Differential uniformity and exceptional APN polynomials.

Ali Issa

Joint work with
Yves Aubry and Fabien Herbaut

Aix-Marseille University

16 February 2023

Introduction

1) Introduction

Definition

Let $n \in \mathbb{N}^*$. For any polynomial $f \in \mathbb{F}_{2^n}[x]$, Nyberg define the differential uniformity $\delta(f)$ of f over $\mathbb{F}_{2^n}$ by:

$$\delta_{\mathbb{F}_{2^n}}(f) = \max_{(\alpha,\beta)\in\mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}} \text{card}\{x \in \mathbb{F}_{2^n} \mid f(x) + f(x+\alpha) = \beta\}.$$

Remark

Let $n \in \mathbb{N}^*$. For any polynomial $f \in \mathbb{F}_{2^n}[x]$, we have $\delta(f) \geq 2$. The polynomials f with $\delta(f) = 2$, are the so-called APN polynomials (Almost Perfect Nonlinear). These polynomials help us to stand against differential cryptanalysis.

1) Introduction

Definition

Polynomials $f \in \mathbb{F}_{2^n}[x]$ which are APN over infinitely many extensions of $\mathbb{F}_{2^n}$ are called exceptional APN.

1) Introduction

Theorem (Voloch, 2007)

Most polynomials $f \in \mathbb{F}_{2^n}[x]$ of degree $m \equiv 0$ or $3 \pmod 4$ have differential uniformity equal to $m-1$ or $m-2$.

More precisely, for $m > 4$ such that $m \equiv 0$ or $3 \pmod 4$ and

$$\delta_0 = \begin{cases} m-1 & \text{if } m \text{ is odd.} \\ m-2 & \text{if } m \text{ is even.} \end{cases}$$

we have:

$$\lim_{n\to\infty} \frac{\text{card}\left(\{f \in \mathbb{F}_{2^n}[x] | \deg(f) = m, \delta(f) = \delta_0\}\right)}{\text{card}\left(\{f \in \mathbb{F}_{2^n}[x] | \deg(f) = m\}\right)} = 1.$$

1) Introduction

Theorem (Voloch, 2007)

Most polynomials $f \in \mathbb{F}_{2^n}[x]$ of degree $m \equiv 0$ or $3 \pmod 4$ have differential uniformity equal to $m-1$ or $m-2$.

More precisely, for $m > 4$ such that $m \equiv 0$ or $3 \pmod 4$ and

$$\delta_0 = \begin{cases} m-1 & \text{if } m \text{ is odd.} \\ m-2 & \text{if } m \text{ is even.} \end{cases}$$

we have:

$$\lim_{n\to\infty} \frac{\operatorname{card}\left(\{f \in \mathbb{F}_{2^n}[x] | \deg(f) = m, \delta(f) = \delta_0\}\right)}{\operatorname{card}\left(\{f \in \mathbb{F}_{2^n}[x] | \deg(f) = m\}\right)} = 1.$$

Aubry, Herbaut and Voloch have exhibited in 2019 an infinite set of odd integers m such that every polynomial $f \in \mathbb{F}_{2^n}[x]$ of degree m has maximal differential uniformity if n is large enough.

Main result

2) First result

Theorem (Aubry, Herbaut and A.I, 2022)

Let $m = 2^r(2^\ell + 1)$ where $\gcd(r, \ell) \leq 2$, $r \geq 2$ and $\ell \geq 1$.

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 $\delta(f)$ is maximal, that is $\delta(f) = m - 2$.

2) Result on trinomials

Definition

We define $\mathcal{M}$ by the set of odd integer m for which, for any ζ_1 and ζ_2 in $\overline{\mathbb{F}}_2 \setminus \{1\}$, the equalities $\zeta_1^{m-1} = \zeta_2^{m-1} = \left(\frac{1+\zeta_1}{1+\zeta_2}\right)^{m-1} = 1$ imply $\zeta_1 = \zeta_2$ or $\zeta_1 = \zeta_2^{-1}$.

2) Result on trinomials

Definition

We define $\mathcal{M}$ by the set of odd integer m for which, for any ζ_1 and ζ_2 in $\overline{\mathbb{F}}_2 \setminus \{1\}$, the equalities $\zeta_1^{m-1} = \zeta_2^{m-1} = \left(\frac{1+\zeta_1}{1+\zeta_2}\right)^{m-1} = 1$ imply $\zeta_1 = \zeta_2$ or $\zeta_1 = \zeta_2^{-1}$.

Theorem (Aubry, Herbaut and A.I, 2022)

Let $m \geqslant 8$ be an integer such that $m \equiv 0 \pmod 4$ and such that $m - 1 \in \mathcal{M}$.

For n sufficiently large and for all trinomials $f(x) = a_0 x^m + a_1 x^{m-1} + a_2 x^{m-2} \in \mathbb{F}_{2^n}[x]$ of degree m such that $a_1 \neq 0$ the differential uniformity $\delta(f)$ is maximal that is $\delta(f) = m - 2$.

Sketch of proof

6) Sketch of proof

- Main ingredient: the Chebotarev theorem.
- Contribution of the Chebotarev theorem in our context
- Preliminaries (Morse polynomials, Hilbert-Serre theorem)

Main Ingredient

Main Ingredient

Theorem (Chebotarev)

Suppose that $\Omega/\mathbb{F}_q(t)$ is a Galois extension having full field of constants $\mathbb{F}_{q^D}$. 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 $\mathbb{F}_{q^D}$. Let $V(\mathcal{C})$ be the number of first degree primes v of $\mathbb{F}_q(t)$ unramified in Ω such that the Artin symbol $\left(\frac{\Omega/\mathbb{F}_q(t)}{v}\right)$ equals $\mathcal{C}$.
Then

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

where g denotes the genus of $\Omega/\mathbb{F}_{q^D}$.

Contribution of the Chebotarev Theorem in our context

Contribution of Chebotarev Theorem in our context

Definition

Let $n \in \mathbb{N}^*$ and t be a transcendental element over $\mathbb{F}_{2^n}$. For any polynomial $f \in \mathbb{F}_{2^n}[x]$ and for all $\alpha \in \mathbb{F}_{2^n}^*$ we define the field Ω_f to be the splitting field of the polynomial $f(x) + f(x + \alpha) - t$ over $\mathbb{F}_{2^n}(t)$.

Contribution of Chebotarev Theorem in our context

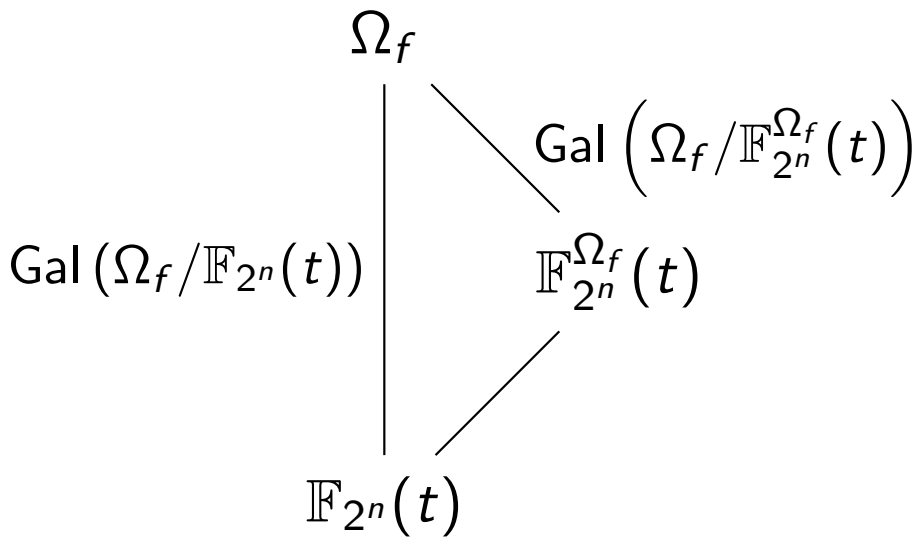
Definition

Let $n \in \mathbb{N}^*$ and t be a transcendental element over $\mathbb{F}_{2^n}$. For any polynomial $f \in \mathbb{F}_{2^n}[x]$ and for all $\alpha \in \mathbb{F}_{2^n}^*$ we define the field Ω_f to be the splitting field of the polynomial $f(x) + f(x+\alpha) - t$ over $\mathbb{F}_{2^n}(t)$.

Theorem (Aubry, Herbaut and Voloch, 2019)

Let $m \geq 7$ be such that $m \equiv 0 \pmod 4$. Then there exists N depending only on m such that for all $n \geq N$, if we set $q = 2^n$ then for all $f \in \mathbb{F}_q[x]$ of degree m, and all $\alpha \in \mathbb{F}_q^*$ such that $\mathbb{F}_q^{\Omega_f} = \mathbb{F}_q$ and $\Omega_f / \mathbb{F}_q(t)$ is separable, we have $\delta(f) = m - 2$.

Contribution of Chebotarev Theorem in our context



How can we compare $\mathrm{Gal}\left(\Omega_f/\mathbb{F}_{2^n}^{\Omega_f}(t)\right)$ and $\mathrm{Gal}\left(\Omega_f/\mathbb{F}_{2^n}(t)\right)$?

Preliminaries

Definition and Proposition (Voloch)

Let $n \in \mathbb{N}$ and let us considerate a polynomial

$$f(x) = \sum_{k=0}^{m} a_{m-k} x^k \in \mathbb{F}_{2^n}[x]$$

of even degree $m \in \mathbb{N}$. For all $\alpha \in \mathbb{F}_{2^n}^*$, there exists a unique polynomial $L_\alpha f$ of degree less than or equal to $\frac{m-2}{2}$ such that

$$L_\alpha f(x^2 + \alpha x) = f(x) + f(x + \alpha).$$

Preliminaries

In even characteristic, following Geyer in an Appendix of Jarden-Razon, we define a Morse polynomial g as:

Definition (Morse polynomials)

A polynomial g is said to be Morse if the three following conditions hold:

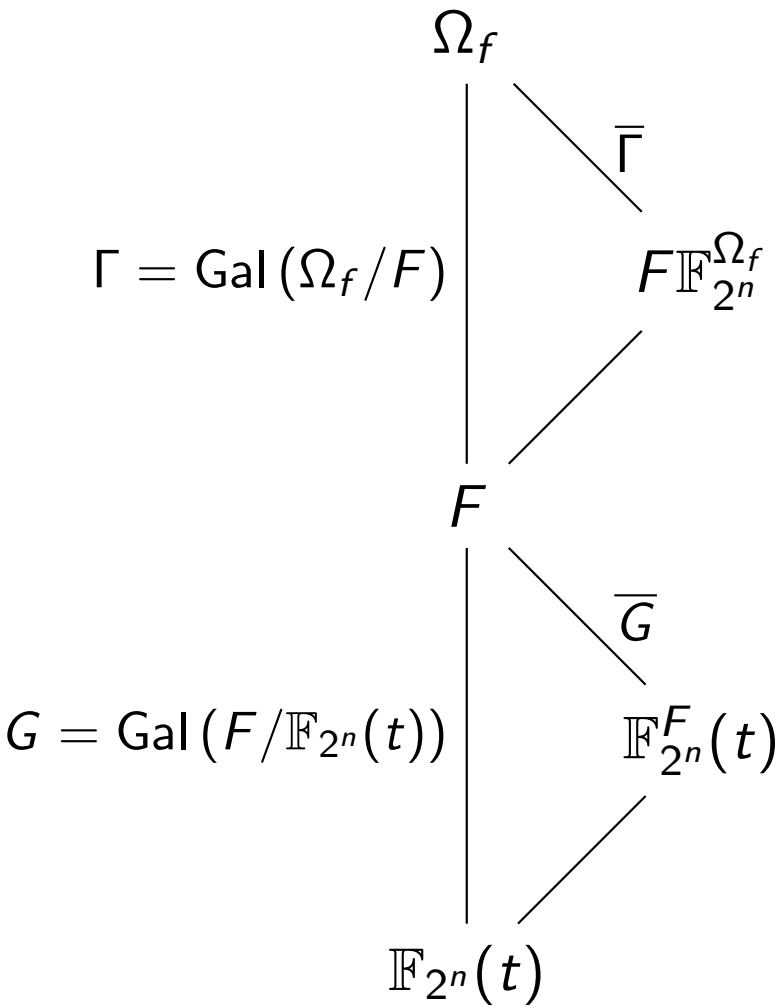
- The critical points of g are non degenerate,i.e $g'(\tau) = 0$ implies that $g^{[2]}(\tau) \neq 0$ where $g^{[2]}$ is the second Hasse-Schmidt derivative,
- the critical values of g are distinct, i.e $(g'(\tau) = g'(\eta) = 0$ and $g(\tau) = g(\eta)) \implies \tau = \eta$,
- the degree of g is prime with the characteristic.

Why we are interested in Morse polynomials?

Why we are interested in Morse polynomials?

f is a Morse polynomial $\xrightarrow{Hilbert-Serre}$ the Galois group of f is the full symmetric group.

Preliminaries



When do we have $F^{\Omega_f} = F$?

$\mathbb{F}_{2^n}^{F} = \mathbb{F}_{2^n}$ and $F/\mathbb{F}_{2^n}(t)$ is separable if

(I.a) $L_\alpha f$ has non-degenerate critical points

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

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

Key Lemma

Lemma (Aubry, Herbaut and Voloch (2019))

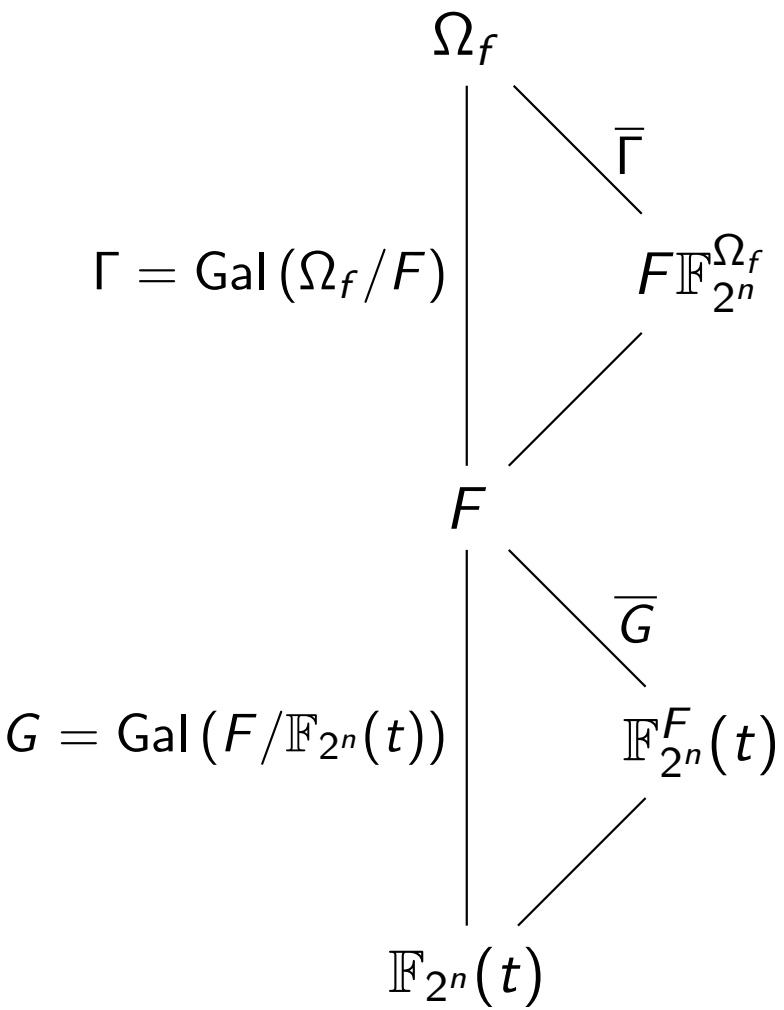
Let $f \in \mathbb{F}_{2^n}[x]$ be a polynomial and $L_\alpha f = \sum_{k=0}^{d} b_{d-k} x^k$ be the associated polynomial of degree less or equal d. If $L_\alpha f$ is Morse and if the equation $x^2 + \alpha x = b_1/b_0$ has a solution in $\mathbb{F}_{2^n}$ then $F^{\Omega_f} = F$.

Key Lemma

Lemma (Aubry, Herbaut and Voloch (2019))

Let $f \in \mathbb{F}_{2^n}[x]$ be a polynomial and $L_\alpha f = \sum_{k=0}^{d} b_{d-k} x^k$ be the associated polynomial of degree less or equal d. 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 $F^{\Omega_f} = F$.

Key theorem



$F^{\Omega_f} = F$ and Ω_f/F is separable as soon as:

$L_\alpha f$ is Morse and when

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

$\mathbb{F}_{2^n}^{F} = \mathbb{F}_{2^n}$ and $F/\mathbb{F}_{2^n}(t)$ is separable if:

(I.a) $L_\alpha f$ has non-degenerate critical points

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

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

Condition (II)

Condition (II)

Condition (II) $\iff$ Trace$(\frac{b_1}{b_0\alpha^2}) = 0$. (Hilbert's theorem 90)

Condition (II)

Condition (II) $\iff$ Trace$(\frac{b_1}{b_0\alpha^2}) = 0$. (Hilbert's theorem 90)

Proposition (Aubry, Herbaut and A.I, 2022)

Let $f = \sum_{i=0}^{m} a_{m-i}x^i \in \mathbb{F}_{2^n}[x]$ be a polynomial of degree m such that $m \equiv 0 \pmod 4$ and $a_1 \neq 0$. Let $L_\alpha f(x) = \sum_{i=0}^{d} b_{d-i}x^i$ be the associated polynomial of degree d. The number of $\alpha \in \mathbb{F}_{2^n}^*$ such that Trace$(\frac{b_1}{b_0\alpha^2}) = 0$ is greater than or equal to $2^{n-1} - 2^{\frac{n}{2}} - 1$.

Condition (I.a)

Condition (I.a)

Proposition (Aubry, Herbaut and A.I, 2022)

Let $m \equiv 0 \pmod 4$ and $f(x) = \sum_{k=0}^{m} a_{m-k} x^k \in \mathbb{F}_{2^n}[x]$ be a polynomial of degree m. The critical points of $L_\alpha f$ are non-degenerate except for at most $(m-1)(m-4)$ values of α in $\mathbb{F}_{2^n}^*$.

Condition (I.b)

Condition (I.b)

Proposition for result 1 (Aubry, Herbaut and A.I, 2022)

Let $m = 2^\ell(2^r + 1)$, where ℓ and r are two integers such that $\gcd(\ell, r) \leq 2, \ell \geq 2$ and $r \geq 1$. Let $L_\alpha f$ be the associated polynomial of degree d. The critical values of $L_\alpha f$ are distinct except for at most $(5d + 4)\binom{(d-1)/2}{2}$ values of $\alpha \in \mathbb{F}_{2^n}^*$.

Proposition for result 2 (Aubry, Herbaut and A.I, 2022)

Let $m \in \mathbb{N}$ be an integer such that $m \equiv 0 \pmod 4$ and $m - 1 \in \mathcal{M}$. For all trinomials $f(x) = a_0x^m + a_1x^{m-1} + a_2x^{m-2} \in \mathbb{F}_{2^n}[x]$ of degree m such that $a_1 \neq 0$, the number of $\alpha \in \mathbb{F}_{2^n}^*$ for which the critical values of $L_\alpha f$ are distinct is at most $(5d + 2)\binom{(d-1)/2}{2}$.

Application

Application

Reminder

The polynomials f with $\delta(f) = 2$, over infinitely many extensions of $\mathbb{F}_{2^n}$ are the so-called exceptional APN polynomials.

Application

Reminder

The polynomials f with $\delta(f) = 2$, over infinitely many extensions of $\mathbb{F}_{2^n}$ are the so-called exceptional APN polynomials.

Conjecture (Aubry, McGuire and Rodier, 2010)

Let $n \in \mathbb{N}^*$. The only exceptional APN polynomials over $\mathbb{F}_{2^n}$ are those which are CCZ equivalent to the monomials $x^{2^\ell+1}$ and $x^{4^\ell-2^\ell+1}$, where $\gcd(\ell, n) = 1$.

Application

Reminder

The polynomials f with $\delta(f) = 2$, over infinitely many extensions of $\mathbb{F}_{2^n}$ are the so-called exceptional APN polynomials.

Conjecture (Aubry, McGuire and Rodier, 2010)

Let $n \in \mathbb{N}^*$. The only exceptional APN polynomials over $\mathbb{F}_{2^n}$ are those which are CCZ equivalent to the monomials $x^{2^\ell+1}$ and $x^{4^\ell-2^\ell+1}$, where $\gcd(\ell, n) = 1$.

Hernando and McGuire (2011) $\rightarrow$ Monomials ✓

Application

Conjecture (Aubry, McGuire and Rodier)

- Odd cases (Aubry, McGuire, Rodier, Delgado,...) ✓
- $m \equiv 2 \pmod 4$ (Aubry, McGuire, Rodier, Bartoli, Schmidt,...) ✓
- $m = 4e$ with $e \equiv 3 \pmod 4$ (Rodier) ✓
- $m = 4e$ with $e \equiv 5 \pmod 8$ (Caullery) ✓
- $m = 4e$ with $e = 2^k + 1$ ×
- $m \equiv 0 \pmod 8$ ×

Application

Conjecture (Aubry, McGuire and Rodier)

- Odd cases (Aubry, McGuire, Rodier, Delgado,...) ✓
- $m \equiv 2 \pmod 4$ (Aubry, McGuire, Rodier, Bartoli, Schmidt,...) ✓
- $m = 4e$ with $e \equiv 3 \pmod 4$ (Rodier) ✓
- $m = 4e$ with $e \equiv 5 \pmod 8$ (Caullery) ✓
- $m = 4e$ with $e = 2^k + 1$ ×
- $m \equiv 0 \pmod 8$ ×

Result 1 allows us to completely treat the case $m = 4(2^k + 1)$.

Application

Conjecture (Aubry, McGuire and Rodier)

- Odd cases (Aubry, McGuire, Rodier, Delgado,...) ✓
- $m \equiv 2 \pmod 4$ (Aubry, McGuire, Rodier, Bartoli, Schmidt,...) ✓
- $m = 4e$ with $e \equiv 3 \pmod 4$ (Rodier) ✓
- $m = 4e$ with $e \equiv 5 \pmod 8$ (Caullery) ✓
- $m = 4e$ with $e = 2^k + 1$ ×
- $m \equiv 0 \pmod 8$ ×

Result 1 allows us to completely treat the case $m = 4(2^k + 1)$.

Result 1 and 2 contribute to the case $m \equiv 0 \pmod 8$.

Thank you for your attention