J Algebr Comb (2014) 40:503–526
DOI 10.1007/s10801-013-0496-z

Planar functions over fields of characteristic two

Kai-Uwe Schmidt · Yue Zhou

Received: 8 February 2013 / Accepted: 20 December 2013 / Published online: 9 January 2014

Abstract Classical planar functions are functions from a finite field to itself and give rise to finite projective planes. They exist however only for fields of odd characteristic. We study their natural counterparts in characteristic two, which we also call planar functions. They again give rise to finite projective planes, as recently shown by the second author. We give a characterisation of planar functions in characteristic two in terms of codes over $\mathbb{Z}_4$. We then specialise to planar monomial functions $f(x) = cx^t$ and present constructions and partial results towards their classification. In particular, we show that $t = 1$ is the only odd exponent for which $f(x) = cx^t$ is planar (for some nonzero c) over infinitely many fields. The proof techniques involve methods from algebraic geometry.

Keywords Algebraic curves · Codes over $\mathbb{Z}_4$ · Finite field · Planar function · Relative difference set

1 Introduction

A function $f : \mathbb{F}_q \to \mathbb{F}_q$ is *planar* if

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

K.-U. Schmidt (✉) · Y. Zhou
Faculty of Mathematics, Otto-von-Guericke University, Universitätsplatz 2, 39106 Magdeburg, Germany
e-mail: kaiuwe.schmidt@ovgu.de

Y. Zhou
e-mail: yue.zhou.ovgu@gmail.com

Present address:
Y. Zhou
Department of Mathematics and System Sciences, College of Science, National University of Defense Technology, Changsha, China

is a permutation of $\mathbb{F}_q$ for each $\epsilon \in \mathbb{F}_q^*$. Planar functions have been introduced by Dembowski and Ostrom [4] to construct finite projective planes and arise in many other contexts. For example, Ganley and Spence [8] showed that planar functions give rise to certain relative difference sets, Nyberg and Knudsen [23], among others, studied planar functions (under the synonym *perfect nonlinear functions*) for applications in cryptography, and Carlet, Ding, and Yuan [3], among others, used planar functions to construct error-correcting codes.

Planar functions cannot exist in characteristic two since, if q is even and x is a solution to $f(x+\epsilon) - f(x) = a$ for $a \in \mathbb{F}_q$, then so is $x+\epsilon$. This is the motivation to define a function $f : \mathbb{F}_q \to \mathbb{F}_q$ to be *almost perfect nonlinear* if (1) is a 2-to-1 map. Such functions have also been studied extensively for applications in cryptography and coding theory (see Carlet, Charpin, and Zinoviev [2], for example). However, there is no apparent link between almost perfect nonlinear functions and finite projective planes.

Recently, the second author proposed [26] a concept to overcome the problem that there is no planar function in characteristic two. The definition of a planar function has to be modified as follows.

Definition 1.1 A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is *planar* if

$$x \mapsto f(x+\epsilon) + f(x) + \epsilon x \tag{2}$$

is a permutation of $\mathbb{F}_{2^n}$ for each $\epsilon \in \mathbb{F}_{2^n}^*$.

Such functions share many of the properties of planar functions in odd characteristic. The next section, which is independent of the rest of this paper, provides further background on planar functions in characteristic two and discusses connections to finite geometries and coding theory.

Every function from $\mathbb{F}_{2^n}$ to itself can be uniquely written as a polynomial function of degree strictly less than 2^n. We consider the simplest nontrivial polynomial functions, namely monomial functions $x \mapsto cx^t$ for some $c \in \mathbb{F}_{2^n}^*$ and some integer t. Such functions are often preferred in applications. We are interested in those exponents t that give rise to planar functions.

Definition 1.2 An integer t satisfying $0 < t < 2^n$ is a *planar exponent* of $\mathbb{F}_{2^n}$ if the function $x \mapsto cx^t$ is planar on $\mathbb{F}_{2^n}$ for some $c \in \mathbb{F}_{2^n}^*$.

Trivially, 2^k is a planar exponent of all fields $\mathbb{F}_{2^n}$ satisfying $n > k$. A nontrivial example is given in Theorem 3.1, which shows that $2^k + 1$ is a planar exponent of $\mathbb{F}_{4^k}$. In an earlier version of this paper, we conjectured that $4^k(4^k+1)$ is a planar exponent of $\mathbb{F}_{64^k}$. This was subsequently proved by Scherr and Zieve [25]. We conjecture that these examples, summarised in Table 1, form the complete list of planar exponents.

As in odd characteristic, the classification of planar monomials in characteristic two seems to be a challenging problem. This motivates us to study the relaxed problem of classifying those numbers that are planar exponents of $\mathbb{F}_{2^n}$ for infinitely many n. The only known such numbers are the powers of 2 and we conjecture that there are no more. Our main result is the following.

Table 1 Conjectured complete list of planar exponents of $\mathbb{F}_{2^n}$

Exponent t	Condition	Reference
2^k	None	Trivial
2^k+1	$n=2k$	Theorem 3.1
$4^k(4^k+1)$	$n=6k$	[25, Theorem 1.1]

Theorem 1.3 *If t is an odd planar exponent of $\mathbb{F}_{2^n}$ for infinitely many n, then $t=1$.*

The problem of classifying the numbers that are planar exponents of $\mathbb{F}_{2^n}$ for infinitely many n parallels the problem of classifying monomial functions $x \mapsto x^t$ on $\mathbb{F}_{2^n}$ that are almost perfect nonlinear for infinitely many n. To attack this problem, Janwa, McGuire, and Wilson [15] proposed to use ideas from algebraic geometry. These ideas were further developed by Jedlicka [16] and Hernando and McGuire [11], leading to a complete solution. The same approach has been used by Hernando and McGuire [12] to prove a conjecture on monomial hyperovals in projective planes and by Leducq [18] and Hernando, McGuire, and Monserrat [13] to give partial results towards a classification of monomial functions $x \mapsto x^t$ on $\mathbb{F}_{p^n}$ (with p odd) that are planar for infinitely many n (which was recently completed by Zieve [27] using different techniques). We use a similar approach to prove Theorem 1.3, though our proof requires several extra ideas.

2 Background and motivation

2.1 Relative difference sets and finite geometries

Let G be a finite group and let N be a subgroup of G. A subset D of G is a *relative difference set* with parameters $(|G|/|N|, |N|, |D|, \lambda)$ and *forbidden subgroup* N if the list of nonzero differences of D comprises every element in $G \setminus N$ exactly λ times. We are interested in relative difference sets D with parameters $(q, q, q, 1)$ and a normal forbidden subgroup, in which case a classical result due to Ganley and Spence [8, Thm. 3.1] shows that D can be uniquely extended to a finite projective plane.

It is known (see [7, 17]) that, for even q, a relative difference set with parameters $(q, q, q, 1)$ in an abelian group necessarily satisfies $q = 2^n$ for some integer n and is a subset of $\mathbb{Z}_4^n$ (where $\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z}$) and the forbidden subgroup is $2\mathbb{Z}_4^n$. This fact was the motivation for the second author to study [26] such relative difference sets, which then led to the notion of planar functions over fields of characteristic two.

We shall follow an approach that is slightly different from that in [26] and identify $\mathbb{Z}_4^n$ with the additive group of the Galois ring R_n of characteristic 4 and cardinality 4^n. We recall some basic facts about such Galois rings (see [22] or [10], for example). The unit group $R_n \setminus 2R_n$ of R_n contains a cyclic subgroup $\Gamma(R_n)^*$ of size $2^n - 1$ and $\Gamma(R_n) = \Gamma(R_n)^* \cup \{0\}$ is called the *Teichmuller set* in R_n. We define addition on $\Gamma(R_n)$ by

$$x \oplus y = x + y + 2\sqrt{xy} \tag{3}$$

(where $+$ is addition in R_n). Then $(\Gamma(R_n), \oplus, \cdot)$ is a finite field with 2^n elements [22, Statement 2]. Every $y \in R_n$ can be written uniquely in the form $y = a + 2b$ for $a, b \in \Gamma(R_n)$.

It is now an easy exercise to show that a relative difference set in R_n with parameters $(2^n, 2^n, 2^n, 1)$ can always be written as

$$D = \left\{x + 2\sqrt{f(x)} : x \in \Gamma(R_n)\right\}, \tag{4}$$

where f is some function from $\Gamma(R_n)$ to itself. The following result characterises the functions f for which (4) is a relative difference set.

Theorem 2.1 *The set D, given in (4), is a relative difference set with parameters $(2^n, 2^n, 2^n, 1)$ and forbidden subgroup $2R_n$ if and only if f is planar.*

Proof By definition, D is a relative difference set with parameters $(2^n, 2^n, 2^n, 1)$ and forbidden subgroup $2R_n$ if and only if, for every $c \in R \setminus 2R$, the equation

$$\left(x + 2\sqrt{f(x)}\right) - \left(y + 2\sqrt{f(y)}\right) = c$$

has exactly one solution $(x, y) \in \Gamma(R_n) \times \Gamma(R_n)$. Equivalently, writing $c = a + 2b$ for $a \in \Gamma(R_n)^*$ and $b \in \Gamma(R_n)$, the two equations

$$\begin{aligned} &x \oplus y = a, \\ &\sqrt{f(x)} \oplus \sqrt{f(y)} \oplus \sqrt{xy} \oplus y = b \end{aligned}$$

hold simultaneously for exactly one pair $(x, y) \in \Gamma(R_n) \times \Gamma(R_n)$. This in turn holds if and only if the mapping

$$x \mapsto f(x \oplus a) \oplus f(x) \oplus ax$$

is a permutation of $\Gamma(R_n)$ for every $a \neq 0$. □

Remark Theorem 2.1 is essentially equivalent to [26, Thm. 2.1], which avoids using Galois rings at the cost of a more delicate proof.

Let $\chi : R_n \to \mathbb{C}$ be a character of the additive group of R_n. For later reference, we recall the following standard result (see [24, Chap. 1], for example): D is a relative difference set in R_n with forbidden subgroup $2R_n$ if and only if

$$\left|\sum_{x \in D} \chi(x)\right|^2 = \begin{cases} 4^n & \text{for } \chi \text{ principal,} \\ 0 & \text{for } \chi \text{ not principal, but principal on } 2R_n, \\ 2^n & \text{otherwise.} \end{cases} \tag{5}$$

2.2 Coding theory

We assume that the reader is familiar with the basic terminology of coding theory, in particular of the theory of codes over $\mathbb{Z}_4$. Otherwise, we advise to consult the seminal paper [10].

Table 2 Weight distribution of $(\mathcal{C}_f)^\perp$ for odd n

Weight	Frequency
0	1
$2^n - 2^{(n-1)/2}$	$2^{n+1}(2^n - 1)$
2^n	$2^{n+2} - 2$
$2^n + 2^{(n-1)/2}$	$2^{n+1}(2^n - 1)$
2^{n+1}	1

Let f be a function from $\mathbb{F}_{2^n}$ to itself satisfying $f(0) = 0$ and let α be a generator of $\mathbb{F}_{2^n}^*$. It is well known (see [2, Thm. 5], for example) that for $n \geq 4$ the code over $\mathbb{F}_2$ having parity check matrix

$$\begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^n-2} \\ f(1) & f(\alpha) & f(\alpha^2) & \cdots & f(\alpha^{2^n-2}) \end{bmatrix} \tag{6}$$

has minimum (Hamming) distance 3, 4 or 5, where the value 5 occurs if and only if f is almost perfect nonlinear. We shall provide a similar characterisation for planar functions in characteristic two.

Let f be a function from $\Gamma(R_n)$ to itself and let β be a generator of $\Gamma(R_n)^*$. Consider the code $\mathcal{C}_f$ over $\mathbb{Z}_4$ having parity check matrix

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 2\sqrt{f(0)} & 1 + 2\sqrt{f(1)} & \beta + 2\sqrt{f(\beta)} & \cdots & \beta^{2^n-2} + 2\sqrt{f(\beta^{2^n-2})} \end{bmatrix}.$$

This code and its dual are free $\mathbb{Z}_4$-modules of rank 4^{2^n-n-1} and 4^{n+1}, respectively.

We remind the reader that the *Lee weights* of $0, 1, 2, 3 \in \mathbb{Z}_4$ are $0, 1, 2, 1$, respectively, and the *Lee weight* $wt_L(c)$ of $c \in (\mathbb{Z}_4)^N$ is the sum of the Lee weights of its components. This weight function defines a metric in $(\mathbb{Z}_4)^N$, called the *Lee distance*.

Write $\mathcal{C}$ for the code $\mathcal{C}_f$ when f is identically zero (in which case f is planar). The dual code $\mathcal{C}^\perp$ is the $\mathbb{Z}_4$-Kerdock code described in [10]. Let

$$\phi : (\mathbb{Z}_4)^N \to (\mathbb{F}_2)^{2N}$$

be the Gray map, which defines an isometry between $(\mathbb{Z}_4)^N$, equipped with the Lee distance, and $(\mathbb{F}_2)^{2N}$, equipped with the Hamming distance. Then, for $n \geq 3$ odd, $\phi(\mathcal{C}^\perp)$ is the classical Kerdock code and $\phi(\mathcal{C})$ has the same parameters as the Preparata code (see [10] for details on these codes).

The Lee weight distribution of $\mathcal{C}^\perp$ has been determined in [10]. The following more general result gives a characterisation of planar functions.

Theorem 2.2 *The code $(\mathcal{C}_f)^\perp$ has the same Lee weight distribution as $\mathcal{C}^\perp$ if and only if f is planar. In particular, if f is planar, the Lee weight distribution of $(\mathcal{C}_f)^\perp$ is given in Table 2 for odd n and in Table 3 for even n.*

Table 3 Weight distribution of $(\mathcal{C}_f)^\perp$ for even n

Weight	Frequency
0	1
$2^n - 2^{n/2}$	$2^n(2^n-1)$
2^n	$2^{n+1}(2^n+1)-2$
$2^n + 2^{n/2}$	$2^n(2^n-1)$
2^{n+1}	1

Proof Let ω be a primitive fourth root of unity. If $c = (c_1, \ldots, c_N)$ is an element of $(\mathbb{Z}_4)^N$, then its Lee weight satisfies

$$\mathrm{wt}_L(c) = N - \mathrm{Re}\left(\sum_{i=1}^{N} \omega^{c_i}\right). \tag{7}$$

Let $T : R_n \to \mathbb{Z}_4$ be the absolute trace function on R_n. We shall index elements of codewords by $\Gamma(R_n)$. For $a \in R_n$ and $b \in \mathbb{Z}_4$, consider the codeword

$$c_{a,b} = \left(T\left(a\left(x + 2\sqrt{f(x)}\right)\right) + b\right)_{x \in \Gamma(R_n)}.$$

By a folklore generalisation of Delsarte's theorem [20, p. 208] to codes over $\mathbb{Z}_4$, these are exactly the 4^{n+1} codewords of $(\mathcal{C}_f)^\perp$. From (7) we have

$$\mathrm{wt}_L(c_{a,b}) = 2^n - \mathrm{Re}\left(\omega^b S_a\right), \tag{8}$$

where

$$S_a = \sum_{x \in \Gamma(R_n)} \omega^{T(a(x+2\sqrt{f(x)}))}.$$

Since $z \mapsto \omega^{T(az)}$ are exactly the characters of the additive group of R_n, by Theorem 2.1 and (5), the function f is planar if and only if

$$|S_a|^2 = \begin{cases} 4^n & \text{for } a = 0, \\ 0 & \text{for } a \in 2R_n \setminus \{0\}, \\ 2^n & \text{for } a \in R_n \setminus 2R_n. \end{cases} \tag{9}$$

Now, let f be planar. Using (8), we easily get the Lee weight distribution of the codewords $c_{a,b}$ when $a \in 2R_n$ and $b \in \mathbb{Z}_4$. Next assume that $a \in R_n \setminus 2R_n$ and write $S_a = X + \omega Y$ for integers X and Y. By Jacobi's two-square theorem, the only solutions to the Diophantine equation $X^2 + Y^2 = 2^n$ are

$$(X, Y) = \begin{cases} (\pm 2^{(n-1)/2}, \pm 2^{(n-1)/2}) & \text{for odd } n, \\ (0, \pm 2^{n/2}) \quad \text{or} \quad (\pm 2^{n/2}, 0) & \text{for even } n. \end{cases}$$

Therefore, for odd n, we have

$$S_a = \pm 2^{(n-1)/2} \pm 2^{(n-1)/2}\omega.$$

Hence, as b ranges over $\mathbb{Z}_4$ and $a \in R_n \setminus 2R_n$ is fixed, the expression $\mathrm{Re}(\omega^b S_a)$ takes on each of the values $\pm 2^{(n-1)/2}$ twice. One can then get the Lee weight distribution from (8). Likewise, for even n, we have

$$S_a = \pm 2^{n/2} \quad \text{or} \quad \pm 2^{n/2}\omega.$$

Hence, as b ranges over $\mathbb{Z}_4$ and $a \in R_n \setminus 2R_n$ is fixed, the expression $\mathrm{Re}(\omega^b S_a)$ is zero twice and takes on each of the values $\pm 2^{n/2}$ once. The Lee weight distribution follows from (8).

Now, if f is not planar, then it easily follows from (8) and the characterisation (9) of planar functions that the Lee weight distribution of $(\mathcal{C}_f)^\perp$ cannot coincide with that of $\mathcal{C}^\perp$. □

For odd n, we have the following alternative characterisations of planar functions.

Theorem 2.3 *For odd $n \geq 3$, the code $\mathcal{C}_f$ has minimum Lee distance 4 or 6, where the value 6 occurs if and only if f is planar.*

Proof Recall that the *type* of a codeword is defined as the enumerator of its nonzero entries. For example a codeword of type $1^2 2^4$ equals 1 at two positions and equals 2 at four positions.

Notice that a nonzero codeword in $\mathcal{C}_f$ of Lee weight at most 3 implies that there exists a codeword in $\mathcal{C}_f$ of type 2^1, 2^2, or 2^3. Such codewords however cannot exist in $\mathcal{C}_f$ (for the same reason as the minimum distance of the extended Hamming code equals 4). Hence the minimum Lee distance of $\mathcal{C}_f$ is at least 4.

If f is planar, the Lee weight distribution of $\mathcal{C}_f$ is independent of f by Theorem 2.2 and a MacWilliams-type identity (see [10, Sect. II.B], for example). Hence, if f is planar, the minimum Lee distance of $\mathcal{C}_f$ equals that of $\mathcal{C}$, which is 6 [10].

We complete the proof by assuming that f is not planar and show that $\mathcal{C}_f$ then contains a codeword of type $1^2(-1)^2$, and so has minimum distance at most 4. The code $\mathcal{C}_f$ contains a codeword of type $1^2(-1)^2$ if and only if there exist distinct elements u, v, x, y in $\Gamma(R_n)$ satisfying simultaneously the following two equations over R_n:

$$\begin{aligned} &u + x = v + y, \\ &u + 2\sqrt{f(u)} + x + 2\sqrt{f(x)} = v + 2\sqrt{f(v)} + y + 2\sqrt{f(y)}. \end{aligned}$$

By the definition (3) of addition in $\Gamma(R_n)$, these equations are equivalent to the following two equations over $\Gamma(R_n)$:

$$\begin{aligned} &u \oplus x = v \oplus y, \\ &ux \oplus f(u) \oplus f(x) = vy \oplus f(v) \oplus f(y). \end{aligned}$$

From the first equation we infer that there exists $z \in \Gamma(R_n)$ such that $u = v \oplus z$ and $y = x \oplus z$. The second equation then becomes

$$f(v) \oplus f(v \oplus z) \oplus vz = f(x) \oplus f(x \oplus z) \oplus xz.$$

Since f is not planar, this equation has a solution (v, x, z), where v and x are distinct and $z \neq 0$. One then verifies that u, v, x, y are also distinct. □

A consequence of Theorem 2.3 is the following.

Corollary 2.4 *For odd $n \geq 3$, the code $\phi(\mathcal{C}_f)$ punctured in one (arbitrary) coordinate has minimum distance* 3, 4, *or* 5, *where the value* 5 *occurs if and only if f is planar.*

Proof The only part that is not immediate from Theorem 2.3 is that the code cannot have minimum distance 6. But this value cannot occur since the code then violates a version of the Johnson bound [9]. □

Let $\mathcal{D}_f$ be the code over $\mathbb{F}_2$ with parity check matrix (6). If f is almost perfect nonlinear, then $\mathcal{D}_f$ has parameters $(2^n - 1, 2^{2^n-2n-1}, 5)$ for $n \geq 4$. In contrast, by Corollary 2.4, if f is planar, then $\phi(\mathcal{C}_f)$ punctured in one coordinate has parameters $(2^n - 1, 2^{2^n-2n}, 5)$ for even $n \geq 4$, and so contains twice as many codewords as $\mathcal{D}_f$. If f is planar, then $\phi(\mathcal{C}_f)$ punctured in one coordinate meets a version of the Johnson bound, and so is nearly perfect [9].

3 Planar monomial functions

We begin with providing a nontrivial example of planar monomial functions, in which

$$\mathrm{Tr}_m(x) = x + x^2 + \cdots + x^{2^{m-1}}$$

denotes the trace function on $\mathbb{F}_{2^m}$.

Theorem 3.1 *Let $c \in \mathbb{F}_{2^k}^*$ be such that $\mathrm{Tr}_k(c) = 0$. Then the function*

$$x \mapsto cx^{2^k+1}$$

is planar on $\mathbb{F}_{4^k}$.

Proof We have to show that, for each $\epsilon \in \mathbb{F}_{4^k}^*$, the mapping

$$x \mapsto c(x+\epsilon)^{2^k+1} + cx^{2^k+1} + \epsilon x$$

is a permutation of $\mathbb{F}_{4^k}$, or equivalently, the linear mapping

$$x \mapsto x^{2^k}\epsilon + x\epsilon^{2^k} + \epsilon x/c \tag{10}$$

is a permutation of $\mathbb{F}_{4^k}$. This holds if the kernel of the mapping (10) is trivial. Hence, it is enough to show that

$$x^{2^k-1} = \epsilon^{2^k-1} + 1/c$$

has no solution (x, ϵ) in $\mathbb{F}_{4^k}^* \times \mathbb{F}_{4^k}^*$. Let Γ be the cyclic subgroup of $\mathbb{F}_{4^k}^*$ with order $2^k + 1$. We show that

$$\Gamma \cap (\Gamma + 1/c) = \varnothing,$$

which will prove the theorem.

Let y be in Γ. Then $y^{2^k+1} = 1$ and, since $c \in \mathbb{F}_{2^k}^*$,

$$(y + 1/c)^{2^k+1} = 1 + 1/c^2 + 1/(cy) + y/c. \tag{11}$$

Now, suppose, for a contradiction, that y also belongs to $\Gamma + 1/c$. Then the left-hand side of (11) equals 1, and thus

$$y^2 + y/c + 1 = 0. \tag{12}$$

We may set $z = yc$ to transform this quadratic equation into the standard form $z^2 + z + c^2 = 0$, which has two solutions in $\mathbb{F}_{2^k}$ if and only if $\mathrm{Tr}_k(c^2) = 0$ [20, Chap. 9, Thm. 15]. Since $\mathrm{Tr}_k(c) = 0$ and $c \in \mathbb{F}_{2^k}$, we find that $y \in \mathbb{F}_{2^k}$. But y is also in Γ, so that

$$1 = y^{2^k+1} = y^2,$$

contradicting (12). □

We conjecture that the only planar exponents of $\mathbb{F}_{2^n}$ are the trivial examples 2^k and those identified in Theorem 3.1 and [25, Thm. 1.1].

Conjecture 3.2 *If t is a planar exponent of $\mathbb{F}_{2^n}$, then t is one of the values given in Table 1.*

The following partial answer to Conjecture 3.2 is easy to prove.

Proposition 3.3 *Let t be an integer satisfying* $\gcd(t-2, 2^n - 1) = 1$. *If t is a planar exponent of $\mathbb{F}_{2^n}$, then t is a power of* 2.

Proof Suppose that $x \mapsto cx^t$ is planar on $\mathbb{F}_{2^n}$ for some $c \in \mathbb{F}_{2^n}^*$. Then

$$x \mapsto c(x + \epsilon)^t + cx^t + \epsilon x$$

is a permutation of $\mathbb{F}_{2^n}$ for each $\epsilon \in \mathbb{F}_{2^n}^*$. Substituting $y = x/\epsilon$, we see that

$$y \mapsto (y + 1)^t + y^t + \left(\epsilon^{2-t}/c\right)y$$

is a permutation of $\mathbb{F}_{2^n}$ for each $\epsilon \in \mathbb{F}_{2^n}^*$. Hence, for each $\epsilon \in \mathbb{F}_{2^n}^*$, the equation

$$(y + 1)^t + y^t + (z + 1)^t + z^t = \left(\epsilon^{2-t}/c\right)(y + z)$$

has no solution (x, y) in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ satisfying $y \neq z$. Equivalently, writing

$$D = \left\{ \frac{(y + 1)^t + y^t + (z + 1)^t + z^t}{y + z} : y, z \in \mathbb{F}_{2^n}, y \neq z \right\},$$

we have $D \cap \{\epsilon^{2-t}/c : \epsilon \in \mathbb{F}_{2^n}^*\} = \varnothing$. But since $t - 2$ is coprime to $2^n - 1$, we have $\{\epsilon^{2-t}/c : \epsilon \in \mathbb{F}_{2^n}^*\} = \mathbb{F}_{2^n}^*$, hence $D = \{0\}$. Therefore, $(y + 1)^t + y^t$ is constant for all $y \in \mathbb{F}_{2^n}$, which implies that t is a power of two. □

Remark Proposition 3.3 corresponds to case (iv) of [1, Thm. 1.1].

We now focus on the relaxed problem of classifying the numbers that are planar exponents of $\mathbb{F}_{2^n}$ for infinitely many n. The only known such numbers are the powers of 2 and we have the following weaker form of Conjecture 3.2.

Conjecture 3.4 *If t is a planar exponent of $\mathbb{F}_{2^n}$ for infinitely many n, then t is a power of 2.*

Our main result, Theorem 1.3, is a partial answer to this conjecture. This result will be proved in the remainder of this paper. The method is outlined below.

Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be of the form $f(x) = cx^t$ for some $c \in \mathbb{F}_{2^n}^*$ and let $\epsilon \in \mathbb{F}_{2^n}^*$. Then the condition that (2) is a permutation is equivalent to the condition that the polynomial

$$c(U+\epsilon)^t + c(V+\epsilon)^t + cU^t + cV^t + \epsilon(U+V)$$

has no zeros (u, v) over $\mathbb{F}_{2^n}$ satisfying $u \neq v$. Substituting $U = \epsilon X$ and $V = \epsilon Y$, we see that this condition is in turn equivalent to the condition that the polynomial

$$(X+1)^t + (Y+1)^t + X^t + Y^t + a(X+Y) \tag{13}$$

has no zeros (u, v) over $\mathbb{F}_{2^n}$ satisfying $u \neq v$, where $a = \epsilon^{2-t}/c$. The polynomial (13) is divisible by $X + Y$. We are therefore interested in the zeros of the polynomial

$$F_{t,a}(X, Y) = \frac{(X+1)^t + (Y+1)^t + X^t + Y^t + a(X+Y)}{X+Y} \tag{14}$$

(which however could still have zeros on the line $X + Y$). We consider the affine plane curve defined by $F_{t,a}$ (and follow the usual convention to denote the curve and a defining polynomial by the same symbol). Then, defining a subset of $\mathbb{F}_{2^n}$ by

$$\mathcal{A}_n = \left\{\epsilon^{2-t}/c : \epsilon \in \mathbb{F}_{2^n}^*\right\}, \tag{15}$$

the function $x \mapsto cx^t$ is planar on $\mathbb{F}_{2^n}$ if and only if the curve $F_{t,a}$ has no rational points (u, v) over $\mathbb{F}_{2^n}$ satisfying $u \neq v$ for some $a \in \mathcal{A}_n$.

The number of rational points on a curve can be estimated using Weil's theorem, which we quote in the following form (see [5, Thm. 5.4.1], for example).

Weil's theorem *Let $F \in \mathbb{F}_q[X, Y]$ be an absolutely irreducible polynomial of degree d and let N be the number of rational points over $\mathbb{F}_q$ on the affine plane curve F. Then*

$$|N - q - 1| \leq (d-1)(d-2)\sqrt{q} + d.$$

A consequence of Weil's theorem is the following.

Proposition 3.5 *If $F_{t,a}$ has an absolutely irreducible factor over $\mathbb{F}_{2^n}$ for some $a \neq 1$ in $\mathcal{A}_n$ and n is sufficiently large, then t is not a planar exponent of $\mathbb{F}_{2^n}$.*

Proof Let $a \in \mathcal{A}_n$ satisfy $a \neq 1$ and suppose that $F_{t,a}$ has an absolutely irreducible factor over $\mathbb{F}_{2^n}$. By the above discussion, it is sufficient to show that, if n is sufficiently large, then the curve $F_{t,a}$ has rational points (u, v) over $\mathbb{F}_{2^n}$ satisfying $u \neq v$. Since the degree of $F_{t,a}$ is at most $t-2$, by Weil's theorem the number of rational points over $\mathbb{F}_{2^n}$ on the curve $F_{t,a}$ is at least

$$2^n - (t-3)(t-4)2^{n/2} - t + 3.$$

By taking partial derivatives of the numerator of $F_{t,a}$, we see that $F_{t,a}$ is never divisible by $X+Y$ since $a \neq 1$ (this fails for $t = 2^s + 1$ with $s > 0$ if we allow $a = 1$). Hence, if (u, u) is on the curve $F_{t,a}$, then u is a root of a nonzero polynomial of bounded degree. Therefore, if n is sufficiently large, the curve $F_{t,a}$ has rational points (u, v) over $\mathbb{F}_{2^n}$ satisfying $u \neq v$. □

In view of Proposition 3.5, Conjecture 3.4 is proved by showing that, when t is not a power of 2, $F_{t,a}$ has an absolutely irreducible factor over $\mathbb{F}_{2^n}$ for some $a \in \mathcal{A}_n$ satisfying $a \neq 1$ and all sufficiently large n.

The following corollary to Lucas' theorem will be useful.

Lemma 3.6 *The binomial coefficient* $\binom{m}{k}$ *is even if and only if at least one of the base-*2 *digits of* k *is greater than the corresponding digit of* m.

Instead of looking at $F_{t,a}$ directly, we consider its homogenised version $H_{t,a}(X, Y, Z)$. If t is not a power of two, we find from Lemma 3.6 that

$$H_{t,a}(X, Y, Z) = \frac{(X+Z)^t + (Y+Z)^t + X^t + Y^t + a(X+Y)Z^{t-1}}{Z^{2^j}(X+Y)}, \tag{16}$$

where j is the largest power of 2 that divides t. Of course, $F_{t,a}$ has an absolutely irreducible factor if and only if $H_{t,a}$ has an absolutely irreducible factor. Our strategy is to consider the projective plane curve defined by $H_{t,a}$ over the algebraic closure $\mathbb{F}$ of $\mathbb{F}_2$ and derive a contradiction to Bezout's theorem (see [6, Sect. 5.3], for example) under the assumption that $H_{t,a}$ has no absolutely irreducible factor over $\mathbb{F}_{2^n}$.

Bezout's theorem *Let* A *and* B *be two projective plane curves over an algebraically closed field* $\mathbb{K}$, *having no component in common. Then*

$$\sum_P I_P(A, B) = (\deg A)(\deg B),$$

where the sum runs over all points in the projective plane $\mathbb{P}^2(\mathbb{K})$.

Notice that $I_P(A, B)$ is the *intersection number* of A and B at P, whose precise definition is neither recalled nor required in this paper. We shall rather use some properties of the intersection number, which allows us to compute it in certain cases of interest. In Sect. 4, we shall obtain general upper bounds on the intersection number $I_P(A, B)$, where $F_{t,a} = AB$ is an arbitrary factorisation of $F_{t,a}$ and P is a point in the plane $\mathbb{P}^2(\mathbb{F})$. The desired contradiction to Bezout's theorem is then derived in Sect. 5.

4 Computation of intersection numbers

4.1 Some results on intersection numbers

Let F be an affine plane curve (which we always assume to be defined over an algebraically closed field), let $P = (u, v)$ be a point in the plane, and write

$$F(X + u, Y + v) = F_0(X, Y) + F_1(X, Y) + F_2(X, Y) + \cdots,$$

where F_i is either zero or a homogeneous polynomial of degree i. The *multiplicity* of F at P, written as $m_P(F)$, is the smallest integer m such that $F_m \neq 0$ and $F_i = 0$ for $i < m$; the polynomial is F_m is the *tangent cone* of F at P. A divisor of the tangent cone is called a *tangent* of F at P. The point P is on the curve F if and only if $m_P(F) \geq 1$. If P is on F, then P is a *simple* point of F if $m_P(F) = 1$, otherwise P is a *singular* point of F.

Now, let $F^*(X, Y, Z)$ be the homogenised polynomial of $F(X, Y)$ and write $P^* = (u, v, 1)$ (in homogeneous coordinates). Then the multiplicity of the projective plane curve F^* at P^*, also written as $m_{P^*}(F^*)$, is by definition $m_P(F)$. Likewise, the intersection number $I_{P^*}(A^*, B^*)$ is by definition $I_P(A, B)$, where A^* and B^* are the homogenised polynomials of A and B, respectively (see [6, Chap. 5] for details). We may therefore restrict our analysis to affine plane curves.

One important property of the intersection number is that $I_P(A, B) = 0$ if P is not a singular point of AB. This is a special case of the following more general property.

Lemma 4.1 [6, Chap. 3, Property (5)] *Let A and B be two affine plane curves and suppose that the tangent cones of A and B do not share a common factor. Let P be a point in the plane. Then $I_P(A, B) = m_P(A)m_P(B)$.*

It is an easy exercise to obtain the following result as a corollary of Lemma 4.1 (see Janwa, McGuire, and Wilson [15, Prop. 2]).

Corollary 4.2 *Let F be an affine plane curve and suppose that $F = AB$. Let $P = (u, v)$ be a point in the plane and write*

$$F(X + u, Y + v) = F_m(X, Y) + F_{m+1}(X, Y) + \cdots,$$

where F_i is zero or a homogeneous polynomial of degree i and $F_m \neq 0$. Let L be a linear polynomial and suppose that $F_m = L^m$ and $L \nmid F_{m+1}$. Then $I_P(A, B) = 0$.

We shall require one further result to compute intersection numbers, whose proof idea follows that of [12, Lemma 8].

Lemma 4.3 *Let F be an affine plane curve over a field of characteristic two and suppose that $F = AB$. Let $P = (u, v)$ be a point in the plane and write*

$$F(X + u, Y + v) = F_m(X, Y) + F_{m+1}(X, Y) + \cdots,$$

where F_i is zero or a homogeneous polynomial of degree i and $F_m \neq 0$. Let L be a linear polynomial and suppose that $F_m = L^m$ and $L \parallel F_{m+1}$. Then $I_P(A, B) = 0$ or m.

Proof Write

$$A(X+u, Y+v) = A_r(X, Y) + A_{r+1}(X, Y) + \cdots$$

and

$$B(X+u, Y+v) = B_s(X, Y) + B_{s+1}(X, Y) + \cdots,$$

where A_i and B_i are zero or homogeneous polynomials of degree i and A_r and B_s are nonzero. Since $F_m = L^m$, we have, up to constant factors, $A_r = L^j$ and $B_s = L^{m-j}$ for some $j \in \{0, \ldots, m\}$. Also,

$$F_{m+1} = A_r B_{s+1} + A_{r+1} B_s, \tag{17}$$

and since $L \parallel F_{m+1}$, we find that $\gcd(A_r, B_s) = 1$ or L. If $\gcd(A_r, B_s) = 1$, then either $m_P(A) = 0$ or $m_P(B) = 0$ and $I_P(A, B) = 0$ by Lemma 4.1.

Now, suppose that $\gcd(A_r, B_s) = L$, which implies that $m \geq 2$. Without loss of generality, we may assume that $A_r = L$ and $B_s = L^{m-1}$, so that $r = 1$ and $s = m-1$. Define

$$C(X, Y) = A(X, Y)L(X-u, Y-v)^{m-2} + B(X, Y).$$

Then, by a general property of intersection numbers [6, Chap. 3, Property (7)], we find that

$$I_P(A, B) = I_P(A, C).$$

We have

$$C(X+u, Y+v) = A_2(X, Y)L(X, Y)^{m-2} + B_m(X, Y) + \text{higher order terms}.$$

If $m = 2$, then it follows from $L \parallel F_{m+1}$ and (17) that $L \nmid A_2 + B_2$. If $m > 2$, we find from (17) that $L \nmid B_m$. In either case, the tangent cones of A and C do not share a common factor and therefore $I_P(A, C) = m_P(A)m_P(C)$ by Lemma 4.1. This completes the proof since $m_P(A) = 1$ and $m_P(C) = m$. □

4.2 Singular points at infinity of $H_{t,a}$

We now study the intersection numbers $I_P(A, B)$, where $H_{t,a} = AB$ is some factorisation and P is a singular point at infinity of $H_{t,a}$, namely a point of the form $(u, v, 0)$. Since $H_{t,a}$ is symmetric in X and Y, we can assume that $v = 1$. It is then sufficient to consider the dehomogenisation

$$G_{t,a}(X, Z) = H_{t,a}(X, 1, Z),$$

so that

$$G_{t,a}(X,Z)=\frac{(X+Z)^t+(Z+1)^t+X^t+a(X+1)Z^{t-1}+1}{Z(X+1)}.$$

The result of this section is the following.

Lemma 4.4 *Let t be a number of the form $2^k\ell+1$ for integers $k\geq 1$ and odd $\ell\geq 3$. Let $P=(u,0)$ be a singular point of $G_{t,a}$ and suppose that $G_{t,a}=AB$ is a factorisation over $\mathbb{F}$. Then $I_P(A,B)\leq 4^{k-1}$.*

Proof Write $\widetilde{G}_{t,a}$ for the numerator of $G_{t,a}$, namely

$$\widetilde{G}_{t,a}(X,Z)=Z(X+1)G_{t,a}(X,Z). \tag{18}$$

Next we compute the multiplicities of $G_{t,a}$ and $\widetilde{G}_{t,a}$ at P. Write

$$G_{t,a}(X+u,Z)=G_0(X,Z)+G_1(X,Z)+G_2(X,Z)+\cdots$$

and

$$\widetilde{G}_{t,a}(X+u,Z)=\widetilde{G}_0(X,Z)+\widetilde{G}_1(X,Z)+\widetilde{G}_2(X,Z)+\cdots,$$

where G_i and $\widetilde{G}_i$ are either zero or homogeneous polynomials of degree i. From (18) we find that

$$\widetilde{G}_i(X,Z)=XZG_{i-2}(X,Z)+Z(u+1)G_{i-1}(X,Z), \tag{19}$$

where, by convention, $G_{-1}=G_{-2}=0$. We have

$$\widetilde{G}_{t,a}(X+u,Z)=\sum_{j=0}^{t}\binom{t}{j}\left[u^{t-j}\left((X+Z)^j+X^j\right)+Z^j\right]+a(X+u+1)Z^{t-1}+1.$$

Since P is a singular point of $G_{t,a}$, and so is a singular point of $\widetilde{G}_{t,a}$, we have $\widetilde{G}_0=\widetilde{G}_1=0$. From Lemma 3.6 we see that $\widetilde{G}_i=0$ for each $i\in\{2,\ldots,2^k-1\}$. Furthermore, since $\ell\geq 3$,

$$\widetilde{G}_{2^k}(X,Z)=\left(u^{t-2^k}+1\right)Z^{2^k} \tag{20}$$

and

$$\widetilde{G}_{2^k+1}(X,Z)=u^{t-2^k-1}\left((X+Z)^{2^k+1}+X^{2^k+1}\right)+Z^{2^k+1}.$$

We now see that the multiplicity of $\widetilde{G}_{t,a}$ at $P=(1,0)$ is 2^k+1, while that of $\widetilde{G}_{t,a}$ at $P=(u,0)$ for $u\neq 1$ can be either 2^k or 2^k+1. Using (19), it is then straightforward to work out the corresponding multiplicities of $G_{t,a}$. The results are summarised in Table 4.

We shall need the following observation, which will be proved at the end of this section.

Table 4 Multiplicities of $G_{t,a}$ and $\widetilde{G}_{t,a}$ at their singular points

Type	Point P	$m_P(\widetilde{G}_{t,a})$	$m_P(G_{t,a})$
A	$(1,0)$	2^k+1	2^k-1
B	$(u,0)$, $u\neq 1$	2^k+1	2^k
C	$(u,0)$, $u\neq 1$	2^k	2^k-1

Claim 4.5 *$\widetilde{G}_{2^k+1}$ splits into 2^k+1 distinct factors over its splitting field.*

We resume the proof of Lemma 4.4 and distinguish three cases for P, according to Table 4.

- P is a point of type A. In this case, the multiplicity of $G_{t,a}$ at P is 2^k-1 and from (19) we have
$$\widetilde{G}_{2^k+1}(X,Z)=XZG_{2^k-1}(X,Z).$$
Therefore, by Claim 4.5, G_{2^k-1}, the tangent cone of $G_{t,a}$ at P, has no multiple factors over its splitting field. Lemma 4.1 then implies $I_P(A,B)=m_P(A)m_P(B)$.
- P is a point of type B. In this case, the multiplicity of $G_{t,a}$ at P is 2^k and from (19) we have
$$\widetilde{G}_{2^k+1}(X,Z)=Z(u+1)G_{2^k}(X,Z).$$
Thus by Claim 4.5, G_{2^k}, the tangent cone of $G_{t,a}$ at P, has no multiple factors over its splitting field and so Lemma 4.1 gives $I_P(A,B)=m_P(A)m_P(B)$.
- P is a point of type C. Now, the multiplicity of $G_{t,a}$ at P is 2^k-1. From (19) we find that
$$\widetilde{G}_{2^k}(X,Z)=Z(u+1)G_{2^k-1}(X,Z),$$
$$\widetilde{G}_{2^k+1}(X,Z)=XZG_{2^k-1}(X,Z)+Z(u+1)G_{2^k}(X,Z).$$
From (20) we see that the tangent cone of $G_{t,a}$ at P equals
$$G_{2^k-1}(X,Z)=\frac{u^{t-2^k}+1}{u+1}Z^{2^k-1}$$
and then, by Claim 4.5, $Z\nmid G_{2^k}$. Thus $I_P(A,B)=0$ by Corollary 4.2.

Now, from the three cases above we conclude that $I_P(A,B)$ equals either zero or $m_P(A)m_P(B)$. But since
$$m_P(A)+m_P(B)=m_P(G_{t,a})\leq 2^k,$$
we find that $I_P(A,B)\leq(2^{k-1})^2$, as required. □

It remains to prove the claim invoked in the proof of Lemma 4.4.

Proof of Claim 4.5 We show that
$$\gcd(\widetilde{G}_{2^k+1},\partial\widetilde{G}_{2^k+1}/\partial X)\in\mathbb{F}[Z] \tag{21}$$

and

$$\gcd\big(\widetilde{G}_{2^k+1}, \partial\widetilde{G}_{2^k+1}/\partial Z\big) \in \mathbb{F}[X]. \tag{22}$$

The assertion (21) follows since

$$\partial\widetilde{G}_{2^k+1}/\partial X = \big(u^{\ell-1}Z\big)^{2^k}.$$

To prove (22), first observe that $P = (0, 0)$ is not a singular point of $\widetilde{G}_{t,a}$ since then $\widetilde{G}_1(X, Z) = Z$, and so it is not a singular point of $G_{t,a}$. Hence we may assume that $u \neq 0$. We have

$$\partial\widetilde{G}_{2^k+1}/\partial Z = \big(u^{\ell-1}X + \big(u^{\ell-1}+1\big)Z\big)^{2^k}.$$

Hence $\partial\widetilde{G}_{2^k+1}/\partial Z$ has only one factor, namely

$$X + \frac{u^{\ell-1}+1}{u^{\ell-1}}Z. \tag{23}$$

We readily verify that

$$\widetilde{G}_{2^k+1}\left(\frac{u^{\ell-1}+1}{u^{\ell-1}}Z, Z\right) = u^{(\ell-1)(2^k-1)}\big(u^{\ell-1}+1\big)Z^{2^k+1}.$$

Hence, since $u \neq 0$, (23) divides $\widetilde{G}_{2^k+1}$ only if $u = 1$. However, for $u = 1$, (23) equals X, which proves (22). □

4.3 Affine singular points of $H_{t,a}$

We are now interested in the intersection numbers $I_P(A, B)$, where $H_{t,a} = AB$ and P is an affine singular point of $H_{t,a}$, namely P is of the form $(u, v, 1)$. We work with the dehomogenisation

$$F_{t,a}(X, Y) = H_{t,a}(X, Y, 1),$$

as given in (14). Let $\widetilde{F}_{t,a}(X, Y)$ be the numerator of $F_{t,a}(X, Y)$, so that

$$\widetilde{F}_{t,a}(X, Y) = (X+1)^t + (Y+1)^t + X^t + Y^t + a(X+Y).$$

Our analysis crucially relies on restricting a to values in a subset of $\mathcal{A}_n$, which we define next.

Definition 4.6 Let $\mathcal{B}_n$ be the set of all $a \in \mathcal{A}_n$ such that all singular points (u, v) of $\widetilde{F}_{t,a}$ satisfy each of

$$(u+1)^{t-2^k} \neq u^{t-2^k},$$
$$(u+1)^{t-2^k-1} \neq u^{t-2^k-1},$$
$$(v+1)^{t-2^k-1} \neq v^{t-2^k-1}.$$

Lemma 4.7 *The set $\mathcal{B}_n$ contains an element not equal to* 1 *for all sufficiently large n.*

Proof Let $\mathcal{P}$ be the set of points $(u, v) \in \mathbb{F} \times \mathbb{F}$ that satisfy at least one of

$$(u+1)^{t-2^k} + u^{t-2^k} = 0,$$
$$(u+1)^{t-2^k-1} + u^{t-2^k-1} = 0,$$
$$(v+1)^{t-2^k-1} + v^{t-2^k-1} = 0.$$

Since $t - 2^k$ is constant, we find by a degree argument that $\mathcal{P}$ has finite size. Then, by Definition 4.6, $a \in \mathcal{A}_n$ belongs to $\mathcal{B}_n$ if no point in $\mathcal{P}$ is a singular point of $\widetilde{F}_{t,a}$. By looking at the homogeneous part of degree 1 of $\widetilde{F}_{t,a}(X+u, Y+v)$, we see that a necessary condition for (u, v) to be a singular point of $\widetilde{F}_{t,a}$ is

$$(u+1)^{t-1} + u^{t-1} = a. \tag{24}$$

But from the definition (15) of $\mathcal{A}_n$ we have

$$|\mathcal{A}_n| = \frac{2^n - 1}{\gcd(2^n - 1, t-2)} \geq \frac{2^n - 1}{t-2},$$

and so, for all sufficiently large n, we can choose an $a \neq 1$ in $\mathcal{A}_n$ such that (24) is not satisfied for each $(u, v) \in \mathcal{P}$. This $a \in \mathcal{A}_n$ belongs to $\mathcal{B}_n$ since none of the points in $\mathcal{P}$ is a singular point of $\widetilde{F}_{t,a}$. □

We now state the main result of this section.

Lemma 4.8 *Let t be a number of the form $2^k\ell + 1$ for integers $k \geq 1$ and odd $\ell \geq 1$ and let $a \in \mathcal{B}_n$. Suppose that $F_{t,a} = AB$ is a factorisation over $\mathbb{F}$ and let P be a singular point of $F_{t,a}$.*

(i) *If $P = (u, u)$, then $m_P(F_{t,a}) = 2^k - 1$ and $I_P(A, B) = 0$.*
(ii) *If $P = (u, v)$ with $u \neq v$, then $m_P(F_{t,a}) = 2^k$ and $I_P(A, B) = 2^k$.*

Proof We shall first compute the multiplicities of $F_{t,a}$ and $\widetilde{F}_{t,a}$ at $P = (u, v)$. Write

$$F_{t,a}(X+u, Y+v) = F_0(X, Y) + F_1(X, Y) + F_2(X, Y) + \cdots$$

and

$$\widetilde{F}_{t,a}(X+u, Y+v) = \widetilde{F}_0(X, Y) + \widetilde{F}_1(X, Y) + \widetilde{F}_2(X, Y) + \cdots,$$

where F_i and $\widetilde{F}_i$ are either zero or homogeneous polynomials of degree i. We have

$$\begin{aligned}\widetilde{F}_{t,a}&(X+u, Y+v)\\ &= a(X + Y + u + v)\\ &\quad + \sum_{j=0}^{t} \binom{t}{j} \left(\left[(u+1)^{t-j} + u^{t-j} \right] X^j + \left[(v+1)^{t-j} + v^{t-j} \right] Y^j \right). \end{aligned} \tag{25}$$

Since P is a singular point of $F_{t,a}$, and so is a singular point of $\widetilde{F}_{t,a}$, we have $\widetilde{F}_0 = \widetilde{F}_1 = 0$. From Lemma 3.6 we see that $\widetilde{F}_i = 0$ for each $i \in \{2, \ldots, 2^k - 1\}$. Furthermore,

$$\widetilde{F}_{2^k}(X, Y) = \left((u+1)^{t-2^k} + u^{t-2^k}\right)X^{2^k} + \left((v+1)^{t-2^k} + v^{t-2^k}\right)Y^{2^k}. \tag{26}$$

Since $a \in \mathcal{B}_n$, we see from Definition 4.6 that $\widetilde{F}_{2^k}$ is never zero and so

$$m_P(\widetilde{F}_{t,a}) = 2^k. \tag{27}$$

To compute the multiplicity of $F_{t,a}$ at P, we use

$$\widetilde{F}_i(X, Y) = (X + Y)F_{i-1}(X, Y) + (u + v)F_i(X, Y), \tag{28}$$

where, by convention, $F_{-1} = 0$. We now prove the two cases of the lemma separately, using the following claim proved at the end of this section.

Claim 4.9 *$\widetilde{F}_{2^k+1}$ splits into $2^k + 1$ distinct factors over its splitting field.*

- $P = (u, u)$. In this case, we have $m_P(F_{t,a}) = 2^k - 1$ by (27) and (28). Furthermore, from (28),

$$\widetilde{F}_{2^k}(X, Y) = (X + Y)F_{2^k-1}(X, Y),$$
$$\widetilde{F}_{2^k+1}(X, Y) = (X + Y)F_{2^k}(X, Y),$$

  and then from (26),

$$F_{2^k-1}(X, Y) = \left((u+1)^{t-2^k} + u^{t-2^k}\right)(X + Y)^{2^k-1}.$$

  By Claim 4.9, $\widetilde{F}_{2^k+1}$ has no multiple factors over its splitting field, and so $X + Y$ does not divide F_{2^k}. Thus $I_P(A, B) = 0$ by Corollary 4.2.
- $P = (u, v)$ with $u \neq v$. In this case, we have $m_P(F_{t,a}) = 2^k$ by (27) and (28). From (28) we have

$$\widetilde{F}_{2^k} = (u + v)F_{2^k},$$
$$\widetilde{F}_{2^k+1} = (X + Y)F_{2^k} + (u + v)F_{2^k+1}.$$

  Since $\widetilde{F}_{2^k+1}$ has no multiple factors by Claim 4.9, we conclude that F_{2^k} and F_{2^k+1} share at most one factor. Furthermore, from (26), we see that

$$F_{2^k}(X, Y) = (a_1X + a_2Y)^{2^k} \quad \text{for some } a_1, a_2 \in \mathbb{F}.$$

  If $a_1X + a_2Y$ does not divide F_{2^k+1}, then $I_P(A, B) = 0$ by Corollary 4.2, so assume that F_{2^k} and F_{2^k+1} share the factor $a_1X + a_2Y$. This factor must divide F_{2^k+1} exactly and thus $I_P(A, B) = 0$ or 2^k by Lemma 4.3.

This completes the proof. □

We now prove the claim invoked in the proof of Lemma 4.8.

Proof of Claim 4.9 From (25) we find that $\widetilde{F}_{2^k+1}(X, Y)$ equals

$$\big((u+1)^{t-2^k-1}+u^{t-2^k-1}\big)X^{2^k+1}+\big((v+1)^{t-2^k-1}+v^{t-2^k-1}\big)Y^{2^k+1}.$$

Since $a \in \mathcal{B}_n$, we readily verify with Definition 4.6 that

$$\gcd(\widetilde{F}_{2^k+1}, \partial\widetilde{F}_{2^k+1}/\partial X) = \gcd(\widetilde{F}_{2^k+1}, \partial\widetilde{F}_{2^k+1}/\partial Y) = 1.$$

This proves the claim. □

5 Proof of Theorem 1.3

Let $t > 1$ be an odd integer. Recall that, in view of Proposition 3.5, we wish to show that $F_{t,a}$, given in (14) (or equivalently $H_{t,a}$, given in (16)) has an absolutely irreducible factor over $\mathbb{F}_{2^n}$ for some $a \neq 1$ in $\mathcal{A}_n$ and for all sufficiently large n.

The case that $t = 2^k + 1$ is particularly easy to handle.

Proposition 5.1 *Let t be a number of the form $2^k + 1$ for integral $k \geq 1$. Then $F_{t,a}$ has an absolutely irreducible factor for some $a \neq 1$ in $\mathcal{A}_n$ and for all sufficiently large n.*

Proof Notice that $F_{t,a}$ simplifies to

$$F_{t,a}(X, Y) = (X + Y)^{2^k-1} + a + 1.$$

We claim that, for all sufficiently large n, we can choose $a \neq 1$ in $\mathcal{A}_n$ such that

$$a + 1 = b^{2^k-1}.$$

for some $b \in \mathbb{F}_{2^n}^*$. This will prove the proposition since then $X + Y + b$ divides $F_{t,a}$. By the definition (15) of $\mathcal{A}_n$, the claim is equivalent to the existence of $\epsilon, b \in \mathbb{F}_{2^n}^*$ such that, for all $c \in \mathbb{F}_{2^n}^*$,

$$\epsilon^{1-2^k}/c + 1 = b^{2^k-1}, \tag{29}$$

which in turn is equivalent to

$$\epsilon^{2^k-1} + x^{2^k-1} = 1/c, \tag{30}$$

where $x = \epsilon b$. It is well known [19, Example 6.38] that the number of solutions $(\epsilon, x) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ to the equation (30) is at least

$$2^n - \big(2^k - 2\big)\big(2^k - 3\big)2^{n/2} - 2^k + 2.$$

Since there are at most $2^k - 1$ solutions of the form $(0, x)$ and at most $2^k - 1$ solutions of the form $(\epsilon, 0)$, we find that, for all sufficiently large n, there exist $\epsilon, x \in \mathbb{F}_{2^n}^*$ satisfying (30). Hence, for all sufficiently large n, there exist $\epsilon, b \in \mathbb{F}_{2^n}^*$ satisfying (29), as required. □

Henceforth, we assume that $t = 2^k\ell + 1$ for integers $k \geq 1$ and odd $\ell \geq 3$. We shall factor $H_{t,a}$ into putative factors A and B over some extension of $\mathbb{F}_{2^n}$ and derive a contradiction to Bezout's theorem, using our estimates for $I_P(A, B)$. Since $I_P(A, B) = 0$ if P is a simple point of AB, the sum in Bezout's theorem can be taken over the singular points of AB. The main results of Sect. 4 can be restated as follows ((i) follows from Lemma 4.4 and the remarks preceding it, and (ii) and (iii) follow from Lemmas 4.7 and 4.8).

Corollary 5.2 *Let t be a number of the form $2^k\ell + 1$ for integers $k \geq 1$ and odd $\ell \geq 3$. Let P be a singular point of $H_{t,a}$ and suppose that $H_{t,a} = AB$ is a factorisation of $H_{t,a}$ over $\mathbb{F}$. Then, for some $a \neq 1$ in $\mathcal{A}_n$ and all sufficiently large n, the following holds*:

(i) *If $P = (u, v, 0)$, then $I_P(A, B) \leq 4^{k-1}$.*
(ii) *If $P = (u, u, 1)$, then $m_P(H_{t,a}) = 2^k - 1$ and $I_P(A, B) = 0$.*
(iii) *If $P = (u, v, 1)$ and $u \neq v$, then $m_P(H_{t,a}) = 2^k$ and $I_P(A, B) \leq 2^k$.*

It remains to count the number of singular points of $H_{t,a}$. To do so, we consider the numerator of $H_{t,a}$, namely

$$\widetilde{H}_{t,a}(X, Y, Z) = (X + Z)^t + (Y + Z)^t + X^t + Y^t + a(X + Y)Z^{t-1}.$$

Recall that a point P on a projective plane curve defined by $H(X, Y, Z)$ is a singular point of H if and only if the partial derivatives of H with respect to X, Y, and Z vanish at P. Since t is odd, we have

$$\begin{aligned}
\partial\widetilde{H}_{t,a}/\partial X &= (X + Z)^{t-1} + X^{t-1} + aZ^{t-1},\\
\partial\widetilde{H}_{t,a}/\partial Y &= (Y + Z)^{t-1} + Y^{t-1} + aZ^{t-1},\\
\partial\widetilde{H}_{t,a}/\partial Z &= (X + Z)^{t-1} + (Y + Z)^{t-1}.
\end{aligned}$$

Recalling that $t = 2^k\ell + 1$ and $\ell \geq 3$, it is then readily verified that the possible singular points of $\widetilde{H}_{t,a}$ are of one of the following types:

- Points at infinity: $(u, 1, 0)$ satisfying $u^\ell = 1$,
- Affine points: $(u, v, 1)$ satisfying

$$\begin{cases}
(u + 1)^\ell = u^\ell + a^{2^{-k}},\\
(v + 1)^\ell = v^\ell + a^{2^{-k}},\\
(u + 1)^\ell = (v + 1)^\ell.
\end{cases} \tag{31}$$

Lemma 5.3 *Let t be a number of the form $2^k\ell + 1$ for integers $k \geq 1$ and odd $\ell \geq 3$. Then, for each nonzero $a \in \mathbb{F}$, the curve $H_{t,a}$ has at most ℓ singular points at infinity and at most $(\ell - 1)(\ell - 2)/2$ affine singular points $(u, v, 1)$ satisfying $u \neq v$.*

Proof First observe that each singular point of $H_{t,a}$ is also a singular point of $\widetilde{H}_{t,a}$. It is readily verified that $\widetilde{H}_{t,a}$ has at most ℓ singular points at infinity, thus $H_{t,a}$ has at most ℓ such singular points.

We now show that $\widetilde{H}_{t,a}$ has at most $(\ell-1)(\ell-1)/2$ affine singular points $(u, v, 1)$ satisfying $u \neq v$. Let $a \in \mathbb{F}$ be nonzero. Since $\ell \geq 3$ is odd, the first two conditions of (31) are not trivially satisfied. Thus we find from a degree argument that there are exactly $(\ell-1)(\ell-2)$ pairs (u, v) with $u \neq v$ that satisfy the first two conditions of (31). Notice that, if (u, v) is such a pair, then $(u+1, v)$ also satisfies the first two conditions of (31). Now, let $(u, v, 1)$ be a singular point of $\widetilde{H}_{t,a}$, so that the pair (u, v) satisfies (31). We claim that $(u+1, v, 1)$ is not a singular point of $\widetilde{H}_{t,a}$, for if $(u+1, v)$ satisfies all three conditions of (31), then $(u+1)^\ell = u^\ell$, which implies $a = 0$ and so contradicts our assumption that a is nonzero. Hence there are at most $(\ell-1)(\ell-2)/2$ affine singular points on $H_{t,a}$. □

We now show that $H_{t,a}$ has an absolutely irreducible factor for some $a \neq 1$ in $\mathcal{A}_n$ and all sufficiently large n.

Proposition 5.4 *Let t be a number of the form $2^k\ell + 1$ for integers $k \geq 1$ and odd $\ell \geq 3$. Then $H_{t,a}$ has an absolutely irreducible factor over $\mathbb{F}_{2^n}$ for some $a \neq 1$ in $\mathcal{A}_n$ and all sufficiently large n.*

To prove the proposition, we shall need one further standard result (see Hernando and McGuire [11, Lemma 10], for example).

Lemma 5.5 *Let $F \in \mathbb{F}_q[X_1, \ldots, X_m]$ be a polynomial of degree d, irreducible over $\mathbb{F}_q$. Then there exists a natural number $s \mid d$ such that, over its splitting field, F splits into s absolutely irreducible polynomials, each of degree d/s.*

Proof of Proposition 5.4 If $H_{t,a} = AB$ is a nontrivial factorisation of $H_{t,a}$ and A and B are not relatively prime, then by definition, $\sum_P I_P(A, B) = \infty$. However, by Lemma 5.3 and Corollary 5.2, $H_{t,a}$ has a finite number of singular points P, each having a finite intersection number $I_P(A, B)$. Hence we can assume that A and B are relatively prime, which allows us to use the conclusion of Bezout's theorem.

Write

$$H_{t,a} = Q_1 Q_2 \cdots Q_r,$$

where Q_i is irreducible over $\mathbb{F}_{2^n}$. Let d_i be the degree of Q_i. By Lemma 5.5 there exist natural numbers s_i such that Q_i splits into s_i absolutely irreducible factors over $\mathbb{F}$, each of degree d_i/s_i. If $s_i = 1$ for some $i \in \{1, \ldots, r\}$, then $H_{t,a}$ has an absolutely irreducible factor over $\mathbb{F}_{2^n}$ and we are done. Thus assume, for a contradiction, that $s_i > 1$ for each $i \in \{1, \ldots, r\}$.

We arrange the factors of Q_i into three polynomials, C_i, D_i, and R_i, such that $\deg C_i = \deg D_i$ and such that $R_i = 1$ if s_i is even and $\deg R_i = d_i/s_i$ if s_i is odd. Write $C = C_1 \cdots C_r$, $D = D_1 \cdots D_r$, and $R = R_1 \cdots R_r$. Let δ be the degree of C (and of D) and let ρ be the degree of R. Since CDR is a factorisation of $H_{t,a}$, which

has degree $t-2$, we find that

$$2\delta + \rho = t - 2, \tag{32}$$

and, since $s_i > 1$,

$$\rho \leq \frac{t-2}{3}, \tag{33}$$

which gives

$$\begin{aligned}(\deg CR)(\deg D) &= (\delta+\rho)\delta \\ &= \frac{(2\delta+\rho)^2 - \rho^2}{4} \\ &\geq \frac{2}{9}(t-2)^2.\end{aligned}$$

Bezout's theorem then gives

$$\sum_P I_P(CR, D) \geq \frac{2}{9}(t-2)^2. \tag{34}$$

On the other hand, we find from Lemma 5.3 and Corollary 5.2 that, for some $a \neq 1$ in $\mathcal{A}_n$ and for all sufficiently large n,

$$\sum_P I_P(CR, D) \leq \ell 4^{k-1} + \frac{(\ell-1)(\ell-2)}{2} 2^k.$$

This contradicts (34) for $k \geq 2$ since $\ell > 1$. We now consider the case $k = 1$, so that $t = 2\ell + 1$. Choose $a \neq 1$ in $\mathcal{A}_n$ and take n sufficiently large so that the assertions of Corollary 5.2 hold. Since $k = 1$, we find from Corollary 5.2 that all affine singular points of $H_{t,a}$ are of the form $(u, v, 1)$ with $u \neq v$ and the multiplicity of such a singular point equals 2. Hence an affine singular point of $H_{t,a}$ can only be a point of at most two of the factors of $H_{t,a}$. Given two factors F and G of $H_{t,a}$, let N_{FG} be the number of affine singular points of $H_{t,a}$ that are on both F and G. Then, by Corollary 5.2,

$$N_{CD} + N_{CR} + N_{DR} \leq \frac{(\ell-1)(\ell-2)}{2}. \tag{35}$$

Bezout's theorem gives

$$\sum_P I_P(CD, R) = 2\delta\rho,$$

$$\sum_P I_P(CR, D) = (\delta+\rho)\delta,$$

$$\sum_P I_P(DR, C) = (\delta+\rho)\delta.$$

We estimate the left-hand sides using Lemma 5.3 and Corollary 5.2 and obtain

$$2(N_{CR} + N_{DR}) + \ell \geq 2\delta\rho,$$
$$2(N_{CD} + N_{DR}) + \ell \geq (\delta + \rho)\delta,$$
$$2(N_{CD} + N_{CR}) + \ell \geq (\delta + \rho)\delta.$$

Summing these equations gives

$$2\delta^2 + 4\delta\rho \leq 4(N_{CD} + N_{CR} + N_{DR}) + 3\ell \leq 2(\ell - 1)(\ell - 2) + 3\ell,$$

using (35). Since $t = 2\ell + 1$, we have from (32) that

$$\ell = \frac{2\delta + \rho + 1}{2}$$

and therefore

$$2\delta(2\rho + 1) \leq \rho(\rho - 1) + 6. \tag{36}$$

From (32) and (33) we conclude that $\delta \geq \rho$, so that

$$2\rho(2\rho + 1) \leq \rho(\rho - 1) + 6,$$

or equivalently $\rho(\rho + 1) \leq 2$, forcing $\rho \leq 1$. But, if $\rho = 0$, then t is even by (32); a contradiction. Hence $\rho = 1$ and then from (36) we find that $\delta = 1$, giving $t = 5$ by (32). But $t = 5$ cannot be written as $2\ell + 1$ for odd ℓ, which completes the proof. □

Now, our main result, Theorem 1.3, follows from Propositions 3.5, 5.1, and 5.4.

6 Final remarks

Since the submission of this paper, various new results have been obtained by other authors. Most notably, Müller and Zieve [21] give a characterisation of low-degree planar monomials, thereby proving Conjecture 3.4 and providing a different proof of Theorem 1.3. New examples of planar functions, in particular planar binomials, have been found by Hu, Li, Zhang, Feng, and Ge in [14].

References

1. Blokhuis, A., Ball, S., Brouwer, A.E., Storme, L., Szőnyi, T.: On the number of slopes of the graph of a function defined on a finite field. J. Combin. Theory Ser. A **86**, 187–196 (1999)
2. Carlet, C., Charpin, P., Zinoviev, V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr. **15**, 125–156 (1998)
3. Carlet, C., Ding, C., Yuan, J.: Linear codes from perfect nonlinear mappings and their secret sharing schemes. IEEE Trans. Inform. Theory **51**, 2089–2102 (2005)
4. Dembowski, P., Ostrom, T.G.: Planes of order n with collineation groups of order n^2. Math. Z. **103**, 239–258 (1968)
5. Fried, M.D., Jarden, M.: Field Arithmetic, 3rd edn. Springer, Berlin (2008)

6. Fulton, W.: Algebraic Curves, 3rd edn. (2008). http://www.math.lsa.umich.edu/~wfulton/
7. Ganley, M.J.: On a paper of P. Dembowski and T. G. Ostrom: "Planes of order n with collineation groups of order n^2." Math. Z. **103**, 239–258 (1968). Arch. Math. (Basel) **27**, 93–98 (1976)
8. Ganley, M.J., Spence, E.: Relative difference sets and quasiregular collineation groups. J. Combin. Theory Ser. A **19**, 134–153 (1975)
9. Goethals, J.-M., Snover, S.L.: Nearly perfect binary codes. Discrete Math., 65–88 (1972)
10. Hammons, A.R. Jr., Kumar, P.V., Calderbank, A.R., Sloane, N.J.A., Solé, P.: The $\mathbf{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes. IEEE Trans. Inform. Theory **40**, 301–319 (1994)
11. Hernando, F., McGuire, G.: Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions. J. Algebra **343**, 78–92 (2011)
12. Hernando, F., McGuire, G.: Proof of a conjecture of Segre and Bartocci on monomial hyperovals in projective planes. Des. Codes Cryptogr. **65**, 275–289 (2012)
13. Hernando, F., McGuire, G., Monserrat, F.: On the classification of exceptional planar functions over $\mathbb{F}_p$ (2013) arXiv:1301.4016v1 [math.AG]
14. Hu, S., Li, S., Zhang, T., Feng, T., Ge, G.: New planar binomials in characteristic two (2013). arXiv:1304.7044v1 [math.CO]
15. Janwa, H., McGuire, G.M., Wilson, R.M.: Double-error-correcting cyclic codes and absolutely irreducible polynomials over GF(2). J. Algebra **178**, 665–676 (1995)
16. Jedlicka, D.: APN monomials over GF(2^n) for infinitely many n. Finite Fields Appl. **13**, 1006–1028 (2007)
17. Jungnickel, D.: On a theorem of Ganley. Graphs Combin. **3**, 141–143 (1987)
18. Leducq, E.: Functions which are PN on infinitely many extensions of $\mathbb{F}_p$, p odd (2012). arXiv:1006.2610v2 [math.NT]
19. Lidl, R., Niederreiter, H.: Finite Fields, 2nd edn. Encyclopedia of Mathematics and Its Applications, vol. 20. Cambridge University Press, Cambridge (1997)
20. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland, Amsterdam (1977)
21. Müller, P., Zieve, M.E.: Low-degree planar monomials in characteristic two (2013). arXiv:1305.6597v1 [math.NT]
22. Nechaev, A.A.: Kerdock code in a cyclic form. Discrete Math. Appl. **1**, 365–384 (1991). Originally published in Russian in Diskret. Mat. **1**, 123–139 (1989)
23. Nyberg, K., Knudsen, L.R.: Provable security against differential cryptanalysis. In: Advances in Cryptology—CRYPTO '92, Santa Barbara, CA, 1992. Lecture Notes in Comput. Sci., vol. 740, pp. 566–574. Springer, Berlin (1993)
24. Pott, A.: Finite Geometry and Character Theory. Lecture Notes in Mathematics, vol. 1601. Springer, Berlin (1995)
25. Scherr, Z., Zieve, M.E.: Planar monomials in characteristic 2 (2013) arXiv:1302.1244v1 [math.CO]
26. Zhou, Y.: $(2^n, 2^n, 2^n, 1)$-relative difference sets and their representations. J. Combin. Des. **21**, 563–584 (2013)
27. Zieve, M.E.: Planar functions and perfect nonlinear monomials over finite fields (2013). arXiv:1301.5004v1 [math.CO]