PLANAR FUNCTIONS AND PLANES OF LENZ-BARLOTTI CLASS II

ROBERT S. COULTER AND REX W. MATTHEWS

Dedicated to Professor Lenz on the occasion of his 80th birthday

ABSTRACT. Planar functions were introduced by Dembowski and Ostrom ([4]) to describe projective planes possessing a collineation group with particular properties. Several classes of planar functions over a finite field are described, including a class whose associated affine planes are not translation planes or dual translation planes. This resolves in the negative a question posed in [4]. These planar functions define at least one such affine plane of order 3^e for every $e \geq 4$ and their projective closures are of Lenz-Barlotti type II. All previously known planes of type II are obtained by derivation or lifting. At least when e is odd, the planes described here cannot be obtained in this manner.

1. INTRODUCTION

The Lenz-Barlotti classification for projective planes has proved to be a useful focal point in discussing properties of projective planes. The 1957 classification by point-line transitivities was based on earlier work by Lenz and refinements by Barlotti. The question of the existence of a plane in each of the classes has been studied by many geometers but there are several classes for which this question remains unsettled. Dembowski in Chapter 3 of [3] gives a detailed description of the classification and outlines the theory behind it. Dembowski also gives a classification of projective planes with quasiregular collineation groups, see 4.2.10 of [3].

The Lenz-Barlotti type II planes are those which have either a single incident point-line transitivity (class II.1) or two point-line transitivities with one incident and one not (class II.2). The first class II planes to appear in the literature were the Ostrom-Rosati planes ([20]) which were later shown to coincide with the derived Hughes planes. Ostrom, through derivation of the dual Lüneburg planes, also provided the second class of examples in [21]. A third class was discovered in 1974 and at present there are eleven classes of type II planes known to the authors. The Hughes planes are type I.1. All other planes whose derivations are class II are duals of translation planes. A list of known suitable translation planes follows:

(i) Lüneburg planes
(ii) Walker planes ([14])
(iii) Kantor's likeable planes of characteristic 5 ([16])
(iv) Kantor's other likeable planes ([16])
(v) Biliotti-Menichetti planes ([1, 13])

1991 *Mathematics Subject Classification.* Primary 51E15, 11T06; Secondary 05B25.
Key words and phrases. planar functions, projective planes, permutation polynomials, finite fields.

(vi) Jha-Johnson planes ([10, 13])
(vii) Fisher flock planes ([12])
(viii) Cohen-Ganley semifield planes ([2, 13])
(ix) The translation planes of the Ree-Tits ovoid ([13])

A further class is Johnson's class II planes ([13]) obtained by the process of "lifting" then dualising (producing planes of order q^4). All derived planes have square order so all the above examples have square prime-power order. Further, all the planes obtained by derivation or lifting are class II.1, no II.2 examples currently being known. Some immediate questions arise from a consideration of the above list. Do all finite projective planes of Lenz-Barlotti class II have square order and are they all representable as derivations or liftings? A result of this paper establishes that this is not the case. In particular we present examples of class II planes of order 3^e for all $e \geq 4$. When e is odd (at least) such planes cannot be obtained by derivation or lifting. The construction of these planes is based on the concept of a *planar function*. Planar functions are also studied under the name of relative difference sets.

In [4] Dembowski and Ostrom considered projective planes of order n which contained a collineation group of order n^2. They introduced the following notion. Let G and H be arbitrary finite groups, written additively, but not necessarily commutative. A function $f : G \to H$ is called a *planar function* if for every non-identity $a \in G$ the functions $\Delta_{f,a} : x \mapsto f(a+x) - f(x)$ and $\nabla_{f,a} : x \mapsto -f(x) + f(x+a)$ are bijections.

Given groups G and H as above and a function $f : G \to H$, an incidence structure $I(G, H; f)$ may be defined as follows: "Points" are the elements of $G \times H$, "Lines" are the symbols $\mathcal{L}(a, b)$ with $a \in G$ and $b \in H$, together with the symbols $\mathcal{L}(c)$ with $c \in G$. Incidence is defined by

$$(x, y) \text{ I } \mathcal{L}(a, b) \text{ if and only if } y = f(x-a) + b; \text{ and}$$
$$(x, y) \text{ I } \mathcal{L}(c) \text{ if and only if } x = c.$$

From the above definitions Dembowski and Ostrom derived the following result.

Lemma 1.1 (Dembowski and Ostrom [4], Lemma 12)**.** *A function $f : G \to H$ is a planar function if and only if $I(G, H; f)$ is an affine plane.*

Moreover, the affine planes defined by planar functions have collineation groups with particular properties (see [4] for further details).

The situation in which most results on planar functions have been obtained is when $G = H = (\mathbb{F}_q, +)$ (throughout we use the following conventions: p is an odd prime, $q = p^e$, $\mathbb{F}_q$ denotes the finite field of order q, and $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$). In this case every function defined from $\mathbb{F}_q$ to itself may be obtained as the evaluation map of some polynomial and so the notion of a planar function may be extended to polynomials. A polynomial $f \in \mathbb{F}_q[X]$ is a *permutation polynomial* over $\mathbb{F}_q$ (PP) if it induces a permutation of $\mathbb{F}_q$. For each $a \in \mathbb{F}_q$, $a \neq 0$, we may define the *difference operator* Δ by $\Delta_{f,a}(X) = f(X+a) - f(X)$. Then f is called a *planar polynomial* over $\mathbb{F}_q$ if $\Delta_{f,a}(X)$ is a PP over $\mathbb{F}_q$ for each $a \in \mathbb{F}_q^*$. Any polynomial $f \in \mathbb{F}_q[X]$ may be reduced mod $X^q - X$ to yield a polynomial of degree less than q which induces on $\mathbb{F}_q$ the same function as f. We will call this the *reduced form* of f.

The classification of planar functions over fields of prime order was settled when in 1989 and 1990 three papers appeared ([7, 8, 22]). These independently showed

Des. Codes Cryptogr. 10 (1997), 167-184

that any planar polynomial over a prime field must reduce to a quadratic. This also established a conjecture of Kallaher ([15, page 145]) which suggested that any affine plane of prime order with a transitive collineation group was desarguesian (see [8] for details).

While most of the results obtained concerning planar functions have been limited to the case where $G = H = (\mathbb{F}_q, +)$ there have been several papers published dealing with the general case. A recent result of Hiramine ([9]) shows that a planar function which describes a semifield plane must have a particular shape, which is explicitly determined.

This paper splits logically into two parts. Sections 2 through 4 deal with algebraic questions, while the remaining sections are concerned with the associated geometries. Let f be a planar polynomial and L an additive polynomial. Then the planes generated by f and $f + L$ are isomorphic, as are those generated by $f(L)$ or $L(f)$ if L is a PP. We then consider a class of polynomials introduced in [4] (which we refer to as Dembowski-Ostrom polynomials) and show that they are precisely those f for which $\Delta_{f,a}(X)$ is additive for every $a \in \mathbb{F}_q^*$. Dembowski and Ostrom noted that any planar Dembowski-Ostrom polynomial produced a translation plane. We describe three such classes.

(i) $f(X) = X^2$, which gives the desarguesian plane over $\mathbb{F}_q$, q odd.
(ii) $f(X) = X^{p^\alpha+1}$ (already mentioned in [4]), which is planar over $\mathbb{F}_{p^e}$, p odd, if and only if $e/(\alpha, e)$ is odd.
(iii) $f(X) = X^{10} + X^6 - X^2$, which is planar over $\mathbb{F}_{3^e}$ if and only if $e = 2$ or e is odd.

It appears that all known planar Dembowski-Ostrom polynomials are equivalent to one of these types in the sense that they define isomorphic planes.

The question of whether all planar polynomials on a finite field are Dembowski-Ostrom polynomials was first posed in [4] and restated in various later papers. A principal result of this article is the description of a class of planar polynomials in characteristic 3 which are not Dembowski-Ostrom polynomials. An interesting feature of these polynomials is that their difference polynomials are Dickson polynomials of the first kind.

Turning to the geometry, we first discuss the problem of isomorphism of two planes described by different planar polynomials and also determine the set of mutually orthogonal Latin squares defined by a planar function.

The remainder of the paper deals with the existence of translation lines in the projective closure of an affine plane described by a planar function. Initially we shall deal with planar functions in the general setting, establishing that the projective plane contains a translation line if and only if the affine plane is a translation plane. We conclude by showing that the projective planes defined by the planar polynomials of Section 4 do not contain a translation line and hence must be Lenz-Barlotti type II.

2. Planar functions over finite fields

In the first part of this paper we shall deal with the algebraic aspects of planar polynomials over finite fields. Later sections will refer to specific classes of planar functions but initially we consider the general case.

Suppose $L : G \to H$, where G and H are finite groups as in Section 1. L is called *additive* on G if $L(x + y) = L(x) + L(y)$ for all $x, y \in G$ (i.e. L is a homomorphism

Des. Codes Cryptogr. 10 (1997), 167-184

of G into H). In the case where $G = H = (\mathbb{F}_q, +)$, G may be considered as a vector space over $\mathbb{F}_p$, and any additive function is an $\mathbb{F}_p$-linear transformation of $\mathbb{F}_q$ (we note that when the field of scalars has non-prime order this does not hold). Polynomials which induce an $\mathbb{F}_p$-linear transformation of $\mathbb{F}_q$ are known in the literature as *linearised polynomials*. There is an explicit description of such polynomials: their reduced form has the shape

$$L(X) = \sum_{i=0}^{e-1} a_i X^{p^i}$$

(recalling that $q = p^e$), where $a_i \in \mathbb{F}_q$.

Since the polynomials may always be considered to be reduced, we may assume that any additive polynomial has the above shape. A polynomial $L(X)+c$, where L is additive, is called an *affine* polynomial. Such polynomials have been thoroughly studied and their more detailed properties may be found in [18, pages 107-124]. The following result is well known (for example, see [18, Theorem 7.9].

Lemma 2.1. *Let $L \in \mathbb{F}_q[X]$ be defined by*

$$L(X) = \sum_{i=0}^{e-1} a_i X^{p^i}.$$

Then L is a PP over $\mathbb{F}_q$ if and only if L has no roots in $\mathbb{F}_q$ other than 0.

The relevance of additive polynomials in the current context is that the planarity property of a polynomial is preserved by composition with an additive polynomial. The following lemma may be established by a direct computation.

Lemma 2.2. *If L is an additive polynomial over $\mathbb{F}_q$ then $\Delta_{f,L(a)}(L(X)) = \Delta_{f(L),a}(X)$.*

It follows immediately from the definition of an additive function that if f is planar over $\mathbb{F}_q$ and L is additive on $\mathbb{F}_q$ then $f + L$ is planar over $\mathbb{F}_q$. Other connections between these classes of polynomials are described in the following result.

Theorem 2.3. *Let $f \in \mathbb{F}_q[X]$ and let $L \in \mathbb{F}_q[X]$ be an additive polynomial. Then the following are equivalent.*

(i) *$f(L)$ is a planar polynomial.*
(ii) *$L(f)$ is a planar polynomial.*
(iii) *f is a planar polynomial and L is a permutation polynomial.*

Proof. Consider the polynomial $\Delta_{L(f),a}(X)$. Then

$$\begin{aligned}\Delta_{L(f),a}(X) &= L(f(X+a)) - L(f(X))\\ &= L(f(X+a) - f(X))\\ &= L(\Delta_{f,a}(X)). \qquad (1)\end{aligned}$$

If $L(f)$ is a planar polynomial then $\Delta_{L(f),a}$ is a permutation polynomial over $\mathbb{F}_q$ for all $a \in \mathbb{F}_q^*$. Hence from (1) the additive polynomial L is a permutation polynomial and f is a planar polynomial. Thus (ii) $\Rightarrow$ (iii). Conversely, if (iii) holds then clearly (1) implies $L(f)$ is planar. Hence (iii) $\Rightarrow$ (ii).

To show that (i) $\Rightarrow$ (iii) consider $f(L)$, and suppose $\Delta_{f(L),a}$ is a permutation polynomial over $\mathbb{F}_q$ for all $a \in \mathbb{F}_q^*$. By Lemma 2.2, $\Delta_{f,L(a)}(L(X))$ is a permutation polynomial over $\mathbb{F}_q$ for all $a \in \mathbb{F}_q^*$, and so L must be a permutation polynomial over $\mathbb{F}_q$. Hence $L(\mathbb{F}_q^*) = \mathbb{F}_q^*$. For any $b \in \mathbb{F}_q^*$ there exists $a \in \mathbb{F}_q^*$ such that $L(a) = b$.

Des. Codes Cryptogr. 10 (1997), 167-184

Consequently, for all $b \in \mathbb{F}_q^*$, $\Delta_{f,b}(X) = \Delta_{f,L(a)}(X)$ permutes $\mathbb{F}_q$ and f is planar over $\mathbb{F}_q$. The converse result (iii) $\Rightarrow$ (i) follows immediately from Lemma 2.2. □

From the definition it is immediate that the planarity property is preserved by linear transformations (i.e. if $f(X)$ is planar so is $\alpha f(\lambda X + \mu) + \beta$, with $\alpha, \lambda \neq 0$).

We conclude this section with some remarks on planar monomials. For any $a \in \mathbb{F}_q^*$ we have

$$(X+a)^n - X^n = a^n\big((X/a+1)^n - (X/a)^n\big),$$

so it is clear X^n is a planar polynomial over $\mathbb{F}_q$ if and only if $(X+1)^n - X^n$ is a PP over $\mathbb{F}_q$. Consequently X^n must also be a planar polynomial over $\mathbb{F}_p$. From the known classification of planar monomials over prime fields [7, 8, 11, 22], the condition $n \equiv 2 \pmod{p-1}$ must hold.

Proposition 2.4. *The polynomial X^n is planar over $\mathbb{F}_q$ if and only if $(X+1)^n - X^n$ is a PP over $\mathbb{F}_q$. Further, if X^n is a planar polynomial over $\mathbb{F}_q$ then $n \equiv 2 \pmod{p-1}$ and $(n, q-1) = 2$.*

Proof. It remains only to establish the final condition. Suppose X^n is planar over $\mathbb{F}_q$. Then there exists a unique $x \in \mathbb{F}_q$ such that $(x+1)^n = x^n$. Equivalently there exists a unique $y \in \mathbb{F}_q$ such that $y^n = 1$ and $y \neq 1$. Thus there are precisely two $y \in \mathbb{F}_q$ with $y^n = 1$ and so $(n, q-1) = 2$. □

In the case where q is prime, Proposition 2.4 was established by Johnson in [11]. In general, no necessary and sufficient conditions for X^n to be planar are known. The condition $n \equiv 2 \pmod{q-1}$ is sufficient but not necessary while the conditions of Proposition 2.4 are not sufficient.

3. Dembowski-Ostrom polynomials

In their seminal paper on planar functions ([4]) Dembowski and Ostrom described a class of polynomials which sometimes give rise to planar functions. We shall refer to these as Dembowski-Ostrom polynomials.

Definition 3.1. *Suppose $f \in \mathbb{F}_q[X]$. Then f is a Dembowski-Ostrom polynomial if the reduced form of f has the shape*

$$f(X) = \sum_{i,j=0}^{e-1} a_{ij} X^{p^i+p^j}.$$

Dembowski and Ostrom observed that if f is a Dembowski-Ostrom polynomial (in reduced form) whose coefficients a_{ij} satisfy the condition

$$\sum_{i,j=0}^{e-1} a_{ij}(x^{p^i}y^{p^j} + x^{p^j}y^{p^i}) = 0 \text{ if and only if } x = 0 \text{ or } y = 0. \quad (2)$$

then f is a planar polynomial. Dembowski and Ostrom asked whether, up to addition of an additive polynomial, every planar polynomial on $\mathbb{F}_q$ is a Dembowski-Ostrom polynomial. This was restated as a conjecture by Rónyai and Szönyi in [22]. In the next section we describe a class of planar polynomials which form counterexamples to this conjecture in characteristic 3.

Our next result characterises Dembowski-Ostrom polynomials as those (reduced) polynomials whose difference polynomials are all additive.

Theorem 3.2. *Let $f \in \mathbb{F}_q[X]$ with deg$(f) < q$. Then the following conditions are equivalent.*

(i) *$f = D + L + c$, where D is a Dembowski-Ostrom polynomial, L is an additive polynomial and $c \in \mathbb{F}_q$ is a constant.*

(ii) *For each $a \in \mathbb{F}_q^*$, $\Delta_{f,a} = L_a + c_a$ where L_a is an additive polynomial and $c_a \in \mathbb{F}_q$ is a constant (both depending on a).*

Proof. It is immediate from the definition of $\Delta_{f,a}$ and Definition 3.1 that (i) $\Rightarrow$ (ii). We show that (ii) $\Rightarrow$ (i). Let

$$f(X) = \sum_{i=0}^{q-1} c_i X^i$$

with some c_i non-zero. Then for each $x \in \mathbb{F}_q$,

$$\begin{aligned}\Delta_{f,a}(x) &= \sum_{i=0}^{q-1} c_i\big((x+a)^i - x^i\big)\\ &= \sum_{i=0}^{q-1} c_i\Big(\sum_{r=0}^{i-1}\binom{i}{r}x^r a^{i-r}\Big)\\ &= \sum_{r=0}^{q-2} x^r\Big(\sum_{i=r+1}^{q-1} c_i\binom{i}{r}a^{i-r}\Big).\end{aligned}$$

From (ii), whenever $r \neq 0$ and $r \neq p^k,\ k \geq 0$,

$$\sum_{i=r+1}^{q-1} c_i\binom{i}{r}a^{i-r} = 0$$

for each $a \in \mathbb{F}_q^*$. Thus under these conditions on r the polynomial

$$C_r(X) = \sum_{i=r+1}^{q-1} c_i\binom{i}{r}X^{i-r}$$

is identically 0. Then if $r \neq 0$ and $r \neq p^k$,

$$c_i\binom{i}{r} = 0 \tag{3}$$

for all i satisfying $r < i < q$, where $\binom{i}{r}$ is interpreted modulo p. Let $i = \sum_j \alpha_j p^j$ and $r = \sum_j \beta_j p^j$ be the base-p expansions of i and r. Then by Lucas' theorem $\binom{i}{r} \equiv 0 \bmod p$ if and only if $\alpha_j < \beta_j$ for some j. By choosing particular values of r in (3) we show that $c_i = 0$ unless $i = 0$, $i = p^k$ or $i = p^k + p^l$. Let $r = p^k + p^l$ with $k \geq l \geq 0$. Then r cannot be 0 or a power of p. There are two cases: either $k > l$ or $k = l$. Consider the case $k > l$. Then by (3), $c_i\binom{i}{r} = 0$ for all i satisfying $p^k + p^l < i < q$. For $p^k + p^l < i < p^k + p^{l+1}$ we have $\binom{i}{r} \neq 0$ by Lucas' theorem. Hence $c_i = 0$ for all i satisfying $p^k + p^l < i < p^k + p^{l+1}$ with $k > l \geq 0$. Now consider the case $k = l$. Once again Equation (3) holds for all i satisfying $2p^k < i < q$. For $2p^k < i < p^{k+1}$, we again apply Lucas' theorem to obtain $\binom{i}{r} \neq 0$ and hence $c_i = 0$

for all i such that $2p^k < i < p^{k+1}$. Rewriting f using the information gained from these two cases shows that

$$f(X) = \sum_{k \geq l \geq 0}^{e-1} c_{p^k+p^l} X^{p^k+p^l} + \sum_{k=0}^{e-1} c_k X^{p^k} + c_0$$

as required. □

A special class of Dembowski-Ostrom polynomials are the monomials of the shape $X^{p^\alpha+1}$ over $\mathbb{F}_q$. The following theorem describes necessary and sufficient conditions on α for $X^{p^\alpha+1}$ to be planar over $\mathbb{F}_q$.

Theorem 3.3. *Let $f(X) = X^{p^\alpha+1}$. Then f is planar over $\mathbb{F}_q$ if and only if $e/(\alpha, e)$ is odd.*

Proof. We need to determine when the affine polynomial $(X+1)^{p^\alpha+1} - X^{p^\alpha+1} = (X^{p^\alpha} + X + 1)$ is a permutation polynomial over $\mathbb{F}_q$. By Lemma 2.1 this holds if and only if $X^{p^\alpha} + X$ has precisely one root in $\mathbb{F}_q$, or equivalently $x^{p^\alpha-1} \neq -1$ for all $x \in \mathbb{F}_q^*$. Let ζ be a primitive element of $\mathbb{F}_q$. Then $\zeta^{i(p^\alpha-1)} \neq \zeta^{(q-1)/2}$ for any integer i. So $X^{p^\alpha+1}$ is planar over $\mathbb{F}_q$ if and only if the congruence

$$i(p^\alpha - 1) \equiv (p^e - 1)/2 \bmod p^e - 1$$

has no integer solution i. Now $iu \equiv v \bmod n$ has a solution i if and only if $(u, n) \mid v$. So we have no solution i if and only if $(p^\alpha - 1, p^e - 1) \not| \, (p^e - 1)/2$, or equivalently $p^{(\alpha,e)} - 1 \not| \, (p^e - 1)/2$. Let $d = (\alpha, e)$. Then there is no integer solution i if and only if the 2-order of $p^d - 1$ is greater than or equal to the 2-order of $p^e - 1$. But

$$p^e - 1 = (p^d - 1)(1 + p^d + p^{2d} + \ldots + p^{((e/d)-1)d})$$

and so this condition is equivalent to $e/(\alpha, e)$ being odd. □

We note that this result differs from that stated in [4]. There Dembowski and Ostrom claim that $X^{p^\alpha+1}$ is planar on $\mathbb{F}_q$ if and only if $\alpha = 0$ or $(\alpha, e) = 1$. However this is not an equivalent condition, as the polynomial X^{10} is planar over $\mathbb{F}_q$ with $q = 3^6$, since $6/(2, 6) = 3$ is odd, but $(2, 6) = 2 \neq 1$.

The condition (2) for a Dembowski-Ostrom polynomial to be planar mentioned above does not appear to be effective in searching for planar functions. Apart from those described in Theorem 3.3, there is another class of Dembowski-Ostrom polynomials whose planarity properties may be fully determined.

Theorem 3.4. *Let $f(X) = X^{10} + X^6 - X^2$. Then f is a Dembowski-Ostrom polynomial over $\mathbb{F}_{3^e}$ which is planar if and only if $e = 2$ or e is odd.*

Proof. Clearly $f(X)$ is a Dembowski-Ostrom polynomial. A direct calculation shows that $\Delta_{f,a}(X) = aX^9 - a^3X^3 + a(a^8 + 1)X + f(a)$. Then $\Delta_{f,a}(X)$ is a permutation polynomial if and only if the linearised polynomial $L_a(X) = X^9 - a^2X^3 + (a^8 + 1)X$ is a permutation polynomial. By Lemma 2.1 this is equivalent to the requirement that $L_a(X)$ has no non-zero root in $\mathbb{F}_q$. Let $i^2 = -1$, $i \in \mathbb{F}_{3^2}$. Then $L_a(X) = X\phi_{1,a}(X)\phi_{2,a}(X)$, where $\phi_{1,a}(X) = X^4 + ia^2X^2 + a^4 + i$, $\phi_{2,a}(X) = X^4 - ia^2X^2 + a^4 - i$. If $e = 2$ then f reduces to X^6 and so is planar. If e is odd then in $\mathbb{F}_{3^e}$, -1 is a non-square. If x is a non-zero root of L_a in $\mathbb{F}_{3^e}$ then $i = \pm(x^4 + a^4)/(a^2x^2 + 1)$. The denominator of this expression is non-zero, so we would deduce that $i \in \mathbb{F}_{3^e}$, a contradiction. Thus L_a does not possess a non-zero root and f is planar.

Des. Codes Cryptogr. 10 (1997), 167-184

If e is even, $e > 2$, we show that there exists $x, a \neq 0$ with $\phi_{1,a}(x) = 0$. Consider $\phi = \phi_{1,a}(X)$ as a bivariate polynomial in X, a. Then we claim that ϕ is absolutely irreducible. If $U = X^{-1}$, $V = aX^{-1}$, then ϕ may be written as $X^4(iU^4 + V^4 + iV^2 + 1)$, and so the absolute irreducibility of ϕ is equivalent to that of $\psi(U, V) = U^4 - i(V^4 + iV^2 + 1)$. Absolute irreducibility of polynomials with the shape $Y^d - cf(X)$ is discussed in [18]. There it is shown (Lemma 6.54) that such a polynomial is absolutely irreducible over $\mathbb{F}_q$ if $f(X)$ has no repeated factors (which holds in this case). An application of Theorem 6.57 of [18] (a form of Weil's theorem) shows that the number N of zeros of ψ in $\mathbb{F}_q$ is at least $q - 3^2 q^{1/2}$. If $q \geq 3^6$ then this guarantees the existence of a pair (x, a) with $\phi_{1,a}(x, a) = 0$, with neither x nor a equal to 0. Consequently f is not planar over $\mathbb{F}_q$. In $\mathbb{F}_{3^4}$ there exists a such that $a^8 + 1 = 0$. If x is chosen such that $x^3 = a$ then $L_a(x) = 0$, and so $f(X)$ is not planar. □

4. A new class of planar functions

To our knowledge all previously described planar polynomials defined over a finite field $(\mathbb{F}_q, +)$ are Dembowski-Ostrom polynomials (as defined in Definition 3.1). We now describe a class of planar function which are not of this type.

Theorem 4.1. *Let $q = 3^e$ and $\alpha \in \mathbb{N}$. Then the polynomial $X^{(3^\alpha+1)/2}$ is planar over $\mathbb{F}_q$ if and only if $(\alpha, e) = 1$ and α is odd.*

We have observed that the Dembowski-Ostrom polynomials f are precisely those whose difference functions $\Delta_{f,a}$ are additive. The difference polynomials which arise from the planar polynomials described here correspond to another well-known class of permutation polynomials, the Chebyshev (or Dickson) polynomials of the first kind. A recent book has appeared on this topic ([17]). The permutation behaviour of these polynomials is well understood, the first results being obtained by Dickson ([5]), with a complete description due to W. Nöbauer ([19], see also [17, 18]): $g_k(X)$ is a PP over $\mathbb{F}_q$ if and only if $(k, q^2 - 1) = 1$. Their explicit form may be obtained by recurrence: $g_0(X) = 2$, $g_1(X) = X$ and $g_{k+2}(X) = X g_{k+1}(X) - g_k(X)$ where $k \in \mathbb{N}$. A more useful representation for our purposes is the following: let $\eta \in \mathbb{F}_{q^2}$ be a root of the quadratic polynomial $Z^2 - xZ + 1$. Then $\eta^k + \eta^{-k}$ can be written as a polynomial in x $(= \eta + \eta^{-1})$ which coincides with $g_k(x)$. In other words $g_k(\eta + \eta^{-1}) = \eta^k + \eta^{-k}$. This representation is classical and is discussed, for example, in [17].

Proof of Theorem 4.1. Suppose $f(X) = X^n$ and define $h(X)$ to be $\Delta_{f,1}(X + 1) = (X - 1)^n - (X + 1)^n$ (in characteristic 3). Then $f(X)$ is planar over $\mathbb{F}_q$ if and only if $h(X)$ is a permutation polynomial over $\mathbb{F}_q$. If $x = \eta + \eta^{-1}$ then

$$\begin{aligned} h(x) &= (\eta + \eta^{-1} - 1)^n - (\eta + \eta^{-1} + 1)^n \\ &= \frac{(\eta^2 + 1 - \eta)^n - (\eta^2 + 1 + \eta)^n}{\eta^n} \\ &= \frac{(\eta + 1)^{2n} - (\eta - 1)^{2n}}{\eta^n}. \end{aligned}$$

If $n = (3^\alpha + 1)/2$, then

$$\begin{aligned} h(x) &= \frac{(\eta+1)^{3^\alpha+1} - (\eta-1)^{3^\alpha+1}}{\eta^{(3^\alpha+1)/2}} \\ &= \frac{2\eta + 2\eta^{3^\alpha}}{\eta^{(3^\alpha+1)/2}} \\ &= -(\eta^{(3^\alpha-1)/2} + \eta^{-(3^\alpha-1)/2}) \\ &= -g_{(3^\alpha-1)/2}(x). \end{aligned}$$

Thus X^n is planar over $\mathbb{F}_q$ if and only if the Chebyshev polynomial of the first kind, $g_{(3^\alpha-1)/2}(X)$, is a permutation polynomial over $\mathbb{F}_q$. A necessary and sufficient condition for this to occur ([19, Theorem 3.2]) is $((3^\alpha-1)/2, q^2-1) = 1$. Since $q^2 \equiv 1 \pmod 4$, this is equivalent to the condition $(3^\alpha - 1, 3^{2e} - 1) = (3^{(\alpha,2e)} - 1)$ $= 2$, which holds if and only if $(\alpha, 2e) = 1$. □

We note that if $f(X) = X^n$ ($n \not\equiv 2.3^k \pmod{q-1}$) is a planar monomial over $\mathbb{F}_q$ as described in Theorem 4.1, then f forms a counterexample to the conjecture mentioned in Section 3. Applications of Theorem 2.3 to such an f would also yield counterexamples to the conjecture.

A related class of planar polynomials are described by the following.

Theorem 4.2. *Let $q = 3^e$ and $n = (3^\alpha + q)/2$, where $\alpha \in \mathbb{N}$. Then the polynomial X^n is planar over $\mathbb{F}_q$ if and only if $(\alpha, e) = 1$ and $\alpha - e$ is odd.*

Proof. If $\alpha = e$ then $X^n = X^q$ is not planar over $\mathbb{F}_q$. If $\alpha > e$ then, replacing α by $\alpha - e$ in Theorem 4.1, we obtain the result that $h(X) = X^{(3^{\alpha-e}+1)/2}$ is planar over $\mathbb{F}_q$ if and only if $(\alpha - e, e) = (\alpha, e) = 1$ and $\alpha - e$ is odd. Since $X^n = (h(X))^{3^e}$, planarity of X^n is equivalent to planarity of $h(X)$. If $\alpha < e$, a similar argument shows that the planarity of X^n is equivalent to that of $g(X) = X^{(3^{e-\alpha}+1)/2}$, since $X^n = (g(X))^{3^\alpha}$. □

The following lemma will be required in Section 6.

Lemma 4.3. *Suppose $q = 3^e$. For each $\alpha \in \mathbb{N}$ define a function $f : \mathbb{F}_q \to \mathbb{F}_q$ by $f_\alpha(x) = x^{(3^\alpha+1)/2}$. Let S be the sequence of functions $\{f_0, f_1, \ldots\}$. Then S is periodic with period $2e$.*

Proof. Let $\alpha = 2\lambda e + \beta$ with $0 \le \beta < 2e$ and $\lambda > 0$. Suppose $x \in \mathbb{F}_q$. Then

$$\begin{aligned} x^{(3^\beta+1)/2} &= x^{(3^{\alpha-2\lambda e}+1)/2} \\ &= (x^{(3^{\alpha-2\lambda e}+1)/2})^{3^{2\lambda e}} \\ &= x^{(3^\alpha+3^{2\lambda e})/2} \\ &= x^{(3^{2\lambda e}-1)/2} x^{(3^\alpha+1)/2} \\ &= x^{(q^\lambda-1)(q^\lambda+1)/2}\, x^{(3^\alpha+1)/2} \\ &= x^{(3^\alpha+1)/2}. \end{aligned}$$

□

5. Planes defined by planar functions

We turn now to the geometric aspects of the results established in the first part of the paper. We begin with a discussion of some isomorphic classes of planes described by different planar polynomials defined over the same finite field. Properties of affine and projective planes defined by planar functions are then considered with particular emphasis on the problem of the existence of a translation line in a plane defined by a planar function.

Two planes Π_1 and Π_2 are isomorphic if and only if there exists a bijection ϕ of the points of Π_1 onto the points of Π_2 mapping lines of Π_1 onto lines of Π_2 and preserving incidence. We denote "is isomorphic to" by $\Pi_1 \approx \Pi_2$ and call ϕ an isomorphism.

The connection with additive polynomials discussed in Section 2 leads to the following two results.

Theorem 5.1. *Let f be a planar polynomial and L an additive polynomial, both defined over $\mathbb{F}_q$. Then $I(\mathbb{F}_q, \mathbb{F}_q; f) \approx I(\mathbb{F}_q, \mathbb{F}_q; f + L)$.*

Proof. Let $\phi : \mathbb{F}_q \times \mathbb{F}_q \to \mathbb{F}_q \times \mathbb{F}_q$ be the bijection defined by $\phi(x, y) = (x, y+L(x))$. If (x, y) lies on the line $\mathcal{L}_f(a, b)$ then it may be verified by an elementary calculation that $\phi(x, y)$ lies on the line $\mathcal{L}'_{f+L}(a, b + L(a))$. Further ϕ maps $\mathcal{L}_f(c)$ to $\mathcal{L}'_f(c)$. Consequently $I(f) \approx I(f + L)$. □

Theorem 5.2. *Let f be a planar polynomial and let L be an additive permutation polynomial, both defined over $\mathbb{F}_q$. Then*

$$I(\mathbb{F}_q, \mathbb{F}_q; f) \approx I(\mathbb{F}_q, \mathbb{F}_q; f(L)) \approx I(\mathbb{F}_q, \mathbb{F}_q; L(f)).$$

Proof. Consider the bijection from $I(f)$ to $I(f(L))$ defined by $\phi(x, y) = (L^{-1}(x), y)$. We claim that ϕ maps $\mathcal{L}_f(a, b)$ to $\mathcal{L}'_{f(L)}(L^{-1}(a), b)$. Suppose that (x, y) lies on $\mathcal{L}_f(a, b)$. Then

$$\begin{aligned} f\Big(L\big(L^{-1}(x) - L^{-1}(a)\big)\Big) + b &= f\Big(L\big(L^{-1}(x)\big) - L\big(L^{-1}(a)\big)\Big) + b \\ &= f(x - a) + b = y. \end{aligned}$$

Consequently the point $\phi(x, y) = (L^{-1}(x), y)$ lies on the line $\mathcal{L}'_{f(L)}(L^{-1}(a), b)$. The image of $\mathcal{L}(c)$ is $\mathcal{L}'(L^{-1}(c))$, and so $I(\mathbb{F}_q, \mathbb{F}_q; f) \approx I(\mathbb{F}_q, \mathbb{F}_q; f(L))$. A similar argument shows that the bijection $\psi : (\mathbb{F}_q, \mathbb{F}_q; f) \approx I(\mathbb{F}_q, \mathbb{F}_q; L(f))$ defined by $\psi(x, y) = (x, L(y))$ defines a collineation. □

Thus constructing new planar polynomials by adding an additive polynomial or by composing with additive permutation polynomials does not alter the associated affine plane.

It is well known that every projective plane is equivalent to a maximal set of mutually orthogonal latin squares (MOLS). For the next result we return to the general setting where G and H are additively written groups (but not necessarily commutative) and provide a description for a set of MOLS which is associated with a planar function.

Theorem 5.3. *Let G and H be finite groups of order n written additively, but not necessarily commutative, and let $f : G \to H$ be a planar function. For each*

$a \in G,\ a \neq 0,$ *define a function* $L_a : G \times H \to H$ *by*

$$L_a(x, y) = -f(x - a) + f(x) + y.$$

Then each L_a *defines a latin square of order* n *and the set* $\{L_a \mid a \in G,\ a \neq 0\}$ *forms a maximal set of* $n - 1$ *mutually orthogonal latin squares.*

Proof. It may be checked directly from the definition that the functions L_a define a set of MOLS. The formula for L_a given above may also be derived from the usual process of obtaining a set of MOLS from an affine plane, where the coordinatising sets of parallel lines are taken to be $\{\mathcal{L}(c) : c \in G\}$ and $\{\mathcal{L}(0, b) : b \in H\}$. This shows that the set of MOLS described does in fact represent the affine plane defined by f. □

The full collineation group $Aut(P(g))$ of the projective extension $P(f)$ of $I(G, H; f)$ contains the subgroup

$$\begin{aligned}\Gamma = \{\phi_{(u,v)} : (x, y) \to (x + u, y + v) \text{ for all } (x, y) \in G \times H \mid (u, v) \in G \times H\}\\ \approx G \times H,\end{aligned} \tag{4}$$

a group of order $|G|^2$ acting sharply transitively on $I(G, H; f)$ ([4]). In its action on $P(f)$, Γ has three orbits, I, $\{(\infty)\}$, and $\mathcal{L}_\infty \backslash \{(\infty)\}$.

When q is not prime and f is defined over a subfield of $\mathbb{F}_q$, the Frobenius automorphism also generates a cyclic collineation group $\mathcal{C}_F$ of $I(\mathbb{F}_q, \mathbb{F}_q; f)$. If f is defined over $\mathbb{F}_p$, then $\mathcal{C}_F$ has order e (with $q = p^e$). In this case Frobenius acts on $\mathbb{F}_q \times \mathbb{F}_q$ by mapping (x, y) to (x^p, y^p), $\mathcal{L}(c)$ maps to $\mathcal{L}(c^p)$ and $\mathcal{L}(a, b)$ maps to $\mathcal{L}(a^p, b^p)$. In the special case that $f(X) = X^n$, a further group of collineations (cyclic of order $q - 1$) is defined by the maps $\phi_\alpha(x, y) = (\alpha x, \alpha^n y)$ (with $\alpha \neq 0$).

A useful approach to the study of projective planes is their coordinatisation by an algebraic structure. We give a brief indication of the approach - a more detailed account may be found in [15].

Let $\mathcal{R}$ be a set with the same cardinality as a line in the projective plane we wish to coordinatise. Coordinatisation produces a ternary operation $T(x, a, b)$ in $\mathcal{R}$ which satisfies certain algebraic properties. Any set $\mathcal{R}$ with such a ternary operation is called a *planar ternary ring*. Addition and multiplication in $\mathcal{R}$ are defined by $a + b = T(a, 1, b)$ and $ab = T(a, b, 0)$ (here the element 1 is determined by the coordinatisation). With respect to addition, $\mathcal{R}$ is a loop with identity 0, while the set $\mathcal{R} \backslash \{0\}$ is a loop with respect to multiplication with identity 1. A planar ternary ring is *linear* if it satisfies $T(x, a, b) = xa + b$ for all $x, a, b \in \mathcal{R}$. A linear ternary ring is called a *cartesian group* if its additive loop is associative and thus a group. A *quasifield* is a cartesian group $\mathcal{R}$ satisfying $(x + y)z = xz + yz$ for all $x, y, z \in \mathcal{R}$, while a *semifield* is a quasifield satisfying the extra condition $x(y + z) = xy + xz$ for all $x, y, z \in \mathcal{R}$.

In [4], Dembowski and Ostrom introduce the notion of a planar function f *normed* with respect to some element $a \in G \setminus \{0\}$. By this it is meant that $f(0) = f(a) = 0$. If g is a planar function on G then for any non-zero $a \in G$ there exists a unique line in $I(G, H; g)$ which contains the points $(0, 0)$ and $(a, 0)$ and this must be of the form $\mathcal{L}(b, c)$. If $f(x) = g(x - b) + c$, then f is a planar function which is normed with respect to a, and $I(G, H; f) \approx I(G, H; g)$. We have the following result from [4].

Lemma 5.4 (Dembowski and Ostrom [4], Theorem 6)**.** *Let f be a normed planar function (with respect to some $a \in G$) from G to H, and define $Q_a : H \to G$ by $Q_a(c) = b$ if $\Delta_{f,a}(b) = c$. Define a multiplication on the set $\mathcal{R} = H$ by the rule*

$$x \cdot y = -f\big(Q_a(x)\big) + f\big(Q_a(x) + Q_a(y)\big) - f\big(Q_a(y)\big).$$

Then the set $\mathcal{R}$ with the original addition of H and this multiplication forms a cartesian group coordinatising $I(G, H; f)$.

Note that in the case where G and H are commutative, for example when $G = H = \mathbb{F}_q$, $x \cdot y = y \cdot x$ for all $x, y \in \mathcal{R}$. Thus if $\{\mathcal{R}, +, \cdot\}$ is a quasifield it must in fact be a semifield. A plane coordinatised by a quasifield is necessarily a translation plane.

We now consider properties of the projective closure of any affine plane described by a planar function. A line $\mathcal{L}$ in a projective plane P is called a *translation line* if the group of elations of P which fix $\mathcal{L}$ pointwise is transitive on the complement of $\mathcal{L}$ in P. If P contains a translation line then either P is desarguesian (in which case every line is a translation line) or the translation line is unique. Throughout this section we shall denote by $P(g)$ the projective closure of the affine plane $I(G, H; g)$, where g is a planar function and G and H are arbitrary finite groups written additively, but not necessarily commutative.

Our main result in this direction is to show that if $P(g)$ is non-desarguesian and contains a translation line then this line must be $\mathcal{L}_\infty$. We consider the lines $\mathcal{L}(a, b)$ and $\mathcal{L}(c)$ separately. Our next result depends on an observation on permutation groups and a theorem of Wagner.

Lemma 5.5. *Suppose that H, K are subgroups of a group G, all acting on a set X. If O_A, O_B are orbits of H, K respectively, with nonempty intersection, then $O_A \cup O_B$ is contained in an orbit of G.*

Theorem 5.6 (Wagner [23], Theorem 3)**.** *If a projective plane P has a transitive collineation group containing a non-trivial perspectivity then P is desarguesian.*

Theorem 5.7. *Let $a \in G$ and $b \in H$. Then the line $\mathcal{L}(a, b)$ in $P(g)$ is a translation line if and only if $P(g)$ is desarguesian.*

Proof. If $P(g)$ is desarguesian then all lines are translation lines. Suppose $\mathcal{L} = \mathcal{L}(a, b)$ is a translation line in $P(g)$ for some $a \in G$ and $b \in H$. The complement A of $\mathcal{L}$ in $P(g)$ is an orbit of the translation group of $\mathcal{L}$. The orbits of Γ (as defined by (4)) are $B = \{(\infty)\}$, $C = \mathcal{L}_\infty \backslash \{(\infty)\}$ and $D = P(g) \backslash \mathcal{L}_\infty$. Each of B, C and D has nonempty intersection with A, and so by Lemma 5.5 their union ($=P(g)$) is an orbit of $Aut(P(g))$. Thus $Aut(P(g))$ has a single orbit and so acts transitively on $P(g)$. Since the collineations $\phi_{(0,v)}$ of (4) are non-trivial perspectivities of $P(g)$, Wagner's Theorem (5.6) implies that $P(g)$ is desarguesian. □

We may also establish that no $\mathcal{L}(a, b)$ can be a translation line by appealing to the Lenz-Barlotti classification of projective planes.

Alternative proof of Theorem 5.7. Suppose $\mathcal{L}(a, b)$ is a translation line for particular $a \in G, b \in H$ and let $T = \{(p, \mathcal{L}) \mid P(g) \text{ is } (p, \mathcal{L})\text{-transitive}\}$. The Lenz-Barlotti types for projective planes are determined by such a set T, see [3, 3.1.20 and comments on page 125]. The only possible Lenz-Barlotti types for a projective plane containing a translation line are types IVa.1, IVa.2, V.1 or VII.2, from 3.1.20 and

Table 1, page 126, of [3]. The type VII.2 refers to the desarguesian plane. Our aim is to show that the other three types cannot arise. By assumption,

$$\{(p, \mathcal{L}(a,b)) \mid p \text{ I } \mathcal{L}(a,b)\} \cup \{((\infty), \mathcal{L}_\infty)\} \subseteq T.$$

For each of the Lenz-Barlotti types IVa.1, IVa.2 and V.1 the set T contains only point-line pairs $(p, \mathcal{L})$ for which the point p always lies on the translation line. Since $(\infty) \notin \mathcal{L}(a,b)$ the plane $P(g)$ can not be any of these types. Hence no line $\mathcal{L}(a,b)$ can be a translation line of $P(g)$ unless $P(g)$ is desarguesian. □

The possibility remains that some line $\mathcal{L}(c)$ may be a translation line when $P(g)$ is non-desarguesian. We eliminate this possibility. The proof is based on the following result, which appears as Theorem 4.1 of [15].

Theorem 5.8. *Let P be a projective plane and let $(\mathcal{R}, T)$ and $(\mathcal{R}', T')$ be two ternary rings coordinatising P with respect to U, V, O, I and U', V', O', I' respectively. The ternary ring $(\mathcal{R}, T)$ is isomorphic to $(\mathcal{R}', T')$ if and only if there exists a collineation ϕ of P satisfying $a\phi = a'$ for all $a \in \{U, V, O, I\}$.*

Theorem 5.9. *A line $\mathcal{L}(c)$ with $c \in G$ is a translation line in $P(g)$ if and only if $P(g)$ is desarguesian.*

Proof. Suppose $\mathcal{L}(c)$ is a translation line in $P(g)$. Then all ternary rings based on $\mathcal{L}(c)$ as the line at infinity are quasifields. Consider an ordered quadrangle U, V, O, I, with $V = (\infty)$ and U on the line $\mathcal{L}(c)$ and its corresponding ternary ring T. Suppose $\gamma \in \Gamma$ fixes V and maps U to U', with U' not lying on $\mathcal{L}(c)$. Then $U\gamma, V\gamma, O\gamma, I\gamma$ $(= U', V, O', I')$ is an ordered quadrangle with respect to a line $\mathcal{L}$ $= \mathcal{L}(c')$, which contains U'. Then $\mathcal{L} \neq \mathcal{L}(c)$, and by Theorem 5.8 the ternary ring T' corresponding to U', V, O', I' is isomorphic to T. Consequently $P(g)$ has two distinct translation lines $\mathcal{L}$ and $\mathcal{L}(c)$, and so must be desarguesian. □

Corollary 5.10. *$P(g)$ contains a translation line if and only if $I(g)$ is an affine translation plane.*

Proof. If $I(g)$ is an affine translation plane then $\mathcal{L}_\infty$ is a translation line. Conversely, either $P(g)$ is desarguesian (in which case the result holds) or the translation line must be $\mathcal{L}_\infty$, by Theorems 5.7 and 5.9. This implies that $I(g)$ is an affine translation plane. □

Under the additional assumption that G and H are commutative we may make some observations on when $I(g)$ is a dual translation plane.

Definition 5.11. *An affine plane A is a* dual translation plane *if there exists a point $V \in \mathcal{L}_\infty$ such that the projective closure of A is $(V, \mathcal{L})$-transitive for all lines $\mathcal{L}$ (including $\mathcal{L}_\infty$) through V.*

Corollary 5.12. *Suppose G and H are commutative finite groups. Then $I(g)$ is a dual translation plane if and only if $I(g)$ is a translation plane.*

Proof. If $I(g)$ is a dual translation plane then its projective closure $P(g)$ must contain a translation point V. If $V \neq (\infty)$ then $P(g)$ is both $((\infty), \mathcal{L}_\infty)$-transitive and $(V, \mathcal{L}_\infty)$-transitive, and so by [15, Theorem 6.1], $I(g)$ is a translation plane. Now assume that $V = (\infty)$. Then ([15, Theorem 6.4]) the ternary ring $\mathcal{R}$ described in Lemma 5.4 is a left quasifield (a cartesian group satisfying left distributivity).

By assumption G and H are commutative and so $(\mathcal{R},+,\cdot)$ is a semifield. Hence $I(g)$ is a translation plane.

Conversely, suppose that $I(g)$ is a translation plane. Then the ternary ring of Lemma 5.4 is a quasifield. By commutativity it is a left quasifield and so $I(g)$ is a dual translation plane by [15, Theorem 6.4]. □

Note that the last result implies that when G and H are commutative the projective plane $P(g)$ can never be of Lenz-Barlotti type IV.1 or IV.2. Either it contains no translation line or point (type II) or it is at least a semifield plane (type V.1). All previously known planar functions describe projective planes which are at least semifield planes.

6. Non-translation Planes defined by planar functions

The planar functions introduced in Theorem 4.1 differ from the other known classes of planar functions in that they do not describe translation planes. This will be established using the ternary ring given by Lemma 5.4 and the following particular case of a result from [4].

Lemma 6.1 (Dembowski and Ostrom [4], Corollary 4)**.** *Let f be a planar polynomial on $\mathbb{F}_q$ normed with respect to some $a \in \mathbb{F}_q^*$ and let Q_a be as defined in Lemma 5.4. Then $I(\mathbb{F}_q,\mathbb{F}_q;f)$ is a translation plane if and only if*

$$\begin{aligned} f(x+z)+f(y+z)-f(x)-f(y)-f(z) \\ = f\big(Q_a(\Delta_{f,a}(x)+\Delta_{f,a}(y))+z\big)-f\big(Q_a(\Delta_{f,a}(x)+\Delta_{f,a}(y))\big) \end{aligned} \quad (5)$$

for all $x,y,z \in \mathbb{F}_q$.

Dembowski and Ostrom note that any planar Dembowski-Ostrom polynomial satisfies (5) so that any affine plane associated with a Dembowski-Ostrom polynomial is necessarily a translation plane (and a semifield plane). We note that the original paper contains a misprint in the statement of this corollary.

Our first result establishes that the affine planes associated with the planar polynomials introduced in Section 4 are not in general translation planes.

Theorem 6.2. *Let $g(X) = X^{(3^\alpha+1)/2}$ be a planar polynomial on $\mathbb{F}_q$ with $q = 3^e$ and suppose that $\alpha \not\equiv \pm 1 \pmod{2e}$. Then the affine plane $I(\mathbb{F}_q,\mathbb{F}_q;g)$ is not a translation plane.*

Proof. Let $n = (3^\alpha+1)/2$. By Lemma 4.3 we may assume that $1 \le \alpha < 2e$. If $\alpha = e+\beta$ with $\beta < e$ then for all $x \in \mathbb{F}_q^*$

$$\begin{aligned} x^{(3^\alpha+1)/2} &= x^{3^e(3^\beta+1)/2}x^{-(3^e-1)/2} \\ &= x^{(3^\beta+1)/2}x^{(3^e-1)/2} \\ &= x^{(3^e+3^\beta)/2} \\ &= (x^{(3^{e-\beta}+1)/2})^{3^\beta}. \end{aligned}$$

This also holds for $x=0$. Consequently the planes defined by $X^{(3^\alpha+1)/2}$ and $X^{(3^{e-\beta}+1)/2}$ are isomorphic and we may restrict ourselves to the range $1 \le \alpha < e$.

Denote by $f(X) = (X+a)^n - a^n$ the normed form with respect to $a \in \mathbb{F}_q^*$ of the planar monomial X^n. Then $\Delta_{f,a}(X) = (X-a)^n-(X+a)^n$, an odd polynomial. Let $Q_a \in \mathbb{F}_q[X]$ be the reduced polynomial satisfying $\Delta_{f,a}(Q_a(x)) = x$ for all $x \in \mathbb{F}_q$.

Then $Q_a(X)$ is also an odd polynomial and further $\Delta_{f,a}(0) = Q_a(0) = 0$. Suppose that $I(\mathbb{F}_q, \mathbb{F}_q; f)$ is a translation plane and consider (5) with $y = -x$. Then the right side of (5) reduces to $f(z)$ and (5) becomes

$$f(z + x) + f(z - x) + f(z) = f(x) + f(-x)$$

for all $x, z \in \mathbb{F}_q$. Now

$$f(z + x) + f(z - x) + f(z) = (z + x + a)^n + (z - x + a)^n + (z + a)^n$$

and for $z = 2a$ we thus have

$$\begin{aligned} -x^n &= f(x) + f(-x) \\ &= (x + a)^n + (-x + a)^n + a^n \\ &= (x + a)^n + (x - a)^n + a^n \end{aligned} \tag{6}$$

for all $x \in \mathbb{F}_q$. Let $2k(X) = (X + a)^n + (X - a)^n + X^n$ so that, by (6), $k(x) = a^n$ for all $x \in \mathbb{F}_q$. Clearly this will hold for $n = 2$. However for $2 < n < q$ we have

$$k(X) = \sum_{i=1}^{(n-2)/2} \binom{n}{2i} X^{2i} a^{n-2i}.$$

Since $\binom{n}{2} \not\equiv 0 \bmod 3$, the degree of k is $n - 2$ and so $0 < \deg(k) < q - 2$. Hence k cannot be a constant polynomial, contradicting (6), and $I(\mathbb{F}_q, \mathbb{F}_q; f)$ cannot be a translation plane for $n > 2$. □

According to Kallaher [15, page 101], all known affine planes which can be described by planar functions are translation planes or dual translation planes. The affine planes defined by the functions in Theorem 4.1 are not in these classes.

Corollary 6.3. *Let $g(X)$ be a planar polynomial described by Theorem 4.1 with $\alpha \not\equiv \pm 1 \pmod{2e}$. Then $I(g)$ is not a dual translation plane. Furthermore, $P(g)$ must be Lenz-Barlotti type II.1 or II.2.*

Proof. The fact that $I(g)$ is not a dual translation plane follows from Corollary 5.12 and Theorem 6.2. Hence $P(g)$ does not contain a translation line or point. Since $P(g)$ does have at least one incident point-line transitivity, $((\infty), \mathcal{L}_\infty)$, by Theorem 1 of [4], $P(g)$ must be Lenz-Barlotti type II. □

In [15, Chapter 9], Kallaher lists four classes of planes which form counterexamples to a conjecture that all affine planes which have a collineation group transitive on the affine points must be a translation plane. We note that the class of planes introduced above also form counterexamples to this conjecture.

A further question of interest is whether the known Dembowski-Ostrom polynomials define non-desarguesian planes. It is remarked in [6] that this is the case but no proof is given. Certainly this can be shown for small orders by calculation. It is possible (and consistent with our experimental data) that if an affine plane defined by a planar polynomial f over $\mathbb{F}_q$ is a translation plane then f is a Dembowski-Ostrom polynomial. The authors have not located any planar polynomials beyond those mentioned in this paper, so it is also possible that the list is complete.

We conclude with some remarks concerning the projective plane $P(g)$ associated with the planar polynomials of Section 4. By Corollary 6.3 the plane $P(g)$ is Lenz-Barlotti type II.1 or II.2. Establishing that the planes are in fact type II.1 is equivalent to showing that the ternary ring of Lemma 5.4 is not associative. For the small examples computed this is in fact the case. As indicated in the Introduction, for non-square orders the planes of Section 6 cannot be amongst those obtained by derivation or lifting, but the square order case remains open.

Added in proof: T. Ostrom has informed us that he has established the proof of the above conjecture on translation planes and J. Yaqub has established $P(g)$ is Lenz-Barlotti class II.1.

References

1. M. Billiotti, V. Jha, N.L. Johnson, and G. Menichetti, *A structure theory for two-dimensional translation planes of order q^2 that admit collineation groups of order q^2*, Geom. Dedicata **29** (1989), 7–43.
2. S.D. Cohen and M.J. Ganley, *Some classes of translation planes*, Quart. J. Math. **35** (1984), 101–113.
3. P. Dembowski, *Finite Geometries*, Springer-Verlag, New York, Heidelberg, Berlin, 1968.
4. P. Dembowski and T.G. Ostrom, *Planes of order n with collineation groups of order n^2*, Math. Z. **103** (1968), 239–258.
5. L.E. Dickson, *The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group*, Ann. of Math. **11** (1897), 65–120, 161–183.
6. D. Gluck, *Affine planes and permutation polynomials*, Coding Theory and Design Theory, part II (Design Theory), The IMA Volumes in Mathematics and its Applications, vol. 21, Springer-Verlag, 1990, pp. 99–100.
7. ———, *A note on permutation polynomials and finite geometries*, Discrete Math. **80** (1990), 97–100.
8. Y. Hiramine, *A conjecture on affine planes of prime order*, J. Comb. Theory Ser. A **52** (1989), 44–50.
9. ———, *On planar functions*, J. Algebra **133** (1990), 103–110.
10. V. Jha and N.L. Johnson, *Some unusual translation planes of order 64*, Arch. Math. **43** (1984), 566–571.
11. N.L. Johnson, *Projective planes of order p that admit collineation groups of order p^2*, J. Geometry **30** (1987), 49–68.
12. ———, *Derived Fisher translation planes*, Simon Stevin **64** (1990), 21–50.
13. ———, *Ovoids and translation planes revisited*, Geom. Dedicata **38** (1991), 13–57.
14. N.L. Johnson and F.C. Piper, *On planes of Lenz-Barlotti class II-1*, Bull. London Math. Soc. **6** (1974), 152–154.
15. M.J. Kallaher, *Affine Planes with Transitive Collineation Groups*, North-Holland, 1982.
16. W.M. Kantor, *On point-transitive affine planes*, Israel J. Math. **42** (1982), 227–234.
17. R. Lidl, G.L. Mullen, and G. Turnwald, *Dickson Polynomials*, Pitman Monographs and Surveys in Pure and Appl. Math., vol. 65, Longman Scientific and Technical, Essex, England, 1993.
18. R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl., vol. 20, Addison-Wesley, Reading, 1983, (now distributed by Cambridge University Press).
19. W. Nöbauer, *Über eine Klasse von Permutationspolynomen und die dadurch dargestellten Gruppen*, J. Reine Angew. Math. **231** (1968), 215–219.
20. T.G. Ostrom, *Semi-translation planes*, Trans. Amer. Math. Soc. **111** (1964), 1–18.
21. ———, *The dual Lüneburg planes*, Math. Z. **92** (1966), 201–209.
22. L. Rónyai and T. Szönyi, *Planar functions over finite fields*, Combinatorica **9** (1989), 315–320.
23. A. Wagner, *On perspectivities of finite projective planes*, Math. Z. **71** (1959), 113–123.

Department of Computer Science, The University of Queensland, St. Lucia, Queensland 4072, Australia.

E-mail address, R S Coulter: shrub@cs.uq.oz.au

E-mail address, R W Matthews: galois@hilbert.maths.utas.edu.au

Des. Codes Cryptogr. 10 (1997), 167-184