Journal of Algebra ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Algebra

journal homepage: www.elsevier.com/locate/jalgebra

# Polynomials with maximal differential uniformity and the exceptional APN conjecture

Yves Aubry [a,b,*], Ali Issa [a], Fabien Herbaut [c,a]

[a] *Institut de Mathématiques de Toulon - IMATH, Université de Toulon, France*
[b] *Institut de Mathématiques de Marseille - I2M, Aix-Marseille Université, UMR 7373 CNRS, France*
[c] *INSPE Nice-Toulon, Université Côte d'Azur, France*

ARTICLE INFO

*Article history:*
Received 26 July 2022
Available online xxxx
Communicated by Emmanuel Thomé

*Keywords:*
Differential uniformity
Exceptional APN functions
Chebotarev theorem

ABSTRACT

We contribute to the exceptional APN conjecture by showing that no polynomial of degree $m = 2^r(2^\ell+1)$ where $\gcd(r, \ell) \leqslant 2$, $r \geqslant 2$, $\ell \geqslant 1$ with a nonzero second leading coefficient can be APN over infinitely many extensions of the base field. More precisely, we prove that for $n$ sufficiently large, all polynomials of $\mathbb{F}_{2^n}[x]$ of such a degree with a nonzero second leading coefficient have a differential uniformity equal to $m - 2$.

## 1. Introduction

### 1.1. Statement of results

The notion of differential uniformity is introduced by Nyberg in [18] to measure the resistance of mappings between finite Abelian groups against differential cryptanalysis.

This work is partially supported by the French Agence Nationale de la Recherche through the SWAP project under Contract ANR-21-CE39-0012.

* Corresponding author.
*E-mail addresses:* yves.aubry@univ-tln.fr (Y. Aubry), ali.issa@univ-tln.fr (A. Issa), fabien.herbaut@univ-cotedazur.fr (F. Herbaut).

https://doi.org/10.1016/j.jalgebra.2023.07.017
0021-8693/© 2023 Elsevier Inc. All rights reserved.

In the context of a finite field $\mathbb{F}_q$ one defines the differential uniformity of a polynomial $f \in \mathbb{F}_q[x]$ as the maximum number of solutions of the set of equations $f(x+\alpha)-f(x)=\beta$ where $\alpha$ and $\beta$ belong to $\mathbb{F}_q$ with $\alpha$ nonzero:

$$\delta_{\mathbb{F}_q}(f) := \max_{(\alpha,\beta)\in\mathbb{F}_q^*\times\mathbb{F}_q} \sharp\{x \in \mathbb{F}_q \mid f(x+\alpha)-f(x)=\beta\}.$$

Particular emphasis is being placed on the even characteristic case and this is the framework that we will consider here. The differential uniformity is then obviously even and its smallest value is 2. Polynomials $f \in \mathbb{F}_{2^n}[x]$ such that $\delta_{\mathbb{F}_{2^n}}(f) = 2$ are highly relevant in cryptography and are called APN polynomials (for Almost Perfect Nonlinear).

APN polynomials which are APN over infinitely many extensions of the base field have also attracted some attention and they are called exceptional APN. Dillon has conjectured in [12] that the only monomials among them have degrees $2^k+1$ and $2^{2k}-2^k+1$ (which are called Gold and Kasami-Welch exponents respectively). The conjecture has been resolved by Hernando and McGuire in [14].

Thereafter, the first author of the present paper together with McGuire and Rodier have conjectured in [3] that up to the CCZ equivalence (an equivalence relation introduced by Carlet, Charpin and Zinoviev in [7] and discussed in [6]), these monomials are the only exceptional APN *polynomials*. This statement is now referred to as the Aubry-McGuire-Rodier conjecture. In this direction, they have established that if the degree of a polynomial $f$ is odd, but neither a Gold nor a Kasami-Welch exponent, then $f$ is not an exceptional APN polynomial. From there some authors have focused on the study of polynomials of degree Gold or Kasami-Welch (see [9] for a survey by Delgado and [10,11] for recent results by Delgado, Janwa and Agrinsoni).

Few is known about the even degree case. The first author, McGuire and Rodier have proved in [3] that if $f$ is a polynomial of degree $2e$ with $e$ odd and if $f$ contains a term of odd degree, then $f$ is not exceptional APN. Moreover, Bartoli and Schmidt have stated in Proposition 1.4 in [4] that if a polynomial of even degree $m$ is exceptional APN, then $m \equiv 0 \pmod 4$.

A case where $f$ has degree $4e$ with $e \equiv 3 \pmod 4$ and satisfies a specific condition has been studied by Rodier in [20]. Caullery has handled in [8] the case where $f$ has degree $4e$ with $e > 3$ such that $\varphi_e$ is absolutely irreducible, where

$$\varphi_e(x,y,z) := \frac{x^e+y^e+z^e+(x+y+z)^e}{(x+y)(x+z)(y+z)}.$$

Results on the absolute irreducibility of the polynomials $\varphi_e$ are for example compiled in [15]. As pointed out in the proof of Lemma 2.2 in [3], the polynomial $\varphi_e$ is not absolutely irreducible when $e$ is even, so the case of polynomials of degree $m \equiv 0 \pmod 8$ is still open. Moreover, the polynomial $\varphi_e$ is not absolutely irreducible if $e$ is a Gold exponent, as shown by Janwa and Wilson in Theorem 4 in [16], so the case of degree $4e$ with $e$ a Gold exponent is also still open.

Rather, one can ask how large the differential uniformity can be. Unless $f$ is an additive polynomial plus a constant, the maximal value that the differential uniformity of a polynomial $f$ of degree $m$ can reach is the degree of the derivative $f(x+\alpha)-f(x)$ which is bounded by $m-1$ if $m$ is odd and by $m-2$ otherwise. Consequently we will say that a polynomial has a maximal differential uniformity if this bound is reached.

A density result has first been established in this direction in [23] where Voloch has proved that *most* polynomials of degree $m$ congruent to 0 or 3 modulo 4 achieve this maximal differential uniformity. One can also find a generalization to the second-order differential uniformity in [1].

Moreover, Voloch and the two first authors provide in Theorems 5.3 and 5.5 in [2] explicit infinite families of odd integers $m$ such that *all* polynomials of degree $m$ (and not just *most of them*) have a maximal differential uniformity for $n$ large enough.

The main purpose of this paper is to extend these results to infinitely many explicit even degrees.

**Theorem.** *(Theorem 4.1) Let $m = 2^r(2^\ell+1)$ where $\gcd(r,\ell) \leqslant 2$, $r \geqslant 2$ and $\ell \geqslant 1$. For $n$ sufficiently large, all polynomials $f = \sum_{k=0}^{m} a_{m-k}x^k \in \mathbb{F}_{2^n}[x]$ of degree $m$ such that $a_1 \neq 0$ have maximal differential uniformity, that is $\delta_{\mathbb{F}_{2^n}}(f) = m-2$.*

*In particular, polynomials $f = \sum_{k=0}^{m} a_{m-k}x^k \in \overline{\mathbb{F}}_2[x]$ of such a degree and such that $a_1 \neq 0$ are not exceptional APN.*

This gives contributions to the exceptional APN conjecture for the two open cases mentioned above. Indeed it almost solves the case of the degrees $m = 4e$ where $e$ is a Gold exponent and it is a first step for the degrees $m \equiv 0 \pmod 8$.

Note that point *(i)* of Theorem 2 in [23] reveals that the condition $a_1 \neq 0$ in the previous theorem is necessary to get the maximality of $\delta_{\mathbb{F}_{2^n}}(f)$.

It is worth stressing that the methods used until now to prove that polynomials are not exceptional APN have rested on algebraic geometric tools. The point was to apply Weil-type bounds for the number of rational points on varieties defined over finite fields. In contrast, our approach comes from algebraic number theory. The point here is to apply the Chebotarev density theorem for functions fields introduced in this context by Voloch in [23].

### 1.2. Context and method of proof

Before entering into details in the next section, we provide here comprehensive lines of our approach which involves the Chebotarev density theorem, monodromy groups and Morse polynomials. We first present the main notions in function fields theory which are involved in our work (one can refer to [21] for further details).

Let $K$ be a function field in one variable over $\mathbb{F}_q$, i.e. $K/\mathbb{F}_q(t)$ is a finite algebraic extension where $t$ is a transcendental element over $\mathbb{F}_q$. The algebraic closure of $\mathbb{F}_q$ in $K$

is a finite extension of $\mathbb{F}_q$, denoted by $\mathbb{F}_q^K$, and called the constant field of $K$. Suppose that $L$ is a finite algebraic extension of $K$ and consider $\mathcal{E}$ the algebraic closure of $\mathbb{F}_q^K$ in $L$. We will denote by $\mathcal{E}K$ the compositum of the fields $\mathcal{E}$ and $K$. Recall that if $L = \mathcal{E}K$ then we say that $L$ is a constant field extension of $K$ and if $\mathcal{E} = \mathbb{F}_q^K$ we say that $L$ is a geometric extension of $K$.

Suppose now that the extension $L/K$ is Galois. For every prime $\mathfrak{P}$ of $L$ unramified over $K$ one can associate an automorphism $(\mathfrak{P}, L/K)$ of $\mathrm{Gal}(L/K)$ called the Frobenius automorphism attached to $\mathfrak{P}$ for the extension $L/K$. One can show that if $P$ is a prime of $K$, unramified in $L$, then the set of automorphisms $\{(\mathfrak{P}, L/K) \mid \mathfrak{P} \text{ above P}\}$ fills out a conjugacy class $\left(\frac{L/K}{P}\right)$ in $\mathrm{Gal}(L/K)$ called the Artin symbol attached to $P$. Moreover, if $g(x)$ is a polynomial in $\mathbb{F}_q[x]$, its arithmetic (respectively geometric) monodromy group is defined as the Galois group of the splitting field $F$ of $g(x) - t$ over $\mathbb{F}_q(t)$ (respectively over $\mathbb{F}_q^F(t)$). Hence the extension $F/\mathbb{F}_q(t)$ will be geometric if and only if these two monodromy groups are equal. We are now able to state the following explicit version of the Chebotarev density theorem for first degree primes given by Pollack in [19].

**Theorem 1.1.** *(**Chebotarev**) Suppose that $\Omega$ is a finite Galois extension of $\mathbb{F}_q(t)$. Let $\mathcal{C}$ be a conjugacy class of $\mathrm{Gal}(\Omega/\mathbb{F}_q(t))$ every element of which restricts down to the qth power map on $\mathbb{F}_q^\Omega$. Let $V(\mathcal{C})$ be the number of first degree primes $P$ of $\mathbb{F}_q(t)$ unramified in $\Omega$ such that the Artin symbol $\left(\frac{\Omega/\mathbb{F}_q(t)}{P}\right)$ equals $\mathcal{C}$. Then*

$$\left| V(\mathcal{C}) - \frac{\sharp\mathcal{C}}{[\Omega : \mathbb{F}_q^\Omega(t)]} q \right| \leqslant 2 \frac{\sharp\mathcal{C}}{[\Omega : \mathbb{F}_q^\Omega(t)]} \left( g q^{1/2} + g + [\Omega : \mathbb{F}_q^\Omega(t)] \right)$$

*where $g$ denotes the genus of $\Omega/\mathbb{F}_q^\Omega$.*

It is worth noticing that $P$ splits in the Galois extension if and only if its Artin symbol reduces to the identity automorphism. So, if one is interested in an estimation of the number of primes which totally split in a Galois extension of function fields, one will focus on geometric extensions.

In the whole paper we will consider a polynomial $f$ of $\mathbb{F}_q[x]$ where $q = 2^n$ and we will denote by $\overline{\mathbb{F}}_2$ an algebraic closure of $\mathbb{F}_2$. For any $\alpha \in \mathbb{F}_q^*$ the derivative of $f$ with respect to $\alpha$ will be denoted by $D_\alpha f(x) := f(x + \alpha) + f(x)$.

We will see in Section 4 that the Chebotarev density theorem ensures that if the geometric and arithmetic monodromy groups of $D_\alpha f$ are equal then for $n$ sufficiently large there exists $\beta \in \mathbb{F}_{2^n}$ such that the number of solutions of the equation $D_\alpha f(x) = \beta$ is equal to the degree of $D_\alpha f$.

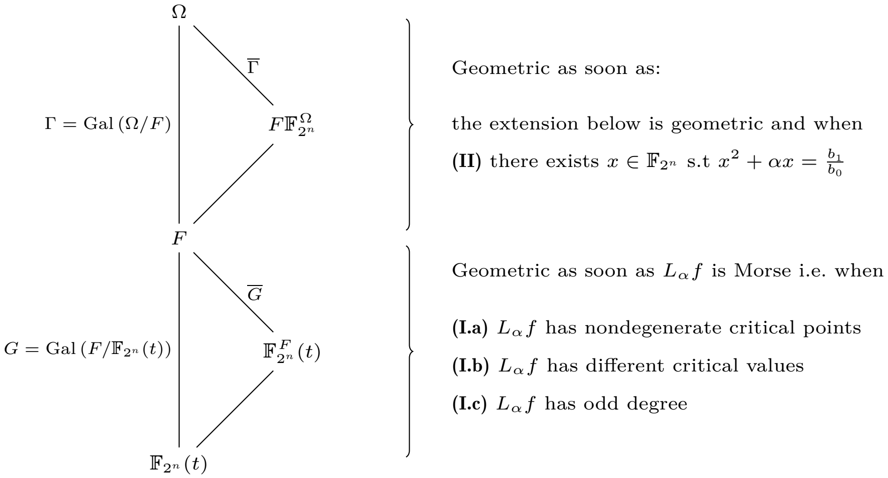
Nevertheless, how can we compare the monodromy groups of $D_\alpha f$? Denote by $\Omega$ the splitting field of the polynomial $D_\alpha f(x) - t$ over the field $\mathbb{F}_q(t)$. The method developed in [23] consists in introducing an intermediate field $F$ between $\Omega$ and $\mathbb{F}_q(t)$, namely the splitting field of the polynomial $L_\alpha f(x) - t$ over the field $\mathbb{F}_q(t)$, where $L_\alpha f$ is the unique polynomial such that $L_\alpha f\left(x(x+\alpha)\right) = D_\alpha f(x)$ (see Proposition 2.3 of [2] for the existence and the unicity of such a polynomial $L_\alpha f$).

The cornerstone of the results obtained in [23] is that for almost all $f$ of a given degree, the associated polynomial $L_\alpha f$ is Morse. Also, it is proven in [2] that for some specific degrees $m$, for any polynomial $f$ of degree $m$ there exists $\alpha$ such that $L_\alpha f$ is Morse. Recall that a polynomial $g \in \mathbb{F}_{2^n}[x]$ is said to be Morse (see the Appendix of Geyer in [17]) if the critical points of $g$ are nondegenerate (i.e. the derivative $g'$ and the second Hasse-Schmidt derivative $g^{[2]}$ have no common roots), if the critical values of $g$ are distinct (different zeros of $g'$ give different values of $g$) and if the degree of $g$ is prime to the characteristic.

The reason we are interested in Morse polynomials comes from the more general form of the Hilbert theorem given by Serre in Theorem 4.4.5 of [22] (and outlined in even characteristic in the Appendix of Geyer in [17]) which asserts that the geometric monodromy group of a Morse polynomial is the full symmetric group.

It remains to identify when the polynomial $g := L_\alpha f$ is Morse. First, the resultant between $g'$ and $g^{[2]}$ is a classical tool to recognize polynomials $g$ with nondegenerate critical points. The main difficulty rests in studying polynomials with distinct critical values. To this end, we make use of the algebraic characterization of such polynomials obtained by Geyer in the same appendix. Last, the parity condition on the degree of $g$ explains the common hypothesis of the results of this paper: when $f$ has an even degree, the polynomial $L_\alpha f$ will have odd degree as soon as the degree of $f$ is divisible by 4 and its second leading coefficient is nonzero.

In order to explain how to get a geometric extension $\Omega/F$, let us write $L_\alpha f = \sum_{k=0}^{d} b_{d-k}x^k$. Proposition 4.6 in [2] states that if $L_\alpha f$ is Morse and if $x^2 + \alpha x = b_1/b_0$ has a solution in $\mathbb{F}_q$ then the extension $\Omega/F$ is geometric. As we know simple expressions


$\Omega$
$\overline{\Gamma}$
$\Gamma = \mathrm{Gal}\,(\Omega/F)$
$F\mathbb{F}_{2^n}^{\Omega}$
$F$
$\overline{G}$
$G = \mathrm{Gal}\,(F/\mathbb{F}_{2^n}(t))$
$\mathbb{F}_{2^n}^{F}(t)$
$\mathbb{F}_{2^n}(t)$

Geometric as soon as:

the extension below is geometric and when

**(II)** there exists $x \in \mathbb{F}_{2^n}$ s.t $x^2 + \alpha x = \frac{b_1}{b_0}$

Geometric as soon as $L_\alpha f$ is Morse i.e. when

**(I.a)** $L_\alpha f$ has nondegenerate critical points

**(I.b)** $L_\alpha f$ has different critical values

**(I.c)** $L_\alpha f$ has odd degree

**Fig. 1.** Galois extensions of function fields and their intermediate constant field extensions.

Please cite this article in press as: Y. Aubry et al., Polynomials with maximal differential uniformity and the exceptional APN conjecture, J. Algebra (2023), https://doi.org/10.1016/j.jalgebra.2023.07.017

of $b_1$ and $b_0$ in terms of the coefficients of $f$ and $\alpha$, Hilbert's Theorem 90 enables us to translate the problem into a polynomial equation.

The diagram in Fig. 1 sums up the different conditions we intend to verify to prove that the extensions are geometric.

As explained in the figure, condition (I.c) will involve a congruence condition on the degree $m$ of $f$, and the non-vanishing of the second leading coefficient of $f$. Conditions (I.a), (I.b) and (II) will translate into algebraic equations. For the specific degrees mentioned in the introduction, we will manage to bound the number of $\alpha$ for which at least one of the conditions fails.

## 2. Polynomials of degree multiple of 4

Before we focus in the rest of the paper on polynomials of degrees $m = 2^r(2^\ell + 1)$ with $r \geqslant 2$, we collect in this section some general results which hold for any degree $m$ congruent to 0 modulo 4.

### *2.1. A unique polynomial $L_\alpha f$ such that $(L_\alpha f)(x(x+\alpha)) = D_\alpha f(x)$*

The following proposition is a particular case of Proposition 2.1, Proposition 2.3 and Lemma 2.5 in [2] whose proofs rest on linear algebra. We consider the polynomial ring $\mathbb{F}_2[a_0, \dots, a_m, \alpha]$ with indeterminates $a_0, \dots, a_m, \alpha$. This ring is endowed with the (weighted) degree $w$ such that $w(a_j) = j$ and $w(\alpha) = 1$. It means that the monomial $a_0^{d_0} a_1^{d_1} \dots a_m^{d_m} \alpha^{d_\alpha}$ has degree $d_1 + 2d_2 + \cdots + md_m + d_\alpha$.

**Proposition 2.1.** *Let $m$ be an integer such that $m \equiv 0 \pmod 4$ and $f = \sum_{k=0}^{m} a_{m-k}x^k \in \mathbb{F}_q[x]$ a polynomial of degree $m$. Consider $\alpha \in \mathbb{F}_q^*$. There exists a unique polynomial $L_\alpha f := \sum_{k=0}^{d} b_{d-k}x^k$ in $\mathbb{F}_q[x]$ of degree less or equal to $d := (m-2)/2$ such that*

$$(L_\alpha f)(x(x+\alpha)) = D_\alpha f(x).$$

*Moreover*

*(i)* *the application $L_\alpha$ is linear,*

*(ii)* *$L_\alpha f$ has degree $d$ if and only if $a_1 \neq 0$,*

$$\textit{(iii)} \begin{cases} b_0 = a_1\alpha & \\ b_1 = a_2\alpha^2 + a_3\alpha & \textit{if } m \equiv 0 \pmod 8 \quad \textit{or} \\ b_1 = a_0\alpha^4 + a_1\alpha^3 + a_2\alpha^2 + a_3\alpha & \textit{if } m \equiv 4 \pmod 8 \end{cases}$$

*(iv)* *when seen as an element of $\mathbb{F}_2[a_0, \dots, a_m, \alpha]$ the coefficient $b_i$ is an homogeneous polynomial of degree $2i+2$ when considering the weight $w$ such that $w(a_j) = j$ and $w(\alpha) = 1$.*

**Remark 2.2.** In order to fullfil condition (I.c) we want the polynomial $L_\alpha f$ to have odd degree. But $d = (m-2)/2$ is odd when $m \equiv 0 \pmod 4$, so a sufficient condition is to take a nonzero $b_0$ i.e. $a_1 \neq 0$.

**Remark 2.3.** The point of view where $L_\alpha f$ is thought as an element of $\mathbb{F}_2[a_0, \ldots, a_m, \alpha]$ will often be adopted in the following. The proof of the existence of a unique $L_\alpha f \in \mathbb{F}_2[a_0, \ldots, a_m, \alpha]$ such that $(L_\alpha f)(x(x+\alpha)) = D_\alpha f(x)$ rests on the same arguments: the equation reduces to a unit triangular system.

### *2.2. The trace condition*

Recall that condition (II) involves the existence of a solution of the equation $x^2 + \alpha x = b_1/b_0$ in $\mathbb{F}_{2^n}$. By Hilbert's Theorem 90 this is equivalent to say that $\operatorname{Tr}\left(\frac{b_1}{b_0\alpha^2}\right) = 0$ where Tr stands for the trace from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$.

**Proposition 2.4.** *Let $f = \sum_{k=0}^{m} a_{m-k}x^k \in \mathbb{F}_{2^n}[x]$ be a polynomial of degree $m$ such that $a_1 \neq 0$.*

*(i) If $m \equiv 0 \pmod 8$ then the number of $\alpha \in \mathbb{F}_{2^n}^*$ such that $\operatorname{Tr}\left(\frac{b_1}{b_0\alpha^2}\right) = 0$ is $2^{n-1} - 1$ if $a_2^2 + a_1a_3 \neq 0$ and $2^n - 1$ otherwise.*

*(ii) If $m \equiv 4 \pmod 8$ then the number of $\alpha \in \mathbb{F}_{2^n}^*$ such that $\operatorname{Tr}\left(\frac{b_1}{b_0\alpha^2}\right) = 0$ is equal to $2^{n-1}$ or $2^{n-1} - 1$ if $a_2^2 + a_1a_3 = 0$, and greater or equal to $\frac{1}{2}(2^n - 2^{n/2+1} - 1)$ otherwise.*

**Proof.** The situation is simpler when $m \equiv 0 \pmod 8$. We have by Proposition 2.1 that $\frac{b_1}{b_0} = \frac{a_2\alpha + a_3}{a_1}$ so $\operatorname{Tr}\left(\frac{b_1}{b_0\alpha^2}\right) = \operatorname{Tr}\left(\frac{a_2^2 + a_1a_3}{a_1^2\alpha^2}\right)$. We notice that if $a_2^2 + a_1a_3 \neq 0$ then the map $\alpha \mapsto \frac{a_2^2 + a_1a_3}{a_1^2\alpha^2}$ is a permutation of $\mathbb{F}_{2^n}^*$.

In the case where $m \equiv 4 \pmod 8$, we find that $\operatorname{Tr}\left(\frac{b_1}{b_0\alpha^2}\right) = 0$ if and only if $\operatorname{Tr}\left(\frac{a_2^2 + a_1a_3}{a_1^2\alpha^2} + \frac{a_0\alpha}{a_1}\right) = n$. If $a_2^2 + a_3a_1 = 0$ then there exist $2^{n-1}$ or $2^{n-1} - 1$ nonzero elements $\alpha$ such that $\operatorname{Tr}\left(\frac{a_0}{a_1}\alpha\right) = n$, depending on the parity of $n$. Otherwise, let us set $C = a_0/a_1$ and $D^2 = \frac{a_2^2 + a_1a_3}{a_1^2}$, so we are reduced to study the equation $\operatorname{Tr}(C\alpha) + \operatorname{Tr}(D/\alpha) = n$. Then if we set $K^2 = CD$ and $v = a_0\alpha/a_1K$, we obtain $\operatorname{Tr}(Kv) + \operatorname{Tr}(K/v) = n$. Choosing $S$ with $\operatorname{Tr}(S) = n$ we can rewrite the last condition as the existence of $w$ such that $Kv + K/v = S + w^2 + w$ and multiplying through by $v^2$ and setting $y = vw$ turns the equation into $K(v^3 + v) + Sv^2 = y^2 + vy$, which defines an elliptic curve $E$ (as $K \neq 0$) whose projective closure is smooth with one point at infinity. Let us set $q = 2^n$. By the Hasse-Weil bound, the number of rational points over $\mathbb{F}_q$ on $E$ is at least $q - 2\sqrt{q}$. Moreover, for any $v$ in $\mathbb{F}_q^*$ there are at most 2 elements

$(v, w)$ on $E$. Therefore, there are at least $\frac{1}{2}(q - 2\sqrt{q} - 1)$ suitable nonzero $v$ and thus as many $\alpha$ which enables us to conclude the proof. □

### *2.3. Nondegenerate critical points*

In this subsection we want to bound for a given polynomial $f$ the number of $\alpha$ such that $L_\alpha f$ has degenerate critical points, that is those which do not satisfy condition (I.a).

**Proposition 2.5.** *Let $m$ be an integer such that $m \equiv 0 \pmod 4$ and let $f = \sum_{k=0}^{m} a_{m-k}x^k \in \mathbb{F}_{2^n}[x]$ be a polynomial of degree $m$ such that $a_1 \neq 0$. The critical points of $L_\alpha f$ are nondegenerate except for at most $(m-1)(m-4)$ values of $\alpha \in \overline{\mathbb{F}}_2$.*

**Proof.** Recall that the second Hasse-Schmidt derivative $(D_\alpha f)^{[2]}$ of the polynomial $D_\alpha f$ is defined by

$$D_\alpha f(t+u) \equiv D_\alpha f(t) + (D_\alpha f)'(t)u + (D_\alpha f)^{[2]}(t)u^2 \pmod{u^3}$$

and that Lemma 3.3 of [2] states that the critical points of $L_\alpha f$ are nondegenerate if and only if $(D_\alpha f)'$ and $(D_\alpha f)^{[2]}$ have no common roots in $\overline{\mathbb{F}}_2$.

We note $h = f - a_0x^m$. The assumption on $m$ implies that $(x^m)'$ and $(x^m)^{[2]} = \binom{m}{2}x^{m-2}$ both vanish. Thus we use the linearity of $D_\alpha$ and of the derivative operators to get $(D_\alpha f)' = (D_\alpha h)'$ and $(D_\alpha f)^{[2]} = (D_\alpha h)^{[2]}$ and so the equality between the two resultants $\mathrm{Res}((D_\alpha f)', (D_\alpha f)^{[2]}) = \mathrm{Res}((D_\alpha h)', (D_\alpha h)^{[2]})$. As $a_1 \neq 0$, we are reduced to the case where the degree of $h$ is congruent to 3 modulo 4. This case is treated in Lemma 3.4 in [2] which states that $\mathrm{Res}((D_\alpha h)', (D_\alpha h)^{[2]})$ is a polynomial of degree $(m-1)(m-4)$ in $\alpha$ with at most $(m-1)(m-4)$ roots in $\overline{\mathbb{F}}_2$. □

### *2.4. Distinct critical values*

In this section we will bound the number of $\alpha \in \mathbb{F}_{2^n}^*$ such that the condition (I.b) is not satisfied. The aim of the two following statements is to study the case of $L_\alpha(x^{m-1})$ when $m \equiv 0 \pmod 4$.

**Lemma 2.6.** *We consider an integer $m \geqslant 8$ such that $m \equiv 0 \pmod 4$ and $d = (m-2)/2$. For all $f = \sum_{k=0}^{m} a_{m-k}x^k \in \mathbb{F}_{2^n}[x]$ of degree $m$ such that $a_1 \neq 0$ the following conditions are equivalent:*

*(i) $(L_\alpha f)'$ has $\frac{d-1}{2}$ distinct (double) roots in $\overline{\mathbb{F}}_2$.*
*(ii) $(D_\alpha f)'$ has $d-1$ distinct (double) roots in $\overline{\mathbb{F}}_2$.*

**Proof.** Let us first assume that $\tau_1, \tau_2, \ldots, \tau_{(d-1)/2}$ are $\frac{d-1}{2}$ distinct roots of $(L_\alpha f)'$. We have that

$$(D_\alpha f)' = (L_\alpha f \circ T_\alpha)' = \alpha (L_\alpha f)' \circ T_\alpha \tag{1}$$

where $T_\alpha(x) := x(x+\alpha)$. So if we choose $z_i \in \overline{\mathbb{F}}_2$ such that $T_\alpha(z_i) = T_\alpha(z_i+\alpha) = \tau_i$ the elements $z_1, z_1+\alpha, z_2, z_2+\alpha, \dots, z_{\frac{d-1}{2}}, z_{\frac{d-1}{2}}+\alpha$ are $d-1$ distinct roots of $(D_\alpha f)'$.

Conversely, $z$ is a root of $(D_\alpha f)' = \alpha(L_\alpha f)' \circ T_\alpha$ if and only if $z+\alpha$ is. So $d-1$ distinct roots of $(D_\alpha f)'$ can always be written as $z_1, z_1+\alpha, z_2, z_2+\alpha, \dots, z_{\frac{d-1}{2}}, z_{\frac{d-1}{2}}+\alpha$. Now set $\tau_i := T_\alpha(z_i) = T_\alpha(z_i+\alpha)$ to get $\frac{d-1}{2}$ distinct roots of $(L_\alpha f)'$. □

**Lemma 2.7.** *We consider an integer $m \geqslant 8$ such that $m \equiv 0 \pmod 4$ and the monomial $f(x) = x^{m-1}$. For any $\alpha \in \mathbb{F}_{2^n}^*$ the polynomial $(L_\alpha f)'$ has $(d-1)/2$ distinct double roots in $\overline{\mathbb{F}}_2$, namely the $\tau_1, \dots, \tau_{(d-1)/2}$ defined by*

$$\tau_i = \frac{\alpha^2}{1+\theta_i} + \frac{\alpha^2}{1+\theta_i^2}$$

*where $\theta_1, \dots, \theta_{(d-1)/2}$ are $(d-1)/2$ different $d$-th roots of the unity in $\overline{\mathbb{F}}_2 \setminus \{1\}$ such that $\theta_i\theta_j \neq 1$ for $i \neq j$.*

**Proof.** We fix $\alpha \in \mathbb{F}_{2^n}^*$. By the previous lemma, it is sufficient to determine the roots of $(D_\alpha f)'$, that is the solutions of the equation $x^{m-2} + (x+\alpha)^{m-2} = 0$. As these solutions are obviously different from 0, it amounts to studying the solutions $\theta$ of $\left(\frac{x+\alpha}{x}\right)^{m/2-1} = 1$. For $\theta = 1$ there is no corresponding solution $x$, but for any other $(m/2-1)$-th root of the unity $\theta$ there is one and only one solution $x = \frac{\alpha}{1+\theta}$. To conclude that $(L_\alpha f)'$ has $m/4-1$ (that is $(d-1)/2$) distinct roots of the claimed form, we use the equality (1) and the fact that for $x = \frac{\alpha}{1+\theta}$ and $x' = \frac{\alpha}{1+\theta'}$, we have $T_\alpha(x) = T_\alpha(x')$ if and only if $\theta\theta' = 1$. □

Following the Appendix of Geyer in [17] we associate to any polynomial $g = \sum_{k=0}^{d} b_{d-k}x^k \in \mathbb{F}_q[x]$ of degree $d$ a nonzero rational function $\Pi \in \mathbb{F}_2[b_0, \dots, b_d][1/b_0]$ whose zeros correspond exactly to the polynomials with non-distinct critical values (note that in [17] $\Pi$ is actually a polynomial in $\mathbb{F}_2[b_0, \dots, b_d]$ as the value of $b_0$ is taken to be 1). We will use the notation $\Pi_d$ to stress the dependance on the degree. Recall that $\Pi_d$ is defined as follows in [17]

$$\Pi_d(g) := \prod_{i \neq j} (g(\tau_i) - g(\tau_j)) \tag{2}$$

where the $\tau_i$ are the (double) roots of $g'$. In the following lemma, which is an adaptation of Lemma 3.8 in [2] to handle the case when $m \equiv 0 \pmod 4$, we prove that for a well chosen value of $N$ the rational function $b_0^N \Pi_d(L_\alpha f)$ becomes a polynomial in $\mathbb{F}_2[a_0, \dots, a_m, \alpha]$ with useful homogeneity properties.

**Lemma 2.8.** *Let $m \geqslant 8$ be an integer such that $m \equiv 0 \pmod 4$. We consider a degree $m$ polynomial $f = \sum_{k=0}^{m} a_{m-k}x^k$ such that $a_1 \neq 0$ and the associated polynomial $L_\alpha f =$*

*$\sum_{k=0}^{d} b_{d-k}x^k$. If we set $d=(m-2)/2$ and $e=\binom{(d-1)/2}{2}$ then $b_0^{de}\Pi_d(L_\alpha f)$ is a polynomial in $\mathbb{F}_2[a_0,\dots,a_m,\alpha]$ each of whose terms contains a product of $(d+2)e$ terms $a_i$. This polynomial is homogeneous of degree $(6d+4)e$ when considering the weight $w$ such that $w(\alpha)=1$ and $w(a_i)=i$.*

**Proof.** Mutatis mutandis, the proof can be read off from Lemma 3.8 in [2]. □

## 3. Polynomials of degree $2^r(2^\ell+1)$

Our strategy is now to prove that $b_0^{de}\Pi_d(L_\alpha f)$ has a simple leading coefficient when seen as a polynomial in $\alpha$ and when $f$ has degree $2^r(2^\ell+1)$. First, the following proposition gives an handy interpretation which involves the trace polynomials $P_k$ defined by

$$P_k(x) := x + x^2 + \cdots + x^{2^{k-1}}$$

for any integer $k \geqslant 1$.

**Proposition 3.1.** *Let $r \geqslant 2$ and $\ell \geqslant 1$. We set $m=2^r(2^\ell+1)$, $d=\frac{m-2}{2}$ and $e=\binom{(d-1)/2}{2}$. We consider a polynomial $f(x)=\sum_{k=0}^{m} a_{m-k}x^k$ of degree $m$ such that $a_1 \neq 0$ and the associated polynomial $L_\alpha f=\sum_{k=0}^{d} b_{d-k}x^k$ as above.*

*Recall that we use the notation $\Pi_d(g)$ for the rational function defined in (2) which describes the locus of polynomials $g$ with non-distinct critical values. Thus*

- *(i) the indeterminate $a_0$ appears in the polynomial $b_0^{de}\Pi_d(L_\alpha f)$ with a power at most $2e$.*
- *(ii) When seen as an element of $\mathbb{F}_2[a_0,\dots,a_m][\alpha]$ the polynomial $b_0^{de}\Pi_d(L_\alpha f)$ has degree at most $(5d+4)e$. Moreover, the only monomial of such a degree that can appear in $b_0^{de}\Pi_d(L_\alpha f)$ is $a_0^{2e}a_1^{de}\alpha^{(5d+4)e}$.*
- *(iii) When seen as an element of $\mathbb{F}_2[a_0,\dots,a_m][\alpha]$ the polynomial $b_0^{de}\Pi_d(L_\alpha f)$ has degree exactly $(5d+4)e$ if and only if for any choice of different roots $\tau_i$ and $\tau_j$ of $L_1(x^{m-1})'$ we have $P_\ell(\tau_i+\tau_j)\neq 0$ where $P_\ell$ is the $\ell$-th trace polynomial.*

**Proof.** We are first looking for the coefficient $a_0$ in the polynomial

$$b_0^{de}\Pi_d(L_\alpha f) = (a_1\alpha)^{de}\prod_{i<j}\left(\sum_{k=0}^{d} b_{d-k}^2(\tau_i^{2k}+\tau_j^{2k})\right). \tag{3}$$

Our point of departure is that when $m$ admits the special form $m=2^r(2^\ell+1)$ then $L_\alpha(x^m)$ has the following very simple expression

$$L_\alpha(x^m) = \alpha^m + \sum_{k=0}^{\ell-1}\alpha^{m-2^{r+k+1}}x^{2^{r+k}}. \tag{4}$$

It can be proved easily by checking that the composition of the right hand side with $x(x+\alpha)$ is actually $x^m + (x+\alpha)^m$.

Then the linearity of $L_\alpha$ yields that when $f = a_0 x^m + \cdots$ the indeterminate $a_0$ appears in few coefficients $b_i$ of $L_\alpha f$, namely in $b_d, b_{d-2^r}, b_{d-2^{r+1}}, \ldots, b_{d-2^{r+\ell-1}}$.

Actually $b_d$ does not contribute in the product (3) since the terms $\tau_i^{2k} + \tau_j^{2k}$ simplify for $k = 0$ in the sum between parentheses. Also, the terms $\tau_i$ do not give rise to the indeterminate $a_0$. Indeed, any monomial in the $b_i$ in (3) will be multiplied by a polynomial $Q$ in the variables $\tau_1^2, \ldots, \tau_{(d-1)/2}^2$ and this polynomial is invariant under the action of the symmetric group $\mathfrak{S}_{(d-1)/2}$. But

$$\left(L_\alpha f\right)'(x) = b_0 x^{d-1} + b_2 x^{d-3} + \cdots + b_{d-3}x^2 + b_{d-1} = b_0(x^2+\tau_1^2)\cdots(x^2+\tau_{(d-1)/2}^2)$$

thus $Q$ belongs to $\mathbb{F}_2[\frac{b_2}{b_0}, \frac{b_4}{b_0}, \ldots, \frac{b_{d-1}}{b_0}]$. Again, the indeterminate $a_0$ does not appear in $Q$ as $d-2^r, d-2^{r+1}, \ldots, d-2^{r+\ell-1}$ are odd.

So to investigate where the largest power of $a_0$ appears in (3) we are reduced to study

$$(a_1\alpha)^{de} \prod_{i<j} \left( b_{d-2^r}^2 (\tau_i+\tau_j)^{2^r} + b_{d-2^{r+1}}^2 (\tau_i+\tau_j)^{2^{r+1}} + \cdots + b_{d-2^{r+l}}^2 (\tau_i+\tau_j)^{2^{r+\ell-1}} \right). \quad (5)$$

This largest power is bounded by $2\binom{(d-1)/2}{2} = 2e$ and point $(i)$ is proven.

To prove point *(ii)*, consider a monomial $a_0^{u_0} a_1^{u_1} \ldots a_m^{u_m} \alpha^v$ arising in $b_0^{de}\Pi_d(L_\alpha f)$. Recall that by Lemma 2.8 we count $2e + de$ indeterminates $a_i$ and we have $u_1 + 2u_2 + \cdots + mu_m + v = (6d+4)e$. As we have just proved that $u_0 \leqslant 2e$, it implies that either $u_0 = 2e$, $u_1 = de$, $u_2 = u_3 = \cdots = 0$ and $v = (5d+4)e$, or in any other case $v < (5d+4)e$.

To treat point $(iii)$, let us now determine when the monomial $a_0^{2e} a_1^{de} \alpha^{(5d+4)e}$ does appear in $b_0^{de}\Pi_d(L_\alpha f)$. We use the expression of the coefficients $b_{d-2^{r+k}}$ obtained above to transform (5) into

$$a_0^{2e} \left[ a_1^{de} \alpha^{de} \prod_{i<j} \left( \sum_{k=0}^{\ell-1} (\alpha^{m-2^{r+k+1}})^2 (\tau_i+\tau_j)^{2^{r+k}} \right) \right].$$

We know that the expression between brackets is a polynomial in $\mathbb{F}_2[a_0, \ldots, a_m][\alpha]$ with no term $a_0$ and we wonder if the monomial $a_1^{de}\alpha^{(5d+4)e}$ does appear. To this end it is sufficient to evaluate it when $\alpha = 1$, $a_1 = 1$ and $a_2 = \cdots = a_m = 0$ that is to consider $\prod_{i<j} P_\ell^{2^r}(\tau_i + \tau_j)$ where the $\tau_i$ are the $(d-1)/2$ different roots of $L_1(x^{m-1})'$ which are described in Lemma (2.7). It concludes the proof. □

The Proposition 3.4 will exploit this interpretation. To make its proof more readable we now provide several lemmas, the first of them being an easy arithmetic result.

**Lemma 3.2.** *Let $r \geqslant 2$ and $\ell \geqslant 1$. We set $m = 2^r(2^\ell + 1)$ and $d = (m-2)/2$.*

*(i)* *If* $\gcd(r,\ell)=1$ *then* $\gcd(d,2^{2\ell}-1)=1$,

*(ii)* *If* $\gcd(r,\ell)=2$ *then* $\gcd(d,2^{2\ell}-1)=3$.

**Proof.** For example, start with the observation that if $t$ divides $2^{2\ell}-1$ then one can write $t=ab$ where $a$ and $b$ are divisors of $2^\ell-1$ and $2^\ell+1$. Thus work modulo $a$ and $b$ and study the order of 2 in the multiplicative group $(\mathbb{Z}/b\mathbb{Z})^\times$. □

We have compiled in the following lemma some basic computational results which will prove useful establishing Proposition 3.4.

**Lemma 3.3.** *Fix two integers* $r\geqslant 2$ *and* $\ell\geqslant 1$ *and set* $m=2^r(2^\ell+1)$. *We have*

*(i)* $L_1(x^{m-1})=x^{2^r-1}+\left(1+\sum_{k=r}^{r+\ell-1}x^{2^k}\right)\sum_{k=0}^{r-1}x^{2^k-1}$,

*(ii)* $x^2(L_1(x^{m-1}))'=P_r^2(x)+P_\ell^{2^r}(x)P_{r-1}^2(x)$.

*(iii)* *If* $\tau_i$ *is a root of* $L_1(x^{m-1})'$ *then* $P_{r-1}(\tau_i)\neq 0$.

*(iv)* *For any choice of different roots* $\tau_i$ *and* $\tau_j$ *of* $L_1(x^{m-1})'$ *such that* $P_\ell(\tau_i+\tau_j)=0$ *we have* $P_{r-1}(\tau_i+\tau_j)\neq 0$ *and*

$$P_\ell(\tau_i)^{2^{r-1}}=\frac{P_r(\tau_i)}{P_{r-1}(\tau_i)}=\frac{P_r(\tau_i+\tau_j)}{P_{r-1}(\tau_i+\tau_j)}=\frac{P_r(\tau_j)}{P_{r-1}(\tau_j)}=P_\ell(\tau_j)^{2^{r-1}}.$$

**Proof.** By definition of $L_1$ it is sufficient for the first point to compute the composition of the right hand side of the equality with the polynomial $x(x+1)$ and to find $D_1(x^{m-1})$, that is $(x+1)^{m-1}+x^{m-1}$.

Just differentiate the former equality and use the relation $P_{r-1}^2(x)+x^{2^r}=P_r^2(x)$ to get the second point.

If $P_{r-1}$ vanishes at a root $\tau_i$ of $L_1(x^{m-1})'$, point *(ii)* leads to $P_r(\tau_i)=0$. But the relation between $P_{r-1}$ and $P_r$ above implies that $\tau_i=0$, a contradiction with Lemma 2.7.

Under the hypotheses of the last item, point *(ii)* applies to get $P_r^2(\tau_i)+P_\ell^{2^r}(\tau_i)P_{r-1}^2(\tau_i)=0$ and thus $P_\ell(\tau_i)^{2^{r-1}}=\frac{P_r(\tau_i)}{P_{r-1}(\tau_i)}$, one of the claimed results. Now adding the equalities *(ii)* for $x=\tau_i,\tau_j$ and using $P_\ell(\tau_i)=P_\ell(\tau_j)$ lead to $P_r^2(\tau_i+\tau_j)+P_l^{2r}(\tau_i)P_{r-1}^2(\tau_i+\tau_j)=0$. Again, if $P_{r-1}(\tau_i+\tau_j)=0$ we obtain $P_r(\tau_i+\tau_j)=0$ and thus $\tau_i=\tau_j$, which is impossible. We have just proven that $P_{r-1}(\tau_i+\tau_j)$ is nonzero and so we can write $P_\ell(\tau_i)^{2^{r-1}}=\frac{P_r(\tau_i+\tau_j)}{P_{r-1}(\tau_i+\tau_j)}$. □

**Proposition 3.4.** *We fix* $r\geqslant 2$ *and* $\ell\geqslant 1$ *and we set* $m=2^r(2^\ell+1)$. *Recall that we denote by* $P_k$ *the* $k$*-th trace polynomial. Thus* $\gcd(r,\ell)\leqslant 2$ *if and only if for any choice of different roots* $\tau_i$ *and* $\tau_j$ *of* $L_1(x^{m-1})'$ *we have* $P_\ell(\tau_i+\tau_j)\neq 0$.

**Proof.** We set $m=2^r(2^\ell+1)$ with $r\geqslant 2$ and $\ell\geqslant 1$ such that $\gcd(r,\ell)\leqslant 2$. Let $\tau_i$ and $\tau_j$ be two different roots of $L_1(x^{m-1})'$ such that $P_\ell(\tau_i+\tau_j)=0$. A classical property of the trace polynomials implies that $\tau_i+\tau_j$ belongs to $\mathbb{F}_{2^\ell}$ and so does $\frac{P_r(\tau_i+\tau_j)}{P_{r-1}(\tau_i+\tau_j)}$. (Remember that by Lemma 3.3 $P_{r-1}(\tau_i+\tau_j)$ is nonzero.)

Please cite this article in press as: Y. Aubry et al., Polynomials with maximal differential uniformity and the exceptional APN conjecture, J. Algebra (2023), https://doi.org/10.1016/j.jalgebra.2023.07.017

By point *(iii)* of Lemma 3.3 again, we know that $P_\ell(\tau_i)^{2^r}$ lies in $\mathbb{F}_{2^\ell}$ and thus $P_\ell(\tau_i)$ too. Now we use the expression $\tau_i = \frac{1}{1+\theta_i} + \frac{1}{1+\theta_i^2}$ given by Lemma 2.7, where $\theta_i$ is a $d$-th root of the unity in $\overline{\mathbb{F}}_2 \setminus \{1\}$. Substituting into $P_\ell(\tau_i + \tau_i^{2^\ell}) = 0$ leads to a telescopic sum which simplifies into $\frac{1}{1+\theta_i} = \frac{1}{1+\theta_i^{2^{2\ell}}}$ and then gives $\theta_i^{2^{2\ell}-1} = 1$. Since $\theta_i^d = 1$ it follows that $\theta_i^{\gcd(2^{2\ell}-1,d)} = 1$.

If $\gcd(\ell, r) = 1$ then Lemma 3.2 gives $\gcd(2^{2\ell} - 1, d) = 1$, so $\theta_i = 1$, a contradiction.

We now turn to the case $\gcd(\ell, r) = 2$. This time Lemma 3.2 asserts $\gcd(2^{2\ell} - 1, d) = 3$. We deduce that $\theta_i \in \mathbb{F}_4$ and so $\tau_i \in \mathbb{F}_4$. As $\ell$ is even, we deduce that $\tau_i \in \mathbb{F}_{2^\ell}$ and in consequence, $P_\ell(\tau_i) \in \mathbb{F}_2$. One can show that $P_\ell(\tau_i) \neq 1$, otherwise point *(ii)* of Lemma 3.3 would imply $P_{r-1}(\tau_i) = P_r(\tau_i)$ and thus $\tau_i = 0$, a contradiction with the expression of $\tau_i$ given by Lemma 2.7. So $P_\ell(\tau_i) = 0$.

Now point *(iii)* of Lemma 3.3 also implies that $P_r(\tau_i) = 0$. But for any $u \in \mathbb{F}_4 \setminus \{0, 1\}$ and for any positive even integer $k$ we have $P_k(u) = 0$ if and only if 4 divides $k$, as $P_k(u) = \sum_{s=0}^{k/2-1} (u + u^2)^{2^{2s}}$. We know that $\tau_i \neq 0$ and when starting the proof with two different roots $\tau_i$ and $\tau_j$ of $L_1(x^{m-1})'$, we could have chosen $\tau_i \neq 1$. Consequently 4 divides $\ell$ and $r$, a contradiction.

Conversely, suppose that $a := \gcd(r, \ell) \geqslant 3$. Since $a$ divides $r$ and $\ell$ then $P_a$ divides $P_r$ and $P_\ell$ (just write $P_{ab} = \sum_{k=0}^{b-1} P_a^{2^{ka}}$). As $a \geqslant 3$ and $P_a$ is separable then there exist $\tau_i$ and $\tau_j$ two different nonzero roots of $P_a$ in $\overline{\mathbb{F}}_2$. From point *(ii)* of Lemma 3.3 we deduce that $\tau_i$ and $\tau_j$ are roots of $L_1(x^{m-1})'$. But by linearity we also have $P_\ell(\tau_i + \tau_j) = 0$ and we are done. □

We can now bring together these different ingredients to bound the number of $\alpha$ such that $L_\alpha f$ does not have distinct critical values, that is such that condition (I.b) fails.

**Theorem 3.5.** *Let $r \geqslant 2$ and $\ell \geqslant 1$. We set $m = 2^r(2^\ell + 1)$, $d = (m-2)/2$ and $e = \binom{(d-1)/2}{2}$. If $\gcd(r, \ell) = 1$ or $2$ then for any positive integer $n$, for any choice of the coefficients $a_i$ in $\mathbb{F}_{2^n}$ such that $a_0 \neq 0$ and $a_1 \neq 0$, the number of $\alpha \in \overline{\mathbb{F}}_2^*$ such that the polynomial $L_\alpha f$ associated to $f(x) = \sum_{k=0}^m a_{m-k} x^k$ has not distinct critical values is at most $(5d + 4)e$.*

**Proof.** Fix $r, \ell$ and then $m$ as in the statement of the theorem. We know by Lemma 2.7 that $L_1(x^{m-1})'$ has $(d-1)/2$ distinct roots $\tau_1, \tau_2, \dots$ in $\overline{\mathbb{F}}_2$ and that by Proposition 3.4 if $i \neq j$ then $P_\ell(\tau_i + \tau_j) \neq 0$. Now for $f(x) = \sum_{k=0}^m a_{m-k} x^k \in \mathbb{F}_2[a_0, \dots, a_m][x]$ Proposition 3.1 ensures that $b_0^{de} \Pi_d(L_\alpha f)$, seen as an element of $\mathbb{F}_2[a_0, \dots, a_m][\alpha]$, has degree exactly $(5d + 4)e$ and that its leading term is $a_0^{2d} a_1^{de} \alpha^{(5d+4)e}$.

Last, if we consider $n \geqslant 1$ and coefficients $a_i$ in $\mathbb{F}_{2^n}$ with $a_0, a_1 \neq 0$, it follows that $b_0^{de} \Pi_d(L_\alpha f)$ is a polynomial in $\mathbb{F}_{2^n}[\alpha]$ of degree $(5d + 4)e$ whose number of roots is bounded by its degree. □

Please cite this article in press as: Y. Aubry et al., Polynomials with maximal differential uniformity and the exceptional APN conjecture, J. Algebra (2023), https://doi.org/10.1016/j.jalgebra.2023.07.017

## 4. Proof of the main theorem

We are finally in a position to prove the main result of this paper.

**Theorem 4.1.** *Let $m = 2^r(2^\ell + 1)$ where $\gcd(r, \ell) \leqslant 2$ and $r \geqslant 2$, $\ell \geqslant 1$. For $n$ sufficiently large, for all polynomials $f = \sum_{k=0}^{m} a_{m-k}x^k \in \mathbb{F}_{2^n}[x]$ of degree $m$ such that $a_1 \neq 0$ the differential uniformity $\delta_{\mathbb{F}_{2^n}}(f)$ is maximal that is $\delta_{\mathbb{F}_{2^n}}(f) = m - 2$.*

*In particular, polynomials $f = \sum_{k=0}^{m} a_{m-k}x^k \in \overline{\mathbb{F}}_2[x]$ of such a degree and such that $a_1 \neq 0$ are not exceptional APN.*

**Proof.** Under the hypotheses of the theorem we set $m = 2^r(2^\ell + 1)$ and $d = (m - 2)/2$. Recall that, in order to apply the Chebotarev density theorem, our goal is to obtain a geometric extension $\Omega/\mathbb{F}_{2^n}(t)$ and that our strategy is to bound the number of $\alpha$ such that the different conditions sum up in Fig. 1 fail.

Consider an integer $N_1$ such that $n \geqslant N_1$ implies

$$\underbrace{\frac{1}{2}\left(2^n - 2^{n/2+1} - 1\right)}_{\substack{\text{Lower bound for the}\\ \text{number of } \alpha \text{ s. t.}\\ \text{condition (II) is satisfied}}} > \underbrace{(m-1)(m-4)}_{\substack{\text{Upper bound for the}\\ \text{number of } \alpha \text{ s. t.}\\ \text{condition (I.a) fails}}} + \underbrace{(5d+4)\binom{(d-1)/2}{2}}_{\substack{\text{Upper bound for the}\\ \text{number of } \alpha \text{ s. t.}\\ \text{condition (I.b) fails}}}. \tag{6}$$

Now fix an integer $n \geqslant N_1$ and $f = \sum_{k=0}^{m} a_{m-k}x^k \in \mathbb{F}_{2^n}[x]$ of degree $m$ such that $a_1 \neq 0$. By Proposition 2.1 the associated polynomial $L_\alpha f$ has odd degree $d$, so condition (I.c) is satisfied. Recall that we have proved in Proposition 2.4 that there are at least $\frac{1}{2}\left(2^n - 2^{n/2+1} - 1\right)$ values of $\alpha \in \mathbb{F}_{2^n}$ such that condition (II) is satisfied. Moreover, by Propositions 2.5 and 3.1 we know that $(m-1)(m-4)$ and $(5d+4)\binom{(d-1)/2}{2}$ respectively bound the number of $\alpha$ such that conditions (I.a) and (I.b) fail. So one can choose $\alpha \in \mathbb{F}_{2^n}^*$ such that conditions (I.a), (I.b) and (II) are satisfied.

For such a choice of $\alpha$ the polynomial $L_\alpha f$ has nondegenerate critical points, distinct critical values, an odd degree, and so is Morse. Thus Proposition 4.2 in the Appendix of Geyer in [17] (which is a form in even characteristic of the Hilbert theorem) applies and gives $G = \overline{G} = \mathfrak{S}_d$ and consequently the extension $F/\mathbb{F}_{2^n}(t)$ is geometric that is with no constant field extension.

Furthermore, since there exists $x \in \mathbb{F}_{2^n}$ such that $x^2 + \alpha x = b_1/b_0$, Proposition 4.6 in [2] yields $\Gamma = \overline{\Gamma} = (\mathbb{Z}/2\mathbb{Z})^{d-1}$ and the second extension $\Omega/F$ is also geometric.

Moreover the extension $\Omega/\mathbb{F}_{2^n}(t)$ is separable since $L_\alpha f$ has odd degree and is obviously normal as a decomposition field, so we finally deduce that the extension $\Omega/\mathbb{F}_{2^n}(t)$ is a geometric Galois extension.

We are now in a position to apply the explicit Chebotarev density theorem (stated as Theorem 1.1 in this paper) to the geometric Galois extension $\Omega/\mathbb{F}_{2^n}(t)$. We denote by

Please cite this article in press as: Y. Aubry et al., Polynomials with maximal differential uniformity and the exceptional APN conjecture, J. Algebra (2023), https://doi.org/10.1016/j.jalgebra.2023.07.017

$V$ the number of places of degree 1 of $\mathbb{F}_{2^n}(t)$ which totally split in $\Omega$, by $d_\Omega$ the degree of $\Omega$ over $\mathbb{F}_{2^n}(t)$ and by $g_\Omega$ the genus of $\Omega$. We thus obtain the following lower bound

$$V \geqslant \frac{2^n}{d_\Omega} - \frac{2}{d_\Omega}\big(g_\Omega 2^{n/2} + g_\Omega + d_\Omega\big). \tag{7}$$

Since $G = \mathfrak{S}_d$ and $\Gamma = (\mathbb{Z}/2\mathbb{Z})^{d-1}$ we have $d_\Omega = d!2^{d-1}$. Furthermore $g_\Omega \leqslant \frac{1}{2}(\deg D_\alpha f - 3)d_\Omega + 1$ by Lemma 14 of [19] so $g_\Omega \leqslant d!2^{d-1}(d-3/2)+1$. We deduce the existence of an integer $N_2$ beyond which $V \geqslant 1$. Thus if $n$ also satisfies $n \geqslant N_2$ there exists $\beta \in \mathbb{F}_{2^n}$ such that $D_\alpha f(x) = \beta$ has $m-2$ distinct (simple) roots and $\delta_{\mathbb{F}_{2^n}}(f)$ is maximal.

As a straightforward consequence we have shown that polynomials of degree $m$ with coefficients in a finite extension of $\mathbb{F}_2$ with a nonzero second leading coefficient cannot be exceptional APN. □

**Remark 4.2.** Note that if $a_1 = 0$, by Proposition 2.1 the degree of $D_\alpha f$ drops below $m-2$ and thus $\delta_{\mathbb{F}_{2^n}}(f) < m-2$ for any integer $n$.

**Remark 4.3.** Let us make explicit the expression *for n sufficiently large* employed in Theorem 4.1. As a matter of example, consider the case of polynomials $f = a_0x^{12} + a_1x^{11} + \dots$ of degree $m = 12$ such that $a_1 \neq 0$. In this case $L_\alpha f$ has degree $d = 5$. Condition (6) leads to take $N_1 = 9$ whereas Condition (7) yields $N_2 = 28$. Thus, for $n \geqslant 28$ we have $\delta_{\mathbb{F}_{2^n}}(f) = 10$. As a corollary a polynomial of degree 12 with a nonzero second leading coefficient defined over a finite field of characteristic 2 cannot be exceptional APN.

**Remark 4.4.** It would be of interest to investigate other contexts where a similar approach could be fruitful. Within the scope of application one can suggest the study of multiplicative differential uniformities (see for instance [5] and [13]). The same method may also lead to results in the context of the odd characteristic.

## Data availability

No data was used for the research described in the article.

## Acknowledgments

The authors would like to thank José Felipe Voloch for the proof of Proposition 2.4.

## References

[1] Y. Aubry, F. Herbaut, Differential uniformity and second order derivatives for generic polynomials, J. Pure Appl. Algebra 222 (2018) 1095–1110, https://doi.org/10.1016/j.jpaa.2017.06.009.

[2] Y. Aubry, F. Herbaut, J.F. Voloch, Maximal differential uniformity polynomials, Acta Arith. 188 (2019) 345–366, https://doi.org/10.4064/aa170806-11-7.

[3] Y. Aubry, G. McGuire, F. Rodier, A few more functions that are not APN infinitely often, in: Finite Fields: Theory and Applications, in: Contemp. Math., vol. 518, Amer. Math. Soc., Providence, RI, 2010, pp. 23–31, https://doi.org/10.1090/conm/518/10193.

[4] D. Bartoli, K.U. Schmidt, Low-degree planar polynomials over finite fields of characteristic two, J. Algebra 535 (2019) 541–555, https://doi.org/10.1016/j.jalgebra.2019.06.026.

[5] N. Borisov, M. Chew, R. Johnson, D. Wagner, Multiplicative differentials, in: Fast Software Encryption: 9th International Workshop, in: Lecture Notes in Computer Science, vol. 2365, Springer, 2002, pp. 17–33, https://doi.org/10.1007/3-540-45661-9_2.

[6] L. Budaghyan, C. Carlet, A. Pott, New classes of almost bent and almost perfect nonlinear polynomials, IEEE Trans. Inf. Theory 52 (2006) 1141–1152, https://doi.org/10.1109/TIT.2005.864481.

[7] C. Carlet, P. Charpin, V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, Des. Codes Cryptogr. 15 (1998) 125–156, https://doi.org/10.1023/A:1008344232130.

[8] F. Caullery, A new large class of functions not APN infinitely often, Des. Codes Cryptogr. 73 (2014) 601–614, https://doi.org/10.1007/s10623-014-9956-2.

[9] M. Delgado, The state of the art on the conjecture of exceptional APN functions, Note Mat. 37 (2017) 41–51, https://doi.org/10.1285/i15900932v37n1p41.

[10] M. Delgado, H. Janwa, Some new results on the conjecture on exceptional APN functions and absolutely irreducible polynomials: the Gold case, Adv. Math. Commun. 11 (2017) 389–396, https://doi.org/10.3934/amc.2017033.

[11] M. Delgado, H. Janwa, C. Agrinsoni, Some new techniques and progress towards the resolution of the conjecture of exceptional APN functions and absolutely irreducibility of a class of polynomials, Des. Codes Cryptogr. 91 (2023) 2481–2495, https://doi.org/10.1007/s10623-023-01202-y.

[12] J.F. Dillon, Geometry, codes and difference sets: exceptional connections, in: Codes and Designs, Columbus, OH, 2000, in: Ohio State Univ. Math. Res. Inst. Publ., vol. 10, de Gruyter, Berlin, 2002, pp. 73–85, https://doi.org/10.1515/9783110198119.73.

[13] P. Ellingsen, P. Felke, C. Riera, P. Stănică, A. Tkachenko, C-differentials, multiplicative uniformity, and (almost) perfect c-nonlinearity, IEEE Trans. Inf. Theory 66 (2020) 5781–5789, https://doi.org/10.1109/TIT.2020.2971988.

[14] F. Hernando, G. McGuire, Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions, J. Algebra 343 (2011) 78–92.

[15] H. Janwa, G.M. McGuire, R.M. Wilson, Double-error-correcting cyclic codes and absolutely irreducible polynomials over GF(2), J. Algebra 178 (1995) 665–676, https://doi.org/10.1006/jabr.1995.1372.

[16] H. Janwa, R.M. Wilson, Hyperplane sections of Fermat varieties in $\mathbf{P}^3$ in char. 2 and some applications to cyclic codes, in: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, San Juan, PR, 1993, in: Lecture Notes in Comput. Sci., vol. 673, Springer, Berlin, 1993, pp. 180–194, https://doi.org/10.1007/3-540-56686-4_43.

[17] M. Jarden, A. Razon, Skolem density problems over large Galois extensions of global fields, in: Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry, Ghent, 1999, in: Contemp. Math., vol. 270, Amer. Math. Soc., Providence, RI, 2000, pp. 213–235, https://doi.org/10.1090/conm/270/04375, with an appendix by Wulf-Dieter Geyer.

[18] K. Nyberg, Differentially uniform mappings for cryptography, in: Advances in Cryptology—Eurocrypt'93, Springer, 1994, pp. 55–64, https://doi.org/10.1007/3-540-48285-7_6.

[19] P. Pollack, Simultaneous prime specializations of polynomials over finite fields, Proc. Lond. Math. Soc. 97 (2008) 545–567, https://doi.org/10.1112/plms/pdn013.

[20] F. Rodier, Functions of degree 4e that are not APN infinitely often, Cryptogr. Commun. 3 (2011) 227–240, https://doi.org/10.1007/s12095-011-0050-6.

[21] M. Rosen, Number Theory in Function Fields, Springer, New York, NY, 2002.

[22] J.P. Serre, Topics in Galois Theory, CRC Press, 2016.

[23] J.F. Voloch, Symmetric cryptography and algebraic curves, in: Algebraic Geometry and Its Applications, in: Ser. Number Theory Appl., vol. 5, World Sci. Publ., Hackensack, NJ, 2008, pp. 135–141, https://doi.org/10.1142/9789812793430_0007.

Please cite this article in press as: Y. Aubry et al., Polynomials with maximal differential uniformity and the exceptional APN conjecture, J. Algebra (2023), https://doi.org/10.1016/j.jalgebra.2023.07.017