Mathematical Problems of Computer Science 31, 5–15, 2008.

On a Class of Irreducible Polynomials Over $\mathcal{F}_p$

Melsik K. Kyuregyan, Edita Yu. Harutyunyan and Mikayel G. Evoyan†

Institute for Informatics and Automation Problems of NAS of RA
†Faculty of Informatics and Applied Mathematics, Yerevan State University
email: edita@ipia.sci.am, email:michael.ipm@gmail.com

Abstract

The paper presents some results regarding constructive theory of synthesis of irreducible polynomials of degree pt over $\mathcal{F}_p$ from the given primitive elements in $\mathcal{F}_p$, where p is an odd prime and t is an integer whose prime factors all divide $p-1$.

1 Introduction

Let $\mathcal{F}_q$ be the Galois field of order $q = p^s$, where p is a prime, s is a natural number, and $\mathcal{F}_q^*$ be its multiplicative group. Recall that the set $\mathcal{F}_q^*$ of nonzero elements of $\mathcal{F}_q$ forms a cyclic group under multiplication. Any generator of this group is called a primitive element of $\mathcal{F}_q$, and a polynomial $f(x) \in \mathcal{F}_q[x]$ of degree $n \geq 1$ is then called a primitive polynomial over $\mathcal{F}_q$ if it is the minimal polynomial over $\mathcal{F}_q$ of a primitive element of $\mathcal{F}_{q^n}$.

The problem of explicitly constructing irreducible polynomials over finite fields is of particular importance in the theory of irreducible polynomials. The main result of the paper consists in giving a general concept of explicitly constructing sequences of irreducible polynomials of degree pt over $\mathcal{F}_p$ from given primitive elements in $\mathcal{F}_p$, where p is an odd prime and t is an integer whose prime factors all divide $p-1$.

2 Preliminaries

Varhamov's operator L^θ, whose domain of definition is $\mathcal{F}_q[x]$, is defined as follows: Denote by $L^\theta f(x)$ the expression

$$L^\theta f(x) = \sum_{u=0}^{n} a_u (\theta(x))^{q^u - 1} = F(x) \tag{1}$$

or

$$L^\theta f(x) = \frac{1}{\theta(x)} \sum_{u=0}^{n} \sum_{v=0}^{m} a_u \theta_v x^{vq^u}, \tag{2}$$

where $f(x) = \sum_{u=0}^{n} a_u x^u$ and $\theta(x) = \sum_{v=0}^{m} \theta_v x^v$, $a_u, \theta_v \in \mathcal{F}_q$, $\theta(x) \neq const$.

We shall now introduce some properties of $L^\theta f(x)$ derived by Varshamov in [3] with no proofs however. In this paper these known results will be given along with their proofs which will naturally provide more validity to the overall assessment.

- **Linearity.** *For any two polynomials* $f(x) = \sum_{u=0}^{n} a_u x^u$ *and* $g(x) = \sum_{u=0}^{k} b_u x^u$ *from the ring* $\mathcal{F}_q[x]$ *and* $\alpha, \beta \in \mathcal{F}_q$ *the equality*

$$L^\theta(\alpha f(x) + \beta g(x)) = \alpha L^\theta f(x) + \beta L^\theta g(x).$$

is true.

Proof. Indeed, since

$$\begin{aligned} L^\theta(\alpha f(x) + \beta g(x)) &= \frac{1}{\theta(x)} \sum_{u=0}^{\max(n,k)} (\alpha a_u + \beta b_u)(\theta(x))^{q^u} = \\ &= \alpha \frac{1}{\theta(x)} \sum_{u=0}^{n} a_u (\theta(x))^{q^u} + \beta \frac{1}{\theta(x)} \sum_{u=0}^{k} b_u (\theta(x))^{q^u} = \\ &= \alpha L^\theta f(x) + \beta L^\theta g(x). \end{aligned}$$

- **Multiplicativity.** *For any function* $f(x)$ *over the field* $\mathcal{F}_q$ *the equality*

$$L^\theta f(x) = L^\theta r(x) L^{\theta L^\theta r(x)} h(x), \tag{3}$$

where $f(x) = r(x)h(x)$ *holds.* Substituting $f(x) = r(x)h(x)$ where $r(x) = \sum_{i=0}^{r} r_i x^i$ and $h(x) = \sum_{j=0}^{h} h_j x^j$ into (2), we obtain

$$\begin{aligned} L^\theta f(x) &= \frac{1}{\theta(x)} \sum_{u=0}^{m} \sum_{i=0}^{r} \sum_{j=0}^{h} \theta_u r_i h_j x^{uq^{i+j}} = \frac{1}{\theta(x)} \sum_{j=0}^{h} h_j \theta(x)^{q^j} (L^\theta r(x))^{q^j} = \\ &= L^\theta r(x) \textstyle\sum_{j=0}^{h} h_j (\theta(x) L^\theta r(x))^{q^j - 1}, \end{aligned}$$

whence by (1) we will have

$$L^\theta f(x) = L^\theta r(x) L^{\theta L^\theta r(x)} h(x).$$

Definition 1 *A polynomial* $f(x)$ *is called separable if it has no multiple roots.*

- **Separability.** *The multiplicity of any root of the polynomial* $xL^x f(x)$ *exactly equals to* q^σ, *where* σ *is the largest integer satisfying the condition* $f(x) = x^\sigma f_1(x)$, *i.e.* $a_\sigma \neq 0$ *(*$a_\omega = 0$, $\omega < \sigma$*).* Under the assumption and due to the property of multiplicativity (i.e. by (3)) we obtain that

$$\begin{aligned} xL^x x^\sigma f_1(x) &= xL^x x^\sigma \cdot L^{xL^x x^\sigma} f_1(x) = x^{q^\sigma} \sum_{u=0}^{n_1} f_u (x^{q^\sigma})^{q^u - 1} = \\ &= \left(\sum_{u=0}^{n_1} f_u x^{q^u} \right)^{q^\sigma} = (xL^x f_1(x))^{q^\sigma}, \end{aligned}$$

that is

$$xL^x f(x) = (xL^x f_1(x))^{q^\sigma}, \tag{4}$$

where $f_1(x) = \sum_{u=0}^{n_1} f_u x^u = \sum_{u=0}^{n_1} a_{u+\sigma} x^u$ and $\sigma + n_1 = n$, wherefrom, since

$$(xL^z f_1(x))' = L^z f_1(x) + x(L^z f_1(x))' = a_\sigma$$

and $a_\sigma \neq 0$, we find that $(xL^z f_1(x), (xL^z f_1(x))') = const$, which implies that $xL^z f_1(x)$ has no multiple roots, i.e. $xL^z f_1(x)$ is separable. Hence, by (4), the multiplicity of any root of the polynomial $xL^z f(x)$ is exactly equal to q^σ. Thus we have proved the property of separability.

The above-mentioned properties of the operator L^θ imply the following corollary.

Corollary 1

$$\text{I.} \quad g.c.d.(L^\theta f(x), L^\theta g(x)) = L^\theta g.c.d.(f(x), g(x)) \tag{5}$$

and

$$\text{II.} L^{\theta L^\theta g(x)} f(x) = \frac{L^{\theta L^\theta \lambda_1(x)} f(x)}{L^{\theta L^\theta \lambda_1(x)} \lambda_2(x)} L^{\theta L^\theta \lambda_1(x)} L^{\theta L^\theta \lambda_1(x)} f(x) \lambda_2(x), \tag{6}$$

where $g(x) = \lambda_1(x)\lambda_2(x)$ *and* $g.c.d.(\lambda_2(x), f(x)) = 1$.

Proof. I. Let $d(x) = g.c.d.(f(x), g(x))$ in the ring $\mathcal{F}_q[x]$. The greatest common divisor $d(x)$ of two polynomials $f(x)$ and $g(x)$ can be always represented in the form

$$d(x) = a(x)f(x) + b(x)g(x), \tag{7}$$

where $a(x)$ and $b(x)$ are polynomials in the ring $\mathcal{F}_q[x]$. By the property of multiplicativity (formula (3)) and the property of linearity it is evident that

$$L^\theta d(x) = L^\theta f(x) \cdot L^{\theta L^\theta f(x)} a(x) + L^\theta g(x) \cdot L^{\theta L^\theta g(x)} b(x), \tag{8}$$

wherefrom, because $L^\theta d(x) | L^\theta f(x)$[1] and $L^\theta d(x) | L^\theta g(x)$, it is clearly seen that

$$L^\theta d(x) | g.c.d.(L^\theta f(x), L^\theta g(x)).$$

From (8) follows directly the expression

$$g.c.d.(L^\theta f(x), L^\theta g(x)) \mid L^\theta d(x).$$

Thus identity (5) is proved, that is

$$g.c.d.(L^\theta f(x), L^\theta g(x)) = L^\theta g.c.d.(f(x), g(x)).$$

II. Since $g(x) = \lambda_1(x)\lambda_2(x)$, then it follows from (3) that

$$L^{\theta L^\theta g(x)} f(x) = L^{\theta L^\theta \lambda_1(x)\lambda_2(x)} f(x) = L^{\theta L^\theta \lambda_1(x)} L^{\theta L^\theta \lambda_1(x)} \lambda_2(x) f(x)$$

and

$$L^{\theta L^\theta \lambda_1(x)} \lambda_2(x) f(x) = L^{\theta L^\theta \lambda_1(x)} \lambda_2(x) L^{\theta L^\theta \lambda_1(x)} L^{\theta L^\theta \lambda_1(x)} \lambda_2(x) f(x),$$

[1] Hereinafter the notation $g(x)|f(x)$ denotes that $f(x)$ is divisible by $g(x)$ and $g(x) \nmid f(x)$ that it is not.

which yields

$$L^{\theta L^{\theta}g(x)}f(x) = \frac{L^{\theta L^{\theta}\lambda_1(x)\lambda_2(x)}f(x)}{L^{\theta L^{\theta}\lambda_1(x)\lambda_2(x)}} = \frac{L^{\theta L^{\theta}\lambda_1(x)}f(x)L^{\theta L^{\theta}\lambda_1(x)L^{\theta L^{\theta}\lambda_1(x)}f(x)\lambda_2(x)}}{L^{\theta L^{\theta}\lambda_1(x)\lambda_2(x)}}.$$

Thus identity (6) is proved, i.e.

$$L^{\theta L^{\theta}g(x)}f(x) = \frac{L^{\theta L^{\theta}\lambda_1(x)}f(x)}{L^{\theta L^{\theta}\lambda_1(x)\lambda_2(x)}} \cdot L^{\theta L^{\theta}\lambda_1(x)L^{\theta L^{\theta}\lambda_1(x)}f(x)\lambda_2(x)}.$$

Lemma 1 *The polynomial $L^{\theta L^{\theta}g(x)} + \alpha_1 f(x)$ is divisible by the polynomial $L^{\theta L^{\theta}\lambda_2(x)} + \alpha_{r(x)}$, where $r(x)|f(x)$, $g(x) = \lambda_1(x)\lambda_2(x)$, $\alpha_1 = \alpha\lambda_1(1)$, $\alpha \in \mathcal{F}_q$, g.c.d.$(\lambda_1(x), r(x)) = 1$ and $r(0) \neq 0$, i.e.*

$$L^{\theta L^{\theta}\lambda_2(x)} + \alpha_{r(x)} | L^{\theta L^{\theta}g(x)} + \alpha_1 f(x).$$

Proof. From (3), due to the fact that $f(x) = r(x)h(x)$, we find that

$$L^{\theta L^{\theta}g(x)} + \alpha_1 f(x) = L^{\theta L^{\theta}g(x)} + \alpha_1 r(x)h(x) =$$

$$= L^{\theta L^{\theta}g(x)} + \alpha_1 r(x) L^{(\theta L^{\theta}g(x) + \alpha_1)L^{\theta L^{\theta}g(x)} + \alpha_1 r(x)}h(x). \tag{9}$$

By definition of L^{θ}

$$L^{\theta L^{\theta}g(x)} + \alpha_1 r(x) = \sum_{u=0}^{r} r_u (\theta L^{\theta}g(x) + \alpha_1)^{q^u - 1}, \tag{10}$$

where $r(x) = \sum_{u=0}^{r} r_u x^u$ and

$$\theta L^{\theta}g(x) + \alpha_1 = \theta L^{\theta}\lambda_1(x)\lambda_2(x) + \alpha_1 = \theta L^{\theta}\lambda_2(x) L^{\theta L^{\theta}\lambda_2(x)}\lambda_1(x) + \alpha_1 =$$

$$= \sum_{i=0}^{n} \lambda_{1i} (\theta L^{\theta}\lambda_2(x) + \alpha)^{q^i},$$

where $\lambda_1(x) = \sum_{i=0}^{n} \lambda_{1i} x^i$, i.e.

$$\theta L^{\theta}g(x) + \alpha_1 = \sum_{i=0}^{n} \lambda_{1i} (\theta L^{\theta}\lambda_2(x) + \alpha)^{q^i}. \tag{11}$$

Substituting relation (11) into formula (10), we obtain

$$L^{\theta L^{\theta}g(x)+\alpha_1}r(x) = \sum_{u=0}^{r} r_u \left(\sum_{i=0}^{n} \lambda_{1i} \left(\theta L^{\theta}\lambda_2(x) + \alpha \right)^{q^i} \right)^{q^u - 1} =$$

$$= \frac{1}{\theta L^{\theta}g(x)+\alpha_1} \cdot \sum_{u=0}^{r} r_u \left(\sum_{i=0}^{n} \lambda_{1i} \left(\theta L^{\theta}\lambda_2(x) + \alpha \right)^{q^i} \right)^{q^u} =$$

$$= \frac{1}{\theta L^{\theta}g(x)+\alpha_1} \cdot \sum_{i=0}^{n} \lambda_{1i} \left(\sum_{u=0}^{r} r_u \left(\theta L^{\theta}\lambda_2(x) + \alpha \right)^{q^u} \right)^{q^i} =$$

$$= \frac{1}{\theta L^{\theta}g(x)+\alpha_1} \cdot \sum_{i=0}^{n} \lambda_{1i} \left(L^{\theta L^{\theta}\lambda_2(x)+\alpha} r(x) \right)^{q^i},$$

or by (1)

$$L^{\theta L^{\theta}g(x)+\alpha_1}r(x) = \frac{(\theta L^{\theta}\lambda_2(x)+\alpha) L^{\theta L^{\theta}\lambda_2(x)+\alpha} r(x)}{\theta L^{\theta}g(x)+\alpha_1} \times$$

$$\times L^{(\theta L^{\theta}\lambda_2(x)+\alpha) L^{\theta L^{\theta}\lambda_2(x)+\alpha} r(x)} \lambda_1(x). \tag{12}$$

Next, since

$$\theta L^{\theta}g(x)+\alpha_1 = \theta L^{\theta}\lambda_1(x)\lambda_2(x)+\alpha_1 = \theta L^{\theta}\lambda_2(x) L^{\theta L^{\theta}\lambda_2(x)}\lambda_1(x) + \alpha_1 =$$

$$= \sum_{i=0}^{n} \lambda_{1i} (\theta L^{\theta}\lambda_2(x))^{q^i} + \alpha \sum_{i=0}^{n} \lambda_{1i} = \sum_{i=0}^{n} \lambda_{1i} (\theta L^{\theta}\lambda_2(x) + \alpha)^{q^i},$$

or

$$\theta L^{\theta}g(x)+\alpha_1 = (\theta L^{\theta}\lambda_2(x)+\alpha) L^{\theta L^{\theta}\lambda_2(x)+\alpha}\lambda_1(x), \tag{13}$$

then setting relation (13) into formula (12), we reach

$$L^{\theta L^{\theta}g(x)+\alpha_1}r(x) =$$

$$= \frac{L^{\theta L^{\theta}\lambda_2(x)+\alpha} r(x)}{L^{\theta L^{\theta}\lambda_2(x)+\alpha}\lambda_1(x)} L^{(\theta L^{\theta}\lambda_2(x)+\alpha) L^{\theta L^{\theta}\lambda_2(x)+\alpha} r(x)} \lambda_1(x), \tag{14}$$

as

$$g.c.d.(L^{\theta L^{\theta}\lambda_2(x)+\alpha}\lambda_1(x), L^{\theta L^{\theta}\lambda_2(x)+\alpha} r(x)) = 1 \text{ for } g.c.d.(\lambda_1(x), r(x)) = 1.$$

It follows directly from (14) that

$$L^{\theta L^{\theta}\lambda_2(x)+\alpha} r(x) \Big| L^{\theta L^{\theta}g(x)+\alpha_1} r(x). \tag{15}$$

Thus, relying on (9) and (15), we have stated that the polynomial $L^{\theta L^\theta \lambda_2(x)+\alpha_{r(x)}}$ is a divisor of the polynomial $L^{\theta L^\theta g(x)+\alpha_1 f(x)}$, i.e.

$$L^{\theta L^\theta \lambda_2(x)+\alpha_{r(x)}} \Big| L^{\theta L^\theta g(x)+\alpha_1 f(x)}.$$

The Lemma is proved.

Lemma 2 *For any two polynomials $\lambda(x)$ and $f(x)$ ($f(0) \neq 0$, $f(1) \neq 0$) the equality*

$$L^{\theta L^\theta (x-1)\lambda(x) f(x)} = \coprod_{\alpha \in \mathcal{F}_q} L^{\theta L^\theta \lambda(x)+\alpha f(x)} \tag{16}$$

holds.

Proof. Assume that $g(x) = (x-1)\lambda(x)$, $\lambda_1(x) = x-1$, $\lambda_2(x) = \lambda(x)$, $r(x) = f(x)$, $\alpha_1 = \alpha \cdot \lambda_1(1) = 0$, $f(1) \neq 0$ and $f(0) \neq 0$. Observe that all conditions of Lemma 1 are satisfied then. This implies that for all $\alpha \in \mathcal{F}_q$ the polynomial $L^{\theta L^\theta (x-1)\lambda(x) f(x)}$ is divisible by the polynomials $L^{\theta L^\theta \lambda(x)+\alpha f(x)}$ by Lemma 1. Moreover, due to the fact that the left-hand and right-hand sides of expression (16) are monic polynomials of equal degree, we conclude that these polynomials are equal. Thus the Lemma is proved.

Corollary 2

$$g.c.d.\left(\theta L^\theta (x-1)\lambda(x),\ L^{\theta L^\theta \lambda(x)+\alpha f(x)}\right) = 1 \tag{17}$$

is true for any $\alpha \in \mathcal{F}_q$ if $f(0) \neq 0$.

Proof. By definition of L^θ

$$L^{\theta L^\theta (x-1)\lambda(x) f(x)} = \sum_{u=0}^{n} a_u \left(\theta L^\theta (x-1)\lambda(x)\right)^{q^u-1}, \tag{18}$$

where $f(x) = \sum_{u=0}^{n} a_u x^u$ and $f(0) = a_0 \neq 0$.

Therefore, by (18), it is evident that

$$g.c.d\left(\theta L^\theta (x-1)\lambda(x), L^{\theta L^\theta (x-1)\lambda(x) f(x)}\right) = 1.$$

Thus, it follows directly from (16) that

$$g.c.d\left(\theta L^\theta (x-1)\lambda(x), L^{\theta L^\theta \lambda(x)+\alpha f(x)}\right) = 1.$$

The corollary is proved.

Theorem 1 ([3], Varshamov's Theorem) . *Let $\theta(x) = p(x)L^p\lambda(x) + \alpha$, where $p(x) \in \mathcal{F}_q[x]$ and $p(x) \neq const$ is an arbitrary polynomial, $\lambda(x)$ and $f(x)$ be polynomials with nonzero free terms from the ring $\mathcal{F}_q[x]$, $f(1) \neq 0$, α be an arbitrary element in the field $\mathcal{F}_q$, $K(\lambda_u, f_u) = L^{pL^p\varepsilon(\alpha)\lambda_u(x) f_u(x)}$, where $\lambda_u(x)|\lambda(x), f_u(x)|f(x)$, $\varepsilon(\alpha) = \alpha^{q-1}x - 1$, $\lambda_u(x)f_u(x) \neq \lambda(x)f(x)$ and N is the polynomial period, $S(x) = \varepsilon(\alpha)\lambda(x)f(x)$. Then the degree c of any irreducible divisor $g(x)$ of the polynomial $L^\theta f(x)$, satisfying the condition $g(x) \nmid K(\lambda_u, f_u)$, is divisible by N.*

Proof. Assume the contrary, that is $g.c.d.(c, N) \neq N$, where c is the degree of the irreducible (over the field $\mathcal{F}_q$) polynomial $g(x)$. Then, from the expression $h(x) - g.c.d.(x^c - 1, S(x))$ we shall have that $h(x) \neq S(x)$, and due to the properties of linearity and multiplicativity

$$L^p h(x) = L^p(x^c - 1) \cdot L^{pL^p(x^c-1)} h_1(x) + L^p S(x) L^{pL^p S(x)} h_2(x), \tag{19}$$

since $h(x) = h_1(x)(x^c - 1) + h_2(x)S(x)$.

By definition of operator L^x, $p(x)L^p(x^c - 1) = \sum_{u=0}^{k} p_u(x^{uq^c} - x^u)$, where $p(x) = \sum_{u=0}^{k} p_u x^u$, which implies that $x^{q^c-1} - 1 \mid p(x)L^p(x^c - 1)$, while $g(x) \mid p(x)L^p(x^c - 1)$. We shall now show that $g.c.d(p(x), g(x)) = const$. Indeed, in view of (3), we achieve

$$L^p S(x) = L^p \varepsilon(\alpha)\lambda(x) f(x) = L^p \varepsilon(\alpha)\lambda(x) L^{p(x)L^p\varepsilon(\alpha)\lambda(x)} f(x). \tag{20}$$

However, by (20), if $\lambda(0) \neq 0$ and $f(0) \neq 0$, then $p(x) \mid p(x)L^p\varepsilon(\alpha)\lambda(x)$ and

$$g.c.d.\left(p(x)L^p\varepsilon(\alpha)\lambda(x), L^{p(x)L^p\varepsilon(\alpha)\lambda(x)} f(x)\right) = 1. \tag{21}$$

Hence

1. If $\alpha = 0$

$$\varepsilon(0) = \begin{cases} 1 & \text{for fields of even characterictic} \\ -1 & \text{for fields of odd characteristic,} \end{cases}$$

we shall obtain

$$L^{p(x)L^p\varepsilon(0)\lambda(x)} f(x) = \sum_{u=0}^{n} a_u (p(x)L^p\lambda(x))^{q^u-1} =$$
$$= \sum_{u=0}^{n} a_u (p(x)L^p\lambda(x))^{q^u-1} = L^{p(x)L^p\lambda(x)} f(x),$$

whence, because $g(x) \mid L^{p(x)L^p\lambda(x)} f(x)$, we find that $(g(x), p(x)) = 1$.

2. If $\alpha \neq 0$, since $\varepsilon(\alpha) = \alpha^{q-1}x - 1 = x - 1$ in the ring $\mathcal{F}_q[x]$, we shall have

$$L^{p(x)L^p\varepsilon(\alpha)\lambda(x)} f(x) = L^{p(x)L^p(x-1)\lambda(x)} f(x).$$

By Lemma 2 (since all the conditions of the lemma are satisfied), we obtain

$$L^{p(x)L^p(x-1)\lambda(x)} f(x) = \prod_{\beta \in \mathcal{F}_q} L^{p(x)L^p\lambda(x)+\beta} f(x). \tag{22}$$

For $\beta = \alpha$, under hypothesis of the theorem, $g(x) \mid L^{pL^p\lambda(x)+\alpha} f(x)$, which implies that $g(x) \mid L^{p(x)L^p\varepsilon(\alpha)\lambda(x)} f(x)$ due to (22). Thus, by (21), we establish that the polynomials $g(x)$ and $p(x)$ are relatively prime. Hence

$$g(x) | L^p(x^c - 1). \tag{23}$$

We shall now show that $g(x) \mid L^p h(x)$. Indeed, by (20), (22), it is clear that

$$g(x) \mid L^p S(x). \tag{24}$$

From (23), (24) and (19) it follows directly that

$$g(x) \mid L^p h(x), \tag{25}$$

wherefrom, under hypothesis of the theorem that $g.c.d(c, N) \neq N$, we find:

1. For $\alpha \neq 0$ it is evident that

$$h(x) = g.c.d.\left((x-1)\lambda(x)f(x), x^c - 1\right) = (x-1)\lambda_u(x)f_u(x).$$

By (3)

$$\begin{aligned} L^p h(x) &= L^p(x-1)\lambda_u(x)f_u(x) = \\ &= L^p(x-1)\lambda_u(x)L^{pL^p(x-1)\lambda_u(x)}f_u(x). \end{aligned} \tag{26}$$

On the other hand, by the property of multiplicativity

$$L^p(x-1)\lambda_u(x) \mid L^p(x-1)\lambda(x).$$

Hence, from (21) we shall have that

$$g.c.d.(L^p(x-1)\lambda_u(x), L^{pL^p(x-1)\lambda(x)}f(x)) = 1.$$

Similarly, from (22) we obtain that

$$g.c.d.(L^p(x-1)\lambda_u(x), g(x)) = 1. \tag{27}$$

2. For $\alpha = 0$ it is clear that

$$h(x) = g.c.d.\left(-\lambda(x)f(x), x^c - 1\right) = \lambda_u(x)f_u(x).$$

By (3)

$$L^p h(x) = L^p\lambda_u(x)L^{p(x)L^p\lambda_u(x)}f_u(x). \tag{28}$$

Since $L^p\lambda_u(x) \mid L^p\lambda(x)$, then it follows from (21) that

$$g.c.d.(L^p\lambda_u(x), L^{pL^p\lambda(x)}f(x)) = 1.$$

Evidently,

$$(L^p\lambda_u(x), g(x)) = 1. \tag{29}$$

Thus, formulas (25-29) yield

$$g(x) \mid L^{pL^p\varepsilon(\alpha)\lambda_u(x)}f_u(x) = K(\lambda_u, f_u),$$

which contradicts the hypothesis of our theorem that $g(x) \nmid K(\lambda_u, f_u)$. Thus our assumption was not true, consequently $(c, N) = N$. The theorem is proved.

The result below will be very helpful in our further research.

Theorem 2 ([1]) *Let $f_1(x), f_2(x), \cdots, f_{\sigma(z)}$ be the $\sigma = m^{-1}\varphi(e)$ (where $\varphi(x)$ is Euler's function) distinct irreducible monic polynomials of degree m over $\mathcal{F}_q$ belonging to the exponent $e = (q^m - 1)d^{-1}$ and t be an integer whose prime factors all divide e but not d. Assume also that $t \not\equiv 0 \pmod 4$ if $q^m \equiv -1 \pmod 4$. Then the polynomials $f_1(x^t), f_2(x^t), \cdots, f_\sigma(x^t)$ are a complete set of monic irreducible polynomials of degree mt over $\mathcal{F}_q$, belonging to the exponent et.*

Proposition 1 ([2]) *If β is an element of an extention of the field $\mathcal{F}_q$, then the order e of β divides $q^n - 1$ but not any smaller number of the form $q^k - 1$, $k < n$, where n is the degree of the minimal function of β.*

3 An application of Varshamov's theorem to the construction of irreducible polynomials over Galois fields and finding the periods of these polynomials

Our goal in this section is to describe a general technique of constructing sequences of irreducible polynomials of degree pt over $\mathcal{F}_p$ from given primitive elements in $\mathcal{F}_p$, where p is a an odd prime, t is an integer whose prime factors all divide $p-1$, relying on the results of Theorem 1 and 2.

Theorem 3 *Let p be an odd prime, α be a primitive element of $\mathcal{F}_q$ and t be an integer whose prime factors all divide $p-1$. Assume also that $t \not\equiv 0 \pmod 4$ if $p^p \equiv -1 \pmod 4$. Then $f_t(x) = \sum_{u=0}^{p-1} \alpha^u x^{(p-u)t} - \alpha$ is an irreducible polynomial of degree pt over $\mathcal{F}_q$ belonging to the exponent et, where e is the exponent of $f_1(x)$.*

Proof. First, we consider the case where $t = p - 1$. Then we shall have

$$f_{p-1}(x) = \sum_{u=0}^{p-1} \alpha^u x^{(p-u)(p-1)} - \alpha = L^{xL^x(x-\alpha)}(x-\alpha).$$

Next we shall show that the polynomial $f_{p-1}(x)$ is relatively prime to

$$L^{xL^x\varepsilon(0)\lambda_u(x)} f_u(x) = L^{xL^x\lambda_u(x)} f_u(x),$$

where $\varepsilon(0) = \begin{cases} 1 & \text{for fields of even characterictics} \\ -1 & \text{for fields of odd characteristics} \end{cases}$ and $\lambda_u(x) \mid (x-\alpha)$, $f_u(x) \mid (x-\alpha)$, $\lambda_u(x) f_u(x) \neq (x-\alpha)^2$.

Indeed, by the property of multiplicativity of operator L^x we have that $L^x(x-1)(x-\alpha)^2 = L^x(x-1)L^{xL^x(x-1)}(x-\alpha)L^{xL^x(x-1)(x-\alpha)}(x-\alpha)$, and by the property of separability the polynomial $L^x(x-1)(x-\alpha)^2$ is separable, which implies that

$$g.c.d.\left(L^{xL^x(x-1)}(x-\alpha),\ L^{xL^x(x-1)(x-\alpha)}(x-\alpha)\right) = 1. \tag{30}$$

Moreover, by Lemma 2

$$L^{xL^x(x-1)(x-\alpha)}(x-\alpha) = \prod_{\beta \in \mathcal{F}_q} L^{xL^x(x-\alpha)+\beta}(x-\alpha)$$

and

$$L^{xL^x(x-1)}(x-\alpha) = \prod_{\beta \in \mathcal{F}_q} L^{x+\beta}(x-\alpha)$$

which produces

$$g.c.d.\left(L^{xL^x(x-1)}(x-\alpha),\ L^{xL^x(x-\alpha)}(x-\alpha)\right) = 1.$$

Next, since $L^{xL^x(x-1)}1 = 1$ we shall obtain

$$g.c.d.\left(L^{xL^x\lambda_u(x)}f_u(x), f_{p-1}(x)\right) = 1.$$

We now observe that the degree of the polynomial $f_{p-1}(x)$ equal to $p(p-1)$ is congruent to the exponent of the polynomial $\varepsilon(0)(x-\alpha)^2$, therefore according to Theorem 1, the polynomial $f_{p-1}(x)$ is irreducible over $\mathcal{F}_p$.

Suppose that β_1 and β are the roots of the polynomials $f_{p-1}(x)$ and $f_1(x)$, respectively and the exponent of the polynomial $f_{p-1}(x)$ is equal to e_1. Since $f_{p-1}(x) = f_1(x^{p-1})$, then the polynomial $f_1(x)$ is irreducible over $\mathcal{F}_p$ and $\beta = \beta_1^{p-1}$. From the relation $\beta^{e_1} = \beta_1^{(p-1)e_1} = 1$ we have that $e \mid e_1$ and from the relation $\beta_1^{(p-1)e} = \beta^e = 1$ that $e_1 \mid (p-1)e$, hence $e_1 = \sigma e$, where $\sigma \mid p-1$. Next by the identity

$$p^{p\sigma} - 1 = (p^p - 1)\left((p^{p(\sigma-1)} - 1) + (p^{p(\sigma-2)} - 1) + \cdots + (p^p - 1 + \sigma)\right)$$

we shall achieve: $e_1 = \sigma e \mid p^{p\sigma} - 1$, however by Proposition 1 $e_1 \nmid p^k - 1$ if $k < p(p-1)$, whence it follows that $\sigma = p-1$, hence $e_1 = (p-1)e$. By Viett theorem

$$\beta^{\frac{p^p-1}{p-1}} = (-1)^p(-\alpha) = \alpha, \tag{31}$$

therefore $e \nmid \frac{p^p-1}{p-1}$. Since $g.c.d.(p-1, \frac{p^p-1}{p-1}) = 1$, then $p^p - 1 = et_1M$, where $g.c.d.(M, p-1) = 1$, $t_1 | p-1$ and $t_1 \neq p-1$. On the other hand, if $1 < t_1 < p-1$, then by (31) $\alpha^{\frac{p-1}{t_1}} = \beta^{\frac{p-1}{t_1}\frac{et_1M}{p-1}} = \beta^{eM} = 1$, which is impossible, since $\frac{p-1}{t_1} < p-1$ and α is primitive in $\mathcal{F}_p$. Thus $p^p - 1 = eM$, $p-1 \mid e$ and $g.c.d.(p-1, M) = 1$, wherefrom, by Theorem 2, if t satisfies the hypothesis of the theorem, it follows that the polynomial $f_t(x)$ of degree pt is irreducible over $\mathcal{F}_p$ and belongs to the exponent te. The theorem is proved.

Theorem 4 *Let p be an odd prime, α be an arbitrary primitive element in $\mathcal{F}_p$, and β be an arbitrary element of $\mathcal{F}_p$. Then the polynomial*

$$F(x) = \sum_{u=0}^{p-1} x^{p(p-1-u)}(\alpha x - \beta)^u - \alpha$$

of degree $p(p-1)$ is irreducible over $\mathcal{F}_p$.

Proof. It is easily seen that

$$\sum_{u=0}^{p-1} x^{p(p-1-u)}(\alpha x - \beta)^u - \alpha = (x^p - \alpha x + \beta)^{p-1} - \alpha = L^{xL^x(x-\alpha)+\beta}(x-\alpha).$$

We now show that the polynomial $F(x)$ is relatively prime to $L^{xL^z\varepsilon(\beta)\lambda_u(x)}f_u(x)$, where $\lambda_u(x) \mid (x-\alpha)$, $f_u(x) \mid (x-\alpha)$, $\lambda_u(x)f_u(x) \neq (x-\alpha)^2$ and $\varepsilon(\beta) = \beta^{p-1}x - 1$.

Indeed, by formula 30 and Lemma 2 we have that

$$g.c.d.\Big(L^{xL^z(x-1)}(x-\alpha),\ L^{xL^z(x\quad\alpha)+\beta(x-\alpha)}\Big) = 1$$

for any $\beta \in \mathcal{F}_p$. Moreover,

$$L^{xL^z(x-1)(x-\alpha)}1 = 1.$$

Hence

$$g.c.d.\Big(L^{xL^z\varepsilon(\beta)\lambda_u(x)}f_u(x),\ F(x)\Big) = 1.$$

Since the exponent $p(p-1)$ of the polynomial $\varepsilon(\beta)(x-\alpha)^2$ is congruent to the degree of the polynomial $F(x)$, then, by Theorem 1, the polynomial $F(x)$ is irreducible over $\mathcal{F}_p$. The theorem is proved.

References

[1] Albert A.A., *Fundamental Concepts of Higher Algebra*, University of Chicago Press, Chicago, 1956.

[2] Peterson W. W., Weldon E. I. *Error-Correcting Codes*, 2nd ed., M.I.T. Press, Cambridge, Mass., 1972.

[3] Varshamov R.R. On a method of constructing irreducible polynomials over finite fields. *Dokladi Akademii Nauk of Armenia*, vol. 79, No.1, 1984, pp. 26–28 (in Russian).

$\mathcal{F}_p$ դաշտի վրա անվերծանելի բազմանդամների մի դասի մասին

Մ. Կյուրեղյան, Մ. Էվոյան, Է. Հարությունյան

Ամփոփում

Հոդվածում ներկայացված են մի շարք արդյունքներ, որոնք առնչվում են անվերածելի բազմանդամների սինթեզի կոնստրուկտիվ տեսությանը, մասնավորապես $\mathcal{F}_p$ դաշտի վրա pt աստիճանի անվերածելի բազմանդամների կառուցմանը օգտագործելով $\mathcal{F}_p$ դաշտի պրիմիտիվ էլեմենտները, որտեղ p-ն պարզ կենտ թիվ է, իսկ t-ն ամբողջ թիվ է, որի բոլոր պարզ բազմապատկիչները բաժանում են $p-1$ թիվը :