Complete permutation polynomials of monomial type

Giovanni Zini

(joint works with D. Bartoli, M. Giulietti and L. Quoos)
(based on the work of thesis of E. Franzè)

Università di Perugia

Workshop BunnyTN 7

Trento, 16 novembre 2016

Outline

1. Permutation polynomials: an introduction

Outline

1. Permutation polynomials: an introduction

2. Monomial complete permutation polynomials: our results

Outline

1. Permutation polynomials: an introduction
2. Monomial complete permutation polynomials: our results
3. Particular cases: degree 8 and 9 in characteristic 2 and 3

Some definitions

$\mathbb{F}_\ell$: *finite field with* $\ell = p^h$ *elements*
Plane curve $\mathcal{C}$: $F(X, Y, T) = 0$
$\mathbb{F}_\ell$*-rational point of* $\mathcal{C}$: $P = (x, y, z) \in PG(2, \ell)$ *such that* $F(x, y, z) = 0$

Definition

$f(x) \in \mathbb{F}_\ell[x]$ is a permutation polynomial (shorlty, a PP) of $\mathbb{F}_\ell$ if $x \mapsto f(x)$ is a bijection of $\mathbb{F}_\ell$ (iff $x \mapsto f(x)$ is injective over $\mathbb{F}_\ell$)

Definition

$f(x) \in \mathbb{F}_\ell[x]$ is a complete permutation polynomial (shorlty, a CPP) of $\mathbb{F}_\ell$ if both $f(x)$ and $f(x) + x$ are PPs of $\mathbb{F}_\ell$

Definition

$f(x) \in \mathbb{F}_\ell[x]$ is an exceptional polynomial over $\mathbb{F}_\ell$ if $f(x)$ is a PP of an infinite number of extensions of $\mathbb{F}_\ell$

CPPs and Cryptography

Definition

$f(x) \in \mathbb{F}_\ell[x]$ is a permutation polynomial (shorlty, a PP) of $\mathbb{F}_\ell$ if $x \mapsto f(x)$ is a bijection of $\mathbb{F}_\ell$ (iff $x \mapsto f(x)$ is injective over $\mathbb{F}_\ell$).

$f(x) \in \mathbb{F}_\ell[x]$ is a complete permutation polynomial (shorlty, a CPP) of $\mathbb{F}_\ell$ if both $f(x)$ and $f(x) + x$ are PPs of $\mathbb{F}_\ell$

Definition

$f : \mathbb{F}_2^n \to \mathbb{F}_2$ Boolean function is

- **bent** if $x \mapsto f(x+a) + f(x)$ is balanced $\forall a \in \mathbb{F}_2^n$ ($\Leftrightarrow f$ is PNF)
- **bent-negabent** if both $x \mapsto f(x+a) + f(x)$ and $x \mapsto f(x+a) + f(x) + Tr(ax)$ are balanced $\forall a \in \mathbb{F}_2^n$

LINK:

any PP of $\mathbb{F}_{2^n}$ gives rise to a bent function over $\mathbb{F}_2^n$

any CPP of $\mathbb{F}_{2^n}$ gives rise to a bent-negabent function over $\mathbb{F}_2^n$

Link with curves

$$f(x) \in \mathbb{F}_\ell[x] \qquad \mapsto \qquad \mathcal{C}_f : \frac{f(x) - f(y)}{x - y} = 0$$

$f(x)$ *is a PP of* $\mathbb{F}_\ell \implies \mathcal{C}_f$ *has no affine* $\mathbb{F}_\ell$*-rational points* (a, b) *with* $a \neq b$

Link with curves

$$f(x) \in \mathbb{F}_\ell[x] \qquad \mapsto \qquad \mathcal{C}_f : \frac{f(x) - f(y)}{x - y} = 0$$

$f(x)$ *is a PP of* $\mathbb{F}_\ell \Longrightarrow \mathcal{C}_f$ *has no affine* $\mathbb{F}_\ell$*-rational points* (a, b) *with* $a \neq b$

Theorem

$\mathcal{C}$ *absolutely irreducible curve of degree* d *defined over* $\mathbb{F}_\ell$
The number N_ℓ *of* $\mathbb{F}_\ell$*-rational points satisfies*

$$N_\ell \geq \ell + 1 - (d - 1)(d - 2)\sqrt{\ell}$$

$\Downarrow$

for ℓ *large enough:*
$f(x)$ *is a PP of* $\mathbb{F}_\ell$

$\Downarrow$

$\mathcal{C}_f$ *has no* $\mathbb{F}_\ell$*-rat. abs. irr. components distinct from* $X = Y$

Conversely:

Theorem (Cohen 1970)

$\mathcal{C}_f$ contains no $\mathbb{F}_\ell$-rational abs. irr. component distinct from $X = Y$

$$\Downarrow$$

$f(x)$ is an exceptional polynomial over $\mathbb{F}_\ell$

Conversely:

Theorem (Cohen 1970)

$\mathcal{C}_f$ contains no $\mathbb{F}_\ell$-rational abs. irr. component distinct from $X = Y$

$$\Downarrow$$

$f(x)$ is an exceptional polynomial over $\mathbb{F}_\ell$

It is not difficult to construct PP without any prescribed structure

Remark

$f(x)$ is a PP of $\mathbb{F}_\ell$ $\iff$

$\alpha f(\gamma x + \delta) + \beta$ is a PP of $\mathbb{F}_\ell$ $(\alpha, \beta, \gamma, \delta \in \mathbb{F}_\ell,\ \alpha, \gamma \neq 0)$

PP-equivalence :

$$f(x) \quad \approx \quad \alpha f(\gamma x + \delta) + \beta\,, \quad \alpha, \beta, \gamma, \delta \in \mathbb{F}_\ell\,,\ \alpha, \gamma \neq 0$$

The monomial case

- $b^{-1}x^d$ is a PP of $\mathbb{F}_\ell \iff (d, \ell - 1) = 1$
- $b^{-1}x^d$ is a CPP of $\mathbb{F}_\ell \iff (d, \ell - 1) = 1$ and $x^d + bx$ is a *PP* of $\mathbb{F}_\ell$

The monomial case

- $b^{-1}x^d$ is a PP of $\mathbb{F}_\ell \iff (d, \ell - 1) = 1$
- $b^{-1}x^d$ is a CPP of $\mathbb{F}_\ell \iff (d, \ell - 1) = 1$ and $x^d + bx$ is a *PP* of $\mathbb{F}_\ell$

$f_b(x) = b^{-1}x^{\frac{q^n-1}{q-1}+1}$ *has been studied as CPP of* $\mathbb{F}_{q^n}$ *for* $n = 2, 3, 4$ *and partially for* $n = 6$

The monomial case

- $b^{-1}x^d$ is a PP of $\mathbb{F}_\ell \iff (d, \ell - 1) = 1$
- $b^{-1}x^d$ is a CPP of $\mathbb{F}_\ell \iff (d, \ell - 1) = 1$ and $x^d + bx$ is a *PP* of $\mathbb{F}_\ell$

$f_b(x) = b^{-1}x^{\frac{q^n-1}{q-1}+1}$ has been studied as CPP of $\mathbb{F}_{q^n}$ for $n = 2, 3, 4$ and partially for $n = 6$

EXPLICIT LIST of all $b \in \mathbb{F}_{q^n}$ such that f_b is a CPP of $\mathbb{F}_{q^n}$, in the cases:

- *$n = 7$, for arbitrary q* (E. Franzè, Master Thesis)
- *$n = 6$, for arbitrary q* (Bartoli-Giulietti-Z., FFA 2016)

The monomial case

- $b^{-1}x^d$ is a PP of $\mathbb{F}_\ell \iff (d, \ell-1) = 1$
- $b^{-1}x^d$ is a CPP of $\mathbb{F}_\ell \iff (d, \ell-1) = 1$ and $x^d + bx$ is a *PP* of $\mathbb{F}_\ell$

$f_b(x) = b^{-1}x^{\frac{q^n-1}{q-1}+1}$ *has been studied as CPP of* $\mathbb{F}_{q^n}$ *for* $n = 2, 3, 4$ *and partially for* $n = 6$

EXPLICIT LIST of all $b \in \mathbb{F}_{q^n}$ *such that* f_b *is a CPP of* $\mathbb{F}_{q^n}$*, in the cases:*

- $n = 7$*, for arbitrary* q (E. Franzè, Master Thesis)
- $n = 6$*, for arbitrary* q (Bartoli-Giulietti-Z., FFA 2016)

Conjecture (Wu-Li-Helleseth-Zhang 2015)

If $n+1$ *is prime,* $n+1 \neq p$, $\gcd(n+1, q^2-1) = 1$*, then:*

there exist CPPs of $\mathbb{F}_{q^n}$ *of type* $b^{-1}x^{\frac{q^n-1}{q-1}+1}$

The monomial case

- $b^{-1}x^d$ is a PP of $\mathbb{F}_\ell \iff (d, \ell - 1) = 1$
- $b^{-1}x^d$ is a CPP of $\mathbb{F}_\ell \iff (d, \ell - 1) = 1$ and $x^d + bx$ is a *PP* of $\mathbb{F}_\ell$

$f_b(x) = b^{-1}x^{\frac{q^n-1}{q-1}+1}$ has been studied as CPP of $\mathbb{F}_{q^n}$ for $n = 2, 3, 4$ and partially for $n = 6$

GOAL : to characterize for any n the $b \in \mathbb{F}_{q^n}$ such that $f_b = b^{-1}x^{\frac{q^n-1}{q-1}+1}$ is a CPP of $\mathbb{F}_{q^n}$

The monomial case

- $b^{-1}x^d$ is a PP of $\mathbb{F}_\ell \iff (d, \ell - 1) = 1$
- $b^{-1}x^d$ is a CPP of $\mathbb{F}_\ell \iff (d, \ell - 1) = 1$ and $x^d + bx$ is a *PP* of $\mathbb{F}_\ell$

$f_b(x) = b^{-1}x^{\frac{q^n-1}{q-1}+1}$ has been studied as CPP of $\mathbb{F}_{q^n}$ for $n = 2, 3, 4$ and partially for $n = 6$

GOAL : to characterize for any n the $b \in \mathbb{F}_{q^n}$ such that $f_b = b^{-1}x^{\frac{q^n-1}{q-1}+1}$ is a CPP of $\mathbb{F}_{q^n}$

WE OBTAIN : complete classification for $n^4 < q = p^m$ with the exception of the cases

- $n + 1 = p^r$, *with* $r > 1$
- $n + 1 = p^r(p^r - 1)/2$, *with* $p \in \{2, 3\}$, $r > 1$, $\gcd(r, 2m) = 1$

$$b \in \mathbb{F}_{q^n} \Longrightarrow A_i(b) := \sum_{0 \le j_1 < j_2 < \ldots < j_i \le n-1} b^{q^{j_1} + q^{j_2} + \ldots + q^{j_i}} \in \mathbb{F}_q$$

i-th elementary symmetrical polynomial in $b, b^q, \ldots, b^{q^{n-1}}$

$$b \in \mathbb{F}_{q^n} \Longrightarrow A_i(b) := \sum_{0 \le j_1 < j_2 < \ldots < j_i \le n-1} b^{q^{j_1} + q^{j_2} + \ldots + q^{j_i}} \in \mathbb{F}_q$$

i-th elementary symmetrical polynomial in $b, b^q, \ldots, b^{q^{n-1}}$

Proposition (Wu-Li-Helleseth-Zhang 2013)

If $n^4 < q$, *then:*

$b^{-1} x^{\frac{q^n-1}{q-1}+1}$ *is a CPP of* $\mathbb{F}_{q^n}$ $\iff$ $\gcd(n+1, q-1) = 1$, $x^{n+1} + A_1(b)x^n + \cdots + A_n(b)x$ *is an exceptional polynomial over* $\mathbb{F}_q$

$$b \in \mathbb{F}_{q^n} \Longrightarrow A_i(b) := \sum_{0 \le j_1 < j_2 < \ldots < j_i \le n-1} b^{q^{j_1} + q^{j_2} + \ldots + q^{j_i}} \in \mathbb{F}_q$$

i-th elementary symmetrical polynomial in $b, b^q, \ldots, b^{q^{n-1}}$

Proposition (Wu-Li-Helleseth-Zhang 2013)

If $n^4 < q$, *then:*

$b^{-1} x^{\frac{q^n-1}{q-1}+1}$ *is a CPP of* $\mathbb{F}_{q^n}$ $\iff$ $\gcd(n+1, q-1) = 1$, $x^{n+1} + A_1(b)x^n + \cdots + A_n(b)x$ *is an exceptional polynomial over* $\mathbb{F}_q$

Remark

$b^{-1} x^{\frac{q^n-1}{q-1}+1}$ *is a CPP of* $\mathbb{F}_{q^n}$ $\iff$ $b^{-q^i} x^{\frac{q^n-1}{q-1}+1}$ *is a CPP of* $\mathbb{F}_{q^n}$

Proposition (Wu-Li-Helleseth-Zhang 2013)

If $n^4 < q$, then:

$b^{-1}x^{\frac{q^n-1}{q-1}+1}$ *is a CPP of* $\mathbb{F}_{q^n}$ $\iff$ $\gcd(n+1, q-1) = 1$, $x^{n+1} + A_1(b)x^n + \cdots + A_n(b)x$ *is an exceptional polynomial over* $\mathbb{F}_q$

Definition

Let

$$g(x) = x^{n+1} + \lambda_1 x^n + \cdots \lambda_{n-1}x^2 + \lambda_n x \in \mathbb{F}_q[x],\ \lambda_n \neq 0\,,$$

be a PP of $\mathbb{F}_q$.

$g(x)$ is good if the roots of

$$v_g(x) := \frac{g(-x)}{-x} = x^n - \lambda_1 x^{n-1} + \cdots + (-1)^{n-1}\lambda_{n-1}x + (-1)^n\lambda_n$$

form a unique orbit under the Frobenius map $z \mapsto z^q$.

Proposition

If $n^4 < q$, then:

$b \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$ *is such that* $b^{-1}x^{\frac{q^n-1}{q-1}+1}$ *is a CPP of* $\mathbb{F}_{q^n}$ $\iff$ b *is a root of* $v_g(x) = \frac{g(-x)}{-x}$ *for some* g *good exceptional pol. of degree* $n+1$ *over* $\mathbb{F}_q$ *with* $g(0) = 0$ *and* $g'(0) \neq 0$

Proposition

If $n^4 < q$, then:

$$b \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q \text{ is such that } b^{-1}x^{\frac{q^n-1}{q-1}+1} \text{ is a CPP of } \mathbb{F}_{q^n} \iff b \text{ is a root of } v_g(x) = \frac{g(-x)}{-x} \text{ for some } g \text{ good exceptional pol. of degree } n+1 \text{ over } \mathbb{F}_q \text{ with } g(0)=0 \text{ and } g'(0) \neq 0$$

Definition

An exceptional polynomial g is decomposable if

$$g(x) = g_1(g_2(x)) \text{ with } g_1, g_2 \text{ exceptional pol., } \deg(g_1), \deg(g_2) > 1$$

Proposition

g good exceptional polynomial $\Longrightarrow$ g indecomposable

Idea

In order to classify all CPPs of type $f(x) = b^{-1}x^{\frac{q^n-1}{q-1}+1}$
take all the good indecomposable exceptional polynomials
and determine the roots of $v_g(x)$

Idea

In order to classify all CPPs of type $f(x) = b^{-1}x^{\frac{q^n-1}{q-1}+1}$

take all the good indecomposable exceptional polynomials

and determine the roots of $v_g(x)$

Unfortunately:

the complete classification of indecomposable exceptional polynomials is not known!

Remark

$f(x)$ *is a good PP of* $\mathbb{F}_\ell$ $\Longleftrightarrow$
$\alpha f(\gamma x)+\beta$ *is a good PP of* $\mathbb{F}_\ell$ *($\alpha,\beta,\gamma\in\mathbb{F}_\ell$, $\alpha,\gamma\neq 0$)*

CPP-equivalence :

$$f(x) \quad \approx \quad \alpha f(\gamma x)+\beta\,, \quad \alpha,\beta,\gamma\in\mathbb{F}_\ell\,,\ \alpha,\gamma\neq 0$$

Remark

$f(x)$ *is a good PP of* $\mathbb{F}_\ell \iff$

$\alpha f(\gamma x) + \beta$ *is a good PP of* $\mathbb{F}_\ell$ *(*$\alpha, \beta, \gamma \in \mathbb{F}_\ell$*,* $\alpha, \gamma \neq 0$*)*

CPP-equivalence :

$$f(x) \quad \approx \quad \alpha f(\gamma x) + \beta\,, \quad \alpha, \beta, \gamma \in \mathbb{F}_\ell\,,\, \alpha, \gamma \neq 0$$

$$\Downarrow$$

We use the known partial classification
of indecomposable exceptional polynomial,
up to CPP-equivalence

Classification of indecomposable exceptional polynomials, up to CPP-equivalence

A) $n+1 \nmid q-1$ *is a prime different from* p *and*

- A1) $g(t) = (t+e)^{n+1} - e^{n+1}$, $e \in \mathbb{F}_q$
- A2) $g(t) = D_{n+1}(t+e, a) - D_{n+1}(e, a)$,

  $a, e \in \mathbb{F}_q$, $a \neq 0$, $n+1 \nmid q^2 - 1$

  $D_{n+1}(t, a)$ *Dickson polynomial of degree* $n+1$

B) $n+1 = p$ *and* $g(t) = (t+e)\left((t+e)^{\frac{p-1}{r}} - a\right)^r - e\left(e^{\frac{p-1}{r}} - a\right)^r$

$r \mid p-1$, $a, e \in \mathbb{F}_q$, $a^{r(q-1)/(p-1)} \neq 1$.

C) $n+1 = s(s-1)/2$

$p \in \{2, 3\}$, $q = p^m$, $r > 1$, $s = p^r > 3$ *and* $(r, 2m) = 1$.

D) $n+1 = p^r$ *with* $r > 1$.

Case A1

$n+1$ is prime, $n+1 \neq p$, $n+1$ does not divide $q-1$

$\zeta_{n+1} :=$ $(n+1)$-th primitive root of unity

Proposition

Let $e \in \mathbb{F}_q^*$. *Then*

$$g(t) = (t+e)^{n+1} - e^{n+1} \text{ is good exceptional over } \mathbb{F}_q \iff ord_{n+1}(q) = n$$

If $ord_{n+1}(q) = n$, *then for each* $e \in \mathbb{F}_q^*$ *and* $i \in \{1, \ldots, n\}$

$$\left(e(\zeta_{n+1}^i - 1)\right)^{-1} x^{\frac{q^n-1}{q-1}+1} \quad \text{is a CPP of } \mathbb{F}_{q^n}$$

Case A2

$n+1$ is prime, $n+1 \neq p$, $n+1$ does not divide q^2-1

(Dickson polynomials)

$$D_{n+1}(t,a) = \sum_{k=0}^{n/2} \frac{n+1}{n+1-k} \binom{n+1-k}{k} (-a)^k t^{n+1-2k}$$

Proposition

$g(x) = D_{n+1}(x+e,a) - D_{n+1}(e,a)$, $e, a \in \mathbb{F}_q$, $a \neq 0$, $D'_{n+1}(e,a) \neq 0$, *is good exceptional over* $\mathbb{F}_q$ *if and only if one of the following cases occurs:*

i) $4 \mid n$ *and* $ord_{n+1}(q) = n$

ii) $4 \nmid n$ *and* $\begin{cases} e^2 - 4a \notin \square_q, & ord_{n+1}(q) = n/2 \\ e^2 - 4a \in \square_q, & ord_{n+1}(q) = n \end{cases}$

Case B

$n+1=p$

$\mathbb{N}_{\mathbb{F}_q/\mathbb{F}_p}$: the norm map $\mathbb{F}_q \to \mathbb{F}_p$, $x \mapsto x^{1+p+p^2+\cdots+q/p}$.

Theorem

Let $n^4 < q$. *Then*

$$b^{-1}x^{\frac{q^n-1}{q-1}+1} \text{ is a CPP of } \mathbb{F}_{q^n}$$

$$\Updownarrow$$

for some $r \mid n$, *one of the following cases occurs:*

i) $b \in \{\zeta_{q-1}^i \mid \gcd(r,i)=1\}$

ii) $b \in \{(v_0-\lambda u_0)^r - e \mid \lambda \in \mathbb{F}_p^*,\ e, u_0^{p-1} \in \mathbb{F}_q^*,\ u_0^{\frac{q-1}{r}} \neq 1,$

$$v_0^r = e,\ ord\left(\mathbb{N}_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{u_0^{p-1}}{e^{(p-1)/r}}\right)\right) = p-1\}$$

$n + 1 = 8,\ p = 2$

$F(x) \in \mathbb{F}_q[x]$ monic of degree 8

Proposition

$F(x)$ is good exceptional over $\mathbb{F}_q$ if and only if $F(x) = x^8 + ax^4 + bx^2 + cx$ is additive and $x^7 + ax^3 + bx + c$ is irreducible over $\mathbb{F}_q$.

$n + 1 = 9, \ p = 3$

No classification is known!

When is

$$F(x) = x^9 + A_1x^8 + A_2x^7 + A_3x^6 + A_4x^5 + A_5x^4 + A_6x^3 + A_7x^2 + A_8x$$

good exceptional?

Theorem (Cohen 1970)

$\mathcal{C}_F$ contains no $\mathbb{F}_\ell$-rational component distinct from $X = Y$

$$\Downarrow$$

$F(x)$ is an exceptional polynomial over $\mathbb{F}_\ell$

- Determine when

$$\mathcal{C}_F := \frac{F(x) - F(y)}{x - y} = 0$$

  has only non-rational components (other than $x - y$)
- Study when the roots of $v_F(x)$ are in a unique orbit under Frobenius

$n+1=9,\ p=3$

Proposition

$F(x)$ is good exceptional over $\mathbb{F}_q$ if and only if

i) $F(x) = x^9 + A_6x^3 + A_8x$
and $x^8 + A_6x^2 + A_8$ irreducible over $\mathbb{F}_q$;

ii) $$F(x) = x^9 + A_3x^6 + A_4x^5 + A_5x^4 + \left(A_2^3 + A_3\frac{A_5^3}{A_4^3} + \frac{A_5^2}{A_4}\right)x^3 + \left(2A_3A_4 + 2\frac{A_5^3}{A_4^2}\right)x^2 + \left(2A_3A_5 + A_4^2 + 2\frac{A_5^4}{A_4^3}\right)x,$$

1. $A_4 \neq 0$,
2. *the polynomial $x^8 + 2A_3x^2 + 2A_4 \in \mathbb{F}_q[x]$ has no roots in $\mathbb{F}_{q^4}$;*

iii) $$F(x) = x^9 + A_2x^7 + A_3x^6 + A_5x^4 + \left(A_2^3 + \frac{A_3A_5}{A_2}\right)x^3 + \left(2A_2A_5 + 2\frac{A_3^3}{A_2}\right)x^2 + \left(A_2^4 + A_3A_5 + \frac{A_5^2}{A_2} + \frac{A_3^4}{A_2^2}\right)x,$$

1. *$2A_2$ is not a square in $\mathbb{F}_q$,*
2. *the polynomial $v_F(x) = F(-x)/(-x)$ is irreducible over $\mathbb{F}_q$.*

Thank you for your attention!