THE CLASSIFICATION OF PLANAR MONOMIALS OVER FIELDS OF ORDER p^3

EMILY BERGMAN, ROBERT S. COULTER, AND IRENE VILLA

Abstract. We classify planar monomials over fields of prime cubed order using Hermite's criteria. More specifically, we prove that the only exponents n for which x^n is planar over fields of order p^3, p a prime, are the exponents $n = p^i + p^j$.

1. Introduction and the Main Result

Dembowski and Ostrom [6] introduced the notion of a planar function in 1968 when studying projective planes of order n with a collineation group $G \times H$, with $|G| = |H| = n$, acting transitively on the affine points. Though their definition dealt with functions $\phi : G \to H$, all known examples of planar functions exist over finite fields $\mathbb{F}_q$ of odd order $q = p^e$, p a prime, and where $G = H = \langle \mathbb{F}_q, + \rangle$.

Let $f \in \mathbb{F}_q[x]$ be a polynomial and $\mathbb{F}_q^\star$ denote the non-zero elements of $\mathbb{F}_q$.

- $f(x)$ is a *permutation polynomial (PP)* over $\mathbb{F}_q$ if f induces a bijection of $\mathbb{F}_q$ under the evaluation map $y \mapsto f(y)$.

  Permutation polynomials have been studied intensively over the past 40 years and there are a number of surveys giving overviews of modern results, the most recent of which we believe to be the survey of Hou [11].
- f is called *planar* if for every $a \in \mathbb{F}_q^\star$, the difference operator $\Delta_f(x, a) = f(x+a) - f(x)$ is a PP over $\mathbb{F}_q$. As was noted by Coulter and Matthews in [5], this condition simplifies significantly if $f(x) = x^n$. Specifically, x^n is *planar* over $\mathbb{F}_q$ if and only if the polynomial $f_n(x) = (x+1)^n - x^n$ is a permutation polynomial.

Planar functions cannot exist over fields of characteristic 2 as every non-trivial difference operator necessarily has a minimum of 2 pre-images for any image, as $\Delta_f(x, a) = \Delta_f(x + a, a)$ for all a. The best case scenario, where each non-trivial difference operator is strictly 2-1, is precisely the definition of an APN function, well-known for their optimal resistance against differential cryptanalysis when used in S-boxes [14].

Planar functions over prime fields were classified in 1989-90, independently by Gluck [8], Hiramine [10], and Rónyai and Szönyi [15]. This remains the only situation where a complete classification has been achieved. Further classification results have been achieved only for planar monomials. In 2006, Coulter [3] classified planar monomials over fields of order p^2, and they were subsequently classified over fields of order p^4 by Coulter and Lazebnik [4] in 2012. It should also be mentioned that Johnson [12] gave a classification of planar monomials over prime fields in 1987, predating the full classifications mentioned above. There is also a result of Zieve, who classified those monomials which are planar

Key words and phrases. planar functions, permtutation polynomials, projective planes.

R.S. Coulter was partially supported by the National Science Foundation, award #1855723.

I. Villa was partially supported by the Research Council of Norway, grant #247742/070, and the Trond Mohn Stiftelse (TMS) Foundation.

over infinitely many extensions of $\mathbb{F}_p$ in [16]. In this paper we classify planar monomials over fields of order p^3. Specifically, we prove

Theorem 1. *Let $q = p^3$ with p an odd prime. The monomial x^n is planar over $\mathbb{F}_q$ if and only if $n \equiv p^i + p^j \bmod (q-1)$ with $0 \leq i, j < 3$.*

For fields of order p, p^2 and p^4 with $p \geq 5$, the only planar monomials possible yield the Desarguesian plane, Thus, our result is the first classification result on planar functions which allows for a non-Desarguesian example: the planar monomial x^{p+1} constructs Albert's twisted field plane of order p^3.

2. The Basics of our Approach

By the definition, to show x^n is planar or not it is sufficient to consider whether $f_n(x) = (x+1)^n - x^n$ is a PP or not. As planarity is a property of functions we need only consider $n < q$. In fact, we may insist on $n \leq q-3$ as it is a necessary condition of planarity that $\gcd(n, q-1) = 2$, see [5], Proposition 2.4.

To prove our result, we use the same methods as those used in [3] and [4]. Specfically, Hermite's criteria is employed to exclude every n apart from those given in the theorem.

Lemma 1 (Hermite, [9]; Dickson, [7])**.** *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 $q-1$.

The t in this lemma is often referred to as a Hermite exponent. Effectively, to exclude a potential n, one only needs to find a single Hermite exponent for which the second condition fails. The criteria can often be unwieldy, and over time has come to be viewed as relatively ineffective. However, it has enjoyed somewhat of a renaissance in recent times, with several results being obtained using it, such as the aforementioned classifications of planar monomials over fields of order p^2 and p^4, and the results of Chou and Hou [2].

There are several points about Hermite's criteria and our specific problem which we now expand on. For arbitrary $0 < t < q-1$, we may write $f_n(x)^t \bmod (x^q - x)$ as

$$f_n^t \bmod (x^q - x) = \sum_{i=0}^{t} \binom{t}{i} (-1)^{t-i} \left[(x+1)^{ni} \bmod (x^q - x)\right] \left[x^{n(t-i)} \bmod (x^q - x)\right], \quad (1)$$

and first reduce each of the terms $(x+1)^{ni}$ and $x^{n(t-i)}$ independently. Connsequently, unless both terms have degree $q-1$, the only way in which we can obtain x^{q-1} terms in the reduced form of $f_n(x)^t$ is via the actual x^{q-1} term generated. This allows for much simplication in our arguments.

The value of binomial coefficients, whether it be in (1) or in the expansion of $(x+1)^{ni}$, is also clearly something we must handle. Fortunately, we have the following classical result of Lucas at our disposal.

Lemma 2 (Lucas, [13])**.** *Let p be a prime and $\alpha \geq \beta$ be positive integers with α and β having base-p expansions $\alpha = (\alpha_t \cdots \alpha_0)_p$ and $\beta = (\beta_t \cdots \beta_0)_p$, respectively. Then*

$$\binom{\alpha}{\beta} \equiv \prod_{i=0}^{t} \binom{\alpha_i}{\beta_i} \bmod p,$$

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

The theorem of Lucas encourages us to consider our exponent n in its base p expansion form. Set $n = (a_{e-1} \cdots a_0)_p$, with $0 \leq a_i < p$ for all i. There are several advantages in considering the base p expansion of n, over and above the possibility of applying Lucas' Theorem.

Firstly, x^{np} is planar over $\mathbb{F}_q$ if and only if x^n is planar over $\mathbb{F}_q$, and the reduction of x^{np} modulo $x^q - x$ is x^m, where $m = (a_{e-2} \cdots a_0 a_{e-1})_p$. Thus, we may cycle the base p digits of n around and could, for instance, choose to place the largest a_i in the most significant bit.

Secondly, if x^n is planar over $\mathbb{F}_q$, then it is necessarily planar over $\mathbb{F}_p$. This follows at once from observing $f_n \in \mathbb{F}_p[x]$. The classification of planar monomials over $\mathbb{F}_p$ now forces $n \equiv 2 \bmod (p-1)$. This provides the necessary condition

$$a_0 + a_1 + \cdots + a_{e-1} = S \equiv 2 \bmod (p-1).$$

Since $a_i < p$ for all $0 \leq i < e$, we have $S = 2 + k(p-1)$ for some $0 \leq k < e$.

Our proof of Theorem 1 can now be outlined. For the remainder of this article, assume $q = p^3$ and let $n = a_0 + a_1 p + a_2 p^2$ with $0 \leq a_i < p$. Set $S = a_0 + a_1 + a_2$. Based on our above discussion, there are three possible cases we must deal with:

Case 1. $S = 2$.
Case 2. $S = 2p$.
Case 3. $S = p + 1$.

The first case will be shown to be the only positive case, in that the latter two cases will prove to be empty of planar examples. While the case of $S = 2p$ can be excluded using a single Hermite exponent, the final case turns out to be exceedingly complicated, first involving two Hermite exponents that we must play off against each other to exclude all but 11 specific choices of n, and then using specific Hermite exponents to eliminate these remaining 11 possible choices for n. Each of these Hermite exponent proofs are long and technical, and due to space limitations we omit them.

3. Cases 1 and 2

Coulter and Matthews showed $x^{p^i+p^j}$ is planar over $\mathbb{F}_{p^e}$ if and only if $e/\gcd(j-i, e)$ is odd, see [5], Theorem 3.3. This completely resolves Case 1.

Proposition 1. *If $S = 2$, then $n = p^i + p^j$ with $0 \leq i \leq j < 3$, and x^n is always planar over $\mathbb{F}_q$.*

The case $S = 2p$ is also relatively straightforward, the proof following very similarly to the classification of planar monomials over $\mathbb{F}_{p^2}$, even down to the Hermite exponent used in [3].

Proposition 2. *If $S = 2p$, then the Hermite exponent $t = p + 1$ shows $f_n(x)$ is never a PP over $\mathbb{F}_q$. Hence, x^n is never planar over $\mathbb{F}_q$.*

4. Case 3

We are left with the case where $S = p + 1$. To eliminate this case from providing potential planar exponents, we must resort to dealing with a sequence of Hermite exponents. Throughout we assume $a_2 \geq a_0, a_1$, which we can safely do thanks to the observation given immediately after Lucas' Theorem concerning x^{np}.

Firstly, we deal with the situation where $a_i \geq 2$ for all i. To eliminate this broad subcase of Case 3 we consider two Hermite exponents.

Proposition 3. *Let $n = a_0 + a_1 p + a_2 p^2$, $S = a_0 + a_1 + a_2 = p + 1$, $a_2 \geq a_0, a_1$, and $a_i \geq 2$ for $i = 0, 1, 2$.*

(i) If $a_2 \geq (p+1)/2$, then the Hermite exponent $t = 2 + p + p^2$ shows $f_n(x)$ is not a PP over $\mathbb{F}_q$.

(ii) If $a_2 \leq (p+1)/2$, then it is impossible for the two Hermite exponents $t_1 = 2+p+p^2$ and $t_2 = 2 + 2p$ to both fail to show $f_n(x)$ is not a PP over $\mathbb{F}_q$.

Thus, x^n is not planar over $\mathbb{F}_q$.

We are unaware of another application of Hermite's criteria which uses two Hermite exponents simultaneously to obtain a non-PP result as we do for this case.

This leaves us to deal with the scenario where at least one of the a_i is less than 2. This last situation degenerates into a multitude of exceptions, with over 25 pages needed to give a full proof. The result can be stated as follows.

Proposition 4. *Let $n = a_0 + a_1 p + a_2 p^2$, $S = a_0 + a_1 + a_2 = p + 1$, $a_2 \geq a_0, a_1$, and $a_i < 2$ for at least one $i \in \{0, 1\}$. The Hermite exponent $t = 2 + 2p + 2p^2$ shows $f_n(x)$ is not a PP over $\mathbb{F}_q$ for all but 11 specific choices of n. The remaining 11 exceptions can also be shown to not be PPs over $\mathbb{F}_q$ using Hermite's criteria. The 11 exceptions, and the Hermite exponents used to eliminate them, are as follows:*

#1: $n = \frac{p+1}{2}(p + p^2)$ *with* $t = (p-2) + p$ *and* $t = (p-6) + p + 4p^2$,
#2: $n = \frac{p+1}{2}(1 + p^2)$ *with* $t = (p-2) + p$ *and* $t = (p-6) + p + 4p^2$,
#3: $n = 1 + (\frac{p+1}{2} - 1)p + \frac{p+1}{2}p^2$ *with* $t = 2p + 4p^2$,
#4: $n = (\frac{p+1}{2} - 1) + p + \frac{p+1}{2}p^2$ *with* $t = (p-2) + p$,
#5: $n = (\frac{p+1}{2} - 1) + (\frac{p+1}{2} + 1)p^2$ *with* $t = (p-6) + p + 2p^2$,
#6: $n = 1 + 3p + (p-3)p^2$ *with* $t = 2 + 4p + 4p^2$,
#7: $n = 1 + 2p + (p-2)p^2$ *with* $t = (p-1)(p + p^2)$,
#8: $n = 2 + p + (p-2)p^2$ *with* $t = 1 + 2p + 3p^2$,
#9: $n = 2 + (p-1)p^2$ *with* $t = 1 + 2p + 3p^2$,
#10: $n = 2p + (p-1)p^2$ *with* $t = 2 + (p-1)p$,
#11: $n = 1 + p + (p-1)p^2$ *with* $t = p - 1$.

Thus, x^n is not planar over $\mathbb{F}_q$.

Throughout all of our proofs, we assume $p \geq 11$, relying on the fact that the smaller values of p can be easily checked computationally. However, for some of these exceptional exponents, we must do further computations for certain primes to complete the proof. Specifically, for exceptions #1 and #2 we must check $p = 29$, while for the exception #6, we deal with all primes $p \leq 17$ and $p = 373$ computationally. All of these computations were carried out using the Magma Algebra package [1].

References

1. W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput. **24** (1997), 235–265.
2. W-S. Chou and X-D. Hou, *On a conjecture of Fernando, Hou and Lappano concerning permutation polynomials over finite fields*, Finite Fields Appl. **56** (2019), 58–92.
3. R.S. Coulter, *The classification of planar monomials over fields of prime square order*, Proc. Amer. Math. Soc. **134** (2006), 3373–3378.
4. R.S. Coulter and F. Lazebnik, *On the classification of planar monomials over fields of square order*, Finite Fields Appl. **18** (2012), 316–336.
5. R.S. Coulter and R.W. Matthews, *Planar functions and planes of Lenz-Barlotti class II*, Des. Codes Cryptogr. **10** (1997), 167–184.

6. P. Dembowski and T.G. Ostrom, *Planes of order n with collineation groups of order n^2*, Math. Z. **103** (1968), 239–258.
7. 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.
8. 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.
9. C. Hermite, *Sur les fonctions de sept lettres*, C.R. Acad. Sci. Paris **57** (1863), 750–757.
10. Y. Hiramine, *A conjecture on affine planes of prime order*, J. Combin. Theory Ser. A **52** (1989), 44–50.
11. X-D. Hou, *Permutaion polynomials over finite fields – A survey of recent advances*, Finite Fields Appl **32** (2015), 82–119.
12. N.L. Johnson, *Projective planes of order p that admit collineation groups of order p^2*, J. Geometry **30** (1987), 49–68.
13. E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math **1** (1878), 184–240, 289–321.
14. K. Nyberg, *Differentially uniform mappings for cryptography*, Advances in Cryptology - EUROCRYPT 1993, LNCS **765** (1993), 55–64.
15. L. Rónyai and T. Szőnyi, *Planar functions over finite fields*, Combinatorica **9** (1989), 315–320.
16. M.E. Zieve, *Planar functions and perfect nonlinear monomials over finite fields*, Des. Codes Cryptogr. **75** (2015), 71–80.

(E. Bergman and R.S. Coulter) Department of Mathematical Sciences, University of Delaware, Newark, Delaware, U.S.A.

(I. Villa) Department of Informatics, University of Bergen, Bergen, Norway

(I. Villa) Department of Mathematics, University of Trento, Trento, Italy