MATEMÁTICAS

POLYNOMIALS WITH A RESTRICTED RANGE AND CURVES WITH MANY POINTS

By

César Andrade Ramos & Álvaro Garzón R.[1]

Abstract

Andrade Ramos, C. & A. Garzón R.: Polynomials with a restricted range and curves with many points. Rev. Acad. Colomb. Cienc. **34** (131): 229-239, 2010. ISSN 0370-3908.

In this paper we present new properties of restricted range polynomials to those developed by L. Rédei in ([1]), we exhibit a new method to determine their exponent set and use them to construct curves over finite fields with many rational points.

Key words: Finite fields, $(\mathbb{F}_q, \mathbb{F}_p)$-polynomial, Algebraic Curves, Rational Points.

Resumen

En este artículo presentamos nuevas propiedades de los polinomios de rango restringido a las estudiadas por L. Rédei en ([1]), exhibimos un nuevo método para el computo su conjunto de exponentes y usamos dichos polinomios para construir curvas sobre cuerpos finitos con muuchos puntos racionales.

Palabras clave: Cuerpos Finitos, $(\mathbb{F}_q, \mathbb{F}_p)$-polinomios, curvas algebraicas, puntos racionales.

1. Introduction

Let p be a prime number, $\mathbb{F}_q$ be the finite field with $q = p^n$ elements and let $\overline{\mathbb{F}}_q$ be an algebraic closure of $\mathbb{F}_q$. Given a polynomial $f(x, y) \in \mathbb{F}_q[x, y]$ which is irreducible over $\overline{\mathbb{F}}_q$, the set

$$\mathcal{C}_f = \{(\alpha, \beta) \in \overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q \text{ such that } f(\alpha, \beta) = 0\}$$

[1] Departamento de Matemáticas, Universidad del Valle, Apartado Aéreo 25360, Cali, Colombia E-mail: cesar@univalle.edu.co & alvarogr@univalle.edu.co

AMS Classification 2000: 14G05.

is an affine plane algebraic curve (over the finite field $\mathbb{F}_q$) and the points $P = (\alpha, \beta) \in \mathcal{C}_f$ such that $(\alpha, \beta) \in \mathbb{F}_q \times \mathbb{F}_q$ are called rational points over $\mathbb{F}_q$.

In 1940 **André Weil** proved the Riemann hypothesis for curves over finite fields. As an immediate corollary he obtained an upper bound for the number of rational points on a geometrically irreducible nonsingular curve $\mathcal{C}$ of genus g over a finite field of cardinality q, namely

$$|\mathcal{C}(\mathbb{F}_q)| \leq q + 1 + 2g\sqrt{q}, (*)$$

where $\mathcal{C}(\mathbb{F}_q)$ denotes the set of rational points of the curve $\mathcal{C}$.

The interest of polynomials with a restricted range resides mainly in its applications to the construction of curves over finite fields, such constructions are often performed using special polynomials $p(x) \in \mathbb{F}_q[x]$. The essential properties of $p(x)$ are sometimes of the following form:

Property I. One has that $p(\mathbb{F}_q) \subseteq \mathbb{F}_p$, and for most elements $\alpha \in \mathbb{F}_q$, α is a simple root of $p(x) - p(\alpha)$.

Property II. The set $\Sigma = \left\{\gamma \in \mathbb{F}_q; p(x) - \gamma \text{ has multiple roots in } \mathbb{F}_q\right\}$ has low cardinality, and one has a nice description of the multiplicities of the roots.

Polynomials that satisfy the property I are known as $(\mathbb{F}_q, \mathbb{F}_p)$-polynomials. The goal of this work is consider those introduced by **L. Rédei** in ([1]). We present a different point of view which allows us to prove new properties. (See Sections 2,3,4.)

We use $(\mathbb{F}_q, \mathbb{F}_p)$-polynomials again in Section 5 to construct curves over $\mathbb{F}_q$ with many rational points i.e, the cardinal of the set $\mathcal{C}(\mathbb{F}_q)$ is close to the Weil bound $(*)$.

2. Polynomials with a Restricted Range.

Definition 2.1. A polynomial $f(x) \in \mathbb{F}_q[x]$ is a restricted range polynomial if $f(\alpha) \in V \subsetneq \mathbb{F}_p$ for some proper subset of $\mathbb{F}_p$ and for all $\alpha \in \mathbb{F}_q$. In particular, when $V = \mathbb{F}_p$, we say that $f(x)$ is a $(\mathbb{F}_q, \mathbb{F}_p)$-polynomial.

Remark 2.1. A classical example of restricted range polynomial is the trace polynomial $Tr_{\mathbb{F}_q/\mathbb{F}_p}(x) = x^{p^{m-1}} + \cdots + x^p + x \in \mathbb{F}_q[x]$.

Definition 2.2. A nonzero $(\mathbb{F}_q, \mathbb{F}_p)$-polynomial $f(x) \in \mathbb{F}_q[x]$ will be called minimal, if $\deg(f(x)) \leq q - 1$ and none its proper partial sums is a $(\mathbb{F}_q, \mathbb{F}_p)$-polynomial.

Example 2.1. Let α a root of $f(x) = x^2+x+2 \in \mathbb{F}_3[x]$. Then, the polynomial $h(x) = \alpha^5 x + \alpha^7 x^3 \in \mathbb{F}_9[x]$ is a minimal $(\mathbb{F}_9, \mathbb{F}_3)$-polynomial. In fact, $\deg(h(x)) \leq 8$ and all its partial sums $\alpha^5 x$ and $\alpha^7 x^3$ are not $(\mathbb{F}_9, \mathbb{F}_3)$-polynomials.

The *p-adic development* of a positive integer a is given by

$$a = k_0 + p\, k_1 + p^2 k_2 + \cdots$$

where the *numerals* k_j satisfies $k_j < p$ for all $j = 0, 1, ...$

Let $k_0 + p\, k_1 + p^2 k_2 + \cdots + p^m k_m$, be the p-adic development of a. We will denote by $a^{\sqcap}$the integer number obtained after applying the permutation

$$a^{\sqcap} = k_m + p\, k_0 + p^2 k_1 + \cdots + p^m k_{m-1},$$

and will be called *cyclic numeral permutation*. By $\sqcap^k$ we will understand the iteration k times of the numeral cyclic permutation. The *period* of a is the small natural integer $l(a)$ such that $a^{\sqcap^{l(a)}} = a$.

A *p-cycle* is an ordered set $(a, a^{\sqcap}, a^{\sqcap^2} ..., a^{\sqcap^{l(a)-1}})$.

The process of determining the p-cycles in the set $I_{q-1} = \{1, 2, \ldots, q-1\}$ play such an important role in this work, that we present in detail some properties related to these cycles as well as the form of determining them.

Let $G = \langle\sigma\rangle$ be a cyclic group of order n. The group G acts on the set I_{q-1} as follows

$$\begin{aligned} \rho : G \times I_{q-1} &\to I_{q-1} \\ (\sigma^k, i) &\mapsto (p^k \cdot i)_{q-1}, \quad k = 0, 1, \ldots, n-1 \end{aligned}$$

where, $(a)_{q-1}$ is the residual class a modulus $q-1$.

Theorem 2.1. *For each $i \in I_{q-1}$, the p-cycle $(i, i^{\sqcap}, i^{\sqcap^2} ..., i^{\sqcap^{l(i)-1}})$, is the orbit of i with respect to the action ρ above.*

Proof: Let us suppose that $i \in \{0, 1, ..., q-1\}$ has p-adic development

$$i = i_0 + i_1 p + i_2 p^2 + \cdots + i_{n-1} p^{n-1},$$

then

$$i^{\sqcap} = i_{n-1} + i_0 p + i_1 p^2 + \cdots + i_{n-2} p^{n-1}.$$

Therefore, we have that

$$\begin{aligned} pi - i^{\sqcap} &= i_0 p + i_1 p^2 + \cdots + i_{n-1} p^n - \\ &\qquad (i_{m-1} + i_0 p + i_1 p^2 + \cdots + i_{n-2} p^{n-1}) \\ &= i_{n-1}(q-1) \end{aligned}$$

and in consequence $i^{\sqcap} \equiv pi \pmod{(q-1)}$. □

Corollary 2.1. *If $q = p^n$ and $\Im = (a_1, a_2, \ldots, a_{l(\Im)})$ is a p-cycle, then $l(\Im)|n$.*

Proof: It is known ([7], II,4.3) that, if G acts on a set S, then $G_x = \{g \in G | \, g \cdot x = x\}$ is a subgroup of G and the cardinal number of the orbit $\bar{x} = \{g \cdot x | \, g \in G\}$ of x, is $(G : G_x)$, the index of G_x in G. □

Proposition 2.1. *Every p-cycle has the form*

$$\Im = (i, pi, \ldots, p^k i, (p^{k+1} i)_{q-1}, \ldots, (p^\ell i)_{q-1})$$

where $\ell + 1$ is the length of $\Im$ and $k \geq 0$ is the smallest integer satisfying $p^k i < q - 1 \leq p^{k+1} i$.

Proof: Since

$$p^{k+j} i = r(q-1) + (p^{k+j} i)_{q-1},$$

then

$$p^{k+j+1} i = p(p^{k+j} i) = (rp+m)(q-1) + (p(p^{k+j} i)_{q-1})_{q-1} \tag{1}$$

where

$$p(p^{k+j} i)_{q-1} = m(q-1) + (p(p^{k+j} i)_{q-1})_{q-1}. \tag{2}$$

This implies

$$(p^{k+j+1} i)_{q-1} = (p(p^{k+j} i)_{q-1})_{q-1}. \tag{3}$$

□

Definition 2.3. An integer i, generates the p-cycle $\Im$, if

$$\Im = (i, pi, \ldots, p^k i, (p^{k+1} i)_{q-1}, \ldots, (p^\ell i)_{q-1})$$

and $i < (p^{k+j} i)_{q-1}$ for $j = 1, \ldots, \ell - k$.

Example 2.2. The set $\{3, 6, 5\}$ is a 2-cycle of period 3, generated by 3. In fact, since

$$3 = 2^0 \cdot 1 + 2^1 \cdot 1 + 2^2 \cdot 0$$

$$6 = 2^0 \cdot 0 + 2^1 \cdot 1 + 2^2 \cdot 1$$

$$5 = 2^0 \cdot 1 + 2^1 \cdot 0 + 2^2 \cdot 1$$

we have $3^{\sqcap} = 6$, $6^{\sqcap} = 5$ and $5^{\sqcap} = 3$.

Example 2.3. In the following table we exhibit the different p-cycles for $p = 2, 3, 5$ and $q = p^n$ for some values of n.

$p = 2$		
$q = 16$	(15)	
	$(5, 10)$	
	$(1, 2, 4, 8)$	$(3, 6, 12, 9)$
	$(7, 14, 13, 11)$.	
$q = 64$	(63)	
	$(21, 42)$	
	$(9, 18, 36)$	$(27, 54, 45)$
	$(1, 2, 4, 8, 16, 32)$	$(3, 6, 12, 24, 48, 33)$
	$(5, 10, 20, 40, 17, 34)$	$(7, 14, 28, 56, 49, 35)$
	$(11, 22, 44, 25, 50, 37)$	$(13, 26, 52, 41, 19, 38)$
	$(15, 30, 60, 57, 51, 39)$	$(23, 46, 29, 5843, 53)$
	$(31, 62, 65, 59, 55, 47)$	
$p = 3$		
$q = 27$	(13)	(26)
	$(1, 3, 9)$	$(2, 6, 18)$
	$(4, 12, 10)$	$(5, 15, 19)$
	$(7, 21, 11)$	$(8, 24, 20)$
	$(14, 16, 22)$	$(17, 25, 23)$
$q = 81$		
	(40)	(80)
	$(10, 30)$	$(20, 60)$
	$(50, 70)$	
	$(1, 3, 9, 27)$	$(2, 6, 18, 54)$
	$(4, 12, 36, 28)$	$(5, 15, 45, 55)$
	$(7, 21, 63, 29)$	$(8, 24, 72, 56)$
	$(11, 33, 19, 57)$	$(13, 39, 37, 31)$
	$(14, 42, 46, 58)$	$(16, 4864, 32)$
	$(17, 51, 73, 59)$	$(22, 66, 38, 34)$
	$(23, 69, 47, 61)$	$(25, 75, 65, 35)$
	$(26, 78, 74, 62)$	$(41, 43, 49, 67)$
	$(44, 52, 76, 68)$	$(53, 79, 77, 71)$
$p = 5$		
$q = 25$	(6)	(12)
	(18)	(24)
	$(1, 5)$	$(2, 10)$
	$(3, 15)$	$(4, 20)$
	$(7, 11)$	$(8, 16)$
	$(9, 21)$	$(13, 17)$
	$(14, 22)$	$(19, 23)$

Definition 2.4. The $p-$*adic weigth* i_p of a number i is the bigger of the numerals present in their p-adic development.

The p-adic weight of a set A is the maximum of the set of p-adic weights of elements of A. Particularly we will denote by f°_p} the p-adic weight of the exponent set of the polynomial $f(x)$ which we will call the p-ádic weight of $f(x)$.

Definition 2.5. A polynomial $f(x) \in \mathbb{F}[x]$ will be called a p-polynomial if their exponent set $\epsilon(f)$ satisfies

$$\epsilon(f) \subseteq \{0, 1, p, p+1, p^2, \ldots, p^2+p+1, p^3, \ldots, \\ p^3+p^2+p+1, \ldots\}$$

Definition 2.6. A polynomial $f(x) \in \mathbb{F}[x]$ will be called p-linear if $f^{\circ_p} = 1$.

In accordance with (2.6) in later sections, we will be interested in determining those polynomials $f(x) \in \mathbb{F}[x]$ whose exponent set $\epsilon(f)$ has weight one, that is, we want to determine those elements $i \in I_{q-1}$, such that $i_p = 1$. By theorem (2.1) and proposition (2.1) will suffice to determine those elements that generate p-cycles of weight one. Firstly observe that we have $2^n - 1$ elements of I_{q-1} of weight one. We will proceed as follows: Let us denote by R_n the quotient ring

$$R_n := \mathbb{F}_2[x]/\langle x^n+1\rangle$$

and by I^1_{q-1} the subset of I_{q-1} containing all elements of weight one. Then we have the following bijections

$$I^1_{q-1} \leftrightarrow \mathbb{F}_2^n \setminus 0 \leftrightarrow R_n$$

$$i = i_0 + \cdots + i_{n-1}p^{n-1} \mapsto (i_0, \cdots, i_{n-1}) \\ \mapsto f_i(x) = \sum_{k=0}^{n-1} i_k x^k$$

with $f_i(p) = i$.

If $j \in I^1_{q-1}$ and $f_j(0) = 0$, then there exist $f_\ell(x) \in R_n$ such that $f_j(x) = x^r f_\ell(x)$ with $f_\ell(0) = 1$, this means that $j = p^r \ell$ where $\ell = f_\ell(p)$.

Now, we are interested in determining all elements $i \in I_{q-1}$ such that $i \equiv 1 (\text{mod } p)$, equivalently, those polynomials $f(x) \in R_n$ such that $f(0) = 1$. This reduces our search to analyze $2^{n-1} - 2$ elements in R_n.

However, there exist polynomials $f(x) \in R_n$ such that $f(0) = 1$ but the element $f(p) \in I_{q-1}$ does not generates p-cycles.

For example, for $f(x) = x^3 + x^2 + 1 \in R_4$ with $p = 3$, $f(3) = 37$, but 37 does not generate a 3-cycle, in fact $37 \in (13, 31, 37, 39)$ which is generated by 13. This occurs because the polynomial $f(x) = x^3 + x^2 + 1$ can be seen as $x^3 g(x)$ with $g(x) = x^3 + x + 1$ and $g(3) = 13$.

More generally, if we denote by H the cyclic group $\{1, x, \ldots, x^{n-1}\}$, then we define an action of H over R_n as follows

$$\tau : H \times R_n \to R_n \\ (x^k, f(x)) \mapsto x^k \cdot f(x).$$

This action leads us to introduce the following terminology. If

$$f(x) = x^m + x^{m-j_1} + x^{m-j_2} + \ldots + x^{m-j_r} + 1 \in R_n$$

with $1 \le j_1 < j_2 < \ldots < j_r \le m-1$ and $m \le n-1$, we will say that $f(x)$ can be factored if there exist j_ℓ such that

$$\begin{aligned} f(x) &= x^m + x^{m-j_1} + \ldots + x^{m-j_\ell} + x^{n+m-j_{\ell+1}} \\ &\qquad + \ldots + x^{n+m-j_r} + x^n \\ &= x^{m-j_\ell}\left(x^{j_\ell} + \ldots + x^{j_\ell - j_{\ell-1}} + 1 + x^{n+j_\ell-j_{\ell+1}}\right. \\ &\qquad \left. + \ldots + x^{n-m+j_\ell}\right) \end{aligned}$$

and $n + j_\ell - j_{\ell+1} < m$ or $n + j_\ell - j_{\ell+1} = m$ and $n + j_\ell - j_{\ell+2} < m - j_1$ or $n + j_\ell - j_{\ell+1} = m$, $n + j_\ell - j_{\ell+2} = m - j_1$ and $n + j_\ell - j_{\ell+3} < m - j_3$ and so on.

If such j_ℓ doesn't exist, then we say that $f(x)$ cannot be factored, case in which $f(p)$ generates a p-cycle of weight one.

Observe that to say "that $f(x)$ can be factored", really means that $f(x)$ belongs to the orbit of some element of R_n.

Now we want to determine all polynomials $f(x) \in R_n$ such that $f(0) = 1$ that cannot be factored. Unfortunately to determine all the non factor bled polynomials is a very difficult task. The following lemmas give an approach to the solution of this problem.

Lemma 2.1. *$f(x) \in R_n$ with $f(0) = 1$ and $deg(f) \le n/2$ cannot be factored.*

Proof: Let $f(x) = x^m + x^{m-j_1} + x^{m-j_2} + \ldots + x^{m-j_r} + 1$ with $1 \le j_1 < j_2 < \ldots < j_r \le m-1$ and $m \le n/2$. If there exist j_ℓ such that

$$\begin{aligned} f(x) &= x^{m-j_\ell}\left(x^{j_\ell} + \ldots + x^{j_\ell-j_{\ell-1}} + 1 + x^{n+j_\ell-j_{\ell+1}}\right. \\ &\qquad \left. + \ldots + x^{n-m+j_\ell}\right) = x^{m-j_\ell} g(x), \end{aligned}$$

then we have

$$\begin{aligned} \deg(g(x)) &= n + j_\ell - j_{\ell+1} \ge m + m + j_\ell - j_{\ell+1} > m \\ &= \deg(f(x)). \end{aligned}$$ □

Lemma 2.2. *Let $f(x) = x^m + x^{m-j_1} + x^{m-j_2} + \ldots + x^{m-j_r} + 1 \in R_n$ with $1 \leq j_1 < j_2 < \ldots < j_r \leq m-1$ and $m = n-k$. If there exist $\ell \in \{0, 1, \ldots, r\}$ (here $j_0 = 0$) such that $j_\ell - j_{\ell-1} > k$ then $f(x)$ can be factored.*

Proof: Observe that $f(x)$ can be write as

$$f(x) = x^m + x^{m-j_1} + x^{m-j_2} + \ldots + x^{m-j_{\ell-1}} + x^{n+m-j_\ell} + \ldots + x^{n+m-j_r} + x^n\,;$$

therefore

$$f(x) = x^{m-j_{\ell-1}} g(x)$$

with

$$g(x) = x^{j_{\ell-1}} + \ldots + 1 + x^{n-j_\ell+j_{\ell-1}} + x^{n-j_{\ell+1}+j_{\ell-1}} + \ldots + x^{n-m+j_{\ell-1}}$$

and $\deg(g(x)) = n - j_\ell + j_{\ell-1} < n-k$. □

Corollary 2.2. *Let $f(x) \in R_n$ with $deg(f(x)) = n-1$ and $f(0) = 1$. Then $f(x)$ can be factored if and only if $f(x) \neq x^{n-1} + x^{n-2} + \ldots + x^2 + x + 1$.*

Proof: Since $f(x) \neq x^{n-1} + x^{n-2} + \ldots + x^2 + x + 1$, there exist j_ℓ such that $j_\ell - j_{\ell-1} > 1$, then the corollary follows by lemma (2.2). □

Corollary 2.3. *The polynomial $f(x) = x^m + x^{m-1} + \ldots + x + 1$ with $m \leq n-1$ cannot be factored.*

Proof: For all $1 \leq k \leq m-1$, the polynomial

$$x^k + x^{k-1} + \ldots + 1 + x^{n-1} + \ldots + x^{n+1-m+k} + x^{n-m+k}$$

has degree $n-1 > m$. □

Corollary 2.4. *The polynomial $f(x) = x^m + 1$ with $m \leq n-1$ can be factored if and only if $2m > n$.*

Proof: It is clear since $f(x) = x^m(1 + x^{n-m})$. □

Example 2.4. As an illustration we will exhibit all the generating elements of cycles of weight one for $n = 4, 5$ and $p = 2, 3$. For $n = 4$, by lemma (2.1) and by corollary (2.2) the polynomials

$$\begin{array}{ll} f_1(x) = x^2 + x + 1 & f_4(x) = 1 \\ f_2(x) = x^2 + 1 & f_5(x) = x^3 + x^2 + x + 1 \\ f_3(x) = x + 1 & \end{array}$$

cannot be factored, therefore each one of $f_i(p)$ generates cycles of weight one, then for $p = 2$ we have that the elements $\{7, 5, 3, 1, 15\}$ generate the cycles in I_{15}, for $p = 3$ the generating elements are $\{13, 10, 4, 1, 40\}$. For $n = 5$ by lemma(2.1) the polynomials

$$\begin{array}{ll} f_1(x) = x^2 + x + 1 & f_3(x) = x + 1 \\ f_2(x) = x^2 + 1 & f_4(x) = 1 \end{array}$$

cannot be factored. By corollary (2.2), all the polynomials of degree 4 except the polynomial $f_5(x) = x^4 + x^3 + x^2 + x + 1$ can be factored. Finally, analyzing the polynomials of degree 3 we have, by (2.3) that $f_6(x) = x^3 + x^2 + x + 1$ cannot be factored, by (2.2) $f_7(x) = x^3 + x + 1$ neither and neither the polynomial $x^3 + 1$ by (2.4)can be factored. Then remains only to analyze $x^3 + x^2 + 1$ but $x^3 + x^2 + 1 = x^2(x^3 + x + 1)$. Then for $p = 2$ the generating elements are $\{7, 5, 3, 1, 31, 15, 11\}$ and for $p = 3$ we have the set $\{13, 10, 4, 1, 121, 40, 31\}$

3. Characterization of restricted range polynomials

In this section we give a characterization of restricted range polynomials, for which initially we exhibit some properties of $(\mathbb{F}_q, \mathbb{F}_p)$-polynomials and finally in the example (3.1), we calculate explicitly all the $(\mathbb{F}_{16}, \mathbb{F}_2)$-polynomials.

Proposition 3.1. *([1]) $f(x) \in \mathbb{F}_q[x]$ is a $(\mathbb{F}_q, \mathbb{F}_p)$-polynomial if and only if*

$$x^q - x \mid f(x)^p - f(x)$$

Proof: If $f(x)$ is a $(\mathbb{F}_q, \mathbb{F}_p)$-polynomial, then $f(\gamma) \in \mathbb{F}_p$ for all $\gamma \in \mathbb{F}_q$, therefore $f(\gamma)^p = f(\gamma)$ for all $\gamma \in \mathbb{F}_q$. If we denote by $g(x) = f(x)^p - f(x)$ then $g(\gamma) = 0$ for all $\gamma \in \mathbb{F}_q$ and therefore $x^q - x \mid g(x)$. Conversely, if $x^q - x \mid f(x)^p - f(x) = g(x)$, since all root of $x^q - x$ is a root of $g(x)$, we have $g(\gamma) = 0$ for all $\gamma \in \mathbb{F}_q$ then $f(\gamma)^p = f(\gamma)$ for all $\gamma \in \mathbb{F}_q$ hence $f(\gamma) \in \mathbb{F}_p$ for all $\gamma \in \mathbb{F}_q$ from which we conclude that $f(x)$ is a $(\mathbb{F}_q, \mathbb{F}_p)$-polynomial. □

Proposition 3.2. *$(\mathbb{F}_q, \mathbb{F}_p)$-polynomials are surjective.*

Proof: Let $q = p^n$, $f : \mathbb{F}_q \to \mathbb{F}_p$ be the polynomial application induced by $f(x)$ and suppose that there exist $\alpha \in \mathbb{F}_p \setminus \mathrm{Im}(f)$. Let $\{u_1, \ldots, u_t\}$ be the set of different zeros of $(\mathbb{F}_q, \mathbb{F}_p)$-polynomial $\Phi_\alpha(x) := f(x) - \alpha$, then there exist a finite extension, $\mathbb{F}_{q^m}/\mathbb{F}_q$ where the polynomial $\Phi_\alpha(x)$ decomposes completely, therefore $\mathbb{F}_{q^m} = \mathbb{F}_q(u_1, \ldots, u_t)$. Now by (3.1), there exist a polynomial $h(x) \in \mathbb{F}_q[x]$ such that

$$\Phi_\alpha^p(x) - \Phi_\alpha(x) = (x^q - x)h(x)$$

and since $u_i \notin \mathbb{F}_q$, $\Phi_\alpha(u_i) = 0$ implies that $h(u_i) = 0$. Consequently, again by (3.1), $f^p(u_i) - f(u_i) = 0$ that is $f(x)$ is a $(\mathbb{F}_{q^m}, \mathbb{F}_p)$-polynomial. On the other hand, since

$$\deg(f(x)) \leq p^n - 1 \text{ and } f^p(x) - f(x) = (x^{q^m} - x)h(x)$$

then

$$p \cdot \deg(f(x)) = q^m + \deg(h(x)) \geq q^m = p^{n \cdot m}\,;$$

therefore

$$p^{n \cdot m} \leq \deg(f(x)) \leq p^n - 1,$$

and this is a contradiction. □

Since one of our goals is to know in detail the set of exponents of a $(\mathbb{F}_q, \mathbb{F}_p)$-polynomial of $\mathbb{F}_q[x]$, we shall concentrate on analyzing the behavior of their coefficients. The next statement is a first approximation to this objective.

Theorem 3.1. ([1]) *A polynomial $f(x) = \sum_{i=0}^{q-1} \alpha_i x^i \in \mathbb{F}_q[x]$ is a $(\mathbb{F}_q, \mathbb{F}_p)$-polynomial if and only if their coefficients satisfy the following conditions*

$$\alpha_j = \alpha_i^p j \equiv pi(mod(q - 1)) \; for \; i, j = 0, ..., q-2\,,$$
$$\alpha_{q-1} = \alpha_{q-1}^p\,. \tag{4}$$

□

Next statement allows us to rewrite the result equations (4) of the pass theorem through the use of the cyclic permutation $\sqcap$.

Proposition 3.3. ([1]) *The conditions of conjugation in* (4) *can be write as follows*

$$\alpha_{i^{\sqcap}} = \alpha_i^p\,,\; i = 0, \ldots, q-1 \tag{5}$$

Proof: Follows from the proofs of theorem (2.1) and theorem (3.1). □

Now, we are in condition of characterizing all $(\mathbb{F}_q, \mathbb{F}_p)$-polynomial. More precisely we have.

Theorem 3.2. ([1]) (Characterization of $(\mathbb{F}_q, \mathbb{F}_p)$-polynomials) *The exponent sets of the minimal $(\mathbb{F}_q, \mathbb{F}_p)$-polynomials are the p-cycles of set $\{0, ..., q-1\}$. For each p-cycle $\Im$ all the minimal $(\mathbb{F}_q, \mathbb{F}_p)$-polynomials with exponent set $\Im$ are*

$$f_{\Im}(x, \alpha) = \sum_{k=0}^{o(\Im)-1} \alpha^{p^k} x^{i^{\sqcap^k}}\;,\; \alpha \in \mathbb{F}^*_{p^{o(\Im)}}$$

where i is an arbitrary but fixed representative of $\Im$. In addition we have all the different $(\mathbb{F}_q, \mathbb{F}_p)$-polynomials of less or equal degree to $q-1$ by sums of polynomials $f_{\Im}(x, \alpha)$ corresponding to different cycles.

Proof: Let $f(x) = \sum_{i=0}^{q-1} \alpha_i\, x^i$ a $(\mathbb{F}_q, \mathbb{F}_p)$-polynomial with $f^{\circ} \leq q-1$ where the coefficients $\alpha_0, ..., \alpha_{q-1}$ are all the solutions of system

$$S : \alpha_{i^{\sqcap}} = \alpha_i^p\,,\; i = 0, \ldots, q-1.$$

For a cycle $\Im$ we shall denote by $S_{\Im}$ the subsystem of S consisting of the equations

$$\alpha_{i^{\sqcap}} = \alpha_i^p\,,\; i \in \Im.$$

Since $i^{\sqcap} \in \Im$, coefficients $\alpha_0, ..., \alpha_{q-1}$ present in $S_{\Im}$ are those with subscript in $\Im$ (i. e. the subsystems $S_{\Im}$ are independent from each other). By induction, $S_{\Im}$ is equivalent to the infinite system of equations

$$\alpha_{i^{\sqcap^k} = \alpha_i^{p^k}}\,,\; i \in \Im\,,\; k = 1, 2, \ldots.$$

Then, taking i fixed for $k = l_p(i) = o(\Im)$ have that

$$\alpha_{i^{\sqcap^k}} = \alpha_i\,.$$

Therefore

$$\alpha_i \in \mathbb{F}_{p^k} = \mathbb{F}_{p^{o(\Im)}}\,. \tag{6}$$

Conversely, if we have (5) it is enough to have the system of equations $\alpha_{i^{\sqcap^k}} = \alpha_i^{pk}$ with $i \in \Im$ fixed for the values $k = 1, ..., o(\Im) - 1$ and this equations can be considered as the explicit solution formulas of system $S_{\Im}$, where all the unknowns are in terms of α_i that are related with the condition $\alpha_i \in \mathbb{F}_{p^{O(\Im)}}$, then all $(\mathbb{F}_q, \mathbb{F}_p)$-polynomial are writen in the form

$$f(x) = \sum_{\Im \subseteq \{0, \ldots, q-1\}} \sum_{k=0}^{o(\Im)-1} \alpha_i^{p^k} x^{i^{\sqcap^k}}\,.$$

□

Remark 3.1. Observe that in the proof of theorem (3.2) each cycle $\Im$ has associated a system of equations $S_{\Im}$ whose solution leads us precisely to determinate the coefficients of the minimal $(\mathbb{F}_q, \mathbb{F}_p)$-polynomials. One of such solutions is the trivial solution $\alpha_i^{\sqcap^k} = 1$. The following result gives us an easy way to determine those $(\mathbb{F}_q, \mathbb{F}_p)$-polynomials such that $\alpha_i = 1$. Before stating the result we need to establish some notation: If $f(x) \in \mathbb{F}_q[x]$, then we will denote by

$$\mathcal{R}_{x^q - x}(f(x))$$

the remainder of the Euclidean division of the polynomial $f(x)$ by $x^q - x$.

Theorem 3.3. *With above notations. Let $a(x) = x^{p^{n-1}} + \ldots + x$ be the trace polynomial corresponding to the extension $\mathbb{F}_q/\mathbb{F}_p$, $i \in I_{q-1}$ and $\Im$ the p-cycle generated by i. If* length$(\Im) = n$, *then*

$$\mathcal{R}_{x^q - x}(a(x^i))$$

is the minimal $(\mathbb{F}_q, \mathbb{F}_p)$-polynomial corresponding to the p-cycle $\Im$.

Proof: We claim, that for all $f(x) \in \mathbb{F}_p[x]$ the polynomial $\mathcal{R}_{x^q-x}(a(f(x)))$ is a $(\mathbb{F}_q, \mathbb{F}_p)$-polynomial. In fact, by (3.1) it is enough to prove that

$$x^q - x | \mathcal{R}_{x^q-x}(a(f(x)))^p - \mathcal{R}_{x^q-x}(a(f(x))) .$$

Since

$$a(f(x)) = (x^q - x)h(x) + \mathcal{R}_\ell(a(f(x))) ,$$

for some polynomial $h(x) \in \mathbb{F}_p[x]$, then

$$\begin{aligned}\mathcal{R}_\ell(a(f(x)))^p - \mathcal{R}_\ell(a(f(x))) = a(f(x))^p \\ - (x^q - x)^p \cdot h(x)^p - a(f(x)) \\ + (x^q - x) \cdot (x),\end{aligned}$$

and since $f(x) \in \mathbb{F}_p[x]$ and $a(T)$ is an additive polynomial, the claim follows. On the other hand it is easy to see that $\mathcal{R}_{x^q-x}(x^{p^\ell i}) = x^{(p^\ell i)_{q-1}}$ and therefore

$$\begin{aligned}a(x^i) &= \sum_{\ell=0}^{n-1} x^{p^\ell i} = \sum_{\ell=0}^{n-1} \left[(x^q - x) \cdot h_i(x) + \mathcal{R}_{x^q-x}(x^{p^\ell i})\right] \\ &= \sum_{\ell=0}^{n-1} (x^q - x) \cdot h_i(x) + \sum_{\ell=0}^{n-1} x^{(p^\ell i)_{q-1}}\end{aligned}$$

Now by proposition (2.1) and comparing coefficients we have the result. □

The next proposition allows us to easily determine the non trivial solutions of the system of equations $S_{\Im}$.

Proposition 3.4. *Let $q = p^n$, $\Im_1, \ldots \Im_r$ be the different p-cycles of length $d|n$ and γ a group-primitive element of $\mathbb{F}_q$. Then, for each $1 \le t \le r$, the set*

$$\left\{\gamma^{i}, \gamma^{i^{p}}, \ldots, \gamma^{i^{p^{l(\Im_t)-1}}}\right\}$$

is a non trivial solution of system of equations:

$$S_{\Im_j} := \alpha_{i^{p^k}} = \alpha_i^{p^k} , \ i \in \Im_j , \ k = 1, 2, \ldots, l(\Im_j).$$

More over if $\Gamma = \left\{\gamma^{i}, \gamma^{i^{p}}, \ldots, \gamma^{i^{p^{l(\Im_t)-1}}}\right\}$ is solution of $S_{\Im_j}$ then

$$\Gamma^{p} := \left\{\gamma^{i^{p^{l(\Im_t)-1}}}, \gamma^{i}, \gamma^{i^{p}}, \ldots, \gamma^{i^{p^{l(\Im_t)-2}}}\right\}$$

is a solution as well.

Proof: Follows from theorem (2.1). □

As an illustration of the previous theorem we will construct some examples of $(\mathbb{F}_q, \mathbb{F}_p)$-polynomials.

Example 3.1. Let $p = 2$, $q = 16$ and $f(x) = x^4+x+1 \in \mathbb{F}_2[x]$. If γ is a root of $f(x)$ then γ is a group-primitive element, that is, γ generates the cyclic group $\mathbb{F}_{16}^*$. By example (2.3) the 2-cycles in the set $\{0, 1, 2, ..., 15\}$ are

$$\varphi_1 = \{1, 2, 4, 8\} , \varphi_2 = \{3, 6, 12, 9\} , \varphi_3 = \{7, 14, 13, 11\}$$
$$\varphi_4 = \{5, 10\} , \varphi_5 = \{15\} , \varphi_6 = \{0\} .$$

Now, with the equations $\alpha_{i^p} = \alpha_i^p$ and φ_1 we have the system

$$S_1 : \quad \alpha_2 = \alpha_1^2 , \alpha_4 = \alpha_2^2 , \alpha_8 = \alpha_4^2 , \alpha_1 = \alpha_8^2 .$$

whose solution sets are

α_1	γ	γ^2	γ^4	γ^8	γ^3	γ^6	γ^{12}	γ^9	γ^7	γ^{14}	γ^{13}	γ^{11}
α_2	γ^2	γ^4	γ^8	γ	γ^6	γ^{12}	γ^9	γ^3	γ^{14}	γ^{13}	γ^{11}	γ^7
α_4	γ^4	γ^8	γ	γ^2	γ^{12}	γ^9	γ^3	γ^6	γ^{13}	γ^{11}	γ^7	γ^{14}
α_8	γ^8	γ	γ^2	γ^4	γ^9	γ^3	γ^6	γ^{12}	γ^{11}	γ^7	γ^{14}	γ^{13}

and whose the polynomials are

$$\begin{array}{ll}
\gamma x + \gamma^2 x^2 + \gamma^4 x^4 + \gamma^8 x^8 & \gamma^2 x + \gamma^4 x^2 + \gamma^8 x^4 + \gamma x^8 \\
\gamma^4 x + \gamma^8 x^2 + \gamma x^4 + \gamma^2 x^8 & \gamma^8 x + \gamma x^2 + \gamma^2 x^4 + \gamma^4 x^8 \\
\gamma^3 x + \gamma^6 x^2 + \gamma^{12} x^4 + \gamma^9 x^8 & \gamma^6 x + \gamma^{12} x^2 + \gamma^9 x^4 + \gamma^3 x^8 \\
\gamma^{12} x + \gamma^9 x^2 + \gamma^3 x^4 + \gamma^6 x^8 & \gamma^9 x + \gamma^3 x^2 + \gamma^6 x^4 + \gamma^{12} x^8 \\
\gamma^7 x + \gamma^{14} x^2 + \gamma^{13} x^4 + \gamma^{11} x^8 & \gamma^{14} x + \gamma^{13} x^2 + \gamma^{11} x^4 + \gamma^7 x^8 \\
\gamma^{13} x + \gamma^{11} x^2 + \gamma^7 x^4 + \gamma^{14} x^8 & \gamma^{11} x + \gamma^7 x^2 + \gamma^{14} x^4 + \gamma^{13} x^8 .
\end{array}$$

If we take now φ_2 to have the system $S_2 :$ $\quad \alpha_6 = \alpha_3^2 , \ \alpha_{12} = \alpha_6^2 , \ \alpha_9 = \alpha_{12}^2 , \ \alpha_3 = \alpha_9^2$ which solution sets

α_3	γ	γ^2	γ^4	γ^8	γ^3	γ^6	γ^9	γ^{12}	γ^7	γ^{11}	γ^{13}	γ^{14}
α_6	γ^2	γ^4	γ^8	γ	γ^6	γ^{12}	γ^3	γ^9	γ^{14}	γ^7	γ^{11}	γ^{13}
α_9	γ^8	γ	γ^2	γ^4	γ^9	γ^3	γ^{12}	γ^6	γ^{11}	γ^{13}	γ^{14}	γ^7
α_{12}	γ^4	γ^8	γ	γ^2	γ^{12}	γ^9	γ^6	γ^3	γ^{13}	γ^{14}	γ^7	γ^{11}

which generate the polynomials

$$\begin{array}{ll}
\gamma x^3+\gamma^2x^6+\gamma^8x^9+\gamma^4x^{12} & \gamma^2x^3+\gamma^4x^6+\gamma x^9+\gamma^8x^{12}\\
\gamma^4x^3+\gamma^8x^6+\gamma^2x^9+\gamma x^{12} & \gamma^8x^3+\gamma x^6+\gamma^4x^9+\gamma^2x^{12}\\
\gamma^3x^3+\gamma^6x^6+\gamma^9x^9+\gamma^{12}x^{12} & \gamma^6x^3+\gamma^{12}x^6+\gamma^3x^9+\gamma^9x^{12}\\
\gamma^9x^3+\gamma^3x^6+\gamma^{12}x^9+\gamma^6x^{12} & \gamma^{12}x^3+\gamma^9x^6+\gamma^6x^9+\gamma^3x^{12}\\
\gamma^7x^3+\gamma^{14}x^6+\gamma^{11}x^9+\gamma^{13}x^{12} & \gamma^{11}x^3+\gamma^7x^6+\gamma^{13}x^9+\gamma^{14}x^{12}\\
\gamma^{13}x^3+\gamma^{11}x^6+\gamma^{14}x^9+\gamma^7x^{12} & \gamma^{14}x^3+\gamma^{13}x^6+\gamma^7x^9+\gamma^{11}x^{12}.
\end{array}$$

Last, take the set φ_3 to have the system

$$S_3: \quad \alpha_{14}=\alpha_7^2 \qquad \alpha_{13}=\alpha_{14}^2 \qquad \alpha_{11}=\alpha_{13}^2 \qquad \alpha_7=\alpha_{11}^2$$

which solution sets

α_7	γ	γ^2	γ^4	γ^8	γ^3	γ^6	γ^9	γ^{12}	γ^7	γ^{11}	γ^{13}	γ^{14}
α_{11}	γ^8	γ	γ^2	γ^4	γ^9	γ^3	γ^{12}	γ^6	γ^{11}	γ^{13}	γ^{14}	γ^7
α_{13}	γ^4	γ^8	γ	γ^2	γ^{12}	γ^9	γ^6	γ^3	γ^{13}	γ^{14}	γ^7	γ^{11}
α_{14}	γ^2	γ^4	γ^8	γ	γ^6	γ^{12}	γ^3	γ^9	γ^{14}	γ^7	γ^{11}	γ^{13}

They provide the polynomials

$$\begin{array}{ll}
\gamma x^7+\gamma^8x^{11}+\gamma^4x^{13}+\gamma^2x^{14} & \gamma^2x^7+\gamma x^{11}+\gamma^8x^{13}+\gamma^4x^{14}\\
\gamma^4x^7+\gamma^2x^{11}+\gamma x^{13}+\gamma^8x^{14} & \gamma^8x^7+\gamma^4x^{11}+\gamma^2x^{13}+\gamma x^{14}\\
\gamma^3x^7+\gamma^9x^{11}+\gamma^{12}x^{13}+\gamma^6x^{14} & \gamma^6x^7+\gamma^3x^{11}+\gamma^9x^{13}+\gamma^{12}x^{14}\\
\gamma^9x^7+\gamma^{12}x^{11}+\gamma^6x^{13}+\gamma^3x^{14} & \gamma^{12}x^7+\gamma^6x^{11}+\gamma^3x^{13}+\gamma^9x^{14}\\
\gamma^7x^7+\gamma^{11}x^{11}+\gamma^{13}x^{13}+\gamma^{14}x^{14} & \gamma^{11}x^7+\gamma^{13}x^{11}+\gamma^{14}x^{13}+\gamma^7x^{14}\\
\gamma^{13}x^7+\gamma^{14}x^{11}+\gamma^7x^{13}+\gamma^{11}x^{14} & \gamma^{14}x^7+\gamma^7x^{11}+\gamma^{11}x^{13}+\gamma^{13}x^{14}.
\end{array}$$

4. Stem Polynomials.

The present section is dedicated to the study of a particular class of $(\mathbb{F}_q,\mathbb{F}_p)$-polynomials: the Stem polynomials, we also show additional properties to the already displayed for restricted range polynomials.

Definition 4.1. A polynomial $f(x)\in\mathbb{F}_q[x]$ is a *Stem* polynomial for $p\mid_1 q$ if

$$f^\circ=\frac{q-1}{p-1}\ ,\ f^{\circ_p}=1,\ ,\ x^q-x\mid f(x)^p-f(x).$$

In accordance with definition (4.1) the Stem polynomials are p-linear and restricted range polynomials.

Example 4.1. Let $p=3, q=3^2=9$ and α a root of the irreducible polynomial $x^2+x+2\in\mathbb{F}_3[x]$. The polynomial

$$h(x)=x^4+\alpha^6x^3+\alpha^2x+2\in\mathbb{F}_9[x]$$

is a Stem polynomial. Indeed, observe that

$$4=3^0\cdot1+3^1\cdot1$$

$$3=3^0\cdot0+3^1\cdot1$$

$$1=3^0\cdot1+3^1\cdot0$$

then $h^{\circ_p}=1$ and also $\dfrac{9-1}{3-1}=4$. From other side

$$\begin{aligned}
h(x)^3-h(x)&=(x^4+\alpha^6x^3+\alpha^2x+2)^3\\
&\quad-(x^4+\alpha^6x^3+\alpha^2x+2)\\
&=x^{12}+\alpha^{18}x^9+\alpha^6x^3+8\\
&\quad-(x^4+\alpha^6x^3+\alpha^2x+2)\\
&=x^{12}+\alpha^2x^9-x^4-\alpha^2x\\
&=(x^3+\alpha^2)(x^9-x).
\end{aligned}$$

Note that examining divisibility in the previous example we have that $h(x)^3-h(x)=(x^3+\alpha^2)(x^9-x)=h'(x)(x^9-x)$. This fact is not casual, more precisely we have next proposition.

Proposition 4.1. *If $f(x)\in\mathbb{F}_q[x]$ is a Stem polynomial, then*

$$f(x)^p-f(x)=(x^q-x)f'(x).$$

Proof: By (3.2) and (2.1) exist $\Im_1, \ldots \Im_t$ p-cycles in I_{q-1} such that $f(x)$ is the sum of polynomials of type

$$\sum_{k=0}^{o(\Im_j)-1} \alpha^{p^k} x^{(p^k i_j)_{q-1}}, \alpha \in \mathbb{F}^*_{p^{o(\Im_j)}}.$$

where $\Im_j$ is a p-cycle of length $\ell_j + 1$ generate by i_j.

We can assume without loss of generality, that there exist a p-cycle $\Im \subseteq I_{q-1}$ generate by i of length $\ell + 1$ such that

$$f(x) = \sum_{k=0}^{\ell} \alpha^{p^k} x^{(p^k i)_{q-1}}, \ \alpha \in \mathbb{F}^*_{p^{\ell+1}},$$

as a consequence,

$$f(x)^p - f(x) = \sum_{k=0}^{\ell-k} \alpha^{p^{k+j+1}} \left(x^{p(p^{k+j} i)_{q-1}} - x^{(p^{k+j+1} i)_{q-1}} \right)$$

with k as in the proposition (2.1). Now, the term

$$\alpha^{p^{k+j+1}} \left(x^{p(p^{k+j} i)_{q-1}} - x^{(p^{k+j+1})_{q-1}} \right) \qquad (7)$$

of $f(x)^p - f(x)$ can be factored as

$$\begin{aligned} &\alpha^{p^{k+j+1}} x^{p^{k+j+1}-(rp+m)(q-1)-1} \\ &\quad \times (x^q - x) \left(x^{(q-1)(m-1)} + \ldots + x^{q-1} + 1 \right), \end{aligned} \qquad (8)$$

equality which shows that $(x^q - x) \,|\, f(x)^p - f(x)$. By hypothesis $\Im$ is generated by an element $i \in I_{q-1}$ of weight 1. We can assume now that i not is trivial, that is $i \neq p^{n-1} + \ldots + p + 1$ and that k, the minor integer such that $p^k i < q - 1 \leq p^{k+1} i$, not is null. Since $p^{k+j} i$ have weight 1 for all $j = 1, \ldots, \ell - k$ then

$$\begin{aligned} q - 1 < p^{k+j} i &\leq p^{n-1} + p^{n-2} + \ldots + p \\ &< p^n + p^{n-1} + p^{n-2} + \ldots + p; \end{aligned}$$

therefore

$$\begin{aligned} p^{k+j} i &< p^n - 1 + p^{n-1} + \ldots + p - 1 \\ &= (q-1) + (p^{n-1} + p^{n-2} + \ldots + p - 1), \end{aligned}$$

thus

$$(p^{k+j} i)_{q-1} \leq p^{n-1} + \ldots + p - 1 < p^{n-1} + \ldots + p$$

like this

$$p(p^{k+j} i)_{q-1} < (q-1) + (p^{n-1} + \ldots + p^2 + 1).$$

This implies that the value of m in equation (2) is 1 and therefore equation (8) is expressed as

$$\alpha^{p^{k+j+1}} x^{p^{k+j+1}-(rp)(q-1)-1} (x^q - x). \qquad (9)$$

Finally it is enough to observe that in agreement with equations (1) and (3)

$$p^{k+j+1} - (rp)(q-1) - 1 = (p^{k+j+1})_{q-1} - 1.$$

And this proof that (9) is exactly the derivative of (7) □

Remark 4.1. In the proof of theorem (4.1) we have a factorization of any $(\mathbb{F}_q, \mathbb{F}_p)$ polynomial which is more precise that the one obtained in theorem (3.1).

In next example we construct systematically all Stem polynomials in $\mathbb{F}_3$.

Example 4.2. Let $p = 3, q = p^2 = 9$ and θ root of polynomial $p(x) = x^2 + x + 2$. Since $p(x)$ is irreducible in $\mathbb{F}_3$ and $ord(\theta)$ in $\mathbb{F}_9^*$ is 8, then θ is a *group-primitive* element, that is, θ generates $\mathbb{F}_9^*$. More precisely

$$\mathbb{F}_9 = \{0, 1 = \theta^8, 2 = \theta^4, \theta, \theta^2, \theta^3, \theta^5, \theta^6, \theta^7\}.$$

Now, since $\dfrac{q-1}{p-1} = \dfrac{p^2-1}{p-1} = p + 1$ then the Stem polynomials in $\mathbb{F}_3$ are of degree 4.

In addition note that Stem polynomials are $(\mathbb{F}_q, \mathbb{F}_p)$-polynomials, thus a first step for his construction should be guided by theorem (3.2), that is, a Stem polynomial is in general a sum of $(\mathbb{F}_9, \mathbb{F}_3)$-polynomials which are induced by 3-cycles of weight one. According with the example (2.3) we have two weight one cycles in I_8 namely (4) and (1, 3) which induce $(\mathbb{F}_9, \mathbb{F}_3)$-polynomials x^4 and $\lambda^3\, x^3 + \lambda\, x + \beta$ with $\lambda \in \mathbb{F}_9$ and $\beta \in \mathbb{F}_3$. Then the general form of the polynomials is given by the expression

$$f(x) = x^4 + \lambda^3\, x^3 + \lambda\, x + \beta.$$

From which a total of 27 Stem polynomials are obtained. We consign them in next table:

Stem Polynomials in $\mathbb{F}_9[x]$	
Polynomial	Factorization in $\mathbb{F}_9[x]$
x^4	x^4
x^4+1	$(x-\theta)(x-\theta^3)(x-\theta^5)(x-\theta^7)$
x^4+2	$(x+1)(x+2)(x-\theta^2)(x-\theta^6)$
x^4+x^3+x	$x(x+2)(x-\theta^5)(x-\theta^7)$
x^4+x^3+x+1	$(x+1)^4$
x^4+x^3+x+2	$(x-\theta^2)(x-\theta^6)(x-\theta)(x-\theta^3)$
x^4+2x^3+2x	$x(x+1)(x-\theta)(x-\theta^3)$
x^4+2x^3+2x+1	$(x+2)^4$
x^4+2x^3+2x+2	$(x-\theta^2)(x-\theta^6)(x-\theta^5)(x-\theta^7)$
$x^4+\theta^3x^3+\theta x$	$x(x-1)(x-\theta^2)(x-\theta^3)$
$x^4+\theta^3x^3+\theta x+1$	$(x-2)(x-\theta)(x+\theta)(x-\theta^6)$
$x^4+\theta^3x^3+\theta x+2$	$(x-\theta^7)^4$
$x^4+\theta^6x^3+\theta^2x$	$x(x-\theta^3)(x-\theta^5)(x-\theta^6)$
$x^4+\theta^6x^3+\theta^2x+1$	$(x-\theta^2)^4$
$x^4+\theta^6x^3+\theta^2x+2$	$(x-1)(x-2)(x-\theta)(x-\theta^7)$
$x^4+\theta x^3+\theta^3x$	$x(x-1)(x-\theta)(x-\theta^6)$

Stem Polynomials in $\mathbb{F}_9[x]$	
Polynomial	Factorization in $\mathbb{F}_9[x]$
$x^4+\theta x^3+\theta^3x+1$	$(x-2)(x-\theta^2)(x-\theta^3)(x-\theta^7)$
$x^4+\theta x^3+\theta^3x+2$	$(x-\theta^5)^4$
$x^4+\theta^7x^3+\theta^5x$	$x(x-2)(x-\theta^6)(x-\theta^7)$
$x^4+\theta^7x^3+\theta^5x+1$	$(x-1)(x-\theta)(x-\theta^2)(x-\theta^5)$
$x^4+\theta^7x^3+\theta^5x+2$	$(x-\theta^3)^4$
$x^4+\theta^2x^3+\theta^6x$	$x(x-\theta)(x-\theta^2)(x-\theta^7)$
$x^4+\theta^2x^3+\theta^6x+1$	$(x-\theta^6)^4$
$x^4+\theta^2x^3+\theta^6x+2$	$(x-1)(x-2)(x-\theta^3)(x-\theta^5)$
$x^4+\theta^5x^3+\theta^7x$	$x(x-2)(x-\theta^2)(x-\theta^5)$
$x^4+\theta^5x^3+\theta^7x+1$	$(x-1)(x-\theta^3)(x-\theta^6)(x-\theta^7)$
$x^4+\theta^5x^3+\theta^7x+2$	$(x-\theta)^4$

Remark 4.2. In accordance with the previous table we could expect that the Stem polynomials have all roots in $\mathbb{F}_q$. Unfortunately in general this is not true, for example for $p = 3$ and $n = 5$ the 3-cycle $(4, 12, 36, 108, 82)$ have 3-adic weight 1, nevertheless the polynomial $f(x) = x^4 + x^{12} + x^{36} + x^{82} + x^{108} + x^{121}$ is a Stem polynomial with three zeros of multiplicity three in $\mathbb{F}_{27}$ and six zeros of multiplicity three in $\mathbb{F}_{729}$

5. An Application: Curves with many Rational Points over Finite Fields

There are many methods used for the construction of curves with many rational points, however, some these methods do not provides explicit equations of curves. The interest for obtaining explicit equations is that one of the main applications of these curves with many points is the construction of good codes ([4]), i.e., codes with goods parameters. This requires having an equation that describes the curve. Among the methods used to construct them are via Kummer extensions, Artin-Schreirer extensions and Abelian elementray p extensions. We will give a brief explanation of why we expect that $(\mathbb{F}_q, \mathbb{F}_p)$-polynomials allow us obtain goods curves.

Let $g(x)$ be a $(\mathbb{F}_q, \mathbb{F}_p)$-polynomial. By Proposition (3.2) there exist $\gamma \in \mathbb{F}_p$, such that polynomial $\ell(x) = g(x) - \gamma$ has at least $\deg(g(x))$ roots in $\mathbb{F}_q$.

Now if we take a polynomial $f(x) \in \mathbb{F}_q[x]$ such that $\mathrm{GCD}(f(x), \ell(x)) = 1$, then by the division algorithm there exist polynomials

$$f(x) = \ell(x)h(x) + \mathcal{R}_\ell(f(x))$$

with $\deg(\mathcal{R}_\ell(f(x))) < \deg(\ell(x))$. Then the rational function

$$\mu(x) := \frac{f(x)}{\mathcal{R}_\ell(f(x))}$$

takes the value one in the set $\Omega_\ell := \{\alpha \in \mathbb{F}_q | \ell(\alpha) = 0\} = \{\alpha \in \mathbb{F}_q | f(\alpha) = \gamma\}$. Therefore if $r | q-1$, then we have at least $r \cdot \deg(g(x))$ points $P = (\alpha, \beta) \in \mathbb{F}_q \times \mathbb{F}_q$ such that $\beta^r = \mu(\alpha) = 1$. Curves of this type were considered in ([2]).

On the other hand, since for all $\alpha \in \mathbb{F}_q$, $g(\alpha) \in \mathbb{F}_p$ then the equation

$$Tr_{\mathbb{F}_q/\mathbb{F}_p}(y) = y^{p^{n-1}} + \ldots + y^p + y = g(\alpha)$$

has p^{n-1} solutions in $\mathbb{F}_q$, therefore we have $p^{n-1} \cdot q$ points $P := (\beta, g(\alpha))) \in \mathbb{F}_q \times \mathbb{F}_q$ such that $Tr_{\mathbb{F}_q/\mathbb{F}_p}(\beta) = g(\alpha)$.

Finally, since the trace function $Tr_{\mathbb{F}_q/\mathbb{F}_p}$ is surjective, then if we choose a suitable $(\mathbb{F}_q, \mathbb{F}_p)$-polynomial $g(x)$ such that $\mathrm{GCD}(g(x), Tr_{\mathbb{F}_q/\mathbb{F}_p}(x)) = h(x) \neq 1$, we have that $\deg(h(x)) \geq 1$ and therefore for all elements $\alpha \in \mathbb{F}_q$ such that $h(\alpha) = 0$ we have p elements $\beta \in \mathbb{F}_q$ such that $\beta^p - \beta = \alpha$.

The above discussion leads us to try to construct curves over the finite field $\mathbb{F}_q$ defined by three types of equations, namely:

$$\text{(I)} \quad y^r = \mu(x) := \frac{f(x)}{\mathcal{R}_\ell(f(x))} \qquad r | q-1$$

$$\text{(II)} \quad Tr_{\mathbb{F}_q/\mathbb{F}_p}(y) = y^{p^{n-1}} + \ldots + y^p + y = g(x)$$

$$\text{(III)} \quad y^p - y = x$$

Constructions of type (I) will be called Constructions via Kummer Extensions, type (II) Abelian elementary p extensions, and of type (III) Artin-Schreirer extensions.

5.1. **Examples.** In this section we exhibit some examples of curves with goods parameters in whose construction we used $(\mathbb{F}_q, \mathbb{F}_p)$-polynomials

Example 5.1. In this example we will construct a curve $\mathbb{C}$ over $\mathbb{F}_9$ with genus $g(\mathcal{C}) = 5$ and 32 rational points. Let us to consider the Stem polynomial $\ell(x) = x^4 + \theta^7 x^2 + \theta^2$ and $f(x) = x^4 + \theta^7 x^2$ with θ as in the example (4.2), then $\mathcal{R}_\ell(f(x)) = -\theta^2$, and therefore

$$\mu(x) = \frac{f(x)}{\mathcal{R}_\ell(f(x))} = \frac{x^2(x^2+\theta^7)}{-\theta^2}$$

Now since $-\theta^2 = \theta^6$ and $(\theta^6)^{-1} = \theta^2$, then $\mu(x) = \theta^2 x^2 (x^2 + \theta^7)$. Now, if we consider the function fields $\mathbb{F}_9(x, y)/\mathbb{F}_9$ defined by the Kummer's equation

$$y^8 = \mu(x) = \theta^2 x^2 (x^2 + \theta^7)$$

we have that the induced curve $\mathbb{C}$ has genus $g(C) = 5$ and 32 rational points. This is the best value known for $(q, g) = (9, 5)$ in [3].

Example 5.2. Here we are going to construct a curve $\mathbb{C}$ over the finite field $\mathbb{F}_{32}$ having genus $g(C) = 60$ and 513 rational points, this number is very close to the Ihara's bound, see ([5]).

Let us to consider the Stem polynomial $s(x) = \theta x^5 + \theta^2 x^{10} + \theta^4 x^{20} + \theta^8 x^9 + \theta^{16} x^{18}$ with θ a root of the irreducible polynomial $g(x) = x^5 + x^2 + 1$. Then the Abelian elementary 2 extension given by the equation

$$\begin{aligned} y^{16} + y^8 + y^4 + y^2 + y &= s(x) \\ &= \theta x^5 + \theta^2 x^{10} + \theta^4 x^{20} + \theta^8 x^9 + \theta^{16} x^{18} \end{aligned}$$

defines a function field over the finite field $\mathbb{F}_{32}$ whose genus is 60 and the number of rational places is 513.

References

[1] **L. Rédei**, *Lacunary polymials over finite fields*, North-Holland, Amsterdam (1973).

[2] **A. Garcia and A. Garzón**, *On Kummer Covers whith many Points* J.P.A.A. **185** (2003), 177–192

[3] **G. van der Geer & M. van der Vlugt**, *Tables for the function $N_q(g)$*, available at http://www.wins.uva.nl/ geer.

[4] **V. D. Goppa**, *Codes on algebraic curves*. Sov. Math. Dokl. **24** (1981), pp. 170–172.

[5] **Y. Ihara**,*Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Tokyo **28** (1981), 721–724.

[6] **H. Stichtenoth**, *Algebraic Function Fields and Codes*, Springer–Verlag, Berlin, 1993.

[7] **T. Hungerford**, *Algebra*, Springer–Verlag, Berlin, 1974.

Recibido el 4 de noviembre de 2009

Aceptado para su publicación el 21 de agosto de 2010