EXCEPTIONAL PLANAR POLYNOMIALS

FLORIAN CAULLERY, KAI-UWE SCHMIDT, AND YUE ZHOU

Abstract. Planar functions are special functions from a finite field to itself that give rise to finite projective planes and other combinatorial objects. We consider polynomials over a finite field K that induce planar functions on infinitely many extensions of K; we call such polynomials exceptional planar. Exceptional planar monomials have been recently classified. In this paper we establish a partial classification of exceptional planar polynomials. This includes results for the classical planar functions on finite fields of odd characteristic and for the recently proposed planar functions on finite fields of characteristic two.

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 a *planar function* (sometimes the synonym *perfect nonlinear function* is used) 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 [6], relative difference sets [8], error-correcting codes [2], and S-boxes in block ciphers [16].

If q is even, a function $f : \mathbb{F}_q \to \mathbb{F}_q$ cannot satisfy the above definition of planar functions. 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. However, there is no apparent link between APN functions and projective planes. Recently, Zhou [19] 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 a *planar function* 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 [19] and Schmidt and Zhou [18], such planar functions have similar properties and applications as their counterparts in odd characteristic.

It is well known that every function from $\mathbb{F}_{q^r}$ to itself is induced by a polynomial over $\mathbb{F}_{q^r}$. In this paper, we study polynomials $f \in \mathbb{F}_q[X]$ that induce planar functions on $\mathbb{F}_{q^r}$ for infinitely many r; a polynomial f satisfying this

Date: 14 February 2014 (revised 16 October 2014).

2010 *Mathematics Subject Classification.* Primary: 11T06; Secondary: 51E20, 11T71.

Key words and phrases. Planar function, exceptional, absolutely irreducible polynomial

property will be called an *exceptional planar polynomial*. Exceptional planar monomials have been completely classified by Leducq [13] and Zieve [20] in odd characteristic and by Müller and Zieve [15] in characteristic two. The aim of this paper is to establish a partial classification of exceptional planar polynomials.

We first discuss the case that q is odd, say $q = p^n$, where p is an odd prime. Two polynomials $f, g \in \mathbb{F}_q[X]$ are *extended affine equivalent* (EA-equivalent) if

$$g(X) = A_1(f(A_2(X))) + A_3(X)$$

for some polynomials $A_1, A_2, A_3 \in \mathbb{F}_q[X]$ with the property that every non-constant term has degree a power of p and such that A_1 and A_2 induce permutations on $\mathbb{F}_q$. This equivalence preserves planarity for finite fields of odd characteristic (see [11] for a discussion on equivalences preserving planarity). Up to EA-equivalence, the only known examples of exceptional planar polynomials on finite fields of odd characteristic are:

$$f(X) = X^{p^k+1} \text{ for some nonnegative integer } k; \tag{2}$$

$$f(X) = X^{(3^k+1)/2} \text{ for some odd positive integer } k, \text{ where } p = 3; \tag{3}$$

$$f(X) = X^{10} - uX^6 - u^2X^2 \text{ for } u \in \mathbb{F}_{3^n} \text{ and odd } n, \text{ where } p = 3. \tag{4}$$

The polynomial (2) is planar on $\mathbb{F}_{p^r}$ for odd $r/\gcd(k, r)$ [4], the polynomial (3) is planar on $\mathbb{F}_{3^r}$ for $\gcd(k, r) = 1$ [4], and the polynomial (4) is planar on $\mathbb{F}_{3^{rn}}$ for odd r [7] (see also [4] for the case $u = -1$). Of course, this prompts the question as to whether these polynomials form the complete list of exceptional planar polynomials.

Indeed, as shown in two papers by Leducq [13] and Zieve [20] (see also [10] for partial prior results), up to EA-equivalence, the polynomials (2) and (3) are the only exceptional planar monomials.

Theorem A (Leducq [13], Zieve [20])**.** *Let p be an odd prime and let $f \in \mathbb{F}_{p^n}[X]$ be a monic monomial of degree d with $p \nmid d$. If f is exceptional planar, then either* (2) *or* (3) *holds.*

A partial classification of exceptional planar polynomials was obtained by Zieve [21].

Theorem B (Zieve [21])**.** *Let p be an odd prime and let $f \in \mathbb{F}_{p^n}[X]$ be of degree d. If f is exceptional planar and $d \not\equiv 0, 1 \pmod p$, then up to EA-equivalence, either $f(X) = X^2$ or* (3) *holds.*

Theorem B allows us to restrict ourselves to polynomials over $\mathbb{F}_{p^n}$ whose degrees are congruent to 0 or 1 modulo p. We prove the following result for the case that the degree is congruent to 1 modulo p.

Theorem 1. *Let $f \in \mathbb{F}_{p^n}[X]$ be monic of degree d. If f is exceptional planar and $d \equiv 1 \pmod p$, then $f(X) = X^{p^k+1} + h(X)$ for some positive integer k, where the degree e of h satisfies $e < p^k + 1$ and either $p \mid e$ or $p \mid e - 1$.*

We remark that, except for the trivial case $e = 1$, no example is known for which $p \mid e - 1$ occurs in Theorem 1. A nontrivial example for which $p \mid e$ occurs in Theorem 1 is (4).

We now turn to finite fields of characteristic two, in which case the only known examples of exceptional planar polynomials are the polynomials in which the degree of every nonconstant term is a power of two (it is trivial to check that such polynomials are exceptional planar). This again leads to the question as to whether there are other exceptional planar polynomials.

Indeed, Müller and Zieve [15] established the following classification of exceptional planar monomials.

Theorem C (Müller and Zieve [15])**.** *Let $f \in \mathbb{F}_{2^n}[X]$ be a monomial of degree d. If f is exceptional planar, then d is a power of 2.*

The case that d is odd in Theorem C was obtained previously by Schmidt and Zhou [18] using different techniques.

We prove the following partial classification of exceptional planar polynomials.

Theorem 2. *Let $f \in \mathbb{F}_{2^n}[X]$ be of degree d. If f is exceptional planar, then either $d \in \{1, 2\}$ or $4 \mid d$.*

To prove our main results, we use an approach that has been used to classify polynomials in $\mathbb{F}_{2^n}[X]$ that induce APN functions on infinitely many extensions of $\mathbb{F}_{2^n}$ [17], [1], [5], [3], which in turn relies on the complete classification of monomials having this property [9].

Let $f \in \mathbb{F}_q[X]$ and define the polynomial $F(X, Y, W)$ to be

$$\frac{f(X + W) - f(X) - f(Y + W) + f(Y)}{(X - Y)W} \tag{5}$$

when q is odd, and

$$\frac{f(X + W) + f(X) + WX + f(Y + W) + f(Y) + WY}{(X + Y)W} \tag{6}$$

when q is even. It is a direct consequence of the definition of planar functions that, if f induces a planar function on $\mathbb{F}_{q^r}$, then all $\mathbb{F}_{q^r}$-rational zeros of F satisfy $X = Y$ or $W = 0$. The strategy is to show that F has an absolutely irreducible factor over $\mathbb{F}_q$, since then, for all sufficiently large r, the polynomial F has many $\mathbb{F}_{q^r}$-rational zeros by the Lang-Weil bound [12], so that f cannot be planar on $\mathbb{F}_{q^r}$. To do so, we use the key idea of [1] and intersect the projective surface defined by F with a hyperplane and then apply the following result (in which $\overline{\mathbb{F}}_q$ denotes the algebraic closure of $\mathbb{F}_q$).

Lemma 3 (Aubry, McGuire, Rodier [1, Lemma 2.1])**.** *Let F and P be projective surfaces in $\mathbb{P}^3(\overline{\mathbb{F}}_q)$ defined over $\mathbb{F}_q$. If $F \cap P$ has a reduced absolutely irreducible component defined over $\mathbb{F}_q$, then F has an absolutely irreducible component defined over $\mathbb{F}_q$.*

We emphasise that the proof of Theorem 1 relies on intermediate results used to prove Theorem A, whereas the proof of Theorem 2 is self-contained, except for the use of the Lang-Weil bound [12] and Lemma 3.

2. The odd characteristic case

In this section we prove Theorem 1. Let q be an odd prime power, let $f \in \mathbb{F}_q[X]$, and let $F(X,Y,W)$ be the polynomial defined by (5). It will be more convenient to consider the polynomial $F(X,Y,Z-X)$, namely

$$G(X,Y,Z) = \frac{f(X)-f(Y)-f(Z)+f(-X+Y+Z)}{(X-Y)(X-Z)}. \tag{7}$$

Then f induces a planar function on $\mathbb{F}_{q^r}$ if and only if all $\mathbb{F}_{q^r}$-rational zeros of G satisfy $X=Y$ or $X=Z$.

Lemma 4. *Let q be an odd prime power, let $f \in \mathbb{F}_q[X]$ be a polynomial such that f' is nonconstant, and let G be defined by (7). If G has an absolutely irreducible factor over $\mathbb{F}_q$, then f is not exceptional planar.*

Proof. Suppose that G has an absolutely irreducible factor over $\mathbb{F}_q$. Then, by the Lang-Weil bound [12] for the number of rational points in varieties over finite fields, the number of $\mathbb{F}_{q^r}$-rational zeros of G is $q^{2r}+O(q^{3r/2})$, where the implicit constant depends only on the degree of G. We claim that G is not divisible by $X-Y$ or $X-Z$. Then $G(X,X,Z)$ and $G(X,Y,X)$ are nonzero polynomials, which have at most $q^r \deg(G)$ zeros in $\mathbb{F}_{q^r}$ (see [14, Theorem 6.13], for example). Hence, for all sufficiently large r, the polynomial G has $\mathbb{F}_{q^r}$-rational zeros that do not satisfy $X=Y$ or $X=Z$, and so f does not induce a planar function on $\mathbb{F}_{q^r}$.

It remains to prove the above claim. By symmetry, it is enough to show that G is not divisible by $X-Y$. Suppose for a contradiction that G is divisible by $X-Y$. Then the partial derivative of the numerator of (7) with respect to Y, namely $f'(-X+Y+Z)-f'(Y)$, must be divisible by $X-Y$. This forces f' to be a constant polynomial, a contradiction. □

Our main result for finite fields of odd characteristic, Theorem 1, will follow from Propositions 5 and 7, to be stated and proved below. Before we proceed, we introduce some notation that will be used throughout the remainder of this section. Let d be the degree $f \in \mathbb{F}_q[X]$. Write $f(X) = \sum_{j=0}^{d} a_j X^j$, where $a_d \neq 0$. Defining

$$\phi_j(X,Y,Z) = \frac{X^j - Y^j - Z^j + (-X+Y+Z)^j}{(X-Y)(X-Z)}, \tag{8}$$

we have

$$G(X,Y,Z) = \sum_{j=2}^{d} a_j \phi_j(X,Y,Z). \tag{9}$$

since $\phi_0 = \phi_1 = 0$. We shall also work with the homogeneous polynomial

$$\widetilde{G}(X, Y, Z, T) = \sum_{j=2}^{d} a_j \phi_j(X, Y, Z)\, T^{d-j}.$$

Proposition 5. *Let p be an odd prime and let $f \in \mathbb{F}_{p^n}[X]$ be of degree d. If f is exceptional planar and $d \equiv 1 \pmod{p}$, then $d = p^k + 1$ for some positive integer k.*

To prove Proposition 5, we require the following lemma.

Lemma 6. *Let p be an odd prime and let $f \in \mathbb{F}_{p^n}[X]$ be of degree d. If f is exceptional planar and $p \nmid d$, then d is even.*

Proof. Suppose for a contradiction that f is exceptional planar and $p \nmid d$ and d is odd. By the definition of a planar function, the degree of f must be at least 2, so that f' is not constant. The intersection of the projective surface defined by $\widetilde{G}$ with the hyperplane $T = 0$ is defined by the polynomial

$$\widetilde{G}(X, Y, Z, 0) = a_d \phi_d(X, Y, Z).$$

Since d is odd, $Y + Z$ divides ϕ_d. By taking the partial derivative of $X^d - Y^d - Z^d + (-X + Y + Z)^d$ with respect to Y, we see that $(Y + Z)^2$ does not divide ϕ_d. Therefore $Y + Z$ is a reduced absolutely irreducible component of ϕ_d and hence, by Lemma 3, $\widetilde{G}$ (and so also G itself) has an absolutely irreducible factor over $\mathbb{F}_{p^n}$. Therefore, by Lemma 4, the polynomial f is not exceptional planar, a contradiction. □

We now prove Proposition 5.

Proof of Proposition 5. Suppose that f is exceptional planar and $d \equiv 1 \pmod{p}$. We show that this is impossible unless d is of the form $p^k + 1$.

If $d = p^i(p^i - 1) + 1$ for some nonnegative integer i, then d is odd and f is not exceptional planar by Lemma 6, so assume that d is not of this form. In particular, f' is not constant. The intersection of the projective surface defined by $\widetilde{G}$ with the hyperplane $T = 0$ is defined by the polynomial

$$\widetilde{G}(X, Y, Z, 0) = \phi_d(X, Y, Z).$$

Since $d \equiv 1 \pmod{p}$ and d is not of the form $p^k(p^k - 1) + 1$, the polynomial

$$\phi_d(U + W, U, V + W) = \frac{(U + W)^d - U^d - (V + W)^d + V^d}{(U - V)W}$$

has an absolutely irreducible factor of $\mathbb{F}_p$ provided that d is not of the form $p^k + 1$, as shown by Leducq [13]. Furthermore, Leducq [13] showed that the number of singular points of $\phi_d(U+W, U, V+W)$ is finite. Hence the variety defined by ϕ_d and all of its partial derivatives has dimension 0, which implies that ϕ_d has no multiple component. Therefore ϕ_d has a reduced absolutely irreducible factor over $\mathbb{F}_p$ and so, by Lemmas 3 and 4, the polynomial f is not exceptional planar, a contradiction. □

Proposition 7. *Let p be an odd prime and let $f \in \mathbb{F}_{p^n}[X]$ be of the form $f(X) = X^{p^k+1} + h(X)$ for some positive integer k, where the degree e of h satisfies $e < p^k + 1$. If f is exceptional planar, then either $p \mid e$ or $p \mid e - 1$.*

In order to prove Proposition 7, we prove two lemmas on the polynomials ϕ_j, defined by (8).

Lemma 8. *Let p be a prime and let $\phi_j \in \mathbb{F}_p[X, Y, Z]$ be defined by* (8).

(i) We have

$$\phi_j(X, X, Z) = j\,\frac{X^{j-1} - Z^{j-1}}{X - Z}.$$

(ii) If $p \nmid j$ and $p \nmid j - 1$, then $\phi_j(X, X, Z)$ is not divisible $X - Z$ and $\phi_j(X, X, Z)$ and $\phi_{p^k+1}(X, X, Z)$ are coprime for every integral $k \geq 0$.

Proof. We may write

$$\begin{aligned}(X - Z)\phi_j(X, Y, Z) &= \frac{X^j - Y^j}{X - Y} - \frac{(-X + Y + Z)^j - Z^j}{(-X + Y + Z) - Z} \\ &= \sum_{i=0}^{j-1} X^i\, Y^{j-i-1} - \sum_{i=0}^{j-1} (-X + Y + Z)^i\, Z^{j-i-1},\end{aligned}$$

from which (i) follows. If $p \nmid j$, then $\phi_j(X, X, Z)$ is not the zero polynomial. If, in addition, $p \nmid j - 1$, then $\phi_j(X, X, Z)$ splits into linear factors different from $X - Z$. From (i) we have $\phi_{p^k+1}(X, X, Z) = (p^k + 1)(X - Z)^{p^k-1}$. Hence, if $p \nmid j$ and $p \nmid j - 1$, then $\phi_j(X, X, Z)$ and $\phi_{p^k+1}(X, X, Z)$ are coprime. This proves (ii). □

Lemma 9. *Let p be a prime and let $\phi_j \in \mathbb{F}_p[X, Y, Z]$ be defined by* (8). *Then ϕ_{p^k+1} is square-free for every integral $k \geq 0$.*

Proof. Write

$$\psi(X, Y, Z) = X^{p^k+1} - Y^{p^k+1} - Z^{p^k+1} + (-X + Y + Z)^{p^k+1}.$$

Then ϕ_{p^k+1} divides ψ. We show that ψ is square-free, for which it is sufficient to show that all of the following conditions are satisfied:

- $\gcd(\psi, \partial\psi/\partial Y) \in \mathbb{F}_p[X, Z]$,
- $\gcd(\psi, \partial\psi/\partial Z) \in \mathbb{F}_p[X, Y]$,
- $X \nmid \psi$.

These conditions are readily verified. □

We now prove Proposition 7, using an approach already used by Aubry, McGuire, an Rodier [1].

Proof of Proposition 7. Suppose that f is exceptional planar. Then G, defined in (7), is not absolutely irreducible by Lemma 4. Suppose further that $p \nmid e$ and $p \nmid e - 1$. We show that this leads to a contradiction.

We may write

$$G(X, Y, Z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0), \tag{10}$$

where P_i and Q_i are zero or homogeneous polynomials of degree i, defined over the algebraic closure of $\mathbb{F}_{p^n}$, and P_sQ_t is nonzero. Since G is not absolutely irreducible, we may also assume that $s, t > 0$. Write

$$f(X) = \sum_{j=0}^{p^k+1} a_j X^j,$$

where $a_{p^k+1} = 1$ and recall from (9) that

$$G(X,Y,Z) = \sum_{j=2}^{p^k+1} a_j \phi_j(X,Y,Z), \tag{11}$$

where the ϕ_j's are defined in (8). Notice that the degree of ϕ_j is $j-2$ and thus, since $a_{p^k+1} = 1$, the degree of G is $p^k - 1$. Hence $s+t = p^k - 1$ by (10). From (10) and (11) we find that

$$P_sQ_t = \phi_{p^k+1}. \tag{12}$$

Therefore, by Lemma 9, P_s and Q_t are coprime. From (10) and (11) we also find that

$$P_sQ_{t-1} + P_{s-1}Q_t = a_{p^k}\phi_{p^k} = 0$$

since $\phi_{p^k} = 0$. Hence P_s divides $P_{s-1}Q_t$ and so P_s divides P_{s-1}, which by a degree argument implies that $P_{s-1} = 0$. Likewise, we see that $Q_{t-1} = 0$. Now, by the assumed form of f, we have

$$a_j = 0 \quad \text{for each } j \in \{p^k, p^k - 1, \ldots, e+1\}. \tag{13}$$

Since $P_{s-1} = Q_{t-1} = 0$, we have from (10) and (11)

$$P_sQ_{t-2} + P_{s-2}Q_t = a_{p^k-1}\phi_{p^k-1}.$$

If $p^k - 1 \geq e+1$, the right hand side equals zero by (13) and, by an argument similar to that used above, we conclude that $P_{s-2} = Q_{t-2} = 0$. We can continue in this way to show that

$$P_{t-1} = \cdots = P_{e-t-1} = Q_{s-1} = \cdots = Q_{e-s-1} = 0.$$

Hence, by invoking (10) and (11) again, we have

$$P_sQ_{e-s-2} + P_{e-t-2}Q_t = a_e\phi_e. \tag{14}$$

If $Q_{e-s-2} = 0$, then Q_t divides ϕ_e and also ϕ_{p^k+1} by (12). This contradicts Lemma 8 (ii). Likewise, we get a contradiction if $P_{e-t-2} = 0$. Hence we may assume that P_{e-t-2} and Q_{e-s-2} are both nonzero. From (12) and Lemma 8 (i) we find that

$$P_s(X,X,Z)Q_t(X,X,Z) = \phi_{p^k+1}(X,X,Z) = (X-Z)^{p^k-1}. \tag{15}$$

Hence $X - Z$ divides $P_s(X,X,Z)$ and $Q_t(X,X,Z)$ and thus $X - Z$ also divides $\phi_e(X,X,Z)$ by (14). From (15) we then see that $\phi_e(X,X,Z)$ and $\phi_{p^k+1}(X,X,Z)$ share the factor $X - Z$, which contradicts Lemma 8 (ii). $\square$

3. The even characteristic case

In this section we prove Theorem 2. Let q be a power of 2, let $f \in \mathbb{F}_q[X]$, and let $F(X,Y,W)$ be the polynomial defined by (6). We consider the polynomial $F(X,Y,Z+X)$, namely

$$H(X,Y,Z) = \frac{f(X)+f(Y)+f(Z)+f(X+Y+Z)}{(X+Y)(X+Z)} + 1. \tag{16}$$

Then f induces a planar function on $\mathbb{F}_{q^r}$ if and only if all $\mathbb{F}_{q^r}$-rational zeros of H satisfy $X=Y$ or $X=Z$.

The following lemma is our counterpart of Lemma 4 in even characteristic.

Lemma 10. *Let q be a power of 2, let $f \in \mathbb{F}_q[X]$, and let H be defined by (16). If H has an absolutely irreducible factor over $\mathbb{F}_q$, then f is not exceptional planar.*

Proof. Suppose that H has an absolutely irreducible factor over $\mathbb{F}_q$. Then, as in the proof of Lemma 4, the number of $\mathbb{F}_{q^r}$-rational zeros of H is $q^{2r} + O(q^{3r/2})$. We show below that H is not divisible by $X+Y$ or $X+Z$, which implies that, for all sufficiently large r, the polynomial H has $\mathbb{F}_{q^r}$-rational zeros that do not satisfy $X=Y$ or $X=Z$, and so f does not induce a planar function on $\mathbb{F}_{q^r}$.

By symmetry, it is enough to show that H is not divisible by $X+Y$. Suppose for a contradiction that H is divisible by $X+Y$. Then the partial derivative of $(X+Y)(X+Z)H(X,Y,Z)$ with respect to Y, namely

$$f'(Y) + f'(X+Y+Z) + X + Z,$$

must be divisible by $X+Y$. This forces $f'(X) = X + c$ for some $c \in \mathbb{F}_q$, which is absurd since q is even. □

We now prove Theorem 2.

Proof of Theorem 2. Write $f(X) = \sum_{j=0}^{d} a_j X^j$, where $a_d \neq 0$. Defining

$$\phi_j(X,Y,Z) = \frac{X^j + Y^j + Z^j + (X+Y+Z)^j}{(X+Y)(X+Z)},$$

the polynomial H, defined in (16), can be written as

$$H(X,Y,Z) = 1 + \sum_{j=3}^{d} a_j \phi_j(X,Y,Z)$$

since $\phi_0 = \phi_1 = \phi_2 = 0$. Consider the homogeneous polynomial

$$\widetilde{H}(X,Y,Z,T) = T^{d-2} + \sum_{j=3}^{d} a_j \phi_j(X,Y,Z)\, T^{d-j}.$$

The intersection of the projective surface defined by $\widetilde{H}$ with the hyperplane $T=0$ is defined by the polynomial

$$\widetilde{H}(X,Y,Z,0) = a_d \phi_d(X,Y,Z).$$

Now suppose for a contradiction that f is exceptional planar and $4 \nmid d$, but $d \notin \{1, 2\}$. We show that ϕ_d has a reduced absolutely irreducible component, which by Lemmas 3 and 10 implies that f is not exceptional planar, a contradiction.

First suppose that d is odd and $d \neq 1$. Then $Y + Z$ divides ϕ_d. By taking the partial derivative of $X^d + Y^d + Z^d + (X + Y + Z)^d$ with respect to Y, we see that $(Y + Z)^2$ does not divide ϕ_d. Therefore $Y + Z$ is a reduced absolutely irreducible component of ϕ_d, as required.

Now suppose that $d \equiv 2 \pmod 4$ and $d \neq 2$. Write $d = 2e$, so that e is odd and $e \neq 1$. It is readily verified that

$$\phi_d = \phi_e^2 \cdot (X + Y)(X + Z).$$

Hence $X + Y$ divides ϕ_d. By taking the partial derivative of $X^e + Y^e + Z^e + (X + Y + Z)^e$ with respect to Y, we find that $X + Y$ does not divide ϕ_e and so $(X + Y)^2$ does not divide ϕ_d. Hence $X + Y$ is a reduced absolutely irreducible component of ϕ_d, as required. □

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] 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.

[3] F. Caullery, *A new large class of functions not APN infinitely often*, Des. Codes Cryptogr. **73** (2014), 601–614.

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

[5] M. Delgado and H. Janwa, *On the conjecture on APN functions*, arXiv:1207.5528v1 [math.IT].

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

[7] C. Ding and J. Yuan, *A family of skew Hadamard difference sets*, J. Combin. Theory Ser. A **113** (2006), 1526–1535.

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

[9] 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.

[10] F. Hernando, G. McGuire, and F. Monserrat, *On the classification of exceptional planar functions over $\mathbb{F}_p$*, arXiv:1301.4016v1 [math.AG] (to appear in Geom. Dedicata).

[11] G. M. Kyureghyan and A. Pott, *Some theorems on planar mappings*, Arithmetic of finite fields, Lecture Notes in Comput. Sci., vol. 5130, Springer, Berlin, 2008, pp. 117–122.

[12] S. Lang and A. Weil, *Number of points of varieties in finite fields*, Amer. J. Math. **76** (1954), 819–827.

[13] E. Leducq, *Functions which are PN on infinitely many extensions of $\mathbb{F}_p$, p odd*, arXiv:1006.2610v2 [math.NT] (to appear in Des. Codes Cryptogr.).

[14] R. Lidl and H. Niederreiter, *Finite fields*, second ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997.

[15] P. Müller and M. E. Zieve, *Low-degree planar monomials in characteristic two*, arXiv:1305.6597v1 [math.NT].

[16] 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.
[17] 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.
[18] K.-U. Schmidt and Y. Zhou, *Planar functions over fields of characteristic two*, J. Algebraic Combin. **40** (2014), 503–526.
[19] Y. Zhou, $(2^n, 2^n, 2^n, 1)$*-relative difference sets and their representations*, J. Combin. Des. **21** (2013), 563–584.
[20] M. E. Zieve, *Planar functions and perfect nonlinear monomials over finite fields*, arXiv:1301.5004v1 [math.CO] (to appear in Des. Codes Cryptogr.).
[21] ———, *Planar polynomials over finite fields*, 2013, preprint.

Institut de Mathématiques de Luminy, CNRS-UPR9016, 163 av. de Luminy, case 907, 13288 Marseille Cedex 9, France.
E-mail address, F. Caullery: florian.caullery@etu.univ-amu.fr

Faculty of Mathematics, Otto-von-Guericke University, Universitätsplatz 2, 39106 Magdeburg, Germany
E-mail address, K.-U. Schmidt: kaiuwe.schmidt@ovgu.de

Faculty of Mathematics, Otto-von-Guericke University, Universitätsplatz 2, 39106 Magdeburg, Germany
Current address: Department of Mathematics and System Sciences, College of Science, National University of Defense Technology, Changsha, China
E-mail address: yue.zhou.ovgu@gmail.com