Polynesian Journal of Mathematics
Volume 1, Issue 2 (Nov. 2024)

Differential uniformity of polynomials of degree 10

Yves Aubry

Institut de Mathématiques de Toulon - IMATH
Université de Toulon, France

Institut de Mathématiques de Marseille - I2M
Aix Marseille Univ, UMR 7373 CNRS, France

Abstract

We prove that polynomials of degree 10 over finite fields of even characteristic with some conditions on their coefficients have a differential uniformity greater than or equal to 6 over $\mathbb{F}_{2^n}$ for all n sufficiently large.

Keywords: Differential uniformity, monodromy groups, Chebotarev theorem.

1 Introduction

Differential uniformity of polynomials over finite fields is a measure of non-linearity and resistance against differential attacks in cryptography. Formally, the differential uniformity $\delta_{\mathbb{F}_q}(f)$ of a polynomial $f \in \mathbb{F}_q[x]$ over the finite field $\mathbb{F}_q$ with q elements is defined as the maximum number of solutions of the set of equations $f(x+\alpha)-f(x)=\beta$ where α and β belong to $\mathbb{F}_q$ with α non-zero (see [7] where it has been first introduced). For practical cryptographic applications, a particular study has been made over finite fields of characteristic 2, which will be the framework of our work here. Polynomials over $\mathbb{F}_{2^n}$ with low differential uniformity are highly sought after, especially those with the smallest possible one, namely equal to 2. The functions associated with these polynomials are called APN (Almost Perfect Nonlinear) functions, and exhaustive research suggests that they are very rare. In fact, Voloch proved in [10] that almost all polynomials have a differential uniformity essentially equal to their degree. Even better, Aubry, Herbaut and Voloch in [2] showed that, for a set of specific odd degrees, not almost all but indeed all polynomials of these degrees have maximal differential uniformity for n sufficiently large. Moreover, these results have been extended in [3] to infinitely many explicit even degrees and in [4] to some trinomials of degree divisible by 4.

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

The study of the differential uniformity of low-degree polynomials was conducted by Voloch in [10]. Apart from the trivial case of polynomials of degrees less than 4, he addressed the cases of degrees 5, 6, and 7 (the case of degree 8 is reduced to that of lower degrees), and he stopped at degree 9.

The main result of our paper concerns polynomials of degree 10 over finite fields of even characteristic. The methods developed in [3] and [4], although applicable to even-degree polynomials, cannot be applied mutatis mutandis to our situation. Therefore, we are led to develop here a specific approach that does not rely on the description of the locus of polynomials with non-distinct critical values, as was the case in [2], [3] and [4].

Precisely, we prove the following results.

Theorem (Theorems 3.2 and 4.6)**.** *Let* $f = \sum_{i=0}^{10} a_{10-i}x^i \in \mathbb{F}_{2^n}[x]$ *be a polynomial of degree* 10.

1) If

(i) $a_1a_3 \neq 0$, *and*

(ii) $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}\left(\frac{a_1a_4+a_5}{a_1^2a_3}\right) = 0$, *and*

(iii) $a_1^2a_4^2 + a_5^2 + a_1^7a_3 + a_1^4a_3^2 + a_1^2a_3a_5 + a_3a_7 \neq 0$,

then $\delta_{\mathbb{F}_{2^n}}(f) \geq 6$ *if* n *is sufficiently large (namely if* $n \geq 13$*).*

2) Suppose that $a_1 = a_3 = 0$ *and suppose that there exists* $\alpha \in \mathbb{F}_{2^n}^*$ *such that:*

(i) $c := \frac{\alpha^2a_5+a_7}{\alpha} \neq 0$ *and the polynomial* $R_3(x) := x^3 + bx^2 + c^2$ *has all its roots in* $\mathbb{F}_{2^n}$ *where* $b := \frac{\alpha^5+\alpha a_4+a_5}{\alpha}$, *and*

(ii) $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}\left(\frac{\alpha^5+\alpha a_4+a_5}{\alpha^3}\right) = 0$,

then $\delta_{\mathbb{F}_{2^n}}(f) = 8$ *if* n *is sufficiently large (namely if* $n \geq 15$*).*

Remark 1.1. Functions which are APN over infinitely many extensions of the base field are called *exceptional* APN. Aubry, McGuire and Rodier conjectured in [1] that, up to a certain equivalence, the Gold functions $f(x) = x^{2^k+1}$ and the Kasami-Welch functions $f(x) = x^{2^{2k}-2^k+1}$ are the only exceptional APN functions. The results of the present paper imply that the polynomials of degree 10 satisfying the conditions of our theorem are *a fortiori* not exceptional APN: we recover a known result since the conjecture in the case of polynomials f of degree $2e$ with e odd and when f contains a term of odd degree has been proved by Aubry, McGuire and Rodier in [1].

Section 2 is dedicated to the strategy of introducing a polynomial whose splitting field produces a Galois extension in which we will prove the existence of a place which totally splits using Chebotarev's density theorem. Section 3 focuses on the first part of the previous theorem and relies on Morse polynomial theory to obtain monodromy groups equal to the symmetric group. Finally Section 4 concentrates on the second part of the previous theorem and uses the characterization of the Galois groups of quartic polynomials through their quadratic and cubic resolvents.

2 Monodromy groups, Morse polynomials and geometric extensions

Let $f(x) = \sum_{i=0}^{10} a_{10-i}x^i \in \mathbb{F}_q[x]$, where $q = 2^n$, be a polynomial of degree $m = 10$ (so a_0 is always supposed to be non-zero). Let $\alpha \in \mathbb{F}_q^*$ and consider $D_\alpha f(x) = f(x+\alpha)+f(x)$ the derivative of f with respect to α. By definition, the differential uniformity of f is given by

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

Consider the unique polynomial $L_\alpha f$ such that $L_\alpha f\,(x(x+\alpha)) = D_\alpha f(x)$ (see Proposition 2.3 of [2] for the existence and the unicity of such a polynomial $L_\alpha f$) and let us denote by d its degree. A simple calculation gives :

$$\begin{aligned} D_\alpha f(x) = {} & (a_0\alpha^2 + a_1\alpha)x^8 + a_3\alpha x^6 + a_3\alpha^2x^5 + (a_3\alpha^3 + a_4\alpha^2 + a_5\alpha)x^4 \\ & + a_3\alpha^4x^3 + (a_0\alpha^8 + a_3\alpha^5 + a_4\alpha^4 + a_7\alpha)x^2 + (a_1\alpha^8 + a_3\alpha^6 + a_5\alpha^4 + a_7\alpha^2)x \\ & + a_0\alpha^{10} + a_1\alpha^9 + a_2\alpha^8 + a_3\alpha^7 + a_4\alpha^6 + a_5\alpha^5 + a_6\alpha^4 + a_7\alpha^3 + a_8\alpha^2 + a_9\alpha \end{aligned} \quad (1)$$

and

$$\begin{aligned} L_\alpha f(x) = {} & (\alpha^2a_0 + \alpha a_1)x^4 + \alpha a_3x^3 + (\alpha^6a_0 + \alpha^5a_1 + \alpha^2a_4 + \alpha a_5)x^2 \\ & + (\alpha^7a_1 + \alpha^5a_3 + \alpha^3a_5 + \alpha a_7)x \\ & + \alpha^{10}a_0 + \alpha^9a_1 + \alpha^8a_2 + \alpha^7a_3 + \alpha^6a_4 + \alpha^5a_5 + \alpha^4a_6 + \alpha^3a_7 + \alpha^2a_8 + \alpha a_9. \end{aligned} \quad (2)$$

Then we consider the splitting field F of the polynomial $L_\alpha f(x) - t$ over the field $\mathbb{F}_q(t)$ with t a transcendental element over $\mathbb{F}_q$ and we set $\mathbb{F}_q^F$ to be the algebraic closure of $\mathbb{F}_q$ in F. We consider now the Galois groups $G = \mathrm{Gal}(F/\mathbb{F}_q(t))$ and $\overline{G} = \mathrm{Gal}(F/\mathbb{F}_q^F(t))$ which are respectively the arithmetic and geometric monodromy groups of $L_\alpha f$.

If $u_0, \ldots, u_{d-1}$ are the roots of $L_\alpha f(x) = t$, then we will denote by x_i a root of $x^2 + \alpha x = u_i$. So the $2d$ elements $x_0, x_0 + \alpha, \ldots, x_{d-1}, x_{d-1} + \alpha$ are the solutions of $D_\alpha f(x) = t$. Then we consider $\Omega = \mathbb{F}_q(x_0, \ldots, x_{d-1})$ the compositum of the fields $F(x_i)$ and $\mathbb{F}_q^\Omega$ the algebraic closure of $\mathbb{F}_q$ in Ω. We set also $\Gamma = \mathrm{Gal}(\Omega/F)$ and $\overline{\Gamma} = \mathrm{Gal}(\Omega/F\mathbb{F}_q^\Omega)$. Then we have the diagram of Figure 1 where the constant field extensions from $k = \mathbb{F}_{2^n}$ are drawn and where C_F and C_Ω stand for the smooth projective algebraic curves associated to the function fields F and Ω.

The purpose here is to apply the Chebotarev density theorem in order to get the existence of an element β in a finite extension $\mathbb{F}$ of $\mathbb{F}_{2^n}$ such that the polynomial $D_\alpha f(x) + \beta$ splits in $\mathbb{F}[x]$. Indeed, the Chebotarev theorem describes the distribution of places in a Galois extension of number fields or in a geometric Galois extension of function fields of one variable over a finite field. It states that for any conjugacy class of the Galois group, there exists a density of places whose Frobenius automorphism falls within that class. For an unramified place, the associated conjugacy class, that is the Artin symbol attached to this place, is reduced to the identity automorphism if and only if the place splits in the Galois extension.

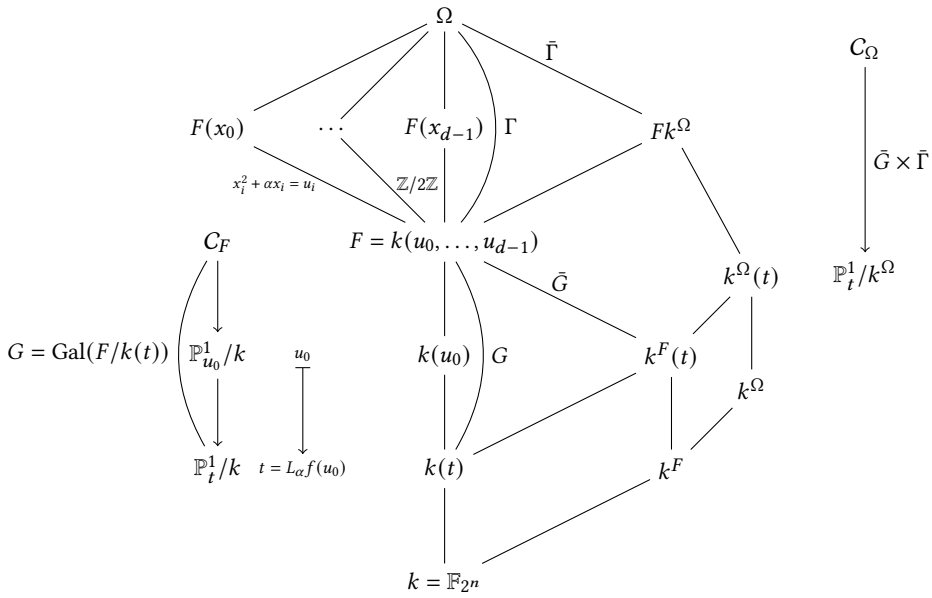


Figure 1: Diagram of field extensions and associated algebraic curves.

So the point is to work with a *geometric* (or *regular*) Galois extension $\Omega/\mathbb{F}_q(t)$, that is with no constant field extension. In other words, we want to find an α such that $G = \overline{G}$ and $\Gamma = \overline{\Gamma}$.

The regularity of the extension Ω/F will be derived from Proposition 4.6 of [2] (and a generalization) and is related to a Trace equation. The regularity of the extension $F/\mathbb{F}_q(t)$, for its part, will come from the theory of Morse polynomials in Section 3 and from quadratic and cubic resolvents in Section 4.

3 The result with $a_1 a_3 \neq 0$

Let $f(x) = \sum_{i=0}^{10} a_{10-i} x^i \in \mathbb{F}_{2^n}[x]$ be a polynomial of degree $m = 10$ with $a_1 \neq 0$ and $a_3 \neq 0$. Consider the choice:

$$\alpha = a_1/a_0.$$

Then Formulas (1) and (2) give that the polynomial

$$D_{\frac{a_1}{a_0}} f(x) = \frac{a_1^3 a_3}{a_0^3} x^6 + \cdots$$

has degree 6 and the polynomial

$$L_{\frac{a_1}{a_0}} f(x) = \frac{a_1a_3}{a_0}x^3 + \left(\frac{a_1^2a_4}{a_0^2} + \frac{a_1a_5}{a_0}\right)x^2 + \left(\frac{a_1^8}{a_0^7} + \frac{a_1^5a_3}{a_0^5} + \frac{a_1^3a_5}{a_0^3} + \frac{a_1a_7}{a_0}\right)x$$
$$+ \frac{a_1^8a_2}{a_0^8} + \frac{a_1^7a_3}{a_0^7} + \frac{a_1^6a_4}{a_0^6} + \frac{a_1^5a_5}{a_0^5} + \frac{a_1^4a_6}{a_0^4} + \frac{a_1^3a_7}{a_0^3} + \frac{a_1^2a_8}{a_0^2} + \frac{a_1a_9}{a_0}$$

has degree $d = 3$.

Recall that a polynomial $g \in \mathbb{F}_{2^n}[x]$ is said to be Morse (see the Appendix of Geyer to the paper [6]) if it has odd degree, if the critical points of g are non degenerate (i.e. the derivative g' and the second Hasse-Schmidt derivative $g^{[2]}$ have no common roots) and if the critical values of g are distinct (g does not take the same value at different zeros of g'). We have:

Proposition 3.1. *Let $f = \sum_{i=0}^{10} a_{10-i}x^i \in \mathbb{F}_{2^n}[x]$ be a polynomial of degree 10. If*

(i) $a_1a_3 \neq 0$, *and*

(ii) $a_0^4a_1^2a_4^2 + a_0^6a_5^2 + a_1^7a_3 + a_0^2a_1^4a_3^2 + a_0^4a_1^2a_3a_5 + a_0^6a_3a_7 \neq 0$,

then the polynomial $L_{\frac{a_1}{a_0}} f$ is Morse.

Proof. Let $f = \sum_{i=0}^{10} a_{10-i}x^i$ be as in the theorem and set $g = L_{\frac{a_1}{a_0}} f$. The polynomial g has odd degree (its degree is 3) and the critical values of g are obviously distinct since g' has degree 2 and thus has only one double root.

Now let us find a necessary and sufficient condition for the critical points of g to be nondegenerate. We have $g'(x) = \frac{a_1a_3}{a_0}x^2 + \frac{a_1^8}{a_0^7} + \frac{a_1^5a_3}{a_0^5} + \frac{a_1^3a_5}{a_0^3} + \frac{a_1a_7}{a_0}$.

Recall that the Hasse-Schmidt derivative $g^{[2]}$ is defined by the equality $g(t+u) \equiv g(t) + g'(t)u + g^{[2]}(t)u^2 \pmod{u^3}$ where u and t are independent variables. Then we get here: $g^{[2]}(x) = \frac{a_1a_3}{a_0}x + \frac{a_1^2a_4}{a_0^2} + \frac{a_1a_5}{a_0}$ which has $x = \frac{a_0a_5+a_1a_4}{a_0a_3}$ as a root. And this root is also a root of g' if and only if

$$a_0^4a_1^3a_4^2 + a_0^6a_1a_5^2 + a_1^8a_3 + a_0^2a_1^5a_3^2 + a_0^4a_1^3a_3a_5 + a_0^6a_1a_3a_7 = 0.$$

Thus condition (ii) ensures that the polynomial $g = L_{\frac{a_1}{a_0}} f$ is Morse. □

Theorem 3.2. *For n sufficiently large, namely for $n \geq 13$, for all polynomials $f = \sum_{i=0}^{10} a_{10-i}x^i \in \mathbb{F}_{2^n}[x]$ of degree 10 such that :*

(i) $a_1a_3 \neq 0$, *and*

(ii) $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}\left(\frac{a_1a_4+a_5}{a_1^2a_3}\right) = 0$, *and*

(iii) $a_1^2a_4^2 + a_5^2 + a_1^7a_3 + a_1^4a_3^2 + a_1^2a_3a_5 + a_3a_7 \neq 0$,

we have $\delta_{\mathbb{F}_{2^n}}(f) \geq 6$.

Proof. Since the differential uniformity of a polynomial is unchanged if it is multiplied by a non-zero scalar element, one can suppose that f is monic i.e. $a_0 = 1$. Conditions (i) and (iii) together with Proposition 3.1 imply that $L_{a_1}f$ is a Morse polynomial of degree $d = 3$. But the analogue of the Hilbert theorem given by Serre in Theorem 4.4.5 of [9] (and detailed in even characteristic in the Appendix of Geyer in [6]) asserts that the geometric monodromy group of a Morse polynomial of degree d is the symmetric group $\mathfrak{S}_d$. But since it is contained in its arithmetic monodromy group which is also a subgroup of $\mathfrak{S}_d$, they coincide. Hence we deduce that the extension $F/\mathbb{F}_{2^n}(t)$ is geometric.

Moreover, Proposition 4.6 of [2] gives us that the extension Ω/F will be geometric if there exists $x \in \mathbb{F}_{2^n}$ such that $x^2 + \alpha x = b_1/b_0$, where the b_i's are given by $L_\alpha f(x) = \sum_{k=0}^{d} b_{d-k}x^k$. In our case, the equation reduces to $x^2+a_1x = (a_1^2a_4+a_1a_5)/a_1a_3$. Hilbert'90 theorem implies that the equation $x^2 + a_1x = \frac{a_1a_4+a_5}{a_3}$ has a solution in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}\left(\frac{a_1a_4+a_5}{a_1^2a_3}\right) = 0$, which is exactly condition (ii) of the theorem.

Thus Proposition 4.6 of [2] implies that the extension Ω/F is geometric. Then we can apply the effective version of the Chebotarev density theorem given by Pollack in [8] to get the following lower bound (depending on n, the degree d_Ω of the extension $\Omega/\mathbb{F}_{2^n}(t)$ and the genus g_Ω of the function field Ω) for the number V of places of degree one in $\mathbb{F}_{2^n}(t)$ which totally split in Ω (see for more details the proof of Theorem 4.1 of [3]):

$$V \geq \frac{2^n}{d_\Omega} - \frac{2}{d_\Omega}(g_\Omega 2^{n/2} + g_\Omega + d_\Omega).$$

If n is sufficiently large, this number is at least one. To be explicit, we have seen above that $G = \overline{G} = \mathfrak{S}_3$ and moreover, by Proposition 4.6 of [2], we have that $\Gamma = \overline{\Gamma} = (\mathbb{Z}/2\mathbb{Z})^2$, so $d_\Omega = 3! \times 2^2 = 24$. Hence $V \geq 1$ as soon as $2^n - 2g_\Omega 2^{n/2} - 2g_\Omega - 72 > 0$.

Now by Lemma 14 of [8] we have $g_\Omega \leq \frac{1}{2}(\deg D_\alpha f - 3)d_\Omega + 1 = 37$. Hence if $n \geq 13$ we have $V \geq 1$ and this gives the existence of $\beta \in \mathbb{F}_{2^n}$ such that the polynomial $D_\alpha f(x) + \beta$ splits in $\mathbb{F}_{2^n}[x]$ with no repeated factors. The differential uniformity of f is thus greater than or equal to the degree of $D_\alpha f$, which is 6 in our present case. □

It implies for example that the polynomial $f(x) = x^{10} + x^9 + x^7 + x^3$ has a differential uniformity over $\mathbb{F}_{2^n}$ greater than or equal to 6 for $n \geq 13$.

Corollary 3.3. *All polynomials*

$$f(x) = x^{10} + a_1x^9 + a_2x^8 + a_3x^7 + a_6x^4 + a_7x^3 + a_8x^2 + a_9x + a_{10}$$

with a_1, a_3 in $\mathbb{F}_{2^n}^*$ and $a_2, a_6, a_7, a_8, a_9, a_{10}$ in $\mathbb{F}_{2^n}$ and such that $a_7 \neq a_1^7 + a_1^4a_3$ have a differential uniformity over $\mathbb{F}_{2^n}$ greater than or equal to 6 for n sufficiently large.

4 The case with $a_1 = 0$ and $a_3 = 0$

Making the choice $\alpha = a_1/a_0$ in the previous section gave a polynomial $D_\alpha f$ of degree 6, so the number of solutions of any equation $D_\alpha f(x) = \beta$ could be at most 6. If we choose $\alpha \neq a_1/a_0$ then the polynomial $D_\alpha f$ will be of degree 8 and the equation

$D_\alpha f(x) = \beta$ can have 8 solutions. Let us study what happens in a particular case of this situation.

Suppose without loss of generality that $a_0 = 1$ and let $\alpha \in \mathbb{F}_{2^n}^*$ be such that $\alpha + a_1 \neq 0$ i.e. $\alpha \neq a_1$. Then, by Formulas (1) and (2), we deduce that $D_\alpha f$ has degree 8 and $L_\alpha f$ has degree $d = 4$. The following proposition gives conditions for the algebraic and geometric monodromy groups of $\frac{1}{\alpha^2} L_\alpha f(x)$ to be the Klein group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Proposition 4.1. *Let $f = \sum_{i=0}^{10} a_{10-i} x^i \in \mathbb{F}_{2^n}[x]$ be a polynomial of degree 10 with $a_0 = 1$, $a_1 = a_3 = 0$. Let $\alpha \in \mathbb{F}_{2^n}^*$ and set $b := \frac{\alpha^5 + \alpha a_4 + a_5}{\alpha}$ and $c := \frac{\alpha^2 a_5 + a_7}{\alpha}$. Suppose that $c \neq 0$ and that the polynomial $R_3(x) := x^3 + bx^2 + c^2$ factors over $\mathbb{F}_{2^n}$ as the product of three linear factors (which means that $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}\left(\frac{b^3}{c^2}\right) = \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(1)$ and the roots of the polynomial $Q(T) := T^2 + c^2 T + b^6$ are cubes in $\mathbb{F}_{2^n}$ (respectively in $\mathbb{F}_{2^{2n}}$) if n is even (respectively if n is odd).*

Then the quartic polynomial $\frac{1}{\alpha^2} L_\alpha f(x)$ has algebraic and geometric monodromy groups isomorphic to the Klein group.

Proof. If we suppose that $a_0 = 1$ and $a_1 = a_3 = 0$, then we get by Formula (2), for any $\alpha \in \mathbb{F}_{2^n}^*$:

$$\begin{aligned} L_\alpha f(x) = {} & \alpha^2 x^4 + (\alpha^6 + \alpha^2 a_4 + \alpha a_5) x^2 + (\alpha^3 a_5 + \alpha a_7) x \\ & + \alpha^{10} + \alpha^8 a_2 + \alpha^6 a_4 + \alpha^5 a_5 + \alpha^4 a_6 + \alpha^3 a_7 + \alpha^2 a_8 + \alpha a_9 \end{aligned}$$

We set $g := \frac{1}{\alpha^2} L_\alpha f$ and we consider the irreducible polynomial

$$g(x) - t = \frac{1}{\alpha^2} L_\alpha f(x) - t \in \mathbb{F}_{2^n}(t)[x]$$

(recall that any polynomial $P(x) \in \mathbb{F}_{2^n}[x]$ gives rise to an irreducible polynomial $P(x) - t$ in the ring $\mathbb{F}_{2^n}(t)[x]$). We have:

$$\begin{aligned} g(x) - t = {} & x^4 + \frac{\alpha^5 + \alpha a_4 + a_5}{\alpha} x^2 + \frac{\alpha^2 a_5 + a_7}{\alpha} x \\ & + \frac{\alpha^9 + \alpha^7 a_2 + \alpha^5 a_4 + \alpha^4 a_5 + \alpha^3 a_6 + \alpha^2 a_7 + \alpha a_8 + a_9}{\alpha} + t. \end{aligned}$$

So we have

$$g(x) - t = x^4 + bx^2 + cx + d$$

with $b := \frac{\alpha^5 + \alpha a_4 + a_5}{\alpha}$, $c := \frac{\alpha^2 a_5 + a_7}{\alpha}$ and $d := \frac{\alpha^9 + \alpha^7 a_2 + \alpha^5 a_4 + \alpha^4 a_5 + \alpha^3 a_6 + \alpha^2 a_7 + \alpha a_8 + a_9}{\alpha} + t$.

The monic quartic polynomial $g(x) - t$ in $\mathbb{F}_{2^n}(t)[x]$ with no cubic term is separable if and only if $c \neq 0$ (see the illustration of Theorem 3.4. of [5]) and its quadratic resolvent $R_2(x)$ and its cubic resolvent $R_3(x)$ are given by (see equations (3.4) and (3.5) of [5]):

$$R_2(x) = x^2 + c^2 x + (b^3 + c^2) c^2$$

and

$$R_3(x) = x^3 + bx^2 + c^2.$$

It is well-known that $R_2(X)$ is reducible if and only if $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}\left(\frac{(b^3+c^2)c^2}{c^4}\right) = 0$ i.e. $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}\left(\frac{b^3}{c^2}\right) = \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(1)$.

Let us consider now the reducibility of the polynomial $R_3(x) = x^3 + bx^2 + c^2$. The substitution $z = x+b$ eliminates the quadratic term: it gives the equation $z^3+b^2z+c^2 = 0$.

Theorem 1 of [11] gives that the polynomial $z^3 + b^2z + c^2$ (with $c \neq 0$) is reducible if and only if

(i) $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}\left(\frac{b^6}{c^4}\right) \neq \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(1)$ (in this case the polynomial has a unique root in $\mathbb{F}_{2^n}$), or

(ii) $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}\left(\frac{b^6}{c^4}\right) = \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(1)$ and the roots of the polynomial $Q(T) := T^2 + c^2T + b^6$ are cubes in $\mathbb{F}_{2^n}$ if n is even, or in $\mathbb{F}_{2^{2n}}$ if n is odd (in this case the polynomial $z^3 + b^2z + c^2$ factors over $\mathbb{F}_{2^n}$ as the product of three linear factors).

So if $\alpha \in \mathbb{F}_{2^n}^*$ is such that $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}\left(\frac{b^6}{c^4}\right) = \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(1)$, i.e. $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}\left(\frac{b^3}{c^2}\right) = \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(1)$, and also such that the roots of the polynomial $Q(T)$ are cubes in $\mathbb{F}_{2^n}$ or in $\mathbb{F}_{2^{2n}}$ (according as n is even or odd), then the polynomials $R_2(x)$ and $R_3(x)$ are reducibles.

Finally, with the hypothesis of the proposition, $g(x) - t$ is a separable irreducible quartic polynomial of $\mathbb{F}_{2^n}(t)[x]$ such that its quadratic and cubic resolvents are reducibles. By Theorem 3.4. of [5], we obtain that the Galois group G_g of the polynomial $g(x) - t = \frac{1}{\alpha^2}L_\alpha f(x) - t$, which is the arithmetic monodromy group of the polynomial $g(x) = \frac{1}{\alpha^2}L_\alpha f(x)$, is isomorphic to the Klein group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Since the polynomial $g(x) - t$ is irreducible over $\mathbb{F}_{2^n}(t)$, the arithmetic and the geometric monodromy groups of $\frac{1}{\alpha^2}L_\alpha f(x)$, seen as permutation groups, are transitive subgroups of the symmetric group $\mathfrak{S}_4$. It is well-known (see [5] for example) that the only transitive subgroups of $\mathfrak{S}_4$ are $\mathfrak{S}_4$ himself, the alternate group $\mathfrak{A}_4$, three conjugate subgroups isomorphic to the dihedral group D_4 of order 8, three conjugate subgroups isomorphic to the cyclic group $\mathbb{Z}/4\mathbb{Z}$ and one subgroup isomorphic to the Klein group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Since the geometric monodromy group $\overline{G}_g$ of $g(x) = \frac{1}{\alpha^2}L_\alpha f(x)$ is a normal subgroup of G_g and a transitive subgroup of $\mathfrak{S}_4$, we obtain that $\overline{G}_g$ is also the Klein group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. □

Remark 4.2. The condition $c \neq 0$ in the previous theorem is equivalent to saying that the polynomial $g(x) - t := \frac{1}{\alpha^2}L_\alpha f(x) - t \in \mathbb{F}_{2^n}(t)[x]$ is separable (see the illustration of Theorem 3.4. of [5]).

Remark 4.3. The condition in the previous theorem saying that the polynomial $R_3(x) := x^3 + bx^2 + c^2$ factors over $\mathbb{F}_{2^n}$ as the product of three linear polynomials is equivalent to saying that (see Theorem 1 of [11]): $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}\left(\frac{b^3}{c^2}\right) = \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(1)$ and the roots of the equation $T^2 + c^2T + b^6$ are cubes in $\mathbb{F}_{2^n}$ (respectively in $\mathbb{F}_{2^{2n}}$) if n is even (respectively if n is odd).

Example 4.4. Let $f = \sum_{i=0}^{10} a_{10-i}x^i \in \mathbb{F}_{2^n}[x]$ be a polynomial of degree 10 with $a_0 = 1$, $a_1 = a_3 = a_4 = a_5 = 0$ and $a_7 = 1$, i.e. the polynomial f has the form

$$f(x) = x^{10} + a_2x^8 + a_6x^4 + x^3 + a_8x^2 + a_9x + a_{10}$$

with $a_2, a_6, a_8, a_9, a_{10}$ in $\mathbb{F}_{2^n}$. Let us show that if $n \equiv 0 \pmod 4$ then there exists $\alpha \in \mathbb{F}_{2^n}^*$ such that the polynomial $\frac{1}{\alpha^2}L_\alpha f(x)$ has algebraic and geometric monodromy groups isomorphic to the Klein group.

Indeed, let $\alpha \in \mathbb{F}_{2^n}^*$ and consider, as in the proof of Proposition 4.1, the irreducible polynomial

$$g(x) - t := \frac{1}{\alpha^2}L_\alpha f(x) - t \in \mathbb{F}_{2^n}(t)[x].$$

So we have

$$g(x) - t = x^4 + bx^2 + cx + d$$

with $b := \alpha^4$, $c := \frac{1}{\alpha}$ and $d := \frac{\alpha^9+\alpha^7a_2+\alpha^3a_6+\alpha^2+\alpha a_8+a_9}{\alpha} + t$.

Since $c \neq 0$ then, by Remark 4.2, the polynomial $g(x) - t$ is separable. Moreover, the condition $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}\left(\frac{b^3}{c^2}\right) = \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(1)$ in Proposition 4.1 remains to

$$\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\alpha^7) = \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(1) = n \pmod 2.$$

Now the equation $T^2 + c^2T + b^6 = 0$ becomes

$$T^2 + \frac{1}{\alpha^2}T + \alpha^{24} = 0.$$

We are looking for α in $\mathbb{F}_{2^n}^*$ such that the solutions of this equation are cubes in $\mathbb{F}_{2^n}$. Note that these roots belong to $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\alpha^{28}) = 0$, i.e. $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\alpha^7) = 0$.

But one can show that there exists $\alpha \in \mathbb{F}_{2^4}^*$ such that the polynomial $T^2+\frac{1}{\alpha^2}T+\alpha^{24}$ has roots which are cubes in $\mathbb{F}_{16}^*$ and with $\mathrm{Tr}_{\mathbb{F}_{2^4}/\mathbb{F}_2}(\alpha^7) = 0$. Indeed, take $\mathbb{F}_{16} = \mathbb{F}_2[X]/(X^4 + X^3 + 1) = \mathbb{F}_2(\theta)$ and choose $\alpha = \theta^{10}$. Then

$$Q(T) = T^2 + \theta^{10}T + 1 = T^2 + \frac{1}{(\theta^{10})^2}T + (\theta^{10})^{24} = (T + (\theta^2)^3)(T + (\theta^3)^3)$$

with

$$\mathrm{Tr}_{\mathbb{F}_{2^4}/\mathbb{F}_2}(\alpha^7) = \mathrm{Tr}_{\mathbb{F}_{2^4}/\mathbb{F}_2}(\theta^{70}) = \mathrm{Tr}_{\mathbb{F}_{2^4}/\mathbb{F}_2}(\theta^{10}) = \mathrm{Tr}_{\mathbb{F}_{2^4}/\mathbb{F}_2}(\theta^5) = \mathrm{Tr}_{\mathbb{F}_{2^4}/\mathbb{F}_2}(\alpha^2) = 0.$$

In conclusion, if $f = \sum_{i=0}^{10} a_{10-i}x^i \in \mathbb{F}_{2^n}[x]$ is a polynomial of degree 10 with $a_0 = a_7 = 1$ and $a_1 = a_3 = a_4 = a_5 = 0$, and if $n \equiv 0 \pmod 4$ there exists $\alpha \in \mathbb{F}_{2^n}^*$ (since in this case $\mathbb{F}_{16}$ is included in $\mathbb{F}_{2^n}$) such that $c \neq 0$ and, by Remark 4.3, such that the polynomial $R_3(x) := x^3 + bx^2 + c^2$ has all its roots in $\mathbb{F}_{2^n}$. Hence by Proposition 4.1 the polynomial $\frac{1}{\alpha^2}L_\alpha f(x)$ has algebraic and geometric monodromy groups isomorphic to the Klein group.

Recall that F is the splitting field of the polynomial $L_\alpha f(x) - t$ over the field $\mathbb{F}_{2^n}(t)$ and $\Omega = \mathbb{F}_{2^n}(x_0, \ldots, x_{d-1})$ is the compositum of the fields $F(x_i)$, where $u_0, \ldots, u_{d-1}$ are the roots of $L_\alpha f(x) = t$ and x_i are the roots of $x^2 + \alpha x = u_i$.

Now let us give a sufficient condition for the extension Ω/F to be geometric.

Lemma 4.5. *Let $f = \sum_{i=0}^{10} a_{10-i} x^i \in \mathbb{F}_{2^n}[x]$ be a polynomial of degree 10 with $a_0 = 1$, $a_1 = a_3 = 0$. Let $\alpha \in \mathbb{F}_{2^n}^*$ and set $b := \frac{\alpha^5 + \alpha a_4 + a_5}{\alpha}$ and $c := \frac{\alpha^2 a_5 + a_7}{\alpha}$. Suppose that $c \neq 0$ and that the polynomial $R_3(x) := x^3 + bx^2 + c^2$ factors over $\mathbb{F}_{2^n}$ as the product of three linear factors.*

Then the extension Ω/F is geometric as soon as the equation $x^2 + \alpha x = \frac{\alpha^5 + \alpha a_4 + a_5}{\alpha}$ has a solution in $\mathbb{F}_{2^n}$.

Proof. We begin proving that if u is a root of $L_\alpha f(x) - t$ in F, then, for each place $\wp$ of F above the place ∞ at infinity of $\mathbb{F}_{2^n}(t)$, we have that u has a simple pole at $\wp$.

Indeed, the field $\mathbb{F}_{2^n}(t)(u)$ is just the rational function field $\mathbb{F}_{2^n}(u)$. The place at infinity P_∞ of $\mathbb{F}_{2^n}(u)$ is the pole of u and it is the place above the place at infinity ∞ of $\mathbb{F}_{2^n}(t)$ (which corresponds to the pole of t). Thus the valuation of u at P_∞ is given by $v_{P_\infty}(u) = -1$ and therefore $v_{P_\infty}(L_\alpha f(u)) = -\deg(L_\alpha f(x))$. Since the ramification index $e(P_\infty|\infty)$ of P_∞ over ∞ verify:

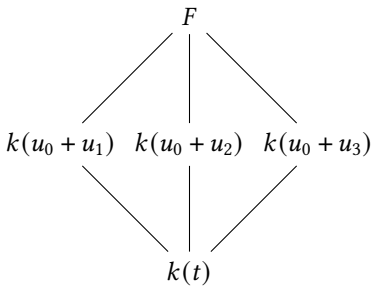
$$v_{P_\infty}(L_\alpha f(u)) = v_{P_\infty}(t) = e(P_\infty|\infty) v_\infty(t) = -e(P_\infty|\infty)$$

thus we obtain:

$$e(P_\infty|\infty) = \deg(L_\alpha f(x)) = 4.$$

But the hypotheses on c and $R_3(x)$ imply by Proposition 4.1 that the Galois extension $F/\mathbb{F}_{2^n}(t)$ has Galois group the Klein group of order 4 (the place at infinity of $\mathbb{F}_{2^n}(t)$ is then totally ramified in $\mathbb{F}_{2^n}(u)$). We conclude that $F = \mathbb{F}_{2^n}(u)$ and then u has a simple pole at $\wp = P_\infty$.

Now we show that if $J \subset \{0, 1, 2, 3\}$ is neither empty nor the whole set then $\sum_{j \in J} u_j$ has a pole at the place at infinity P_∞ of F. Since the coefficient of x^3 in the polynomial $L_\alpha f$ is zero (see Formula (2)), we have that $u_0 + u_1 + u_2 + u_3 = 0$. We are then reduced to show that $u_0 + u_1$, $u_0 + u_2$ and $u_0 + u_3$ have a pole at P_∞. But we are in the situation where the Galois extension $F/\mathbb{F}_{2^n}(t)$ has a Galois group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, so the following diagram summarize the situation (where $k := \mathbb{F}_{2^n}$ and all the extensions have degree 2).



If we denote by ∞_i the place at infinity of $\mathbb{F}_{2^n}(u_0+u_i)$, for $i=1,2,3$, we have that the ramification index $e(P_\infty|\infty_i)=e(\infty_i|\infty)=2$ for all i since ∞ is totally ramified in the extension $F/\mathbb{F}_{2^n}(t)$.

So we have

$$v_{P_\infty}(u_0+u_i)=e(P_\infty|\infty_i)v_{\infty_i}(u_0+u_i)=2\times(-1)=-2\leq -1$$

which proves that P_∞ is a pole of u_0+u_i.

Then, the proof of Proposition 4.6 of [2] remains true with polynomials of degree 10 with geometric and arithmetic monodromy groups the Klein group: if there exists $x\in\mathbb{F}_{2^n}$ such that $x^2+\alpha x=b_1/b_0$ where the b_i's are defined by $\frac{1}{\alpha^2}L_\alpha f(x)=\sum_{i=0}^4 b_{4-i}x^i$ then $\mathrm{Gal}\,(F(x_0,x_1,x_2,x_3)/F)$ and $\mathrm{Gal}\left(F\mathbb{F}_{2^n}^\Omega(x_0,x_1,x_2,x_3)/F\mathbb{F}_{2^n}^\Omega\right)$ are isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$, where $\mathbb{F}_{2^n}^\Omega$ denotes the algebraic closure of $\mathbb{F}_{2^n}$ in Ω and $F\mathbb{F}_{2^n}^\Omega$ denotes the compositum of the fields F and $\mathbb{F}_{2^n}^\Omega$. The coefficients b_i's come from Equation (2): $b_1/b_0=\frac{\alpha^5+\alpha a_4+a_5}{\alpha}$, and the existence of a solution in $\mathbb{F}_{2^n}$ of the equation $x^2+\alpha x=b_1/b_0$ is exactly the last condition of the Lemma. Thus we conclude that the extension Ω/F is geometric. □

Theorem 4.6. *Let $f=\sum_{i=0}^{10}a_{10-i}x^i\in\mathbb{F}_{2^n}[x]$ be a polynomial of degree 10 with $a_1=a_3=0$.*

Suppose that there exists $\alpha\in\mathbb{F}_{2^n}^*$ such that:

(i) $c:=\frac{\alpha^2a_5+a_7}{\alpha}\neq 0$ and the polynomial $R_3(x):=x^3+bx^2+c^2$ has all its roots in $\mathbb{F}_{2^n}$ where $b:=\frac{\alpha^5+\alpha a_4+a_5}{\alpha}$, and

(ii) $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}\left(\frac{\alpha^5+\alpha a_4+a_5}{\alpha^3}\right)=0$.

Then $\delta_{\mathbb{F}_{2^n}}(f)=8$ if n is sufficiently large (namely if $n\geq 15$).

Proof. Let f be a polynomial as in the theorem. Looking at its differential uniformity, one can suppose that f is monic. Condition (i) implies by Proposition 4.1 that the polynomial $\frac{1}{\alpha^2}L_\alpha f(x)$ has algebraic and geometric monodromy groups isomorphic to the Klein group. Hence the splitting field F of the polynomial $g(x):=\frac{1}{\alpha^2}L_\alpha f(x)-t$ is a geometric extension of $\mathbb{F}_{2^n}(t)$.

Moreover, by Lemma 4.5, the extension Ω/F is geometric as soon as the equation $x^2+\alpha x=\frac{\alpha^5+\alpha a_4+a_5}{\alpha}$ has a solution in $\mathbb{F}_{2^n}$. By the Hilbert'90 Theorem, this is equivalent to $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}\left(\frac{\alpha^5+\alpha a_4+a_5}{\alpha^3}\right)=0$, which is precisely Condition (ii).

Then we use the Chebotarev theorem, as in the proof of Theorem 3.2, to obtain, if n is sufficiently large (namely here if $n\geq 15$), the existence of $\beta\in\mathbb{F}_{2^n}$ such that the polynomial $D_\alpha f(x)+\beta\alpha^2$ splits in $\mathbb{F}_{2^n}[x]$ with no repeated factors.

Thus the differential uniformity of f is equal to the degree of $D_\alpha f$ that is 8. □

Example 4.7. Let us come back to Example 4.4, and since the differential uniformity is unchanged if we add an additive polynomial, let us just consider the polynomial $f(x)=x^{10}+x^3\in\mathbb{F}_{2^n}[x]$. We have seen that, if $n\equiv 0\pmod 4$, then there exists $\alpha\in\mathbb{F}_{16}^*\subset\mathbb{F}_{2^n}^*$ such that the polynomial $T^2+\frac{1}{\alpha^2}T+\alpha^{24}$ has roots which are cubes in

$\mathbb{F}_{16}^*$ and with $\mathrm{Tr}_{\mathbb{F}_{16}/\mathbb{F}_2}(\alpha^7) = \mathrm{Tr}_{\mathbb{F}_{16}/\mathbb{F}_2}(\alpha^2) = 0$. Hence there exists $\alpha \in \mathbb{F}_{2^n}^*$ such that the polynomial $\frac{1}{\alpha^2} L_\alpha f(x)$ has algebraic and geometric monodromy groups isomorphic to the Klein group. Moreover the equation $x^2 + \alpha x = \frac{b_1}{b_0}$ has a solution in $\mathbb{F}_{2^n}$ since $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}\left(\frac{\alpha^5+\alpha a_4+a_5}{\alpha^3}\right) = \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\alpha^2) = 0$. Finally we conclude by Theorem 4.6 that if n is sufficiently large and $n \equiv 0 \pmod 4$ then $\delta_{\mathbb{F}_{2^n}}(f) = 8$.

Acknowledgements. The author would like to thank Fabien Herbaut for many discussions on this topic.

References

[1] Yves Aubry, Gary McGuire and François Rodier. A few more functions that are not APN infinitely often, Finite Fields: Theory and Applications, Contemporary Mathematics 518 (2010), 23-31.

[2] Yves Aubry, Fabien Herbaut, and José Felipe Voloch. Maximal differential uniformity polynomials, *Acta Arithmetica*, *Vol.* 188 no. 4 (2019), 345-366.

[3] Yves Aubry, Fabien Herbaut, and Ali Issa. Polynomials with maximal differential uniformity and the exceptional APN conjecture, *J. Algebra*, *Vol.* 635 no. 4 (2023), 822-837.

[4] Yves Aubry, Fabien Herbaut, and Ali Issa. Trinomials with high differential uniformity, *arXiv*: 2404.09594v1 [math.NT], 15 Apr 2024.

[5] Keith Conrad. Galois groups of cubics and quartics in all characteristics. https://kconrad.math.uconn.edu/blurbs/galoistheory/cubicquarticallchar.pdf

[6] 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.

[7] Kaisa Nyberg. Differentially uniform mappings for cryptography. In *Advances in cryptology—Eurocrypt'93*, pages 55–64. Springer, 1994.

[8] Paul Pollack. Simultaneous prime specializations of polynomials over finite fields. *Proc. London Math. Soc.*, 97(3):545–567, 2008.

[9] Jean-Pierre Serre. *Topics in Galois theory.* CRC Press, 2007.

[10] José Felipe Voloch. Symmetric cryptography and algebraic curves. In *Proceedings of the First SAGA Conference, Papeete, France*. World Scientific, 2007.

[11] Kenneth S. Williams. Notes on Cubics over $GF(2^n)$ and $GF(3^n)$. Journal of Number Theory 7, 361-365 (1975). World Scientific, 2007.