TRINOMIALS WITH HIGH DIFFERENTIAL UNIFORMITY

Yves Aubry, Fabien Herbaut, Ali Issa

TRINOMIALS WITH HIGH DIFFERENTIAL UNIFORMITY

YVES AUBRY, FABIEN HERBAUT, AND ALI ISSA

Abstract. The context of this work is the study of the differential uniformity of polynomials defined over finite fields of even characteristic. We provide infinite families of trinomials with high differential uniformity when the base field is large enough. It means in particular that these trinomials are not exceptional almost perfect nonlinear. [1]

1. Introduction

In the whole paper we consider polynomials $f \in \mathbb{F}_{2^n}[x]$. The differential uniformity of f, denoted by $\delta_{\mathbb{F}_{2^n}}(f)$ or simply $\delta(f)$, is defined as the maximum number of solutions of the equation $f(x+\alpha)-f(x)=\beta$ in $\mathbb{F}_{2^n}$ where α and β run over $\mathbb{F}_{2^n}$ and α is nonzero. In general $\delta(f)$ is not easy to compute. Polynomials f of $\mathbb{F}_{2^n}[x]$ such that $\delta(f)=2$ are called almost perfect nonlinear (APN) and have numerous application in various fields (see [16], and [6] for a survey). Such polynomials which are also APN over infinitely many extensions of $\mathbb{F}_{2^n}$ are called *exceptional* APN and also receive special attention (see for instance [14], [5] and [12] for a survey). One conjecture proposed in [4] and still open is whether the only exceptional APN polynomials are the polynomials x^{2^k+1} and $x^{2^{2k}-2^k+1}$ for $k \geq 1$, up to the CCZ equivalence, a relation whose definition ([11]) is expressed in terms of affine permutations of the graphs.

Concretely it is rather difficult to determine whether a polynomial is APN (or exceptional APN) and in the two last decades many works have been dedicated to this question. Quite naturally the progress achieved have often involved lacunary polynomials. For example results in the direction of the conjecture quoted above were regularly obtained for polynomials $f(x) = x^{2^k+1}+h(x)$ or $f(x)=x^{2^{2k}-2^k+1}+h(x)$ with extra conditions on h which in particular involve the degree. In the case of polynomials of degree 2^k+1 this serie of results culminates with the recent work [1]. Also, binomials of the form $x^{2^s+1}+wx^{2^{ik}+2^{mk+s}}$ with specific conditions on n and $w \in \mathbb{F}_{2^n}^*$ are shown to be APN in [9] and similar results are obtained in [8] for trinomials of the form $x^{2^{2i}+2^i}+bx^{2^n+1}+cx^{2^n(2^{2i}+2^i)}$. In another direction, since the introduction in [13] of a first APN binomial $x^3+ux^{36} \in \mathbb{F}_{2^{10}}[x]$ which is

Date: April 15, 2024.

2010 *Mathematics Subject Classification.* Primary 14G50 Secondary 11T71.

Key words and phrases. Polynomials over finite fields differential uniformity Chebotarev theorem exceptional APN conjecture.

not CCZ equivalent to a monomial, such results have been obtained for trinomials ([7]) and quadrinomials ([10]).

Actually Voloch proved in [17] that for large values of n most polynomials of $\mathbb{F}_{2^n}[x]$ of degree $m \equiv 0$ or $3 \pmod 4$ have a differential uniformity equal to $m-1$ or $m-2$, which confirms the fact that polynomials with a differential uniformity equal to 2 are very rare. A set $\mathcal{M}$ of odd integer has been introduced in [2] with the following property: if $m \in \mathcal{M}$ is such that $m \equiv 7 \pmod 8$, then for n sufficiently large, all degree m polynomials $f \in \mathbb{F}_{2^n}[x]$ satisfy $\delta(f) = m-1$. For the even degree case, a similar result is obtained in [3] for a specific family of degrees $m = 2^r(2^\ell + 1)$ when $r \geq 2$, $\ell \geq 1$ and $\gcd(r, \ell) \leq 2$.

In this paper we show how we can adapt the methods of [17] and [2] so we can transfer the property of high differential uniformity to some trinomials of degree m when $m-1 \in \mathcal{M}$ and m is divisible by 4. The methods of [2] rely on the use of the Chebotarev density theorem which necessitates to compare monodromy groups in order to ensure that some Galois extensions of function fields are geometric. It requires a characterization of Morse polynomials given in an Appendix of Geyer in [15]. This characterization involves the property for a polynomial to have distinct critical values, and a key point of our work (which is developed in subsection 3.1) is the transfer of this property to the case of trinomials.

2. Main result

First recall that a polynomial g with coefficients in a field k is said to have distinct critical values if for any τ, η in the algebraic closure $\overline{k}$ the equalities $g'(\tau) = g'(\eta) = 0$ and $g(\tau) = g(\eta)$ imply $\tau = \eta$.

From now on we will denote by $D_\alpha f(x) := f(x+\alpha) - f(x)$ the derivative of f along α. As a consequence of the action of the involution $x \mapsto x + \alpha$ on the set of the roots of $D_\alpha f$ one can associate to any polynomial $f \in \mathbb{F}_{2^n}[x]$ of degree $m \geq 7$ a unique polynomial $L_\alpha f$ of degree less than or equal to $(m-1)/2$ such that $L_\alpha f(x(x+\alpha)) = D_\alpha f(x)$ (see Proposition 2.3 of [2] and also Proposition 2.1 of [3] for more details).

The set $\mathcal{M}$ is introduced in [2] as the set of odd integer m such that $L_\alpha(x^m)$ has distinct critical values. Proposition 3.11 in [2] explains that this assumption does not depend on the choice of α and leads to the following equivalent definition.

Definition 2.1. We define $\mathcal{M}$ as the set of odd positive integers m such that $L_\alpha(x^m)$ has distinct critical values (for any nonzero value of α) or equivalently such that

$$\forall \zeta_1, \zeta_2 \in \overline{\mathbb{F}}_2 \setminus \{1\},\ \zeta_1^{m-1} = \zeta_2^{m-1} = \left(\frac{1+\zeta_1}{1+\zeta_2}\right)^{m-1} = 1 \Longrightarrow \zeta_1 = \zeta_2 \text{ or } \zeta_1 = \zeta_2^{-1}. \tag{1}$$

It follows immediately from this definition that if m is odd, then $m \in \mathcal{M}$ if and only if $2(m-1)+1 \in \mathcal{M}$, or if and only if $2^k(m-1)+1 \in \mathcal{M}$ for any nonnegative integer k. And even if m is even, if m satisfies Condition (1) in

Definition (2.1) then $2^k(m-1)+1 \in \mathcal{M}$ for any $k \geq 1$.

We can now formulate the main result of this paper.

Theorem 2.2. *Let $m \geq 8$ be an integer such that $m \equiv 0 \pmod 4$ and $m-1 \in \mathcal{M}$. For n sufficiently large if $f(x) = a_0x^m + a_1x^{m-1} + a_2x^{m-2} \in \mathbb{F}_{2^n}[x]$ is a polynomial of degree m such that $a_1 \neq 0$ then $\delta_{\mathbb{F}_{2^n}}(f)$ is maximal, that is $\delta_{\mathbb{F}_{2^n}}(f) = m-2$. In particular such polynomials are not exceptional APN.*

To be concrete we conclude this section by providing in the following table examples of degrees m for which Theorem 2.2 applies.

	Ex. of degrees m for which Th. 2.2 applies	**Comments**
1	m =8 or 12, 20, 24, 28, 36, 40, 48, 52, 56, 60, 68, 76, 80, 84, 88, 96, 108, 112, 116, 120, 124, 132, 136, 140, 144, 160, 164, 168, 176, 192, 196, 200	Degrees $m \leq 200$ for which Th. 2.2 applies.
2	$m = 2^k + 4$ for $k \geq 2$	Point (ii) of Proposition 5.2 in [2].
3	$m = 2\ell^k + 2$ for $k \geq 0$ and $\ell \in \{3, 5, 11, 13, 17, 19, 23, 29, 37, 41, 43, 47, 53, 59, 61, 67, 71, 79, 83, 97, 101, 103, 107, 109, 113, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199,...\}$	Point (iii) of Proposition 5.2 in [2]. Holds for any odd prime ℓ such that: - $2^{\ell-1} \not\equiv 1 \pmod{\ell^2}$ and - $m' := \ell + 1$ satisfies Condition (1).

The first list of examples comes from Example 3.16 in [2]. It arises from a computer-assisted checking of Condition (1) which involves an enumeration of the $(m-1)$th roots of unity.

The second family of degrees $m = 2^k + 4$ is derived from Point (ii) of Proposition 5.2 in [2] where we take $s = 2$.

The third family can be deduced from Point (iii) of Proposition 5.2 in [2] where we take $s = 1$. The odd prime ℓ has to fulfilll $2^{\ell-1} \not\equiv 1 \pmod{\ell^2}$ while the integer $m' := \ell + 1$ must satisfy Condition (1). The given list of such integers $\ell < 200$ is obtained again with the help of a computer algebra system (example 3.21 in [2]).

3. The proof

3.1. **Distinct critical values.** This subsection aims to control the number of α such that $L_\alpha f$ fails to have distinct critical values when f is a trinomial of the form $a_0x^m + a_1x^{m-1} + a_2x^{m-2}$. We proceed in two steps. First we

treat the case when f is a binomial $a_0x^m + a_1x^{m-1}$. Second we will relate the case of binomials to the case of trinomials.

Lemma 3.1. *Let $m \geq 8$ be an integer such that $m \equiv 0 \pmod 4$ and $m-1 \in \mathcal{M}$. We set $d = (m-2)/2$. For all binomials $f(x) = a_0x^m + a_1x^{m-1} \in \mathbb{F}_{2^n}[x]$ such that $a_1 \neq 0$, the critical values of $L_\alpha f$ are distinct except for at most $(6d+4)\binom{(d-1)/2}{2}$ values of $\alpha \in \mathbb{F}_{2^n}^*$.*

Proof. The appendix of Geyer in [15] describes the locus of the degree d polynomials $g = \sum_{k=0}^{d} b_{d-k}x^k \in \mathbb{F}_q[x]$ which fail to have distinct critical values as the closed set defined by

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

where the τ_i are the (double) roots of g'. To be more precise $\Pi_d(g)$ is a polynomial when g is monic, or else is an element of $\mathbb{F}_2[b_0, \ldots, b_d][1/b_0]$.

We point out that as a consequence of Proposition 2.1 in [2] the polynomial $L_\alpha(a_0x^m + a_1x^{m-1})$ has degree exactly $d = (m-2)/2$ provided that $a_1 \neq 0$ and even if $a_0 = 0$. So when $a_1 \neq 0$ we know that $L_\alpha(a_0x^m + a_1x^{m-1})$ has distinct critical values if and only if $\Pi_d(L_\alpha(a_0x^m + a_1x^{m-1}))$ is nonzero.

We set $e := \binom{(d-1)/2}{2}$, that is the number of ways to choose two different roots of g'. By Lemma 2.8 in [3] we know that $b_0^{de}\Pi_d(L_\alpha f)$ is an homogeneous polynomial of degree $(6d+4)e$ if we consider that a_i has weight i whereas α has weight 1. We also know that each term in $b_0^{de}\Pi_d(L_\alpha f)$ contains a product of $(d+2)e$ coefficients a_i. In the case where $f(x) = a_0x^m + a_1x^{m-1}$ these homogeneity conditions impose strong constraints on $b_0^{de}\Pi_d(L_\alpha f)$ which will necessarily take the form

$$b_0^{de}\Pi_d(L_\alpha f) = \sum_{i=0}^{(d+2)e} c_i a_0^{(d+2)e-i} a_1^i \alpha^{(6d+4)e-i} \tag{3}$$

where the coefficients c_i's belong to $\mathbb{F}_2$. If we consider $b_0^{de}\Pi_d(L_\alpha f)$ in the ring $\mathbb{F}_2[a_0, a_1][\alpha]$, the lowest degree in α is possibly $(5d+2)e$ which would correspond to the term $a_1^{(d+2)e}\alpha^{(5d+2)}$.

To determine if this monomial does appear in (3) it is sufficient to evaluate in $a_0 = 0$ and $a_1 = 1$. By definition of Π_d, the issue comes down to determining whether the critical values of $L_\alpha(x^{m-1})$ are distinct, which is the case because we have supposed that $m - 1 \in \mathcal{M}$.

As a consequence, for any choice of the a_i's in $\mathbb{F}_{2^n}$ such that $a_1 \neq 0$ the polynomial $b_0^{de}\Pi_d(L_\alpha f) \in \mathbb{F}_{2^n}[\alpha]$ is nonzero. As its degree is bounded by $(6d+4)e$, it admits at most $(6d+4)e$ roots which amounts to saying that there are at most $(6d+4)e$ values of α such that $L_\alpha(a_0x^m + a_1x^{m-1})$ does not have distinct critical values.

□

The task is now to relate the case of trinomials to the case of binomials.

Lemma 3.2. *Let $m \geq 8$ be an integer such that $m \equiv 0 \pmod 4$ and $a_0, a_1, a_2 \in \mathbb{F}_{2^n}$ such that $a_0 \neq 0$ and $a_1 \neq 0$. Consider the two polynomials $f(x) = a_0x^m + a_1x^{m-1} + a_2x^{m-2}$ and $h(x) = a_0x^m + a_1x^{m-1}$. The critical values of $L_\alpha f$ are distinct if and only if the critical values of $L_\alpha h$ are.*

Proof. First we recall that we can reformulate the requirements for $L_\alpha f$ to have distinct critical values the following way: f shall satisfy

$$\begin{cases} \textbf{C1}: \ (D_\alpha f)'(\tau) = (D_\alpha f)'(\eta) = 0 \\ \\ \textbf{C2} \ : \ D_\alpha f(\tau) = D_\alpha f(\eta) \end{cases} \implies \tau = \eta \text{ or } \tau = \eta + \alpha.$$

Indeed if we set $T_\alpha(x) = x(x+\alpha)$ one can write $(L_\alpha f) \circ T_\alpha = D_\alpha f$ and then $(D_\alpha f)' = \alpha (L_\alpha f)' \circ T_\alpha$. The result follows from the obvious fact that $T_\alpha(\tau) = T_\alpha(\eta)$ if and only if $\tau \in \{\eta, \eta + \alpha\}$, as quoted in Lemma 3.7 of [2].

We will now prove that in our context f satisfies **C1** and **C2** if and only if h does. Indeed, for both f and h the condition **C1** reads

$$a_1(\tau+\alpha)^{m-2} + a_1\tau^{m-2} = a_1(\eta+\alpha)^{m-2} + a_1\eta^{m-2} = 0$$

which can be simplified by the nonzero coefficient a_1. So, when condition **C1** is satisfied, the condition **C2** for f which expresses

$$\begin{array}{rl} & a_0(\tau+\alpha)^m + a_0\tau^m + a_1(\tau+\alpha)^{m-1} + a_1\tau^{m-1} + a_2(\tau+\alpha)^{m-2} + a_2\tau^{m-2} \\ = & a_0(\eta+\alpha)^m + a_0\eta^m + a_1(\eta+\alpha)^{m-1} + a_1\eta^{m-1} + a_2(\eta+\alpha)^{m-2} + a_2\eta^{m-2} \end{array}$$

is equivalent to

$$a_0(\tau+\alpha)^m + a_0\tau^m + a_1(\tau+\alpha)^{m-1} + a_1\tau^{m-1} = a_0(\eta+\alpha)^m + a_0\eta^m + a_1(\eta+\alpha)^{m-1} + a_1\eta^{m-1}$$

that is the condition **C2** for h. It concludes the proof. □

3.2. **Application of the Chebotarev density theorem.** Suppose that f satisfies the hypotheses of Theorem 2.2. The choice of the degree $m \equiv 0 \pmod 4$ and the hypothesis $a_1 \neq 0$ imply by Lemma 2.5 in [2] that $L_\alpha f$ has odd degree $d = (m-2)/2$, which is prime to the characteristic of the base field. Lemma 3.1 and Lemma 3.2 ensure that $L_\alpha f$ has distinct critical values except for at most $(6d+4)\binom{(d-1)/2}{2}$ values of α. By Proposition 2.5 of [3], the critical points of $L_\alpha f$ are nondegenerate (i.e. the derivative $(L_\alpha f)'$ and the second Hasse-Schmidt derivative $(L_\alpha f)^{[2]}$ have no common roots) except for at most $(m-1)(m-4)$ values of α in $\overline{\mathbb{F}}_2$. Frow now on we suppose that n is sufficiently large, so we can choose α such that the three conditions above are satisfied. As a consequence of an analogue of the Hilbert theorem in even characteristic given in the Appendix of Geyer in [15] the geometric monodromy group of $L_\alpha f$ is the full symmetric group. Hence, the splitting field F of $L_\alpha f(x) - t$ over $\mathbb{F}_{2^n}(t)$ with t transcendental over $\mathbb{F}_{2^n}$ is a geometric extension of $\mathbb{F}_{2^n}(t)$ (i.e. there is no constant field extension).

Then we consider the splitting field Ω of the polynomial $D_\alpha f(x) - t$ over the field $\mathbb{F}_{2^n}(t)$ and we write $L_\alpha f(x) = \sum_{k=0}^{d} b_{d-k} x^k$. Proposition 4.6 of [2] ensures that if $L_\alpha f$ is Morse and if the equation $x^2 + \alpha x = b_1/b_0$ has a solution in $\mathbb{F}_{2^n}$ then the extension Ω/F is also geometric. But Proposition 2.4 of [3] states that the number of $\alpha \in \mathbb{F}_{2^n}^*$ such that the trace (from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$) of $\frac{b_1}{b_0 \alpha^2}$ is equal to zero (i.e. such that the equation $x^2 + \alpha x = b_1/b_0$ has a solution in $\mathbb{F}_{2^n}$) is at least $\frac{1}{2}(2^n - 2^{n/2+1} - 1)$. We conclude that for n sufficiently large there exists $\alpha \in \mathbb{F}_{2^n}^*$ such that the extension $\Omega/\mathbb{F}_{2^n}(t)$ is a geometric Galois extension.

We now use the Chebotarev density theorem to obtain, once again for n sufficiently large depending only on the degree m the existence of a place of degree 1 of $\mathbb{F}_{2^n}(t)$ which totally splits in Ω, or in other words the existence of $\beta \in \mathbb{F}_{2^n}$ such that the equation $f(x+\alpha) - f(x) = \beta$ admits $m-2$ distinct roots. For this purpose we employ Inequality (7) in [3] .

Finally we have proved that $\delta_{\mathbb{F}_{2^n}}(f) = m - 2$ for n sufficiently large depending only on m.

References

[1] Carlos Agrinsoni, Heeralal Janwan, and Moises Delgado. Resolution of the exceptional APN conjecture in the Gold degree case. *Preprint*, 2024.

[2] Yves Aubry, Fabien Herbaut, and José Felipe Voloch. Maximal differential uniformity polynomials. *Acta Arith.*, 188(4):345–366, 2019.

[3] Yves Aubry, Ali Issa, and Fabien Herbaut. Polynomials with maximal differential uniformity and the exceptional APN conjecture. *J. Algebra*, 635:822–837, 2023.

[4] Yves Aubry, Gary McGuire, and François Rodier. A few more functions that are not APN infinitely often. In *Finite fields: theory and applications*, volume 518 of *Contemp. Math.*, pages 23–31. Amer. Math. Soc., Providence, RI, 2010.

[5] Daniele Bartoli and Kai-Uwe Schmidt. Low-degree planar polynomials over finite fields of characteristic two. *J. Algebra*, 535:541–555, 2019.

[6] Céline Blondeau and Kaisa Nyberg. Perfect nonlinear functions and cryptography. *Finite Fields Appl.*, 32:120–147, 2015.

[7] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire. New families of quadratic almost perfect nonlinear trinomials and multinomials. *Finite Fields Appl.*, 14(3):703–714, 2008.

[8] Lilya Budaghyan and Claude Carlet. Classes of quadratic APN trinomials and hexanomials and related structures. *IEEE Trans. Inform. Theory*, 54(5):2354–2357, 2008.

[9] Lilya Budaghyan, Claude Carlet, and Gregor Leander. Two classes of quadratic APN binomials inequivalent to power functions. *IEEE Trans. Inform. Theory*, 54(9):4218–4229, 2008.
[10] Lilya Budaghyan, Tor Helleseth, and Nikolay Kaleyski. A new family of APN quadrinomials. *IEEE Trans. Inform. Theory*, 66(11):7081–7087, 2020.
[11] Claude Carlet, Pascale Charpin, and Victor Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Des. Codes Cryptogr.*, 15(2):125–156, 1998.
[12] Moisés Delgado. The state of the art on the conjecture of exceptional APN functions. *Note Mat.*, 37(1):41–51, 2017.
[13] Yves Edel, Gohar Kyureghyan, and Alexander Pott. A new APN function which is not equivalent to a power mapping. *IEEE Trans. Inform. Theory*, 52(2):744–747, 2006.
[14] Fernando Hernando and Gary McGuire. Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions. *J. Algebra*, 343:78–92, 2011.
[15] Moshe Jarden and Aharon Razon. Skolem density problems over large Galois extensions of global fields. In *Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999)*, volume 270 of *Contemp. Math.*, pages 213–235. Amer. Math. Soc., Providence, RI, 2000. With an appendix by Wulf-Dieter Geyer.
[16] Kaisa Nyberg. Differentially uniform mappings for cryptography. In *Advances in cryptology—Eurocrypt'93*, pages 55–64. Springer, 1994.
[17] José Felipe Voloch. Symmetric cryptography and algebraic curves. In *Algebraic geometry and its applications*, volume 5 of *Ser. Number Theory Appl.*, pages 135–141. World Sci. Publ., Hackensack, NJ, 2008.

(Aubry) Institut de Mathématiques de Toulon - IMATH, Université de Toulon, France

(Aubry) Institut de Mathématiques de Marseille - I2M, Aix Marseille Univ, UMR 7373 CNRS, France
Email address: yves.aubry@univ-tln.fr

(Herbaut) INSPE Nice-Toulon, Université Côte d'Azur, France

(Herbaut) Institut de Mathématiques de Toulon - IMATH, Université de Toulon, France
Email address: fabien.herbaut@univ-cotedazur.fr

(Issa) Institut de Mathématiques de Marseille - I2M, Aix Marseille Univ, UMR 7373 CNRS, France
Email address: aliissa24895@gmail.com