A Note on Planar Functions and Their Planes

by

Donna Pierce and Michael J. Kallaher

Department of Mathematical Sciences
Washington State University
Pullman, WA 99164
dpierce@whitworth.edu; mkallaher@wsu.edu

1. **Introduction.** Planar functions were introduced by Dembowski and Ostrom in 1968. Prior to 1997 the only examples of planar functions were Dembowski-Ostrom polynomials. In that year Coulter and Matthews announced the discovery of a planar monomial which was not a Dembowski-Ostrom polynomial. At present these are the only known types of planar polynomials.

Planar functions define affine planes in the Lenz-Barlotti Class II.1 or higher. Since Dembowski-Ostrom polynomials have distributive multiplication, Dembowski-Ostrom planar polynomials define translation planes. We show that the converse is also true; if $\mathcal{U}(f, q)$ is a translation plane defined by a planar polynomial f, then f is a Dembowski-Ostrom polynomial. This answers a question in [1]. Multiplication is also commutative. Therefore if f is a Dembowski-Ostrom polynomial, $\mathcal{U}(f, q)$ is in Lenz-Barlotti Class V.1. We show that there are no affine planes described by planar polynomials between LB II.1 and LB V.1. Thus the Coulter-Matthews polynomials are in LB II.1. We give examples of Dembowski-Ostrom polynomials which describe non-Desarguesian and Desarguesian planes, answering another question raised in [1].

We then consider planar monomials. When $f(x) = x^n$ we show that $U(f, q)$ is a Desarguesian plane if and only if $n = 2$. The Coulter-Matthews polynomials are monomials of the form $x^{(3^\alpha+1)/2}$. This result cannot be generalized to other primes, i.e., the monomial $x^{(p^a+1)/2}$ is not planar if $p \neq 3$,

Since the difference function of a planar polynomial is a permutation polynomial, number theoretic results for permutation polynomials have been used to discover necessary conditions for a polynomial to be planar. In 1987 Johnson [6] proved that x^n is not planar over $GF(p)$ for $n \neq 2$. Johnson's result can equivalently be stated: for $1 \leq n \leq p-1$, $n \neq 2$, the monomial x^n is not planar over $GF(p)$. We extend this result to $GF(p^e)$ be showing that if $n \neq 2$ then a necessary condition for n to be planar is that $n > p$.

Section 1: Background

1.1 Planar Functions Let $K = (GF(q), +)$, where $q = p^e$ with p an odd prime and $e \geq 1$, and let $f(x)$ be a function from K into K. Define a binary operation on K by

$$x \bullet m = f(x + m) - f(x) - f(m).$$

Note that

$$x \bullet m = m \bullet x.$$

An incidence structure $I = I(K; f)$ is defined as follows:
points: elements of $K \times K$
lines: i. For each pair m, b of elements of K the set $\{(a, a \bullet m + b) | a \epsilon K$
ii. For each element $c \epsilon K$ the set $\{(c, a) | a \epsilon K\}$.

The first type of line is represented by the equation

$$y = x \bullet m + b,$$

and the second by the equation

$$x = c$$

Definition 1.1 *Let $K = (GF(q), +)$. A function $f : K \to K$ is called a planar function if for every non-zero $a \epsilon K$, the function $\delta(f, a) : x \mapsto f(x + a) - f(x)$ is a bijection.*

Note that without loss of generality, we can let $f(0) = 0$. For if f is planar and if $f(0) = b$, $b \neq 0$, then define a new function g as

$$g(x) = f(x) - b$$

For $a \neq 0$, $a \epsilon K$, we have

$$\begin{aligned} g(x + a) - g(x) &= f((x + a) - b - f(x) + b \\ &= f(x + a) - f(x) \end{aligned}$$

This implies that $g(x)$ is planar and $g(0) = 0$.

The important relationship between planar functions and affine planes is given in the following theorem.

Theorem 1.1 . *A function $f : K \to K$, where $K = (GF(q), +)$, is a planar function if and only if $I(K; f)$ is an affine plane.*

Proof. *See Dembowski and Ostrom [3], Lemma 12, pg 252.*

We denote this affine plane by $\mathcal{U}(f; q)$. The lines $y = x \bullet m + b$ for a given $m \epsilon K$ form a parallel class with slope (m) in $\mathcal{U}(f; q)$. The lines $x = c$ form a parallel class in both the Desarguesian plane and in $\mathcal{U}(f; q)$

If f is a planar function over $K = (GF(q), +)$ then q is odd (see [3], Lemma 9).

The study of planar functions is closely related to the study of permutation polynomials. In exploring this relationship, we begin with a definition.

Definition 1.2. *A polynomial $g \epsilon GF(q)[x]$ is a permutation polynomial over $GF(q)$ if it induces a permutation of $GF(q)$.*

Let $K = (GF(q), +)$ and f be a function from $K \to K$. For each $a \epsilon GF(q)$, $a \neq 0$, we define the difference operator $\delta(f, a)(x) = f(x + a) - f(x)$. Then by Definition 1.1, if $\delta(f, a)$ is a permutation polynomial f is a planar polynomial.

Any polynomial $f \epsilon GF(q)[x]$ may be reduced mod $x^q - x$ to yield a polynomial of degree $\leq q - 1$ which induces on $GF(q)$ the same function as f. We call this the reduced form of f. (See Lemma 7.2 of Lidl and Niederreiter [7].) Then a planar polynomial over $GF(q)$ can be written as $\sum_{i=0}^{q-1} a_i x^i$ with certain restriction on the a_i's. For example, by Definition 1.1, a quadratic polynomial $f(x) = a_2 x^2 + a_1 x + a_0, a_2 \neq 0$, is planar since $\delta(f, m)(x) = 2a_2 xm + (a_2 m^2 + a_1 m)$ is a permutation polynomial for all $a_1, a_2 \epsilon K$.

Classification of planar functions over fields of prime order was settled in 1989 and 1990 when three papers (Gluck [4], Hiramine [5], Rónyai and Szönyi [9]) appeared. They showed that every planar polynomial over a prime field $GF(p)$ must reduce to a quadratic polynomial. If $q = p^e$ with $e > 1$, it had been conjectured that every planar polynomial with $f(0) = 0$ has the form $\sum_{i,j=0}^{e-1} a_{ij} x^{p^i + p^j}$ with $a_{ij} \epsilon GF(q)$. Coulter and Matthews [1] proved that this conjecture is untrue with their discovery of the planar monomial $x^{(3^a+1)/2}$.

One question that has been investigated is:

How can a planar function be transformed or combined with other functions and still maintain its planarity?

Coulter and Matthews discussed this question in the finite case (see Theorem 1.3 and Corollary 1.4 below). For the infinite case see Polster[8].

Definition 1.3. *If $K = (GF(q), +)$ then an* *additive polynomial* *(in reduced form) is a polynomial of the form*

$$L(x) = \sum_{i=0}^{e-1} a_i x^{p^i}, a_i \epsilon GF(q), q = p^e.$$

Theorem 1.2 *Let $L \epsilon GF(q)[x]$ be defined by $L(x) = \sum_{i=0}^{e-1} a_i x^{p^i}$. The polynomial L is a permutation polynomial over $GF(q)$ if L has no roots in $GF(q)$ other than zero.*

Proof. *See Theorem 7.9 of Lidl and Niederreiter [7].*

Theorem 1.3 *Let $f \epsilon GF(q)[x]$ and let $L \epsilon GF(q)[x]$ be an additive polynomial. The following statements are equivalent:*

1. *The polynomial $f(L)$ is a planar polynomial.*
2. *The polynomial $L(f)$ is a planar polynomial.*
3. *The polynomial f is a planar and L is a permutation polynomial.*

Proof. *See Theorem 2.3 of Coulter and Matthews [1].*

Corollary 1.4. *If $L \epsilon GF(q)[x]$ is an invertible linear transformation over $GF(q)[x]$ and $f \epsilon GF(q)[x]$, f a planar polynomial, then $L(f)$ and $f(L)$ are planar.*

Proof. *The polynomial L is an additive permutation polynomial. By Theorem 1.3, $L(f)$ and $f(L)$ are planar.*

Planarity is also preserved under a translation $x \mapsto x + a$. For example, if $f(x)$ is a planar polynomial then $af(\lambda x + \mu) + \beta, a, \lambda \neq 0$ is planar. To see this let $h(x) = \lambda x + \mu$. Then h is a permutation polynomial and thus to each $x \epsilon GF(q)$ there corresponds a unique $y \epsilon GF(q)$ such that $\lambda x + \mu = y$. Let

$$g(y) = af(y) + \beta.$$

Then

$$\delta(g, m)(y) = (af(y + m) + \beta) - (af(y) + \beta) = a(f(y + m) - f(y))$$

which is a permutation polynomial since f is planar.

1.2 Dembowski-Ostrom Polynomials

In their 1968 paper Dembowski and Ostrom [3] described a class of polynomials which sometimes give rise to planar functions. These polynomials are called Dembowski-Ostrom polynomials and are defined in the following manner.

Definition 1.4. *The polynomial $f(x) \epsilon GF(q)[x]$, $q = p^e$, is a* *__Dembowski-Ostrom polynomial__* *if the reduced form of f has the form*

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

Let f be a Dembowski-Ostrom polynomial (in reduced form) whose coefficients a_{ij} satisfy the condition

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

It follows that f is planar. In other words $x \bullet y$ has no zero divisors, where $x \bullet y = f(x + y) - f(x) - f(y)$. For example if

$$f(x) = a_{ij} x^{p^i + p^j}$$

then

$$x \bullet y = f(x + m) - f(x) - f(m) = a_{ij}(x^{p^i} y^{p^j} + x^{p^i} y^{p^j} = 0$$

if and only if $x = 0$ or $y = 0$.

The following theorem characterizes Dembowski-Ostrom polynomials as those reduced polynomials whose difference polynomials are all additive.

Theorem 1.5. *Let $f \epsilon GF(q)[x]$with $deg(f) < g$. The following statements are equivalent:*

1. *The polynomial $f = D + L + c$, where D is a Dembowski-Ostrom polynomial, L is an additive polynomial and $c \epsilon GF(q)$ is a constant.*
2. *For each $a \epsilon GF^*(q)$, $\delta(f, a) = L_a + c_a$ where L_a is an additive polynomial and $c_a \epsilon GF(q)$ is a constant (both depending on a).*

Proof. *See Theorem 3.2 of Coulter and Matthews [1].*

Section 2: Planar Functions and Affine Planes

2.1 Planes of Order n Having a Group of Order n^2

In Section 1 we saw that a function $f : K \to K$, $K = GF(q)$, is planar if and only if the incidence structure $I(K; f)$ is an affine plane. We denoted this affine plane determined by f as $\mathcal{U}(f, q)$. Lines were defined by the equations $y = x \bullet m + b$ and $x = c$ where $x \bullet m = m \bullet x = f(x+m) - f(x) - f(m)$.

The idea of a planar function grew out of the study of a projective plane $\mathcal{P}$ of order n which has a group Γ of order n^2 satisfying the following conditions:

1. The plane $\mathcal{P}$ is (C, l)-transitive for some flag (C, l) and Γ contains the group Π of all (C, l)-elations as a normal subgroup.
2. The group Γ permutes the points (and lines) of $\mathcal{P}$ in three orbits.
3. The group Γ contains a subgroup Φ with $\Gamma = \Phi \times \Pi$.

The incidence structure $I(K; f)$ possesses a collineation group of order q^2 as given below.

Theorem 2.1. *Let $K = (GF(q), +)$, where $q = p^e$ with p an odd prime and $e \geq 1$. Let $f(x)$ be a function from K to K, and let $I = I(K; f)$ be the incidence structure defined above. For each pair of elements in K the mapping $\phi_{u,v} : I \to I$ defined by*

$$\phi_{u,v} : (x, y) \to (x + u, y - x \bullet u - f(u) + v)$$

is a collineation of I. Furthermore, the set $\mathcal{C} = \{\phi_{u,v} | u, v \epsilon K\}$ is an abelian collineation group of I of order q^2, sharply transitive on the points of I.

Proof. *See Lemma 10, Theorem 5, and Corollary 2 of Dembowski-Ostrom [3].*

Let $\mathcal{U}(f; q)$ be an affine plane defined by planar function f, and let $\mathcal{B}$ be its extension to a projective plane. Theorem 2.1 showed that for $u, v \epsilon GF(q)$, the mappings

$$\phi_{u,v} : (x, y) \mapsto (x + u,\ y - x \bullet u - f(u) + v)$$

form an abelian collineation group of order n^2, transitive on the affine points.

A line of the form $y = x \bullet m + b$ is mapped by $\phi_{u,v}$ to the line $y = x \bullet (m - u) + \{f(m - u) - f(m) + b + v\}$. The line $x = c$ is mapped to

$x = c + u$. The slope point (m) is mapped to $(m - u)$ and the point $(0,0)$ is mapped to $(u, -f(u) + v)$.

The collineation group $\Gamma = \{\phi_{u,v} | u, v \epsilon GF(q)\}$ has 3 point orbits: $\{(\infty)\}, l_\infty - \{(\infty)\}$, and the affine points.

Let $\Pi = \{\phi_{0,v} | v \epsilon GF(q)\}$ where $\phi_{0,v} : (x, y) \to (x, y + v), (0,0) \to (0, v)$. The set Π is a subgroup of Γ consisting of $((\infty), l_\infty)$ elations. These elations keep every line $x = c$ fixed and are transitive on $x = 0$. Thus the group Π is a transitive group of $((\infty), l_\infty)$-elations. The set $\Phi = \{\phi_{u,0} \, | u \epsilon GF(q)\}$, where

$$\phi_{u,0} : (x, y) \mapsto (x + u, \; y - x \bullet u - f(u)),$$

is also a subgroup of Γ. The line $y = x \bullet m + b$ is mapped by $\phi_{u,0}$ to

$$y = x \bullet (m - u) + \{f(m - u) - f(m) + b\}$$

and the line $x = c$ is mapped to the line $x = c + u$. Thus the group Φ is sharply transitive on the set of lines $x = c$. It follows that $\Gamma = \Phi \times \Pi$. Since $\mathcal{P}$ contains a transitive group of $((\infty), l_\infty)$-elations, the plane $\mathcal{P}$ is coordinatized by a Cartesian group, i.e., the plane $\mathcal{P}$ is in the Lenz Barlotti Class II or higher. The projective extension of $\mathcal{P}$ of $\mathcal{U}(f; q)$ also satisfies conditions 1-3 listed above.

Let $f(x)$ be a planar function over $GF(q)$, let $\mathcal{U}(f; q)$ be the affine plane determined by f, and let $\mathcal{P}$ be the projective extension of $\mathcal{U}(f; q)$. The discussion at the beginning of this section showed that the plane $\mathcal{P}$ is $((\infty), l_\infty)$-transitive. Consequently the plane $\mathcal{U}(f; q)$ was in at least LB Class II.1 or higher. If the affine plane is (P, l)-transitive for an additional pair we have the following result.

Theorem 2.2 *Let $\mathcal{U}(f; q)$ be an affine plane determined by a planar function. If $\mathcal{U}(f; q)$ is (P, l)-transitive for a pair (P, l) in addition to $((\infty), l_\infty)$ then $\mathcal{U}(f; q)$ is a semifield plane.*

Proof. *To prove the proposition we need to show that $\mathcal{U}(f; q)$ is not in the Lenz Barlotti Class LB II.2. This is a sufficient condition since for finite fields the classes LB II.3 and LB III are empty. If $\mathcal{P}$ is a translation plane then it is a semifield plane (recall that $x \bullet m = m \bullet x$). So suppose $\mathcal{U}(f; q)$, the affine plane determined by a planar function f, is a finite affine plane of Lenz-Barlotti Class LB II.2. The projective extension of affine planes in LB II.2 contain 2 pairs of (P, l)-transitivities: $((\infty), l_\infty)$-transitive and (B, m)-transitive where $B \epsilon l_\infty, B \neq (\infty)$, and $l_\infty \cap m = (\infty)$. Since the collineations in Φ are transitive on the lines through (∞) and on $l_\infty - \{(\infty)\}$, without loss of generality we can assume m is the line $x = 0$ and $B = (0)$. But then* *the mappings $\varphi_{u,o}$, which map (0) to $(-u)$ and the line $x = 0$ to $x = u$, imply that $\mathcal{U}(f;q)$ is in LB II.3 which is empty.*

Note that the planes of Lenz-Barlotti class LB II.3 can be described in the following way:

In the plane there exists a point R and a line r through R. Furthermore, there is a bijection θ between the points on r and the lines through R with $\theta(R) = r$ such that the plane is $(P, \theta(P))$ transitive for all $P\epsilon r$.

In our case $R = (\infty), r = l_\infty$ and θ is the mapping given by:

$$\theta((\infty)) \text{ is } l_\infty \text{ and } \theta((-u)) \text{ is the line } x = u.$$

This theorem shows that there are no affine planes described by planar polynomials between LB II.1 and LB V.1.

2.2 Isomorphic Planes

Coulter and Matthews [1] showed that with certain restrictions on a polynomial L, a planar polynomial f could be combined in various ways with L to yield a plane isomorphic to $\mathcal{U}(f;q)$. The proofs of the following two theorems are adaptations of their arguments (see Theorems 5.1 and 5.2 of Coulter and Matthews [1]).

Theorem 2.3 *If f is a planar polynomial and L is an additive polynomial, both defined over $GF(q)$, then $\mathcal{U}(f;q) \cong \mathcal{U}(f+L;q)$.*

Proof. *We need to show that there exists a bijection ϕ of the points of $\mathcal{U}(f;q)$ onto the points of $\mathcal{U}(f+L;q)$ mapping the lines of $\mathcal{U}(f;q)$ onto the lines of $\mathcal{U}(f+L;q)$ and preserving incidence. Let $\phi : GF(q) \times GF(q) \to GF(q) \times GF(q)$ be the bijection defined by $\phi : (x,y) \to (x,y)$. If (x,y) lies on the line*

$$y = x \bullet m + b = f(x+m) - f(x) - f(m) + b,$$

then

$$y = f(x+m) + L(x) + L(m) - f(x) - L(x) - f(m) - L(m) + b.$$

Since L is additive we have $L(x) + L(m) = L(x+m)$. It follows that $(x,y)\phi = (x,y)$ lies on the line

$$y = (f+L)(x+m) - (f+L)(x) - (f+L)(m) + b.$$

Theorem 2.4 *If f is a planar polynomial and L is an additive permutation polynomial, both defined over $GF(q)$ then $\mathcal{U}(f;q) \cong \mathcal{U}(f(L);q) \cong \mathcal{U}(L(f);q)$.*

Proof. *First consider the bijection from $\mathcal{U}(f;q)$ to $\mathcal{U}(f(L);q)$ defined by $(x,y)\phi = (L^{-1}(x), y)$. If (x,y) lies on*

$$\begin{aligned} y &= f(x+m) - f(x) - f(m) + b \\ &= f(LL^{-1}(x+m) - f(LL^{-1}(x)) - f(LL^{-1}(m)) + b \\ &= (f(L))(L^{-1}(x) + L^{-1}(m)) - (f(L))(L^{-1}(x)) - (f(L))(L^{-1}(m)) + b, \end{aligned}$$

then the point $(x,y)\phi = (L^{-1}(x), y)$ lies on

$$y = (f(L))(x + L^{-1}(m)) - (f(L))(x) - (f(L))(L^{-1}(m)) + b.$$

The image of $x = c$ is $x = L^{-1}(c)$. Consequently, $\mathcal{U}(f;q) \cong \mathcal{U}(f(L);q)$.

Now consider the bijection ψ defined by $(x,y)\psi = (x, L(y))$. This gives a collineation mapping the line

$$y = f(x+m) - f(x) - f(m) + b$$

to the line

$$y = (L(f))(x+m) - (L(f))(x) - (L(f))(m) + L(b).$$

This follows from

$$\begin{aligned} L(y) &= L(f(x+m) - f(x) - f(m) + b) \\ &= L(f(x+m)) - L(f(x)) - L(f(m)) + L(b) \end{aligned}$$

by the additivity of L. Thus, if (x,y) is on the line

$$y = f(x+m) - f(x) - f(m) + b,$$

then $(x,y)\psi = (x, L(y))$ is on the line

$$y = (L(f))(x+m) - (L(f))(x) - (L(f))(m) + L(b).$$

Note that by Theorem 1.3, if f is a planar polynomial over $GF(q)$ and L is a permutation polynomial over $GF(q)$ then $L(f)$ is a planar polynomial over $GF(q)$. Thus, the planarity property is preserved. But Theorem 2.4 gives us the additional result that the planes they define are actually isomorphic. The following application of Theorem 2.4 is used in the proof of the Corollary 5.10.

Corollary 2.5 *Let $L = x^{p^a}$ be an additive permutation polynomial. If $f(x) = x^n$ is a planar polynomial then the planes defined by $f(x) = x^n$ and $f(x^{p^a}) = (x^{p^a})^n = (x^n)^{p^a}$ are isomorphic.*

Section 3: Multiplicative Properties

3.1 Properties of the • and the ∘ Multiplication

Definition 1.1 says that a function $f : K \to K$, where $K = (GF(q), +)$, is a planar function if for every $a \epsilon K, a \neq 0$, the function $\delta(f, a) : x \to f(x+a) - f(x)$ is a bijection. An incidence structure $I = I(K; f)$ was also defined with points being the elements of $K \times K$ and lines being of the form $x = 0$ or $y = x \bullet m + b$ where $x \bullet m = f(x+m) - f(x) - f(m) = m \bullet x$.

By Theorem 1.1, the structure $I(K; f)$ is an affine plane if and only if f is a planar function. We denoted this affine plane by $\mathcal{U}(f; q)$. Note that $\mathcal{U}(f; q)$ is coordinatized by a Cartesian group whose elements are the elements of K.

In this section we examine the properties of the • multiplication over $K = (GF(q), +)$. Since without loss of generality we may assume $f(0) = 0$, there holds

$$x \bullet 0 = f(x+0) - f(x) - f(0) = 0 = 0 \bullet x.$$

The • multiplication as defined does not have an identity for an arbitrary f. We define a new multiplication, ∘, in the following way.

Choose an element $e \neq 0$ in K. For $x \epsilon K$, define

$$\tilde{x} = x \bullet e = e \bullet x.$$

For $x, m \epsilon K$, define

$$\tilde{x} \circ \tilde{m} = x \bullet m = m \bullet x = \tilde{m} \circ \tilde{x}.$$

Then,

$$\tilde{x} \circ \tilde{e} = x \bullet e = \tilde{x}$$

and

$$\tilde{e} \circ \tilde{x} = e \bullet x = \tilde{x}.$$

Thus $\tilde{e} = e \bullet e$ is the identity for the ∘ multiplication.

Lemma 3.1. *If the • multiplication has an identity e, then the • multiplication and the ∘ multiplication obtained using the same element e are equal.*

Proof. *Let $e \neq 0$ be the identity for the • multiplication. Then $\tilde{x} = x \bullet e = x$ and $\tilde{x} \circ \tilde{m} = x \circ m$. But $\tilde{x} \circ \tilde{m}$ was defined to be $x \bullet m$ so $x \circ m = x \bullet m$, thus the ∘ multiplication is the same as the • multiplication.*

Theorem 3.2. *If the $\bullet$ multiplication is distributive then the $\circ$ multiplication is distributive.*

Proof. *Let $m, x\epsilon GF(q)$. Then*

$$\tilde{m} \circ \tilde{x} + \tilde{m} \circ \tilde{y} = m \bullet x + m \bullet y = m \bullet (x + y) = \tilde{m} \circ (x + y).$$

The $\circ$ multiplication is distributive if and only if $\tilde{x} + \tilde{y} = x + y$. But

$$\tilde{x} + \tilde{y} = x \bullet e + y \bullet e = (x + y) \bullet e = x + y.$$

Theorem 3.3. *If the $\bullet$ multiplication is associative then the $\circ$ multiplication is associative.*

Proof. *Let $a, b, c\epsilon GF(q)$. Then*

$$(\tilde{a} \circ \tilde{b}) \circ \tilde{c} = (a \bullet b) \circ \tilde{c}.$$

Now since $\bullet$ is the operation of a loop on $K - \{0\}$, there exists a unique d such that $a \bullet b = d \bullet e = \tilde{d}$. So

$$(\tilde{a} \circ \tilde{b}) \circ \tilde{c} = \tilde{d} \circ \tilde{c} = d \bullet c.$$

Similarly

$$\tilde{a} \circ (\tilde{b} \circ \tilde{c}) = \tilde{a} \circ (b \bullet c) = \tilde{a} \circ \tilde{h} = a \bullet h.$$

where h is the unique element of K such that $b \bullet c = h \bullet e$. Hence $(\tilde{a} \circ \tilde{b}) \circ \tilde{c} = \tilde{a} \circ (\tilde{b} \circ \tilde{c})$ if and only if $d \bullet c = a \bullet h$ where $a \bullet b = d \bullet c$ and $b \bullet c = h \bullet e$.

Since the $\bullet$ multiplication is commutative and is assumed here to be associative, then $(a \bullet b) \bullet c = a \bullet (b \bullet c)$ implies that $(d \bullet e) \bullet c = a \bullet (h \bullet e)$ is equivalent to $(d \bullet c) \bullet e = (a \bullet h) \bullet e$. By the planarity of f then $d \bullet c = a \bullet h$ and the $\circ$ multiplication is thus associative.

Theorem 3.4. *Let $f(x)$ be a planar function over $K = (GF(q), +)$. The plane $\mathcal{U}(f; q)$ is a translation plane if and only if the $\bullet$ multiplication is distributive.*

Proof. *See Corollary 4 of Dembowski and Ostrom [3]. The plane $\mathcal{U}(f; q)$ is a translation plane if and only if the Cartesian group satisfies the distributive law: $(u + v) \bullet w = u \bullet w + v \bullet w$.*

Remark: Since $\bullet$ multiplication is commutative, then if $\mathcal{U}(f; q)$ is a translation plane, it is actually a semifield plane.

Dembowski-Ostrom polynomials have distributive multiplication (Dembowski-Ostrom [3], pg. 257). The following theorem shows that the converse is true: if $\mathcal{U}(f;q)$ is a translation plane defined by a planar polynomial f, then f is a Dembowski-Ostrom polynomial.

Theorem 3.5. *Let $f(x)$ be a planar function on $K = (GF(q), +)$. If the $\bullet$ multiplication is distributive then $\mathcal{U}(f;q)$ is isomorphic to a plane defined by a Dembowski-Ostrom planar polynomial.*

Proof. *For $a \epsilon K$, we have*

$$\begin{aligned} \delta(f,a)(x) &= f(x+a) - f(x) \\ &= f(x+a) - f(x) - f(a) + f(a) \\ &= x \bullet a + f(a). \end{aligned}$$

Let $L_a(x) = x \bullet a$. If $(x+y) \bullet a = x \bullet a + y \bullet a$ then $L_a(x+y) = L_a(x) + L_a(y)$. Thus L_a is an additive polynomial. Then $\delta(f,a) = L_a + c_a$ where $f(a) = c_a$ is a fixed element of $(K, \bullet)$ dependent on a. By Theorem 1.5 (Coulter and Matthews [1], Theorem 3.2), $f = D + L + c$ where D is a Dembowski-Ostrom polynomial, L is an additive polynomial and $c \epsilon K$ is a constant. By Theorem 2.3 (Coulter and Matthews [1], Theorem 5.1) if L is an additive polynomial and g is a planar polynomial both defined over $GF(q)$ then $\mathcal{U}(g;q) \cong \mathcal{U}(g+L;q)$. Since $\phi : (x,y) \to (x, y+c)$ is an isomorphism mapping the line $y = x \bullet m + b$ to the line $y = x \bullet m + (b+c)$, the planes $\mathcal{U}(g;q)$ and $\mathcal{U}(g+c;q)$ are also isomorphic. So if the $\bullet$ multiplication is distributive then the plane determined by $f = D + L + c$ is isomorphic to the plane determined by a Dembowski-Ostrom polynomial.

All indications are that planar polynomials are even. Additive polynomials over $GF(p^e)$ are of the form $\sum_{j=0}^{e-1} b_j x^{p^j}$. Thus, if f is even and $\bullet$ is distributive then $f = D + c$ where D and c are as above.

Recall that planar functions describe an affine plane which is in Lenz-Barlotti class at least II.1, with the next Lenz-Barlotti class containing a plane described by a planar function being the class LB V.1 (a semifield plane).Thus either the plane contains no translation line or point (LB II.1) or it is at least a semifield plane (LB V.1). If $f(x)$ is not a Dembowski-Ostrom, the $\mathcal{U}(f;q)$ is in LB II.1.

For planar monomials we have the following result.

Theorem 3.6 *Let $f(x)$ be a planar function over $K = (GF(q), +)$. If $f(x) = x^n, n < q$ and the $\bullet$ multiplication has an identity, then $n = 2$.*

Proof. *Assume $e \neq 0$ and $x \bullet e = x = e \bullet x$. Then*

$$x \bullet e = (x+e)^n - x^n - e^n = \sum_{i=1}^{n-1} \binom{n}{i} x^{n-i} e^i.$$

Now if $x \bullet e = x$ for all x then

$$x \bullet e = \sum_{i=1}^{n-1} \binom{n}{i} x^{n-i} e^i = x$$

implies that $\binom{n}{i} \equiv 0 (mod\ p)$ except when $i = n-1$. But $\binom{n}{n-1} = \binom{n}{1} = n$ so $\binom{n}{i}$ is not congruent to $0(mod\ p)$ also when $i = 1$. Thus $x \bullet e = x$ for all x implies that $nxe^{n-1} + nx^{n-1}e = x$ for all x. Since $n < q, x^{n-1} \neq cx$ unless $n = 2$. Then $x \bullet e = x$ implies $n = 2$. When $n = 2$, $x \bullet e = (x+e)^2 - x^2 - e^2 = 2xe = x$, which implies that $e = \frac{1}{2}$.

Theorem 3.7. *Let $f(x)$ be a planar function over $K = (GF(q), +)$. If $f(x) = x^n$ and the $\bullet$ multiplication is associative, then $n = 2$.*

Proof. *Now $(K - \{0\}, \bullet)$ is a finite quasigroup with binary operation $\bullet$. If the $\bullet$ multiplication is also associative then $(K - \{0\}, \bullet)$ is a semigroup as well. Thus $(K - \{0\}, \bullet)$ is a group and has an identity element e such that $x \bullet e = x$ for all x. By Theorem 3.6, $n = 2$.*

Dembowski and Ostrom [3] have shown that if $f(x) = ax^2$ then the plane $\mathcal{U}(f; q)$ is Desarguesian. An affine plane coordinatized by a Cartesian group in which multiplication is commutative, distributive and associative is Desarguesian. Theorem 3.7 proves that if $\mathcal{U}(f; q)$ is a Desarguesian plane defined by a planar monomial with $f(x) = x^n$, then $n = 2$.

3.2 Construction of Planar Polynomials Which Define Desarguesian Planes There are planar polynomials other than ax^2, where a is a constant, which define a Desarguesian plane. Since the ternary ring coordinatizing the Desarguesian plane has the distributive property, these polynomials must be Dembowski-Ostrom polynomials by Theorem 3.5.

The following example shows how to construct planar polynomials whose associated plane is Desarguesian.

Let $f(x) = \dfrac{x^2}{2}$. Then $f(x)$ is planar over $GF(q)$ and defines a Desarguesian plane ([3] p. 255). Define $g(x) = L(f(L^{-1}(x)))$ where L is an invertible linear transformation. By Theorem 1.3 the function $g(x)$ is planar.

Define a $\star$ multiplication by

$$\begin{aligned}
x \star m &= g(x+m) - g(x) - g(m) \\
&= L(f(L^{-1}(x+m))) - L(f(L^{-1}(x))) - L(f(L^{-1}(m))) \\
&= L[\frac{1}{2}(L^{-1}(x) + L^{-1}(m))^2 - \frac{1}{2}(L^{-1}(x))^2 - \frac{1}{2}(L^{-1}(m))^2] \\
&= L[L^{-1}(x)L^{-1}(m)].
\end{aligned}$$

Then

$$\begin{aligned}
(x \star m) \star u &= L[L^{-1}(x \star m)L^{-1}(u)] \\
&= L[L^{-1}(L(L^{-1}(x)L^{-1}(m)))L^{-1}(u)] \\
&= L[L^{-1}(x)L^{-1}(m)L^{-1}(u)] \\
&= L[L^{-1}(x)(L^{-1}(m)L^{-1}(u))] \\
&= L[L^{-1}(x)L^{-1}L(L^{-1}(m)L^{-1}(u))] \\
&= L[L^{-1}(x)L^{-1}(m \star u)] \\
&= x \star (m \star u).
\end{aligned}$$

Hence the $\star$ multiplication is associative.

If e is the identity for the $\bullet$ multiplication defined by the function f

$$x = x \bullet e = f(x+e) - f(x) - f(e)$$

then $x \star L(e) = x$:

$$\begin{aligned}
x \star L(e) &= L[f(L^{-1}(x + L(e)))] - L[f(L^{-1}(x))] - L[f(L^{-1}(L(e)))] \\
&= L[f(L^{-1}(x) + e) - f(L^{-1}(x)) - f(e)] \\
&= L[L^{-1}(x) \bullet e] \\
&= L[L^{-1}(x)] \\
&= x.
\end{aligned}$$

This illustrates the fact that although the only planar monomial which defines a Desarguesian plane is of the form $f(x) = ax^2$ for some constant a, there are many Dembowski-Ostrom polynomials which define a Desarguesian plane. Construction of these polynomials can be obtained by using an invertible linear transformation over $GF(p^r)$ and defining the Dembowski-Ostrom planar polynomial to be $g(x) = L(f(L^{-1}(x)))$ where $f(x) = \dfrac{x^2}{2}$.

This raises the following question:

Given planar Dembowski-Ostrom polynomial g which defines a Desarguesian plane $\overline{F}$ does there exist a linear transformation that maps g back to x^2?

This question has been answered by Ostrom.

Theorem 3.8. *(Ostrom, private communication) If g is a planar polynomial which defines a Desarguesian affine plane over $GF(p^r)$ then there exists a linear transformation which maps g into the polynomial x^2 that also defines a Desarguesian plane over $GF(p^r)$.*

Section 4. Planar Monomials

4.1 General Results

In this section we examine the algebraic properties of planar monomials $f(x) = x^n$ over $GF(q)$. The first theorem shows that $f(x) = x^n$ can be replaced by a monomial of degree less than q which induces on $GF(q)$ the same function as $f(x)$.

Lemma 4.1. *Let $f(x) = x^n$ be a planar monomial over $GF(q)$ with q odd. If $n > q-1$ then $f(x) = x^n$ induces on $GF(q)$ the same function as $g(x) = x^s$ for some s with $s < n$.*

Proof. *Assume $n \geq q$ and let $n = q+t$. Then $x^n = x^{q+t} = xx^t = x^{t+1}$ and $t+1 = n-q+1 < n$.*

Note that $n > 1$; for if $n = 1$ then $f(x+a) - f(x) = a$ for all x which contradicts the planarity of f. Furthermore, it follows by induction from Lemma 4.1 that if $f(x) = x^n$ with $n > q-1$, then $f(x) = x^n$ induces on $GF(q)$ the same function as a monomial $h(x) = x^m$ with $m < q$.

Lemma 4.2 *If f is a planar function defined over $K = (GF(q), +)$, then f cannot be odd.*

Proof. *If f is odd then $f(-x) = -f(x)$. But then*

$$x \bullet (-x) = f(x-x) - f(x) - f(-x) = f(0) - f(x) + f(x) = 0$$

for all x. This contradicts the fact that there are no zero divisors in a Cartesian group.

Theorem 4.3. *The polynomial $f(x) = x^n$ is planar over $GF(q)$ if and only if $(x+1)^n - x^n$ is a permutation polynomial over $GF(q)$. If $f(x) = x^n$ is a planar polynomial over $GF(q)$ then $(n, q-1) = 2$.*

Proof. *The polynomial $f(x) = x^n$ is planar over $GF(q)$ if and only if $\delta(f,a)(x) = (x+a)^n - x^n$ is a permutation polynomial for all $a \in GF^*(q)$. (See Definitions 1.1 and 1.2.) But $\delta(f,a)(x) = a^n((\frac{x}{a}+1)^n - (\frac{x}{a})^n)$, which* *is a permutation polynomial if and only if $(x+1)^n - x^n$ is a permutation polynomial. If x^n is a planar polynomial over $GF(q)$ it is also planar polynomial over $GF(p)$. Since all planar monomials over the prime field are of the form ax^2, the condition $n \equiv 2(mod\ p-1)$ must hold. Assume now that x^n is planar over $GF(q)$. Then $(x+1)^n - x^n = 0$ for a unique $x \in GF(q)$ if and only if $((x+1)x^{-1})^n = 1$ for a unique x. Thus, $(n, q-1) = |\{y|y^n = 1\}| \leq 2$ and must be 2, since by Lemma 4.2, the power n is even.*

Note that Theorem 4.3 implies that if $n \neq 2$ and $f(x) = x^n$ is planar over $GF(q)$ then $n \not| \, (q-1)$.

In general no necessary and sufficient conditions for $f(x) = x^n$ to be planar over $GF(q)$ are known. If q is a prime then x^n is planar if and only if $n = 2$. The condition $n \equiv 2(mod\ p-1)$ is sufficient but not necessary while the conditions of Theorem 4.3 are not sufficient.

4.2 Dembowski-Ostrom planar monomials, $x^{p^\alpha+1}$

Only two types of planar monomials over $GF(q)$ are known. The first are monomials of the form $f(x) = x^{p^\alpha+1}$. Originally (see Dembowski-Ostrom [3]) it was thought that f was planar if and only if $\alpha = 0$ or $(\alpha, e) = 1$. Coulter and Matthews [1] proved the following.

Theorem 4.4 *Let $f(x) = x^{p^\alpha+1}$. The polynomial f is planar over $GF(p^e)$ if and only if $\alpha = 0$ or $\frac{e}{(\alpha,e)}$ is odd.*

Proof. *See Theorem 3.3 of Coulter and Matthews [1] for the case $\frac{e}{(\alpha,e)}$ is odd. If $\alpha = 0$ then $f(x) = x^2$ which is planar.*

Coulter and Matthews show that the condition of Theorem 4.4 is not equivalent to the condition $(\alpha, e) = 1$ originally stated in Dembowski and Ostrom [3]. For example, $x^{10} = x^{3^2+1}$ is planar over $GF(3^6)$ since $\frac{6}{(2,6)}$ is odd but $(2,6) \neq 1$. Another example showing that the two conditions are not equivalent is found in Section 4.4

The next result shows that we can restrict the power α in $f(x) = x^{p^\alpha+1}$ when determining planarity. As noted in Section 1.1 if $f(x) = cx^2$ then $\delta(f,a)(x) = f(x+a) - f(x) = c(x^2 + 2ax + a^2) - cx^2 = 2acx + ca^2$ is a permutation polynomial.

Therefore, if $\alpha = 0$, then $f(x) = x^{p^\alpha+1}$ is planar. For $\alpha > 0$ we have the following results which are adaptations of Coulter and Matthews' results for $x^{(3^\alpha+1)/2}$ (See Lemma 4.3 and Theorem 6.2 of Coulter and Matthews [1].)

Theorem 4.5 *Determination of the planarity of monomials of the form $f(x) = x^{p^\alpha+1}, \alpha \neq 0$, over $GF(p^e)$ can be restricted to the case where*

$1 \leq \alpha < e$.

Before proving the theorem, we show the following.

Lemma 4.6 *Assume $q = p^e$. For each $\alpha \in \mathbb{N}$ define a function $f_a : GF(q) \to GF(q)$ by $f_\alpha(x) = x^{p^\alpha+1}$. If S is the sequence of functions $\{f_0, f_1, \cdots\}$ then S is periodic with period $2e$.*

Proof. *Let* $\alpha = 2\lambda e + \beta$ with $0 \leq \beta < 2e$ and $\lambda > 0$. *Suppose $x \in GF(q)$. Then*

$$\begin{aligned} x^{p^\beta+1} &= x^{p^{(\alpha-2\lambda e)}+1} = \left(x^{p^{\alpha-2\lambda e}+1}\right)^{p^{2\lambda e}} = x^{p^\alpha+p^{2\lambda e}} = \left(x^{p^{2\lambda e}-1}\right)\left(x^{p^\alpha+1}\right) \\ &= x^{(p^{e\lambda}-1)(p^{e\lambda}+1)}x^{p^\alpha+1} = x^{(q^\lambda-1)(q^\lambda+1)}x^{p^\alpha+1} = x^{p^{\alpha+1}}. \end{aligned}$$

Thus

$$x^{p^\beta+1} = x^{p^\alpha+1}$$

We can now prove Theorem 4.5.

Proof of Theorem 4.5: *Let $n = p^\alpha + 1$. By the above Lemma we may assume that $1 \leq \alpha \leq 2e$. If $\alpha = 2e$ then $x^{p^\alpha+1} = (x^{p^e})^{p^e}x = xx = x^2$. So consider the case $1 \leq \alpha < 2e$ with $\alpha = e + \beta$, $\beta < e$. Then, for all $x \in GF^*(q)$:*

$$x^{p^\alpha+1} = (x^{p^e})^{(p^\beta+1)}x^{-(p^e-1)} = x^{p^\beta+1}x^{p^e-1} = x^{p^e+p^\beta} = (x^{p^{(e-\beta)}+1})^{p^\beta}.$$

This holds also for $x = 0$. Therefore the planes defined by $x^{p^\alpha+1}$ and $x^{p^{(e-\beta)}+1}$ are isomorphic and we may restrict ourselves to the range $1 \leq \alpha < e$.

4.3. Coulter-Matthews Planar Monomials, $x^{(3^\alpha+1)/2}$.

A new class of planar monomials was described by Coulter and Matthews [1]. This new class is related to Dickson polynomials of the first kind.

For any positive integer k, the *Dickson polynomial of the first kind* $g_k(x)$ over $GF(q)$, is the polynomial

$$g_k(x) = \sum_{i=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-i}\binom{k-i}{i}(-1)^i x^{k-2i}.$$

(See Lidl and Niederreiter [8].) Note that the substitution $x = \eta + \eta^{-1}$ gives the identity

$$g_k(\eta + \eta^{-1}) = \eta^k + \eta^{-k}.$$

Theorem 4.7 *The Dickson polynomial $g_k(x)$ is a permutation polynomial over $GF(q)$ if and only if $gcd(k, q^2 - 1) = 1$.*

Proof. *See Theorem 7.16 of Lidl and Niederreiter [7].*

Theorem 4.8. *Let $q = 3^e$ and $\alpha \in \mathbb{N}$. The polynomial $f(x) = x^{(3^\alpha+1)/2}$ is planar over $GF(q)$ if and only if $(\alpha, e) = 1$ and α is odd.*

Proof: *See Theorem 4.1 of Coulter and Matthews [1].*

Coulter and Matthews proved their theorem by showing that $x^{(3^\alpha+1)/2}$ is planar over $GF(3^e)$ if and only if the Dickson polynomial of the first kind $g_{(3^\alpha-1)/2}(x)$ is a permutation polynomial over $GF(3^e)$.
Writing $x = \eta + \eta^{-1}$, then

$$g_{(3^\alpha-1)/2}(\eta + \eta^{-1}) = \eta^{(3^\alpha-1)/2} + \eta^{-(3^\alpha-1)/2}.$$

A necessary and sufficient condition for $g_{(3^\alpha-1)/2}(\eta + \eta^{-1})$ to be a permutation polynomial is that $((3^\alpha - 1)/2, q^2 - 1) = 1$, which they show is equivalent to $(\alpha, 2e) = 1$.

A related class of planar monomials is described in the following theorem.

Theorem 4.9. *Let $q = 3^e$ and $n = (3^\alpha + q)/2$ where $\alpha \in \mathbb{N}$. The polynomial x^n is planar over $GF(q)$ if and only if $(\alpha, e) = 1$ and $\alpha - e$ is odd.*

Proof. *See Theorem 4.2 Coulter and Matthews [1].*

In considering candidates for α such that $x^{(3^\alpha+1)/2}$ is planar, we can again restrict ourselves to the case $1 \leq \alpha < e$. See Lemma 4.3 and Theorem 6.2 of Coulter and Matthews [1].

A natural question is: Are there planar monomials over $GF(p^e)$ of the form $x^{(p^\alpha+1)/2}$ for primes other than 3? The following result, which was known to Coulter and Matthews, shows that the answer is no.

Theorem 4.10. *The polynomials $f(x) = x^{(p^\alpha+1)/2}$ is planar over $GF(p^e)$ if and only if $p = 3$ and $(\alpha, 2e) = 1$.*

Proof: *If $p = 3$ and $(\alpha, 2e) = 1$ then $x^{(p^\alpha+1)/2}$ is planar over $GF(3^e)$ by Theorem 4.8. Now suppose $p > 3$ and $f(y) = y^n$. Then f is planar if and only if $(y + a)^n - y^n$ is a permutation polynomial over $GF(q)$ for all $\alpha \in GF(q)$. Let $y = x - 2$. If $h(x) = \delta(f, 4)(x - 2)$ then*

$$\begin{aligned} h(x) &= ((x-2)+4)^n - (x-2)^n \\ &= (x+2)^n - (x-2)^n. \end{aligned}$$

If $h(x)$ is not a permutation polynomial, then f is not planar. We will show that $h(x)$ is a Dickson polynomial of the first kind, i.e. $h(x) = 2g_{(p^\alpha-1)/2}(x)$, and that this is a permutation polynomial if and only if $p=3$. If $x = \eta + \eta^{-1}$ then

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

If $n = \frac{p^\alpha+1}{2}$ then

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

Now $h(x) = 2g_{(p^\alpha-1)/2}(x)$ is a permutation polynomial over $GF(q)$ if and only if $((p^\alpha-1)/2, q^2-1) = 1$. Since $q^2 \equiv 1(mod\ 4)$ (for all primes $p > 2$) this is equivalent to the condition that $2 = (p^\alpha - 1, p^{2e}-1) = (p^{(\alpha,2e)}-1)$, which holds if and only if $(\alpha, 2e) = 1$ and $p = 3$.

4.4 Planes Determined by Planar Monomials $x^{p^\alpha+1}$ and $x^{(3^\alpha+1)/2}$

From Section 3 we have the result that if $\mathcal{U}(f,q)$ is a Desarguesian plane defined by a planar monomial with $f(x) = x^n$, then $n = 2$. We now consider planes determined by planar monomials $x^{p^\alpha+1}$ and $x^{(3^\alpha+1)/2}$. Every planar polynomial over a prime field $GF(p)$ reduces to a quadratic polynomial. The only known planar polynomials over $GF(p^e)$ are $f(x) = x^{p^\alpha+1}$, where $\alpha = 0$ or $\frac{e}{(\alpha,e)}$ is odd, and $f(x) = x^{(p^\alpha+1)/2}$, where $(\alpha, e) = 1, \alpha$ odd and $p = 3$.

Theorem 4.11 *The planes defined by planar monomials of the form* $x^{p^\alpha+1}$ *and* $x^{(3^\alpha+1)/2}$ *over* $GF(p^2)$ *are Desarguesian.*

Proof: *If* $\alpha = 0$, *then* $x^{p^\alpha+1} = x^2$ *whose associated plane is Desarguesian. If* $f(x) = x^{p^\alpha+1}, \alpha \neq 0$ *or* $f(x) = x^{(3^\alpha+1)/2}, \alpha \neq 0$, *is a planar function then by Theorem 4.5 and Theorem 6.2 of Coulter and Matthews [2], we can restrict ourselves to the case where* $1 \leq \alpha < e$. *Thus* $e = 2$ *implies* $\alpha = 1$. *Then* $x^{(3^\alpha+1)/2} = x^2$ *whose corresponding plane is Desarguesian. For* $x^{p^\alpha+1}$, $\frac{2}{(1,2)}$ *is not odd so the only planar monomial of the form* $x^{p^\alpha+1}$ *over* $GF(p^2)$ *is* $f(x) = x^2$.

Note: Dembowski-Ostrom planar polynomials described a semifield and all semifields of order p^2, where p is a prime, are fields (with corresponding planes that are Desarguesian). By Theorem 3.7 the only planar monomials that describe a Desarguesian plane are of the form ax^2. The Coulter-Matthews condition for $x^{p^\alpha+1}$ to be planar over $GF(p^e)$, i.e. that $\frac{e}{(\alpha,e)}$ is odd, differs from the previously held sufficient condition that $\alpha = 0$ or $(\alpha, e) = 1$. While $\alpha = 0$ is a sufficient condition ($f(x) = x^2$ in this case) $(\alpha, e) = 1$ would imply x^{p+1} is planar over $GF(p^2)$ but this contradicts the results of Theorem 3.7 which states that in this case $n = 2$.

For $GF(3^3)$, the polynomial $f(x) = x^{(3^\alpha+1)/2}$ in reduced form is planar if and only if $1 \leq \alpha < 3, \alpha$ odd, and $(\alpha, 3) = 1$. This implies that α must be 1. Again, $x^{(3^\alpha+1)/2} = x^2$ and the corresponding plane is Desarguesian.

The Dembowski-Ostrom monomial, $f(x) = x^{p^\alpha+1}, 1 \leq \alpha < 3$ is planar over $GF(p^3)$ if and only if $\frac{3}{(\alpha,3)}$ is odd. If $\alpha = 1$, then $f(x) = x^{p+1}$ is planar over $GF(p^3)$ and if $\alpha = 2$ then $x^{p^\alpha+1}$ is planar over $GF(p^3)$. Note that x^{p+1} and x^{p^2+1} are planar monomials over $GF(p^3)$ that define non-Desarguesian planes. This answers a question raised by Coulter and Matthews [2, p.183].

Section 5: Exponent Bounds of Planar Polynomials.

5.1 Background of the Problem

By Definition 1.1 a quadratic polynomial is planar over $GF(q)$. Therefore in looking for other planar monomials of the form x^r, we may assume $r > 2$. Note that $f(x) = x^r$ is a planar polynomial over the field $GF(q)$ if and only if $(x + d)^r - x^r$ is a permutation polynomial over $GF(q)$ for each $d \in GF^*(q)$. In Johnson [6] the author proves the polynomial

$\varphi(x) = (x+1)^r - x^r$ for $1 \leq r \leq p-1$ is a permutation over $GF(p)$, p an odd prime, if and only if $r = 2$. Since $(x+d)^r - x^r = d^r[(\frac{x}{d}+1) - (\frac{x}{d})^r]$, the polynomial $f(x) = x^r$ is a planar polynomial over $GF(q)$ if and only if $(x+1)^r - x^r$ is a permutation polynomial over $GF(q)$. Johnson's result showed that over $GF(p)$ the only planar monomial is x^2.

In other words, Johnson showed that if $f(x) = x^r, r \leq p-1, r \neq 2$, then $f(x)$ is not a planar monomial. Corollary 5.2 is an extension of this result. It considers planar monomials over $GF(q), q = p^e$, and shows that if $r \leq p$ and $r \neq 2$, then $f(x) = x^r$ is not a planar monomial.

Johnson's proof uses the following result:

Consider the permutation polynomial $\varphi(x)$ over $GF(p^e)$. For each integer k with $(k,p) = 1$ and $2 \leq k \leq p^e - 2$ the polynomial $(\varphi(x))^k$ must reduce to a polynomial of degree $\leq p^e - 2$ when replacing x^{p^e} by x.

He then chooses k to be $2n$ with $n = \lfloor \frac{p-1}{r} \rfloor$ where $2 < r < p$ (with r even and $r \not| (p-1)$ being necessary conditions for x^r to be a planar polynomial) and shows that $(\varphi(x))^{2n} = \{(x+1)^r - x^r\}^{2n}$ has only one term of degree $p-1$. The binomial coefficients for this term are not congruent to 0 mod p since they involve numbers less than p. The $(\varphi(x))^{2n}$ reduces to a polynomial of degree $p-1$ and thus cannot be a permutation polynomial (and hence x^r cannot be a planar polynomial).

In Hiramine [5] the author considers planar polynomials over $GF(p)$. Let $d \in GF(p) - \{0\}$. If the function $f_d : GF(p) \to GF(p)$ defined by $f_d(x) = f(x+d) - f(x)$ is bijective, then f is a planar function. He gives two condition for a function f to be planar. Using these conditions, Hiramine shows that over $GF(p)$ the only planar functions are the quadratic polynomials.

Hiramine's proof resembles Johnson's proof for planar monomials in that he shows $(f(x+d) - f(x))^{2n}$, where $n = \lfloor \frac{p-1}{r} \rfloor$ and r is the degree of the polynomial $f(x)$ with $r \neq 2$, has only one term of degree $p-1$ and the coefficients of this term are not congruent to zero modulo p. This contradicts his given conditions for the planarity of f. His proof differs from Johnson's in that he considers the sum $\sum_{x \in GF(p)} (f(x+d) - f(x))^m$ in determining the unique term of degree $p-1$.

In this section we show that if $f(x) = x^r$ is planar over $GF(p^e)$ with $e \geq 1$, then either $r = 2$ or $r > p$. This generalizes Hiramine's and Johnson's results in the case where $e = 1$. A proof combining both techniques of Hiramine and Johnson was found by one of the authors. It is possible that it can be refined to determine completely which monomials are planar over $GF(p^e)$. In another direction, it may be refined to show that all planar polynomials over $GF(p^e)$ have degree 2 or degree $> p$.

However, we give a different proof which is based on Hiramine's result and applies to a larger class of polynomials. We define strongly planar polynomials and show that such polynomials have degree 2 or degree r where r

is at least p.

5.2 Strongly Planar Polynomials over $GF(p^e)$

Definition 5.1 *A strongly planar polynomial is a planar polynomial over $GF(p^e)$ which fixes $GF(p)$.*

Theorem 5.1 *Let $f(x)$ be a strongly planar polynomial over $GF(p^e)$. Then either deg $f(x) = 2$ or deg $f(x) \geq p$.*

Proof: *If f is a planar polynomial over $GF(p^e)$ then f is planar over $GF(p)$. Every planar polynomial over a prime field $GF(p)$ must reduce to a quadratic polynomial (see Gluck [4], Hiramine [5], Rónyai and Szönyi [9]). Thus $f(x)$ induces on $GF(p)$ the same function as $ax^2 + bx + c$ for some $a, b, c \in GF(p), a \neq 0$. Consider $g(x) = f(x) - (ax^2 + bx + c)$ as a polynomial over $GF(p^e)$. If $g(x)$ is not the zero polynomial then $g(x)$ has at least p roots, namely the elements of $GF(p)$. Therefore deg $g(x) \geq p$ so deg $f(x) \geq p$. If deg $f(x) = p$ then deg $g(x) = p$ and $x^p - x | g(x)$. Therefore, $g(x) = f(x) - (ax^2 - bx + c) = \alpha(x^p - x), \alpha \in GF(p^e)$. Then $f(x) = \alpha(x^p - x) + ax^2 + bx + c$.*

Corollary 5.2 *If $f(x) = x^n$ is a planar polynomial over $GF(p^e)$ then either $n = 2$ or $n > p$.*

Proof: *Assume $n > 2$. Since $f(x) = x^n$ fixes $GF(p)$ then by Theorem 5.1, $n \geq p$. If $n = p$, then $f(x) = x^p$. By Coulter and Matthews [1], $f(x) = x^p = (x^1)^p$ is planar if and only if $h(x) = x$ is planar. Since $h(x) = x$ is not planar, $f(x) = x^p$ is also not planar. Thus $n > p$.*

REFERENCES

[1] Coulter, R., and Matthews, R.W., Planar Functions and Planes of Lenz-Barlotti Class II. *Des. Codes Cryptogr.* 10, **2** (1997), 167-184.

[2] Dembowski, P., "Finite Geometries", Springer, New York, N. Y. 1968.

[3] Dembowski, P. and Ostrom, T. G., Planes of Order n with Collineation Groups of Order n^2, *Math. Zeit.* **103** (1968), 239-258.

[4] Gluck, D., A Note on Permutation Polynomials and Finite Geometries, *Discrete Mathematics* **80** (1990), 97-100.

[5] Hiramine, Y., A Conjecture on Affine Planes of Prime Order, J. Combin.Theory Ser. A 52,**1** (1989), 44-50.

[6] Johnson, N. L., Projective Planes of Order p That Admit Collineation Groups of Order p^2, *J. of Geom.* **30** (1987), 49-68.

[7] Lidl, R. and Niederreiter, H., "Finite Fields", Cambridge University Press, Cambridge, Great Britain, 1997.

[8] Polster, B., Continuous Planar Functions, *Abh. Math. Sem. Univ., Hamburg* **66** (1996), 113-129.

[9] Rónyai, L and Szönyi, T., Planar Functions over Finite Fields, *Combinatorica 9*, **3** (1989), 315-320.