PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 134, Number 11, November 2006, Pages 3373–3378
S 0002-9939(06)08346-8
Article electronically published on May 12, 2006

THE CLASSIFICATION OF PLANAR MONOMIALS OVER FIELDS OF PRIME SQUARE ORDER

ROBERT S. COULTER

(Communicated by John R. Stembridge)

Abstract. Planar functions were introduced by Dembowski and Ostrom in 1968 to describe affine planes possessing collineation groups with particular properties. To date their classification has only been resolved for functions over fields of prime order. In this article we classify planar monomials over fields of order p^2 with p a prime.

1. Preliminary results and notation

Let p be a prime, e a natural number, $q = p^e$ and let $\mathbb{F}_q$ denote the finite field of order q. The ring of polynomials in X over $\mathbb{F}_q$ is denoted by $\mathbb{F}_q[X]$. It is well known that any function over $\mathbb{F}_q$ can be uniquely represented by a polynomial in $\mathbb{F}_q[X]$ of degree at most $q-1$. A polynomial $f \in \mathbb{F}_q[X]$ is called a *permutation polynomial* over $\mathbb{F}_q$ if f induces a bijection of $\mathbb{F}_q$ under substitution. We will use the classical criterion of Hermite for a polynomial to be a permutation polynomial.

Lemma 1.1 (Hermite [6]; Dickson [4])**.** *A polynomial $f \in \mathbb{F}_q[X]$, $q = p^e$, is a permutation polynomial over $\mathbb{F}_q$ if and only if*

(i) *f has exactly one root in $\mathbb{F}_q$, and*
(ii) *the reduction of $f^t \bmod (X^q - X)$, with $0 < t < q-1$ and $t \not\equiv 0 \bmod p$, has degree less than $q-1$.*

A polynomial $f \in \mathbb{F}_q[X]$ is called a *planar polynomial* if for every non-zero $a \in \mathbb{F}_q$, the polynomial $f(X+a) - f(X)$ is a permutation polynomial over $\mathbb{F}_q$. Any quadratic polynomial is planar over any field of odd characteristic. It is also straightforward to show that there are no planar polynomials over fields of characteristic 2. Consequently all statements given in this article concern fields of odd prime characteristic p.

The motivation for studying planar functions stems from an article of Dembowski and Ostrom [3], where they used such functions to construct affine planes of order n with collineation groups of order n^2. In addition, it was recently shown that the classification of planar polynomials of the form

$$\sum_{i,j=0}^{e-1} a_{ij} X^{p^i+p^j} \in \mathbb{F}_{p^e}[X],$$

Received by the editors April 26, 2005 and, in revised form, May 17, 2005.
2000 *Mathematics Subject Classification.* Primary 51E15, 11T06.

p an odd prime, is equivalent to the classification of commutative semifields of order p^e; see [1]. The Dembowski-Ostrom conjecture implies the classification of all planar polynomials is equivalent to classifying planar polynomials of this form. Although shown to be false in characteristic 3, the conjecture remains open for characteristic 5 and greater.

The classification of planar monomials over prime fields was given by Johnson (the full classification over prime fields followed soon after, independently, in [5], [7], and [12]).

Lemma 1.2 (Johnson, [8, Theorem 4.6])**.** *The polynomial X^n is planar over $\mathbb{F}_p$ if and only if $n \equiv 2 \bmod (p-1)$.*

Few necessary conditions are known in the general case, even for monomials. Among the stronger statements is the following part of [2], Proposition 2.4.

Lemma 1.3. *If X^n is planar over $\mathbb{F}_q$, then $(n, q-1) = 2$.*

By [2], Proposition 2.4, X^n is planar over $\mathbb{F}_q$ if and only if $f(X) = (X+1)^n - X^n$ is a permutation polynomial over $\mathbb{F}_q$. Since $f(\mathbb{F}_q) \subseteq \mathbb{F}_q$ for any $f \in \mathbb{F}_p[X]$, the following is clear.

Lemma 1.4. *If X^n is planar over $\mathbb{F}_q$, then X^n is planar over every subfield of $\mathbb{F}_q$.*

The next result is a special case of [2], Theorem 2.3.

Lemma 1.5. *The monomial X^n is planar over $\mathbb{F}_q$ if and only if X^{np^i} is planar over $\mathbb{F}_q$ for any non-negative integer i.*

We will also need the following well-known theorem of Lucas.

Lemma 1.6 (Lucas, [9])**.** *Let p be a prime and let $\alpha \geq \beta$ be positive integers with base p expansions $\alpha = \sum_i \alpha_i p^i$ and $\beta = \sum_j \beta_j p^j$. Then*

$$\binom{\alpha}{\beta} \equiv \prod_i \binom{\alpha_i}{\beta_i} \bmod p,$$

where we use the convention $\binom{n}{k} = 0$ if $n < k$.

2. The classification of planar monomials over $\mathbb{F}_{p^2}$

Theorem 2.1. *The polynomial X^n is planar over $\mathbb{F}_{p^2}$, p an odd prime, if and only if $n \equiv 2 \bmod (p^2-1)$ or $n \equiv 2p \bmod (p^2-1)$.*

Proof. We need only consider $n < p^2$ since for $n \geq p^2$ the monomial X^k with $k \equiv n \bmod (p^2-1)$ acts the same as X^n under evaluation. Let $n = a + bp$ be the base p expansion of n. If X^n is planar over $\mathbb{F}_{p^2}$, then $n \equiv 2 \bmod (p-1)$ by Lemmas 1.2 and 1.4. It follows that we need only consider two cases: $a + b = 2$ or $a + b = p + 1$.

If $a + b = 2$, then we have $n \in \{2, p+1, 2p\}$. If $n = 2$, then X^n is planar over $\mathbb{F}_{p^2}$, as any quadratic is planar over any finite field of odd characteristic. It follows that X^{2p} is planar over $\mathbb{F}_{p^2}$ by applying Lemma 1.5. If $n = p + 1$, then $(n, p^2-1) = p + 1 > 2$, so that X^{p+1} is not planar over $\mathbb{F}_{p^2}$ by Lemma 1.3.

Now suppose $a + b = p + 1$. Note that $2 \leq a \leq p-1$ and $2 \leq b \leq p-1$. If $p = 3$, then $a = b = 2$ and $n = p^2 - 1 = 8$ and so X^n cannot be planar by Lemma 1.3.

For the remainder of the proof we assume $p \geq 5$. Set $f(X) = (X+1)^n - X^n$ and consider the polynomial

$$\begin{aligned} g(X) &= f(X)^{p+1} \bmod (X^{p^2} - X) \\ &= (X+1)^{n(p+1)} + X^{n(p+1)} - X^{np}(X+1)^n - X^n(X+1)^{pn} \bmod (X^{p^2} - X). \end{aligned}$$

We show $g(X)$ has degree $p^2 - 1$. It will then follow from Lemma 1.1 that f cannot be a permutation polynomial over $\mathbb{F}_{p^2}$ and so X^n is not planar over $\mathbb{F}_{p^2}$, establishing the result. We consider each of the components of $g(X)$ in turn, determining the coefficient of X^{p^2-1} generated in each case.

Set $h(X) = (X+1)^n$. It follows from Lemma 1.6 that

$$h(X) = \sum_{\alpha=0}^{a} \sum_{\beta=0}^{b} \binom{a}{\alpha} \binom{b}{\beta} X^{\alpha+\beta p}.$$

Since $h \in \mathbb{F}_p[X]$, $h(X)^p = h(X^p)$, and so

$$h(X)^p \equiv \sum_{\alpha=0}^{a} \sum_{\beta=0}^{b} \binom{a}{\alpha} \binom{b}{\beta} X^{\beta+\alpha p} \bmod (X^{p^2} - X).$$

Hence

$$h(X)^{p+1} \equiv \sum_{\alpha=0}^{a} \sum_{\beta=0}^{b} \sum_{\gamma=0}^{a} \sum_{\delta=0}^{b} \binom{a}{\alpha} \binom{b}{\beta} \binom{a}{\gamma} \binom{b}{\delta} X^{\beta+\gamma+(\alpha+\delta)p} \bmod (X^{p^2} - X).$$

Now $\beta + \gamma + (\alpha + \delta)p \leq (p+1) + (p+1)p < 2(p^2 - 1)$ for $p \geq 5$. Hence the only terms of degree $p^2 - 1$ in $h(X)^{p+1} \bmod (X^{p^2} - X)$ are those terms where $\beta + \gamma = \alpha + \delta = p - 1$. In particular, δ and γ are completely determined by α and β. Since $0 \leq \alpha \leq a$, $0 \leq \delta \leq b$ and $a + b = p + 1$, the only way we can have $\alpha + \delta = p - 1$ is if $a - 2 \leq \alpha \leq a$ and $\delta = p - 1 - \alpha$. A similar argument yields $b - 2 \leq \beta \leq b$. Thus the coefficient, c, of X^{p^2-1} in $h(X)^{p+1} \bmod (X^{p^2} - X)$ is

$$\sum_{\alpha=a-2}^{a} \sum_{\beta=b-2}^{b} \binom{a}{\alpha} \binom{b}{\beta} \binom{a}{p-1-\beta} \binom{b}{p-1-\alpha}.$$

Recalling $\binom{n}{k} = \binom{n}{n-k}$ and $a + b = p + 1$, we write this in the equivalent form

$$c = \sum_{\alpha=a-2}^{a} \sum_{\beta=b-2}^{b} \binom{a}{\alpha} \binom{b}{\beta} \binom{a}{\beta+2-b} \binom{b}{\alpha+2-a}.$$

Expanding, we have

$$\begin{aligned}
c &= \sum_{\alpha=a-2}^{a}\sum_{\beta=b-2}^{b}\binom{a}{\alpha}\binom{b}{\beta}\binom{a}{\beta+2-b}\binom{b}{\alpha+2-a}\\
&= \left(\sum_{\alpha=a-2}^{a}\binom{a}{\alpha}\binom{b}{\alpha+2-a}\right)\left(\sum_{\beta=b-2}^{b}\binom{b}{\beta}\binom{a}{\beta+2-b}\right)\\
&= \left(\binom{a}{2}+\binom{a}{1}\binom{b}{1}+\binom{b}{2}\right)^2\\
&= \left(\frac{a(a-1)}{2}+ab+\frac{b(b-1)}{2}\right)^2\\
&\equiv \left(\frac{a(a-1)}{2}+a(1-a)+\frac{-a(1-a)}{2}\right)^2 \bmod p\\
&\equiv \left(\frac{a(a-1)}{2}-a(a-1)+\frac{a(a-1)}{2}\right)^2 \bmod p\\
&\equiv 0 \bmod p.
\end{aligned}$$

Hence we get no term of degree p^2-1 from $h(X)^{p+1} \bmod (X^{p^2}-X)$.

Since $n(p+1) \equiv 2p+2 \bmod p^2-1$, it follows that $X^{n(p+1)} \equiv X^{2p+2} \bmod (X^{p^2}-X)$. For $p \geq 5$, $2p+2 < p^2-1$, and so we get no term of degree p^2-1 from this component.

Next we have

$$X^{np}(X+1)^n = X^{np}h(X) \equiv \sum_{\alpha=0}^{a}\sum_{\beta=0}^{b}\binom{a}{\alpha}\binom{b}{\beta}X^{b+\alpha+(a+\beta)p} \bmod (X^{p^2}-X).$$

Now $b+\alpha+(a+\beta)p < 2(p^2-1)$ for $p \geq 5$, and so the only term of degree p^2-1 in $X^{np}(X+1)^n \bmod (X^{p^2}-X)$ is the term where $b+\alpha = a+\beta = p-1$. The coefficient of this term is

$$\binom{a}{p-1-b}\binom{b}{p-1-a} = \binom{a}{2}\binom{b}{2}.$$

The final component is

$$X^n(X+1)^{pn} = X^n h(X)^p \equiv \sum_{\alpha=0}^{a}\sum_{\beta=0}^{b}\binom{n}{\alpha+\beta p}X^{a+\beta+(b+\alpha)p} \bmod (X^{p^2}-X).$$

In a case similar to the previous one, we have $a+\beta+(b+\alpha)p < 2(p^2-1)$, so that the coefficient of the only term of degree p^2-1 in $X^n(X+1)^{pn} \bmod (X^{p^2}-X)$ is

$$\binom{a}{p-1-b}\binom{b}{p-1-a} = \binom{a}{2}\binom{b}{2}.$$

Overall, the coefficient of X^{p^2-1} in $f(X)^{p+1} \bmod (X^{p^2}-X)$ is therefore

$$\begin{aligned} -2\binom{a}{2}\binom{b}{2} &= -2\left(\frac{a(a-1)}{2}\frac{b(b-1)}{2}\right) \\ &\equiv -2\left(\frac{a(a-1)}{2}\right)^2 \bmod p \\ &\not\equiv 0 \bmod p, \end{aligned}$$

as $2 \le a \le p-1$. Hence $g(X)$ has degree p^2-1, and so Hermite's Criteria now shows $f(X)$ cannot be a permutation polynomial over $\mathbb{F}_{p^2}$. It follows that X^n is not planar over $\mathbb{F}_{p^2}$ if $n = a + bp$ and $a + b = p + 1$. □

It should be mentioned that both possibilities in the theorem define Desarguesian planes.

3. Some remarks on the classification of planar monomials over $\mathbb{F}_p$

When restricted to monomials, the Dembowski-Ostrom conjecture implies that every planar monomial over $\mathbb{F}_{p^e}$ is of the form X^n with $n = p^i + p^j$. The planarity of such monomials is well understood, [2, Theorem 3.2]: with $n = p^i + p^j$ and $i \ge j$, X^n is planar over $\mathbb{F}_{p^e}$ if and only if $\frac{e}{(i-j,e)}$ is odd. The conjecture remains open for characteristic $p \ge 5$. However, it was shown to be false in characteristic 3 by Matthews and the author in [2]. There it was shown that X^n with $n = \frac{3^\alpha+1}{2}$ is planar over $\mathbb{F}_{3^e}$ if and only if $(\alpha, 2e) = 1$. Using the identity $n = \frac{p^\alpha+1}{2} = \frac{p^\alpha+p}{2} - \frac{p-1}{2}$, it is straightforward to show $n \equiv 1 - \alpha\left(\frac{p-1}{2}\right) \bmod (p-1)$. If X^n is planar over $\mathbb{F}_{p^e}$, then it is planar over $\mathbb{F}_p$ by Lemma 1.4, and now Lemma 1.2 yields $n \equiv 2 \bmod (p-1)$. This implies α is odd and $p = 3$, and so this case does not yield a counterexample to the conjecture for $p \ge 5$; see also [11].

For general n, a consequence of Lemmas 1.2 and 1.4 is that if X^n is planar over $\mathbb{F}_{p^e}$, then $n = 2 + k(p-1)$ for some integer k. Thus $n = 2, p+1, 2p$ are the three smallest possibilities. Since each of these may be written as $p^i + p^j$ for particular i, j, the planarity of each of these is easily determined. In fact, the smallest exponent n for which the planarity of X^n over $\mathbb{F}_{p^e}$ is not known is $n = 3p-1$. For $p \ge 5$, a combination of Lemma 1.4 and Theorem 2.1 shows that X^{3p-1} is not planar over $\mathbb{F}_{p^e}$ whenever e is even. We can also eliminate characteristic 3 with little effort. Let $n = 3^t - 1$. Then

$$(X-1)^{3^t-1} - X^{3^t-1} = \frac{(X-1)^{3^t}}{X-1} - X^{3^t-1} = \frac{X^{3^t}-1}{X-1} - X^{3^t-1} = h_{3^t-2}(X),$$

where $h_k(X) = 1 + X + \cdots + X^k$. The permutation behaviour of $h_k(X)$ over fields of odd characteristic was completely determined by Matthews in [10]: $h_k(X)$ permutes $\mathbb{F}_{p^e}$ with p odd if and only if $k \equiv 1 \bmod p(p^e-1)$. Now $3^t - 1 \equiv 3^{t \bmod e} - 1 \bmod (3^e-1)$, and so $3^t - 2 \equiv 1 \bmod 3(3^e-1)$ if and only if $3^{t \bmod e} = 3$. Thus $h_{3^t-2}(X)$ is a permutation polynomial over $\mathbb{F}_{3^e}$ (and hence X^n is planar over $\mathbb{F}_{3^e}$) if and only if $t \equiv 1 \bmod e$. In summary:

Proposition 3.1. *Let t and e be positive integers. The monomial X^{p^t-1} is planar over $\mathbb{F}_{p^e}$ if and only if $p = 3$ and $t \equiv 1 \bmod e$.*

In particular, X^8 cannot be planar over $\mathbb{F}_{3^e}$ unless $e = 1$. In another direction, an application of Lemma 1.3 yields the following statement.

Proposition 3.2. *Let $p \equiv 3 \bmod 4$, e be even, k be odd, and $n = 2 + k(p-1)$. Then X^n is not planar over $\mathbb{F}_{p^e}$.*

It follows from the above discussion that the smallest exponent n for which the planarity of X^n over $\mathbb{F}_{p^e}$ is not known is:

- for $p = 3$, $n = \begin{cases} 16 & \text{if } e \text{ is odd,} \\ 22 & \text{if } e \text{ is even,} \end{cases}$
- for $p \geq 5$, $n = \begin{cases} 3p-1 & \text{if } e \text{ is odd,} \\ p^2+2p-1 & \text{if } e \text{ is even.} \end{cases}$

References

[1] R.S. Coulter and M. Henderson, *Commutative presemifields and semifields*, preprint.

[2] R.S. Coulter and R.W. Matthews, *Planar functions and planes of Lenz-Barlotti class II*, Des. Codes Cryptogr. **10** (1997), 167–184. MR1432296 (97j:51010)

[3] P. Dembowski and T.G. Ostrom, *Planes of order n with collineation groups of order n^2*, Math. Z. **103** (1968), 239–258. MR0226486 (37:2075)

[4] 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. MR1502214, MR1502221

[5] D. Gluck, *A note on permutation polynomials and finite geometries*, Discrete Math. **80** (1990), 97–100. MR1045927 (91b:11141)

[6] C. Hermite, *Sur les fonctions de sept lettres*, C.R. Acad. Sci. Paris **57** (1863), 750–757.

[7] Y. Hiramine, *A conjecture on affine planes of prime order*, J. Combin. Theory Ser. A **52** (1989), 44–50. MR1008158 (90g:51011)

[8] N.L. Johnson, *Projective planes of order p that admit collineation groups of order p^2*, J. Geometry **30** (1987), 49–68. MR0914241 (88m:51011)

[9] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math **1** (1878), 184–240, 289–321. MR1505161, MR1505164, MR1505176

[10] R. Matthews, *Permutation properties of the polynomials $1 + x + \cdots + x^k$ over a finite field*, Proc. Amer. Math. Soc. **120** (1994), 47–51. MR1165062 (94b:11118)

[11] D. Pierce and M.J. Kallaher, *A note on planar functions and their planes*, Bull. Inst. Combin. Appl. **42** (2004), 53–76. MR2082481 (2005f:51007)

[12] L. Rónyai and T. Szőnyi, *Planar functions over finite fields*, Combinatorica **9** (1989), 315–320. MR1030384 (91d:51008)

Department of Mathematical Science, 520 Ewing Hall, University of Delaware, Newark, Delaware 19716