a)^{-1}$.

Assume first that ϕ fixes $V(0)$ and $V(\infty)$. The same computation as in Lemma 4.5 shows

$$a_i^{2^s} a^{-2^i} b = a'_i, \quad 0 \leq i < n,$$

where $L(X) = \sum_i a_i X^{2^i}$ and $L'(X) = \sum_i a'_i X^{2^i}$. The first nonvanishing coefficient in $L(X)$ ($L'(X)$) is $a_\ell = c_0$ ($a'_{\ell'} = c'_0$). This implies $\ell = \ell'$ and $c_0^{2^s} a^{-2^\ell} b = c'_0$. The second nonvanishing coefficient in $L(X)$ ($L'(X)$) is $a_{d_1} = c_1$ ($a'_{d'_1} = c'_1$) implying $d_1 = d'_1$ and $c_1^{2^s} a^{-2^{d_1}} b = c'_1$. Moreover

$$c_0^{2^s} a^{-2^{j+d_1+\ell}} b = c'_0, \quad 0 \leq j < d_1; \quad c_1^{2^s} a^{-2^{i+d_1}} b = c'_1, \quad 0 < i < d_1.$$

Set $x^\alpha = x^{2^s}$. This together with an obvious induction gives assertion (a).

Assume now that ϕ interchanges $V(0)$ and $V(\infty)$. Let $L^{-1}(X) = \sum_i \bar{a}_i X^{2^i}$. A similar argument gives

$$\bar{a}_i^{2^s} a^{-2^i} b = a'_i, \quad 0 \leq i < n.$$

Assertion (b) follows in the same manner as the previous case. \square

Theorem 5.4 (a) *A plane of type I is not isomorphic to a plane of type II.*

(b) *A plane of type I or II is not isomorphic to generalized twisted field plane, a nearfield plane, a generalized André plane or a plane of Kantor Williams [18].*

Proof. (a) Assume that $\mathbf{A} \simeq \mathbf{A}'$ where \mathbf{A} has type I and \mathbf{A}' has type II. Let $\phi : \mathbf{A} \rightarrow \mathbf{A}'$. Since interchanging the roles of $V(0)$ and $V(\infty)$ for \mathbf{A}' just means that we replace a parameters (\underline{c}_h, ℓ) by the inverse parameters $(\underline{f}_h, d_1 - \ell)$ we may assume that ϕ fixes $V(0)$ and $V(\infty)$. As usual we conclude $\text{spi}(L) = \text{spi}(L')$ where the polynomial $L(X)$ ($L'(X)$) is associated to \mathbf{A} (\mathbf{A}'), a contradiction, since $0 \in \text{spi}(L) - \text{spi}(L')$.

(b) Let \mathbf{A} be of type I or II. From the structure of the automorphism groups (Theorems 4.8 and 4.10) we can rule out immediately that \mathbf{A} is a generalized twisted field plane or a nearfield plane. If however \mathbf{A} is isomorphic to a generalized André plane we see by [22, Thm. 11.7], or [8] that \mathbf{A} admits homologies of order \bar{p} with axis $V(\infty)$ and center (0) . That is in conflict with the structure of S .

Assume finally that \mathbf{A} is isomorphic to a plane of Kantor and Williams [18]. Then \mathbf{A} has a kernel of size > 2 . Therefore \mathbf{A} has type II, say $\mathbf{A} = \mathbf{A}_{n, \underline{c}_n, \underline{d}_n, \ell}$. Let \mathbf{A}' be a plane of order 2^n of [18]. Then this plane is described by a permutation polynomial $L'(X)X$ with

$$L'(X) = X + \sum_{i=1}^{h'} [c'_{i-1} T_{n:d'_i}(c'_{i-1}X) + c'_i T_{n:d'_i}(c'_iX)]$$

where $d'_{h'} | \cdots | d'_2 | d'_1 | n$, $n/d'_{h'}$ odd, and $c'_i \in F_{d'_i}^*$, $1 \leq i \leq h'$ ($c'_0 = 1$). As $1 + \sum_{i=1}^{h'} [(c'_{i-1})^2 + (c'_i)^2] = (c'_{h'})^2 \neq 0$ we see $0 \in \text{spi}(L') \subseteq \{i \mid d'_{h'} \mid i\}$. Assume $\phi : \mathbf{A} \rightarrow \mathbf{A}'$ is an isomorphism. We know that ϕ normalizes S and fixes the set $\{V(0), V(\infty)\}$. Again we deduce from Lemma 4.2 and Lemma 5.3 that $\text{spi}(L) = \text{spi}(L')$ or $\text{spi}(L^{-1}) = \text{spi}(L')$ where $L(X)$ is associated with \mathbf{A} . But this contradicts $0 \notin \text{spi}(L) \cup \text{spi}(L^{-1})$ (use Lemma 4.12). \square

6 Are the spreads symplectic?

The spreads defining the planes of Kantor and Williams [18] are symplectic. These planes are closely related to planes of type II: It can be shown (using the notation of Theorem 3.3) that if $L(X) = (1 + \sum_{i=1}^h c_i)X + \sum_{i=1}^h c_i T_{n:d_i}(X)$ the polynomial $L(X)X$ defines a permutation polynomial and the associated spread is symplectic. In fact with some additional work one can show that these planes are of Kantor and Williams type and vice versa every plane of Kantor and Williams type is defined by a polynomial as above. So the planes of type II can be considered as perturbations of the planes of Kantor and Williams. However, we will see they produce no longer symplectic spreads. We also will see that the planes of type I do not arise from symplectic spreads.

Lemma 6.1 *We use the notation of the previous sections.*

- (a) For all $0 \leq k < n$ and $b \in F$ we have $T_k(b)^* = T_{-k}(b^{2^{-k}})$.
- (b) Assume that the spread defined by the spread set $\{N(x) \mid x \in F\}$ is symplectic. Then $N(x)^*A = A^*N(x)$ for some $A \in \text{GL}_{\text{GF}(2)}(F)$ and all $x \in F$.

Proof. (a) follows from $T_{n:1}((T_k(b)x)y) = T_{n:1}(x(T_{-k}(b^{2^{-k}})y))$.

(b) We consider F as a vector space over the prime field. According to the theorem of Witt all non-degenerate symplectic bilinear forms on F^2 are

equivalent. Moreover

$$F^2 \times F^2 \ni ((u, w), (u_1, w_1)) \mapsto T_{n:1}(uw_1) - T_{n:1}(wu_1) \in \text{GF}(2)$$

is a nondegenerate symplectic bilinear form such that $V(0)$ and $V(\infty)$ are isotropic. Combining these facts it is easy to see that a nondegenerate symplectic form associated with the symplectic spread can be written in the form as

$$((u, w), (u_1, w_1)) = T_{n:1}((Au)w_1) - T_{n:1}(w(Au_1))$$

for some $A \in \text{GL}_{\text{GF}(2)}(F)$. Since for $u, w \in F$ the vectors $(u, N(x)u)$ and $(w, N(x)w)$ are perpendicular, an obvious computation shows that $N(x)^*A = A^*N(x)$ must hold. \square

Proposition 6.2 *A plane of type I is not isomorphic to the plane defined by the dual spread. In particular the spread is not symplectic.*

Proof. The proof is similar to the proof of Theorem 5.1. The spreadset defining a plane $\mathbf{A} = \mathbf{A}_{n,m}$ of type I has the form $\Sigma = \{N(x) \mid x \in F\}$, $N(x) = L_x = T_0(x^k)LT_0(x)$ with $L = \sum_{i=0}^{m-1} T_i(1)$ and m and k have their usual meaning. The spread set of the plane \mathbf{A}' defined by dual spread has the form $\Sigma^* = \{N(x)^* \mid x \in F\}$, $N(x)^* = T_0(x)L^*T_0(x^k)$. Assume that the two planes are isomorphic. As usual an isomorphism ϕ can be written as $\phi(x, y) = (T_s(a)x, T_t(b)y)$ or $= (T_t(b)y, T_s(a)x)$. But using Lemma 4.2 and Lemma 4.9 as in the proof of 5.1 we see that only the first case is possible. Adjusting ϕ with an element from Z we may assume that the fiber represented by $L = N(1)$ is mapped onto fiber represented by $L^* = N(1)^*$. Adjusting further with an element of the form $\tau_{1,1,\alpha}$ we may even assume $t = 0$. Hence

$$\sum_{i=0}^{m-1} T_{-i}(1) = L^* = T_0(b)LT_s(a)^{-1} = \sum_{i=0}^{m-1} T_{i-s}(ba^{-2^{i-s}}).$$

This shows $s = m - 1$ and $a = b = 1$. The group Z acting on \mathbf{A} is represented by the operators $\mu_c : (x, y) \mapsto (T_0(c^{-1})x, T_0(x^k)y)$ and acting on \mathbf{A}' the operation has the form $\hat{\mu}_c : (x, y) \mapsto (T_0(c^k)x, T_0(x^{-1})y)$ where $c \in F^*$. Now $\phi^{-1}\hat{\mu}_c\phi = \mu_{c'}$ where $c \mapsto c'$ is an automorphism of F^* . We compute

$$\phi^{-1}\hat{\mu}_c\phi(x, y) = (T_0(c^{k2^{m-1}})x, T_0(c^{-1})y).$$

Set $c = d^{-k'2^{1-m}}$. So that $\phi^{-1}\hat{\mu}_c\phi(x, y) = (T_0(d^{-1})x, T_0(d^{k'2^{1-m}})y)$ i.e. $c' = d$ and therefore $k \equiv k'2^{1-m} \pmod{2^n - 1}$. Multiplying with k we get $k^2 \equiv 1 \pmod{2^n - 1}$ which is false. The case that the plane is of the form $\mathbf{A}_{n,m}^*$ is handled similarly. \square

Remark The planes $\mathbf{A}_{n,m}$ and $\mathbf{A}_{n,m}^*$ are defined by spreads which are dual to each other: A typical element of the spread set of $\mathbf{A}_{n,m}$ has the form $N(x) = \sum_{i=0}^{m-1} T_i(x^{k+2^i})$. A computation shows $T_{m-1}(1)N(x)^* = \sum_{i=0}^{m-1} T_i(x^{2^{m-1}+k2^i})$. Define y by $y^{k'} = x^{2^{m-1}}$. Then $T_{m-1}(1)N(x)^* = \sum_{i=0}^{m-1} T_i(y^{k'+2^i})$ which is a typical element of the spread set associated with $\mathbf{A}_{n,m}^*$.

Proposition 6.3 *The spread defining a plane of type II is not symplectic.*

Proof. Let $\Sigma = \{N(x) \mid x \in F\}$ be a spread set defining a plane of type II and assume that Σ defines a symplectic spread. Then

$$N(x) = S_0(x) + S_1(x), \quad S_0(x) = \sum_{j=0}^{d_1-1} T_{jd_1+\ell}(c_0 x^{2^{jd_1+\ell}+1})$$

and

$$S_1(x) = \sum_{i=1}^h \sum_{j=0}^{d_i-1} T_{jd_i}(c_i x^{2^{jd_i}+1}).$$

From Lemma 6.1 we deduce

$$S_0(x)^* = \sum_{j=0}^{d_1-1} T_{jd_1-\ell}(c_0^{2^{-\ell}} x^{2^{jd_1-\ell}+1}), \quad S_1(x)^* = S_1(x).$$

Choose $A = \sum_{k=0}^{n-1} T_k(a_k)$ as in Lemma 6.1 and write the equation $N(x)^*A = A^*N(x)$ as $\sum_{s=0}^{n-1} T_s(b_s)$. We compute $N(x)^*A$ and $A^*N(x)$ explicitly and consider the term $T_s(b_s)$ for a fixed s . We obtain the equation

$$\sum_{j=0}^{d_1-1} u_j x^{2^{jd_1-\ell}+1} + \sum_{i=1}^h \sum_{j=0}^{d_i-1} u_{i,j} x^{2^{jd_i}+1} = \sum_{j=0}^{d_1-1} w_j x^{2^s+2^{s-jd_1-\ell}} + \sum_{i=1}^h \sum_{j=0}^{d_i-1} w_{i,j} x^{2^s+2^{s-jd_i}}$$

with $u_j = c_0^{2^{-\ell}} a_{s+\ell-jd_1}^{2^{jd_1-\ell}}$, $u_{i,j} = c_i a_{s-jd_i}^{2^{jd_i}}$, $w_j = c_0^{2^{s-jd_1-\ell}} a_{-s+jd_1+\ell}^{2^{s-jd_1-\ell}}$, and $w_{i,j} = c_i^{2^{s-jd_i}} a_{-s+jd_i}^{2^{s-jd_i}}$.

Let $s > 0$. We consider the exponents of x reduced modulo 2^n . The exponents occurring on the LHS have the form $2^{jd_1-\ell} + 1$ and $2^{jd_i} + 1$ and on the RHS we have exponents of the form $2^s + 2^{s-jd_1-\ell}$ and $2^s + 2^{s-jd_i}$.

We leave it to the reader to show that exponents of the form $2^{jd_1-\ell} + 1$ or $2^s + 2^{s-jd_1-\ell}$ occur just once. Since our equation holds for all $x \in F$ we obtain $a_{s+\ell-jd_1} = a_{-s+jd_1+\ell} = 0$ for $0 < s < n$ and $0 \leq j < d_1$, i.e. all a_i 's are 0, a contradiction. \square

References

- [1] M. Biliotti, V. Jha, N. Johnson: *Handbook of Finite Translation Planes*, CRC, 2007.
- [2] 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.
- [3] Stephen D. Cohen and Rex W. Matthews: Exceptional polynomials over finite fields, *Finite Fields Appl.*, 1(1995), 261-277.

- [4] P. Dembowski: *Finite Geometries*, Springer, 1968.
- [5] U. Dempwolff: A characterization of the generalized twisted field planes, *Archiv Math.* 50(1988), 477-480.
- [6] U. Dempwolff, P. Müller: Translation planes of odd order via Dembowski-Ostrom Polynomials, submitted to *Osaka J. Math.*.
- [7] J. F. Dillon and Hans Dobbertin: New cyclic difference sets with Singer parameters, *Finite Fields Appl.*, 10(2004), 342-389.
- [8] D. Foulser: A generalization of André's systems, *Math. Z.* 100(1967), 380-395.
- [9] M. Fried, R. Guralnick, J. Saxl: Schur covers and Carlitz's conjecture, *Israel J. Math.*, 83(1993), 157-225.
- [10] R. Guralnick, P. Müller: Exceptional polynomials of affine type, *J. Algebra* 194(1997), 429-454.
- [11] Robert M. Guralnick and Michael E. Zieve: Polynomials with $\text{PSL}(2)$ monodromy, *Ann. of Math. (2)*, 172(2010), 1315-1359.
- [12] R. Guralnick, J. Rosenberg, M. Zieve: A new family of exceptional polynomials in characteristic two, *Ann. of Math. (2)* 172(2010), 1361-1390.
- [13] C. Hering: Transitive linear groups and linear groups which contain irreducible subgroups of prime order I, *Geom. Ded.* 2(1974), 425-460.
- [14] C. Hering: Transitive linear groups and linear groups which contain irreducible subgroups of prime order II, *J. Algebra* 93(1985), 151-164.
- [15] B. Huppert: *Endliche Gruppen I*, Springer 1967.
- [16] D. Hughes, F. Piper: *Projective Planes*, Springer 1973.
- [17] V. Jha, N. Johnson: The planes of Suetake, *J. Geom.* 94(2009), 89-105.
- [18] W. Kantor, M. Williams: Nearly flag-transitive affine planes, *Advances in Geometry*, 10(2010), 161-183.
- [19] R. Lidl, G. L. Mullen, and G. Turnwald: *Dickson Polynomials*, volume 65 of *Pitman Monographs and Surveys in Pure and Applied Mathematics*. Longman, Essex, 1993.
- [20] Rudolf Lidl and Harald Niederreiter: *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997.
- [21] M. Liebeck: The affine permutation groups of rank three, *Proc. Lond. Math. Soc.* (3)54(1987), 477-516.

- [22] H. Lüneburg: *Translation Planes*, Springer 1980.
- [23] 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.
- [24] Michael Zieve: Bivariate factorizations via Galois theory, with application to exceptional polynomials, *J. Algebra*, 210(1998), 670-689.
- [25] K. Zsigmondy: Zur Theorie der Potenzreste, *Monatshefte Math. Phys.* 3(1892), 163-185.