LOW-DEGREE PLANAR POLYNOMIALS OVER FINITE FIELDS OF CHARACTERISTIC TWO

DANIELE BARTOLI AND KAI-UWE SCHMIDT

ABSTRACT. Planar functions are mappings from a finite field $\mathbb{F}_q$ to itself with an extremal differential property. Such functions give rise to finite projective planes and other combinatorial objects. There is a subtle difference between the definitions of these functions depending on the parity of q and we consider the case that q is even. We classify polynomials of degree at most $q^{1/4}$ that induce planar functions on $\mathbb{F}_q$, by showing that such polynomials are precisely those in which the degree of every monomial is a power of two. As a corollary we obtain a complete classification of exceptional planar polynomials, namely polynomials over $\mathbb{F}_q$ that induce planar functions on infinitely many extensions of $\mathbb{F}_q$. The proof strategy is to study the number of $\mathbb{F}_q$-rational points of an algebraic curve attached to a putative planar function. Our methods also give a simple proof of a new partial result for the classification of almost perfect nonlinear functions.

1. Introduction and Results

Let q be a prime power. If q is odd, a function $f : \mathbb{F}_q \to \mathbb{F}_q$ is *planar* or *perfect nonlinear* if, for each nonzero $\epsilon \in \mathbb{F}_q$, the function

$$x \mapsto f(x+\epsilon) - f(x) \tag{1}$$

is a permutation on $\mathbb{F}_q$. Such planar functions can be used to construct finite projective planes [8], relative difference sets [11], error-correcting codes [4], and S-boxes in block ciphers [19].

If q is even, a function $f : \mathbb{F}_q \to \mathbb{F}_q$ cannot satisfy the above definition of planar functions because $x = a$ and $x = a + \epsilon$ are mapped by (1) to the same image. This is the motivation to define a function $f : \mathbb{F}_q \to \mathbb{F}_q$ for even q to be *almost perfect nonlinear* (APN) if (1) is a 2-to-1 map. Such functions are highly relevant again for the construction of S-boxes in block ciphers [19]. However, there is no apparent link between APN functions and projective planes. More recently, Zhou [25] defined a natural analogue of planar functions on finite fields of characteristic two: If q is even, a function $f : \mathbb{F}_q \to \mathbb{F}_q$ is *planar* if, for each nonzero $\epsilon \in \mathbb{F}_q$, the function

$$x \mapsto f(x+\epsilon) + f(x) + \epsilon x$$

is a permutation on $\mathbb{F}_q$. As shown by Zhou [25] and Schmidt and Zhou [24], such planar functions have similar properties and applications as their counterparts in odd characteristic.

Date: 17 September 2018.

We refer to [20] for an excellent survey of recent results for the functions defined above.

The main result of this paper is a classification of the latter type of planar functions, namely those defined in characteristic two. Recall that every function from $\mathbb{F}_q$ to itself is induced 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 2-*polynomial* if the degree of every monomial in f is a power of two. For even q, such polynomials trivially induce planar functions on $\mathbb{F}_{q^r}$ for all $r \geq 1$. We show that among all polynomials of sufficiently small degree there are no other planar functions in characteristic two.

From now on q will always be a power of two.

Theorem 1.1. *Let $f \in \mathbb{F}_q[X]$ be a polynomial of degree at most $q^{1/4}$. If f is planar on $\mathbb{F}_q$, then f is a 2-polynomial.*

Now consider polynomials $f \in \mathbb{F}_q[X]$ with the property that f is planar on $\mathbb{F}_{q^r}$ for infinitely many positive integers r. As in [6], we call such a polynomial an *exceptional* planar polynomial. As a corollary, we obtain a complete classification of such polynomials.

Corollary 1.2. *If $f \in \mathbb{F}_q[X]$ is an exceptional planar polynomial, then f is a 2-polynomial.*

Theorem 1.1 considerably strengthens the main result of [18], which is the specialisation of Theorem 1.1 to the case that f is a monomial. It should be noted that there are examples of planar functions on $\mathbb{F}_q$ for even q that are not induced by 2-polynomials, see [14, 21, 23–25]. Of course all of these examples have degree larger than $q^{1/4}$.

Our methods also give a simple proof of a partial classification result for APN functions. As in [1], we call a polynomial $f \in \mathbb{F}_q[X]$ an *exceptional* APN polynomial if f induces an APN function on $\mathbb{F}_{q^r}$ for infinitely many positive integers r. It is well known (see [20], for example) that, for each positive integer k, the monomials X^{2^k+1} and $X^{4^k-2^k+1}$ are exceptional APN polynomials, also called *Gold* and *Kasami-Welch* monomials, respectively. In fact these monomials induce APN functions on $\mathbb{F}_{2^r}$ for all positive integers r that are coprime to k.

The following conjecture was proposed by Aubry, McGuire, and Rodier [1].

Conjecture 1.3 ([1])**.** *If $f \in \mathbb{F}_q[X]$ is an exceptional APN polynomial, then f is equivalent to a Gold or a Kasami-Welch monomial.*

In this conjecture, equivalence refers to CCZ-equivalence, whose precise definition is not required here (see [3] for details). Conjecture 1.3 has been proved by Hernando and McGuire [12] in the case that f is a monomial and many other special cases have been proved in several papers. We refer to [7] for a nice survey of the extensive recent literature on Conjecture 1.3.

We give a simple proof of the following new result.

Proposition 1.4. *Let $f \in \mathbb{F}_q[X]$ be a polynomial of even degree d at most $q^{1/4}$. If f is APN on $\mathbb{F}_q$, then $4 \mid d$.*

Proposition 1.4 solves one of the five pending cases listed in [7, Section 4] and strengthens [1, Theorem 2.4] essentially by removing the additional assumption that f has a term of odd degree.

In our proof of Theorem 1.1 we study an algebraic surface depending on a polynomial $f \in \mathbb{F}_q[X]$, such that if $f \in \mathbb{F}_q[X]$ induces a planar function on $\mathbb{F}_q$, then the surface has only very few $\mathbb{F}_q$-rational points. This surface is then intersected with a plane and we consider the resulting algebraic curve. The difficult part is to show that this curve has a component defined by an absolutely irreducible polynomial with coefficients in $\mathbb{F}_q$. The Hasse-Weil bound then asserts that the curve, and so also the surface, has many $\mathbb{F}_q$-rational points, provided that the degree of f is not too large. This leads to a contradiction unless f is a 2-polynomial.

This approach seems to be first used by Janwa and Wilson [15] for monomial APN functions and by Aubry, McGuire, and Rodier [1] for general APN functions. Besides the classification problem for APN functions, classification problems for other combinatorial objects have been attacked with this method, for example for planar functions in odd characteristic [6, 17, 26], hyperovals [5, 13, 26], and maximum scattered linear sets [2]. However a complete classification, as in Corollary 1.2, has been obtained so far only in one other case, namely in the classification problem for polynomials that induce hyperovals in finite Desarguesian planes [5]. We also remark that our methods for proving absolute irreducibility differ considerably from previous techniques.

2. Proof strategy

In this section we present the principal approach for proving Theorem 1.1. In Section 4 we then describe the required modifications of this approach to obtain a simple proof of Proposition 1.4.

Let q be a power of two and let $f \in \mathbb{F}_q[X]$ be a nonzero polynomial in which the degree of every monomial is not a power of two. Note that there is no loss of generality here since the addition of a 2-polynomial preserves the planarity of the function induced by f. Define the polynomial

$$\phi(X,Y,W) = \frac{f(X+W)+f(X)+WX+f(Y+W)+f(Y)+WY}{(X+Y)W}.$$

It is a direct consequence of the definition of planar functions that f induces a planar function on $\mathbb{F}_q$ if and only if all $\mathbb{F}_q$-rational points on the affine surface defined by $\phi(X,Y,W)=0$ satisfy $X=Y$ or $W=0$.

Put $\psi(X,Y,Z)=\phi(X,Y,X+Z)$, so that

$$\psi(X,Y,Z) = 1 + \frac{f(X)+f(Y)+f(Z)+f(X+Y+Z)}{(X+Y)(X+Z)}.$$

Then f induces a planar function on $\mathbb{F}_q$ if and only if all $\mathbb{F}_q$-rational points of the affine surface defined by $\psi(X,Y,Z)=0$ satisfy $X=Y$ or $X=Z$. Now write

$$f=\sum_{i=0}^{d} A_i X^i,$$

where $A_d\neq 0$. Since d is not a power of two, the homogenised form of ψ is

$$\widetilde{\psi}(X,Y,Z,T)=T^{d-2}+\sum_{i=3}^{d} A_i \frac{X^i+Y^i+Z^i+(X+Y+Z)^i}{(X+Y)(X+Z)} T^{d-i}.$$

We study the intersection of the projective surface defined by $\widetilde{\psi}(X,Y,Z,T)=0$ with the plane defined by $Z=X+1$. In fact, we consider the affine curve defined by $F(X,Y)=0$, where $F(X,Y)=\widetilde{\psi}(X,1,X+1,Y)$. We have

$$F(X,Y)=Y^{d-2}+\sum_{i=3}^{d} A_i \frac{X^i+1+(X+1)^i}{X+1} Y^{d-i}$$

and, after expanding,

$$F(X,Y)=Y^{d-2}+\sum_{i=3}^{d} A_i Y^{d-i} \sum_{k=0}^{i-1} \left[\binom{i-1}{k}+1\right] X^k. \tag{2}$$

If f induces a planar function on $\mathbb{F}_q$, then all $\mathbb{F}_q$-rational points of the affine curve defined by $F(X,Y)=0$ satisfy $X=1$ or $Y=0$.

The following result is a consequence of the Hasse-Weil bound for the number of $\mathbb{F}_q$-rational points on curves.

Proposition 2.1. *Let $f\in\mathbb{F}_q[X]$ be a polynomial of degree at most $q^{1/4}$ in which the degree of every monomial is not a power of two. If F has an absolutely irreducible factor over $\mathbb{F}_q$, then f does not induce a planar function on $\mathbb{F}_q$.*

Proof. Let d be the degree of f. Then the degree of F is $d-2$. Since d is not a power of two, we have $d\geq 3$, so that $q\geq 2^7$. Suppose that F has an absolutely irreducible factor over $\mathbb{F}_q$. Then, by the Hasse-Weil bound (see [10, Theorem 5.4.1], for example), the number of $\mathbb{F}_q$-rational points on the affine curve defined by $F(X,Y)=0$ is at least

$$q-(d-3)(d-4)q^{1/2}-d+3.$$

Since $F(1,Y)$ and $F(X,0)$ are polynomials of degree at most $d-2$, the number of $\mathbb{F}_q$-rational points that are not on the lines $X=1$ or $Y=0$ is at least

$$q-(d-3)(d-4)q^{1/2}-3d+7,$$

which (since $d\leq q^{1/4}$ and $q\geq 2^7$) is positive. The discussion preceding the proposition then implies that f is not planar. □

The difficulty in applying Proposition 2.1 is to show that the polynomial F has an absolutely irreducible factor over $\mathbb{F}_q$. Our strategy will be to apply certain transformations repeatedly to F and then use the following lemma.

Lemma 2.2. *Let $G \in \mathbb{F}_q[X,Y]$ be a nonzero polynomial and define*

$$H(X,Y) = \frac{G(X,XY)}{X^n},$$

where n is the smallest degree of a monomial in G. If H has an absolutely irreducible factor in $\mathbb{F}_q[X,Y]$, then G has an absolutely irreducible factor in $\mathbb{F}_q[X,Y]$.

Proof. Suppose that H has an absolutely irreducible factor over $\mathbb{F}_q$. We may as well suppose that H itself is absolutely irreducible. Assume that we can factor G as $G = AB$, where $A, B \in \mathbb{F}_{q^r}[X,Y]$ for some positive integer r and A and B have positive degree. Then we have

$$H(X,Y) = \frac{A(X,XY)}{X^a}\,\frac{B(X,XY)}{X^b} \tag{3}$$

for some nonnegative integers a and b satisfying $a + b = n$. If $A = \gamma X^a$ or $B = \gamma X^b$ for some nonzero $\gamma \in \mathbb{F}_{q^r}$, then clearly G has an absolutely irreducible factor in $\mathbb{F}_q[X,Y]$. Otherwise, both of the factors on the right-hand side of (3) have positive degree, contradicting that H is absolutely irreducible. □

Now let $H \in \mathbb{F}_q[X,Y]$ be a polynomial and let $P = (x_0, y_0)$ be a point in the plane. Write

$$H(X + x_0, Y + y_0) = H_0(X,Y) + H_1(X,Y) + H_2(X,Y) + \cdots,$$

where H_i is either the zero polynomial or a homogeneous polynomial of degree i. If $H_m \neq 0$ and $H_i = 0$ for all $i < m$, then the polynomial H_m is called the *tangent cone* of F at P. Whenever we refer to the tangent cone of a polynomial without specific reference to a point, we mean the tangent cone at the origin $(0,0)$.

The following lemma gives a simple criterion for the existence of an absolutely irreducible factor over $\mathbb{F}_q$ of a polynomial in $\mathbb{F}_q[X,Y]$.

Lemma 2.3. *Let $H \in \mathbb{F}_q[X,Y]$ and suppose that the tangent cone of H contains a reduced linear factor over $\mathbb{F}_q$. Then H has an absolutely irreducible factor over $\mathbb{F}_q$.*

Proof. Note that the tangent cone of the product of two polynomials is the product of the individual tangent cones. Therefore, we may assume without loss of generality that H is irreducible in $\mathbb{F}_q[X,Y]$, otherwise consider the appropriate factor of H in $\mathbb{F}_q[X,Y]$. By a routine argument (see [16], for example) there exists $c \in \mathbb{F}_q$ and an absolutely irreducible polynomial $h \in \mathbb{F}_{q^r}[X,Y]$ for some positive integer r such that

$$H = c \prod_{\sigma \in \mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)} \sigma(h),$$

where $\sigma(h)$ means that σ is applied to the coefficients of h. Letting $T \in \mathbb{F}_q[X,Y]$ be the tangent cone of H and $t \in \mathbb{F}_{q^r}[X,Y]$ be the tangent cone of h, we have

$$T = c \prod_{\sigma \in \mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)} \sigma(t).$$

Since T contains a reduced linear factor over $\mathbb{F}_q$, there is a unique $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ such that $\sigma(h)$ is divisible by this factor. But since this factor is in $\mathbb{F}_q[X,Y]$, it divides $\sigma(t)$ for every $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$. This forces $r = 1$ and thus H is already absolutely irreducible. □

The following proposition combines Proposition 2.1 and Lemmas 2.2 and 2.3 and summarises the main tool in our proof of Theorem 1.1.

Proposition 2.4. *Let $f \in \mathbb{F}_q[X]$ be a polynomial of degree at most $q^{1/4}$ in which the degree of every monomial is not a power of two. Suppose that after the application of a sequence of variable substitutions and transformations of the form $g(X,Y) \mapsto g(X,XY)/X^n$, where n is the smallest degree of a monomial in g, to the associated polynomial F, we arrive at a polynomial whose tangent cone contains a reduced linear factor over $\mathbb{F}_q$. Then F has an absolutely irreducible factor over $\mathbb{F}_q$ and consequently f cannot be planar.*

We shall also frequently use the following corollary to Lucas's theorem (see [9], for example).

Lemma 2.5. *The binomial coefficient $\binom{n}{m}$ is even if and only if at least one of the base-2 digits of m is greater than the corresponding digit of n.*

A consequence of Lemma 2.5 is that, if i is not a power of two, then $X^{2^{\nu(i)}}Y^{d-i}$ is the monomial of smallest degree in $F(X,Y)$ with coefficient A_i, where $\nu(i)$ is the 2-adic valuation of i. Note also that the only monomial in F of the form Y^i is Y^{d-2}. We shall frequently use these facts without specific reference in our proof of Theorem 1.1.

3. Proof of Theorem 1.1

As before, we assume that $f \in \mathbb{F}_q[X]$ is a nonzero polynomial in which the degree of every monomial is not a power of two. We now assume in addition that the degree of f is at most $q^{1/4}$ and that f is planar on $\mathbb{F}_q$. We show that this leads to a contradiction.

We shall study the associated polynomial F given in (2). Put $F_0 = F$ and define $F_1, F_2, \ldots, F_t$ recursively by

$$F_r(X,Y) = \frac{F_{r-1}(XY,Y)}{Y^{n_r}},$$

where n_r is the smallest degree of a monomial in F_{r-1} and t is the smallest number such that the tangent cone of F_t (at the origin) is not divisible by X. This t exists because of the presence of the monomial Y^{d-2} in F. Since f is not a 2-polynomial, we also have $t \geq 1$. Define u to be the smallest integer

such that the tangent cone of F_{t-1} contains the monomial $X^{2^u}Y^\ell$ for some ℓ (by "contain" we mean that the monomial is present with some nonzero coefficient).

In the first part of the proof we show that the tangent cone of F_t equals Y^{2^u-2}. To do so, we consider the polynomial $G(X,Y) = F(X+1,Y)$, so that

$$G(X,Y) = Y^{d-2} + \sum_{i=3}^{d} A_i \frac{X^i + 1 + (X+1)^i}{X} Y^{d-i}.$$

For $3 \le i \le d$ and $1 \le k \le i-1$, the coefficient of $X^{k-1}Y^{d-i}$ in G is $A_i\binom{i}{k}$. Lemma 2.5 then implies that, if i is not a power of two, then

$$X^{2^{\nu(i)}-1}Y^{d-i}$$

is the monomial of smallest degree in G with coefficient A_i (recall that $\nu(i)$ is the 2-adic valuation of i). Put $G_0 = G$ and define $G_1, G_2, \ldots, G_t$ recursively by

$$G_r(X,Y) = \frac{G_{r-1}(XY,Y)}{Y^{n_r-1}},$$

where $n_1, n_2, \ldots, n_r$ are the same numbers that occur in the definition of $F_1, F_2, \ldots, F_t$. Note that $n_r - 1$ is the smallest degree of a monomial in G_{r-1}, so that we can apply Proposition 2.4 to $G_1, G_2, \ldots, G_t$.

In order to prove that the tangent cone of F_t equals Y^{2^u-2}, we require the following two lemmas

Lemma 3.1. *We have $2 \le u \le \nu(d)$.*

Proof. By assumption, f contains no monomials whose degree is a power of two. In particular d is not a power of two. Hence F, and therefore also F_{t-1}, contains the monomial $X^{2^{\nu(d)}}$. Thus we have $u \le \nu(d)$.

If $u = 0$, then the tangent cone of F_{t-1} would be divisible by X, but not by X^2. This leads to a contradiction by Proposition 2.4.

Now suppose that $u = 1$. Then the tangent cone of F_{t-1} contains the monomial X^2Y^ℓ for some ℓ and does not contain the monomial $XY^{\ell+1}$. By the remarks preceding the lemma, for $r < t$, the tangent cone of G_r equals the tangent cone of F_r divided by X. Therefore the tangent cone of G_{t-1} is divisible by X and not by X^2. This again leads to a contradiction by Proposition 2.4. □

Lemma 3.2. *For all $r \le t$ we have $2^u \mid n_r$.*

Proof. By Lemma 3.1 we have $u \le \nu(d)$, and so $2^u \mid d$. Let s be an integer satisfying $0 \le s \le t-1$ and assume that $2^u \mid n_r$ for all $r \le s$, which is vacuously true for $s = 0$. We proceed by induction on s. Recall that F_{t-1} contains the monomial $X^{2^u}Y^\ell$ for some ℓ. The preimage in F_s of this monomial is of the form

$$X^{2^u}Y^{2^u s - n_1 - \cdots - n_s + d - i} \tag{4}$$

for some i satisfying $\nu(i) = u$. By the inductive hypothesis, 2^u divides the degree of (4). Now suppose that F_s also contains a monomial

$$X^{2^{\nu(j)}} Y^{2^{\nu(j)} s - n_1 - \cdots - n_s + d - j} \tag{5}$$

of degree smaller than the degree of (4). If $\nu(j) < u$, then by looking at the image in F_{t-1} of (5), we find a contradiction to the minimality of u. Otherwise, 2^u divides the degree of (5) and so 2^u divides the smallest degree of a monomial in F_s. Hence $2^u \mid n_{s+1}$, as required. □

We now show that the tangent cone of F_t equals Y^{2^u-2}.

Lemma 3.3. *The tangent cone of F_t is Y^{2^u-2}.*

Proof. Notice that, since the tangent cone of F_t is not divisible by X, it must contain the image of the monomial Y^{d-2} in F, namely $Y^{d-2-n_1-\cdots-n_t}$. Since $2^u \mid d$ by Lemma 3.1 and $2^u \mid n_r$ for all $r \le t$ by Lemma 3.2, we find that that the tangent cone of F_t contains Y^j for some j satisfying $j \equiv -2 \pmod{2^u}$.

By definition, the tangent cone of F_{t-1} contains $X^{2^u} Y^\ell$ for some ℓ, and therefore F_t contains X^{2^u}. Hence the tangent cone of F_t has degree at most 2^u. Since we also have $u \ge 2$ by Lemma 3.1, we find that $j = 2^u - 2$. Hence the tangent cone of F_t has degree $2^u - 2$.

Now suppose for a contradiction that the tangent cone of F_t contains $X^{2^v} Y^{2^u-2-2^v}$ for some integer v satisfying $0 \le v < u$. By Lemma 3.2, the preimage in F of this monomial is of the form $X^{2^v} Y^\ell$ for some ℓ satisfying $\ell \equiv -2 \pmod{2^v}$. If $v \ge 2$, then Lemma 2.5 implies that F also contains $X^2 Y^\ell$, whose image in F_t has degree strictly smaller than $2^u - 2$, a contradiction. If $v = 1$, then the tangent cone of F_t equals

$$\alpha X^2 Y^{2^u-4} + \beta X Y^{2^u-3} + Y^{2^u-2}$$

for some $\alpha, \beta \in \mathbb{F}_q$ with $\alpha \ne 0$, and the tangent cone of G_t equals

$$\alpha X Y^{2^u-4} + \beta Y^{2^u-3} = Y^{2^u-4}(\alpha X + \beta Y),$$

which gives a contradiction by Proposition 2.4. If $v = 0$, then the tangent cone of F_t must be $Y^{2^u-3}(\beta X + Y)$ for some $\beta \in \mathbb{F}_q$ with $\beta \ne 0$, which again gives a contradiction by Proposition 2.4. □

In view of Lemma 3.3, define

$$F_{t+1}(X, Y) = \frac{F_t(X, XY)}{X^{2^u-2}}.$$

Then F_{t+1} still contains Y^{2^u-2} and the tangent cone of F_{t+1} has degree 2 and contains X^2 (coming from $X^{2^u} Y^\ell$ in F_{t-1}). Note that, since Y^{2^u-2} is the unique monomial of degree $2^u - 2$ in F_t, the only monomial of the form Y^i in F_{t+1} is Y^{2^u-2}.

Now define

$$F_{t+2}(X, Y) = \frac{F_{t+1}(XY^{2^{u-1}-2}, Y)}{Y^{2^u-4}}.$$

Note that F_{t+2} is obtained from F_{t+1} by $2^{u-1}-2$ applications of the transformation $g(X,Y) \mapsto g(XY,Y)/Y^2$. Also, in each step the smallest degree of a monomial is 2: a constant term cannot appear because F_{t+1} contains only one monomial that is pure in Y, namely Y^{2^u-2}, and a linear tangent cone would lead to a contradiction by Proposition 2.4. The tangent cone of F_{t+2} contains X^2 and Y^2. We now show that it does not contain XY.

Lemma 3.4. *The tangent cone of F_{t+2} equals $\alpha X^2 + Y^2$ for some nonzero $\alpha \in \mathbb{F}_q$.*

Proof. A monomial X^kY^j in F_t is mapped to $X^{k+j-2^u+2}Y^j$ in F_{t+1} and to

$$X^{k+j-2^u+2}Y^{(2^{u-1}-2)(k+j-2^u+2)+j-2^u+4}$$

in F_{t+2}. Now suppose, for a contradiction, that the latter monomial is XY, which means that $k = 2^{u-1}$ and $j = 2^{u-1}-1$. Since $u \geq 2$ by Lemma 3.1 and $2^u \mid n_r$ for all $r \leq t$ by Lemma 3.2, the corresponding monomial in F is $X^{2^{u-1}}Y^\ell$ for some odd ℓ. Lemma 2.5 then implies that F also contains the monomial XY^ℓ with the same nonzero coefficient as $X^{2^{u-1}}Y^\ell$. However, since $u \geq 2$ and $t \geq 1$, the image in F_t of XY^ℓ has degree strictly smaller than $2^u - 1$. This contradicts Lemma 3.3, namely that the tangent cone of F_t equals Y^{2^u-2}. □

In the remainder of our proof of Theorem 1.1 we shall apply further transformations to F_{t+2}, which will ultimately lead to a contradiction. To do so, we first study the images in F_{t+2} of the monomials in F. We record the properties of these images in the following lemma.

Lemma 3.5. *Suppose that F contains the monomial X^kY^{d-i}. Then its image in F_{t+2} is X^rY^s, where*

$$\begin{aligned} r &= k(t+1) - i + 2, \\ s &= k(2^{u-1}(t+1) - t - 2) - i(2^{u-1}-1) + 2^u. \end{aligned}$$

Proof. The image in F_t of X^kY^{d-i} is

$$X^kY^{kt+d-i-n_1-\cdots-n_t} = X^kY^{kt-i+2^u},$$

since

$$\sum_{r=1}^{t} n_r = (d-2) - (2^u - 2) = d - 2^u,$$

using Lemma 3.3. Then the image in F_{t+1} of X^kY^{d-i} is

$$X^{k(t+1)-i+2}Y^{kt-i+2^u}$$

and the image in F_{t+2} is

$$X^{k(t+1)-i+2}Y^{kt-i+2^u+(2^{u-1}-2)(k(t+1)-i+2)-2^u+4}.$$ □

Lemma 3.5 implies that the putative monomial X^kY^{d-i} in F is mapped to a monomial in F_{t+2} of degree

$$k(2^{u-1}(t+1)-1)-2^{u-1}i+2^u+2.$$

In particular, since $u \geq 2$ by Lemma 3.1, this degree is congruent to k modulo 2. Define

$$o(i)=\begin{cases} 2^{u-1}(t+1)-1-2^{u-1}i+2^u+2 & \text{for odd } i \\ (2^{\nu(i)}+1)(2^{u-1}(t+1)-1)-2^{u-1}i+2^u+2 & \text{for even } i \end{cases}$$

and

$$e(i)=\begin{cases} 2^z(2^{u-1}(t+1)-1)-2^{u-1}i+2^u+2 & \text{for odd } i \\ 2^{\nu(i)}(2^{u-1}(t+1)-1)-2^{u-1}i+2^u+2 & \text{for even } i, \end{cases}$$

where z is determined as follows. If $i=\sum_{n\geq 0} a_n 2^n$ with $a_n \in \{0,1\}$ is the base-2 expansion of i, then z is the smallest positive integer n such that $a_n=0$. Note that $z \geq 1$ for odd i.

Recall our assumption that f contains no monomials whose degree is a power of two and that f is not the zero polynomial. Lemmas 2.5 and 3.5 imply that, among all monomials with coefficient A_i in F_{t+2}, the smallest odd degree is $o(i)$ and, if $i+1$ is not a power of two, then the smallest even degree is $e(i)$ (if $i+1$ is a power of two, then there are no monomials in F_{t+2} of even degree with coefficient A_i). Accordingly, define

$$m=\min\{o(i) : A_i \neq 0\}. \tag{6}$$

We shall first prove some properties of this number.

Lemma 3.6. *We have $m=o(i)$ for some uniquely determined i.*

Proof. Suppose for a contradiction that $m=o(i)=o(i')$ for some integers $i \neq i'$. We first show that one of i and i' is odd and the other is even. If i and i' are both odd or more generally $\nu(i)=\nu(i')$, then we force $i=i'$, a contradiction. If i and i' are both even and $\nu(i)<\nu(i')$, then we obtain using $u \geq 2$ by Lemma 3.1

$$o(i')-o(i) \equiv 2^{\nu(i)} \pmod{2^{\nu(i)+1}},$$

contradicting $o(i)=o(i')$. This proves our claim and so we can assume without loss of generality that i is even and i' is odd.

Next we show that $e(i)=2$. If there is an even j such that $e(j)<e(i)$ and $A_j \neq 0$, then it follows immediately from the definitions that $o(j)<o(i)$, which contradicts $m=o(i)$. If there is an odd j such that $e(j)<e(i)$ and $A_j \neq 0$, then

$$o(j)<e(j)<e(i)<o(i),$$

which again contradicts $m=o(i)$. Hence $e(i)$ is the smallest even degree of a monomial in F_{t+2}. Since F_{t+2} contains the monomial X^2 and no monomials of smaller degree, we find that $e(i)=2$.

Since i is even and $e(i) = 2$, we obtain $o(i) = 2^{u-1}(t+1)+1$. The equality $o(i) = o(i')$ then gives $2^{u-1}i' = 2^u$, so $i' = 2$, contradicting that i' is odd. □

Lemma 3.7. *Every monomial in F_{t+2} of degree strictly less than m has even degree in X and even degree in Y.*

Proof. Let i be an integer such that $A_i \neq 0$. If i is odd, then $o(i) < e(i)$, and so $o(i)$ is the smallest degree of a monomial in F_{t+2} with coefficient A_i. Hence, if there is a monomial in F_{t+2} of even degree less than $o(i)$ with the same coefficient A_i, then i must be even. By Lemma 3.5, such a monomial has degree

$$k(2^{u-1}(t+1)-1) - 2^{u-1}i + 2^u + 2.$$

Since $u \geq 2$ by Lemma 3.1, we force k to be even. It then follows from Lemma 3.5 that this monomial has even degree in X and even degree in Y. □

We now complete the proof of Theorem 1.1.

Proof of Theorem 1.1. Recall the definition of m from (6). Put $H_0 = F_{t+2}$ and define $H_1, H_2, \ldots, H_{(m-1)/2}$ recursively by

$$H_{i+1}(X,Y) = \frac{H_i(X, c_iX + XY)}{X^2},$$

where c_i is such that c_i^2 is the coefficient of X^2 in H_i. Note that H_{i+1} is obtained from H_i by a variable substitution $(X,Y) \mapsto (X, c_iX + Y)$ followed by the transformation $g(X,Y) \mapsto g(X,XY)/X^2$. We shall see that $H_1, H_2, \ldots, H_{(m-1)/2}$ are indeed polynomials and that the tangent cone of $H_{(m-1)/2}$ equals αX for some nonzero $\alpha \in \mathbb{F}_q$, which then leads to a contradiction by Proposition 2.4.

By Lemma 3.6, the polynomial $H_0 = F_{t+2}$ contains a unique monomial of degree m, and so $H_0(X, c_0X + Y)$ contains αX^m for some nonzero $\alpha \in \mathbb{F}_q$. Lemma 3.7 asserts that every monomial in H_0 of degree strictly less than m has even degree in X and even degree in Y. Since $\binom{n}{k}$ is even for even n and odd k by Lemma 2.5, the images of such monomials in $H_1, H_2, \ldots, H_{(m-1)/2-1}$ also have even degree in X and even degree in Y. Hence the tangent cones of $H_1, H_2, \ldots, H_{(m-1)/2-1}$ have degree two and never contain XY. This also implies that $H_1, H_2, \ldots, H_{(m-1)/2}$ are indeed polynomials and that the tangent cone of $H_{(m-1)/2}$ equals αX. □

4. Proof of Proposition 1.4

We now give a proof of Proposition 1.4. As before, let q be a power of two and let $f \in \mathbb{F}_q[X]$ be a polynomial in which the degree of every monomial is not a power of two. Again there is no loss of generality since the addition of a 2-polynomial preserves the APN property of the function induced by f. Define the polynomial

$$\psi(X,Y,Z) = \frac{f(X)+f(Y)+f(Z)+f(X+Y+Z)}{(X+Y)(X+Z)(Y+Z)}.$$

It is well known (see [22, Proposition 3.1], for example) that f induces an APN function on $\mathbb{F}_q$ if and only if all $\mathbb{F}_q$-rational points on the affine surface defined by $\psi(X,Y,Z)=0$ satisfy $(X+Y)(X+Z)(Y+Z)=0$. Write

$$f=\sum_{i=0}^{d} A_i X^i,$$

where $A_d \neq 0$. Then the homogenised form of ψ is

$$\widetilde{\psi}(X,Y,Z,T)=\sum_{i=3}^{d} A_i \frac{X^i+Y^i+Z^i+(X+Y+Z)^i}{(X+Y)(X+Z)(Y+Z)} T^{d-i}.$$

As for planar functions, we consider the affine curve defined by $F(X,Y)=0$, where $F(X,Y)=\widetilde{\psi}(X,1,X+1,Y)$. We have

$$F(X,Y)=\sum_{i=3}^{d} A_i \frac{X^i+1+(X+1)^i}{(X+1)X} Y^{d-i}$$

and, after expanding,

$$F(X,Y)=\sum_{i=3}^{d} A_i Y^{d-i} \sum_{k=1}^{i-1} \left[\binom{i-1}{k} + 1 \right] X^{k-1}.$$

If f induces an APN function on $\mathbb{F}_q$, then all $\mathbb{F}_q$-rational points of the affine curve defined by $F(X,Y)=0$ satisfy $XY(X+1)=0$.

Now assume that $d \leq q^{1/4}$ and $d \equiv 2 \pmod 4$. Then $F(0,0)=0$ and Lemma 2.5 implies that the tangent cone of F equals $A_d X + A_{d-1} Y$. Since $A_d \neq 0$, we find from Lemma 2.3 that F has an absolutely irreducible factor over $\mathbb{F}_q$. An argument that is almost identical to that used in the proof of Proposition 2.1 then shows that the curve defined by $F(X,Y)=0$ has $\mathbb{F}_q$-rational points not on one of the lines $X=0$, $Y=0$, or $X=1$. Hence f cannot be APN on $\mathbb{F}_q$.

Acknowledgements

Daniele Bartoli was partially supported by the Italian Ministero dell'Istruzione, dell'Università e della Ricerca (MIUR) and the Gruppo Nazionale per le Strutture Algebriche, Geometriche e le loro Applicazioni (GNSAGA-INdAM). This work was carried out when the first author was visiting Paderborn University under the programme "Research Stays for University Academics and Scientists" funded by the German Academic Exchange Service (DAAD).

References

[1] Y. Aubry, G. McGuire, and F. Rodier, *A few more functions that are not APN infinitely often*, Finite fields: theory and applications, Contemp. Math., vol. 518, Amer. Math. Soc., Providence, RI, 2010, pp. 23–31.

[2] D. Bartoli and Y. Zhou, *Exceptional scattered polynomials*, J. Algebra **509** (2018), 507–534.

[3] L. Budaghyan, C. Carlet, and A. Pott, *New classes of almost bent and almost perfect nonlinear polynomials*, IEEE Trans. Inform. Theory **52** (2006), no. 3, 1141–1152.
[4] C. Carlet, C. Ding, and J. Yuan, *Linear codes from perfect nonlinear mappings and their secret sharing schemes*, IEEE Trans. Inform. Theory **51** (2005), no. 6, 2089–2102.
[5] F. Caullery and K.-U. Schmidt, *On the classification of hyperovals*, Adv. Math. **283** (2015), 195–203.
[6] F. Caullery, K.-U. Schmidt, and Y. Zhou, *Exceptional planar polynomials*, Des. Codes Cryptogr. **78** (2016), no. 3, 605–613.
[7] M. Delgado, *The state of the art on the conjecture of exceptional APN functions*, Note Mat. **37** (2017), no. 1, 41–51.
[8] P. Dembowski and T. G. Ostrom, *Planes of order n with collineation groups of order n^2*, Math. Z. **103** (1968), 239–258.
[9] N. J. Fine, *Binomial coefficients modulo a prime*, Amer. Math. Monthly **54** (1947), 589–592.
[10] M. D. Fried and M. Jarden, *Field arithmetic*, 3rd ed., Springer-Verlag, Berlin, 2008.
[11] M. J. Ganley and E. Spence, *Relative difference sets and quasiregular collineation groups*, J. Combin. Theory Ser. A **19** (1975), 134–153.
[12] F. Hernando and G. McGuire, *Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions*, J. Algebra **343** (2011), 78–92.
[13] ———, *Proof of a conjecture of Segre and Bartocci on monomial hyperovals in projective planes*, Des. Codes Cryptogr. **65** (2012), no. 3, 275–289.
[14] S. Hu, Sh. Li, T. Zhang, T. Feng, and G. Ge, *New pseudo-planar binomials in characteristic two and related schemes*, Des. Codes Cryptogr. **76** (2015), no. 2, 345–360.
[15] H. Janwa and R. M. Wilson, *Hyperplane sections of Fermat varieties in $\mathbf{P}^3$ in* char. 2 *and some applications to cyclic codes*, Applied algebra, algebraic algorithms and error-correcting codes (San Juan, PR, 1993), Lecture Notes in Comput. Sci., vol. 673, Springer, Berlin, 1993, pp. 180–194.
[16] S. Kopparty and S. Yekhanin, *Detecting rational points on hypersurfaces over finite fields*, IEEE Conference on Computational Complexity, IEEE Computer Society, 2008, pp. 311–320.
[17] E. Leducq, *Functions which are PN on infinitely many extensions of $\mathbb{F}_p$, p odd*, Des. Codes Cryptogr. **75** (2015), no. 2, 281–299.
[18] P. Müller and M. E. Zieve, *Low-degree planar monomials in characteristic two*, J. Algebraic Combin. **42** (2015), no. 3, 695–699.
[19] K. Nyberg and L. R. Knudsen, *Provable security against differential cryptanalysis*, Advances in cryptology—CRYPTO '92 (Santa Barbara, CA, 1992), Lecture Notes in Comput. Sci., vol. 740, Springer, Berlin, 1993, pp. 566–574.
[20] A. Pott, *Almost perfect and planar functions*, Des. Codes Cryptogr. **78** (2016), no. 1, 141–195.
[21] L. Qu, *A new approach to constructing quadratic pseudo-planar functions over $\mathbb{F}_{2^n}$*, IEEE Trans. Inform. Theory **62** (2016), no. 11, 6644–6658.
[22] F. Rodier, *Borne sur le degré des polynômes presque parfaitement non-linéaires*, Arithmetic, geometry, cryptography and coding theory, Contemp. Math., vol. 487, Amer. Math. Soc., Providence, RI, 2009, pp. 169–181.
[23] Z. Scherr and M. E. Zieve, *Some planar monomials in characteristic 2*, Ann. Comb. **18** (2014), no. 4, 723–729.
[24] K.-U. Schmidt and Y. Zhou, *Planar functions over fields of characteristic two*, J. Algebraic Combin. **40** (2014), no. 2, 503–526.
[25] Y. Zhou, *$(2^n, 2^n, 2^n, 1)$-relative difference sets and their representations*, J. Combin. Des. **21** (2013), 563–584.
[26] M. E. Zieve, *Planar functions and perfect nonlinear monomials over finite fields*, Des. Codes Cryptogr. **75** (2015), no. 1, 71–80.

Department of Mathematics and Computer Science, University of Perugia, Perugia, 06123, Italy.
E-mail address: daniele.bartoli@unipg.it

Department of Mathematics, Paderborn University, Warburger Str. 100, 33098 Paderborn, Germany.
E-mail address: kus@math.upb.de