LOW-DEGREE PLANAR MONOMIALS IN CHARACTERISTIC TWO

PETER MÜLLER AND MICHAEL E. ZIEVE

ABSTRACT. Planar functions over finite fields give rise to finite projective planes and other combinatorial objects. They exist only in odd characteristic, but recently Zhou introduced an even characteristic analogue which has similar applications. In this paper we determine all planar functions on $\mathbb{F}_q$ of the form $c \mapsto ac^t$, where q is a power of 2, t is an integer with $0 < t \le q^{1/4}$, and $a \in \mathbb{F}_q^*$. This settles and sharpens a conjecture of Schmidt and Zhou.

1. INTRODUCTION

Let $q = p^r$ where p is prime and r is a positive integer. If p is odd then a *planar function* is a function $f\colon \mathbb{F}_q \to \mathbb{F}_q$ such that, for every $b \in \mathbb{F}_q^*$, the function $c \mapsto f(c + b) - f(c)$ is a bijection on $\mathbb{F}_q$. Planar functions have been used to construct finite projective planes [4], relative difference sets [6], error-correcting codes [3], and S-boxes in block ciphers which are optimally resistant to differential cryptanalysis [12].

If $p = 2$ then there are no functions $f\colon \mathbb{F}_q \to \mathbb{F}_q$ satisfying the defining property of a planar function, since 0 and b have the same image as one another under the map $c \mapsto f(c + b) - f(c)$. Recently Zhou [16] introduced a characteristic 2 analogue of planar functions, which have the same types of applications as do odd-characteristic planar functions. These will be the focus of the present paper. If $p = 2$, we say that a function $f\colon \mathbb{F}_q \to \mathbb{F}_q$ is planar if, for every $b \in \mathbb{F}_q^*$, the function $c \mapsto f(c + b) + f(c) + bc$ is a bijection on $\mathbb{F}_q$. Schmidt and Zhou showed that any function satisfying this definition can be used to produce a relative difference set with parameters $(q, q, q, 1)$, a finite projective plane, and certain codes with unusual properties [14, 16]. In what follows, whenever we refer to a planar function in characteristic 2, we mean a function satisfying Zhou's definition.

We will make progress towards a classification of planar polynomials in characteristic 2. All known planar functions in characteristic 2 have

the form $c \mapsto f(c)$ where $f(X) \in \mathbb{F}_q[X]$ is a polynomial in which the degree of every term is the sum of at most two powers of 2 [13, 14, 16]. Our main result describes all planar monomials of degree at most $q^{1/4}$:

Theorem 1.1. *Let t be a positive integer such that $t^4 \leq 2^r$, and let a be any element of $\mathbb{F}_{2^r}^*$. The function $c \mapsto ac^t$ is planar on $\mathbb{F}_{2^r}$ if and only if t is a power of 2.*

When t is odd, this result strengthens the main result of [14], which required $c \mapsto ac^t$ to be planar on infinitely many finite extensions of $\mathbb{F}_{2^r}$. In case t is even, Schmidt and Zhou have conjectured that if $c \mapsto ac^t$ is planar on infinitely many finite extensions of $\mathbb{F}_{2^r}$ then t must be a power of 2 [14, Conj. 10]. Theorem 1.1 settles and sharpens this conjecture, and gives a simpler proof of their result for odd t.

In the recent paper [18], the second author proved an analogue of Theorem 1.1 over finite fields of odd cardinality. However, in light of the subtle difference between the definitions of planarity in odd and even characteristics, the arguments in the odd characteristic proof are irrelevant here, and vice-versa. We also remark that our proof is completely different from the proof of the weaker version of the "odd t" case of Theorem 1.1 proved in [14], which involved a 14-page computation of the shapes of singularities of certain curves.

Our proof of Theorem 1.1 relies on a version of Weil's bound for singular plane curves. We apply Weil's bound to a carefully constructed auxiliary curve C which by construction has few $\mathbb{F}_q$-rational points. In order to apply Weil's bound, we must first show that C is irreducible over the algebraic closure of $\mathbb{F}_q$. We will show that, due to the specific form of the map $c \mapsto ac^t$, this irreducibility can be deduced from a generalization of Capelli's 1898 result about irreducibility of binomials [2]. We also sketch an alternate proof which, instead of Capelli's result, uses Lorenzini's theorem about the number of irreducible translates of a bivariate polynomial [10].

2. The main result

Our proof relies on a version of Weil's bound for (possibly singular) affine plane curves. Write $\overline{\mathbb{F}}_q$ for a fixed algebraic closure of $\mathbb{F}_q$.

Definition 2.1. A polynomial in $\mathbb{F}_q[X, Y]$ is *absolutely irreducible* if it is irreducible in $\overline{\mathbb{F}}_q[X, Y]$.

Lemma 2.2. *Any absolutely irreducible $H(X, Y) \in \mathbb{F}_q[X, Y]$ of (total) degree d has at least $q + 1 - (d-1)(d-2)\sqrt{q} - d$ zeroes in $\mathbb{F}_q \times \mathbb{F}_q$.*

Remark. The key ingredient in the proof of Lemma 2.2 is Weil's bound on the number of $\mathbb{F}_q$-rational points on a smooth projective curve over $\mathbb{F}_q$ of prescribed genus [15, p. 70, Cor. 3]. Lemma 2.2 is deduced from Weil's bound in [1, Cor. 2.5] and [8, Cor. 2(b)]. Since this result has been the source of some confusion, we now clarify the relevant literature. The first attempt to prove a version of Lemma 2.2 occurred in [9, p. 331], and was based on the mistaken notion that Weil's bound for the number of points on a smooth projective curve remains true for singular curves (a counterexample is $X^3 + Y^3 + XYZ + X^2Y = 0$ over $\mathbb{F}_2$). Soon thereafter it was claimed in [11, (14)] that Weil's upper bound holds true for the number of points on a singular affine plane curve, which is false for $X^3 + Y^3 + X + Y + X^2Y + XY = 0$ over $\mathbb{F}_2$. Another version of Lemma 2.2 occurs as [5, Thm. 4.9], whose proof relies on the mistaken notion that the number of points on a singular projective curve is no bigger than the number of degree-one places in its function field (a counterexample is $XY^2 + XYZ + XZ^2 + Y^3 + Y^2Z + Z^3 = 0$ over $\mathbb{F}_2$). The version of Lemma 2.2 stated in [17, Rem. 8.4.18] is missing the final d. Finally, we note that one must replace the stated value of k_d in [1, Lemma 3.2] by $(d-1)(d-2)/2$, in order to make the result follow from its proof. The stated value of k_d appears to have arisen from an incorrect formula for the discriminant of a quadratic polynomial.

Proof of Theorem 1.1. If t is a power of 2 then $c \mapsto ac^t$ is planar on $\mathbb{F}_q$ for every (even) q and every $a \in \mathbb{F}_q^*$, since $a(X+b)^t + aX^t + bX = ab^t + bX$ is a degree-one polynomial (and hence is bijective on $\mathbb{F}_q$) for every $b \in \mathbb{F}_q^*$. Henceforth assume that t is a positive integer which is not a power of 2, so $t \geq 3$. Let r be a positive integer such that $t^4 \leq 2^r$, and put $q := 2^r$. Pick $a \in \mathbb{F}_q^*$, and suppose that the function $c \mapsto ac^t$ is planar on $\mathbb{F}_q$. This means that $c \mapsto a(c+b)^t + ac^t + bc$ is bijective on $\mathbb{F}_q$ for every $b \in \mathbb{F}_q^*$. Upon composing on the right with $c \mapsto bc$ and on the left with $c \mapsto b^{-t}c$, it follows that $c \mapsto a((c+1)^t + c^t) + b^{2-t}c$ is bijective on $\mathbb{F}_q$. Set $f(X,Y) := a((X+1)^t + X^t) + Y^{t-2}X \in \mathbb{F}_q[X,Y]$. Upon replacing b with b^{-1} we see that $c \mapsto f(c,b)$ is bijective on $\mathbb{F}_q$ for all $b \in \mathbb{F}_q^*$. Set

$$H(X,Y) := \frac{f(X,Y) + f(0,Y)}{X} = a\frac{(X+1)^t + X^t + 1}{X} + Y^{t-2}.$$

Let N be the number of pairs (d,b) of elements of $\mathbb{F}_q$ such that $H(d,b) = 0$. Note that if $b, d \in \mathbb{F}_q^*$ satisfy $H(d,b) = 0$ then $f(d,b) = f(0,b)$, which contradicts bijectivity of $c \mapsto f(c,b)$. Since t is not a power of 2, both $H(X,0)$ and $H(0,Y)$ are nonzero univariate polynomials of degree at most $t-2$; therefore each of these polynomials has at most $t-2$

roots, so that $N \leq 2(t-2)$. Below we show that $H(X,Y)$ is absolutely irreducible, so by Lemma 2.2 we have $N \geq q+1-(t-3)(t-4)\sqrt{q}-(t-2)$. Since $q \geq t^4$ and $t \geq 3$, we compute

$$
\begin{aligned}
2(t-2) \geq N &\geq q + 1 - (t-3)(t-4)\sqrt{q} - (t-2) \\
&= \sqrt{q} \cdot (\sqrt{q} - (t-3)(t-4)) + 1 - (t-2) \\
&\geq t^2 \cdot (t^2 - (t-3)(t-4)) + 1 - (t-2) \\
&= 2(t-2) + 7t^3 - 12t^2 - 3t + 7 \\
&> 2(t-2),
\end{aligned}
$$

a contradiction.

It remains to show that $H(X,Y)$ is absolutely irreducible. Suppose otherwise. Then Capelli's 1898 theorem about reducibility of binomials (see e.g. [7, Chapter VI, Thm. 9.1]) yields a prime divisor ℓ of $t-2$ such that $\frac{(X+1)^t + X^t + 1}{X}$ is an ℓ–th power in $\overline{\mathbb{F}}_q(X)$. Write $t = 2^m o$ with o odd. Since t is not a power of 2, we have $o \geq 3$. Thus both 0 and 1 are simple roots of $(X+1)^o + X^o + 1$, so the multiplicities of 0 and 1 as roots of $\frac{(X+1)^t + X^t + 1}{X} = \frac{((X+1)^o + X^o + 1)^{2^m}}{X}$ are $2^m - 1$ and 2^m, respectively. Hence ℓ divides both 2^m and $2^m - 1$, which is impossible. $\square$

Remark. The above proof yields the conclusion of Theorem 1.1 under a slightly weaker hypothesis than $t^4 \leq 2^r$, namely that

$$
2^{r/2} > t^2 - 7t + 12 + \frac{6t - 14}{(t-2)\sqrt{t^2 - 10t + 29} + t^2 - 7t + 12}.
$$

Remark. A different approach to proving Theorem 1.1 relies on the auxiliary polynomial $\overline{H}(X,Y) = ((X+1)^t + X^t + (Y+1)^t + Y^t)/(X+Y)$. As above, if $c \mapsto ac^t$ is planar then $\overline{H}(X,Y) + b^{t-2}/a$ cannot be absolutely irreducible for any $b \in \mathbb{F}_q^*$. By a result of Lorenzini's [10], it follows that $\overline{H}(X,Y) = F(G(X,Y))$ for some $F \in \overline{\mathbb{F}}_q[X]$ and $G \in \overline{\mathbb{F}}_q[X,Y]$ with $\deg(F) > 1$. Then a short argument implies that t is the sum of two powers of 2. However, under this approach the case that t is the sum of two powers of 2 requires more work.

References

[1] Y. Aubry and M. Perret, *A Weil theorem for singular curves*, in: Arithmetic, Geometry and Coding Theory, de Gruyter, Berlin (1996), 1–7. 3

[2] A. Capelli, *Sulla riduttibilità delle equazioni algebriche*, Ren. Accad. Sc. Fis. Mat. Soc. Napoli **4** (1898), 84–90. 2

[3] C. Carlet, C. Ding and J. Yuan, *Linear codes from perfect nonlinear mappings and their secret sharing schemes*, IEEE Trans. Inform. Theory **51** (2005), 2089–2102. 1

[4] P. Dembowski and T. G. Ostrom, *Planes of order n with collineation groups of order n^2*, Math. Z. **103** (1968), 239–258. 1

[5] M. Fried and M. Jarden, Field Arithmetic, Springer–Verlag, Berlin, 1986. 3

[6] M. J. Ganley and E. Spence, *Relative difference sets and quasiregular collineation groups*, J. Combin. Theory Ser. A **19** (1975), 134–153. 1

[7] S. Lang, Algebra, revised third edition, Springer–Verlag, New York, 2002. 4

[8] D. B. Leep and C. C. Yeomans, *The number of points on a singular curve over a finite field*, Arch. Math. (Basel) **63** (1994), 420–426. 3

[9] R. Lidl and H. Niederreiter, Finite Fields, Addison-Wesley, Reading, 1983. 3

[10] D. Lorenzini, *Reducibility of polynomials in two variables*, J. Algebra **156** (1993), 65–75. 2, 4

[11] D. A. Mit'kin, *Polynomials with minimal set of values and the equation $f(x) = f(y)$ in a finite prime field*, Math. Notes **38** (1985), 513–520. 3

[12] K. Nyberg and L. R. Knudsen, *Provable security against differential cryptanalysis*, in: Advances in Cryptology (CRYPTO '92), Lecture Notes in Computer Science 740, Springer-Verlag (1992), 566–574. 1

[13] Z. Scherr and M. E. Zieve, *Planar monomials in characteristic* 2, Ann. Comb. **18** (2014), 723–729. 2

[14] K.-U. Schmidt and Y. Zhou, *Planar functions over fields of characteristic two*, J. Algebr. Comb. **40** (2014), 503–526. 1, 2

[15] A. Weil, Sur les Courbes Algébriques et les Variétés qui s'en Déduisent, Paris, 1948. 3

[16] Y. Zhou, *$(2^n, 2^n, 2^n, 1)$-relative difference sets and their representations*, J. Combin. Des. **21** (2013), 563–584. 1, 2

[17] M. E. Zieve, *Exceptional polynomials*, in: Handbook of Finite Fields, CRC Press (2013), 229–233. 3

[18] M. E. Zieve, *Planar functions and perfect nonlinear monomials over finite fields*, Des. Codes Cryptogr. **75** (2015), 71–80. 2

INSTITUT FÜR MATHEMATIK, UNIVERSITÄT WÜRZBURG, AM HUBLAND, D-97074, WÜRZBURG, GERMANY
E-mail address: Peter.Mueller@mathematik.uni-wuerzburg.de
URL: www.mathematik.uni-wuerzburg.de/~mueller

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MICHIGAN, 530 CHURCH STREET, ANN ARBOR, MI 48109-1043 USA
E-mail address: zieve@umich.edu
URL: http://www.math.lsa.umich.edu/~zieve/