International J. of Math. Sci. & Engg. Appls. (IJMSEA)
ISSN 0973-9424, Vol. 9 No. III (September, 2015), pp. 19-35

CONSTRUCTION OF INFINITE SEQUENCES OF IRREDUCIBLE POLYNOMIALS OVER F_2

P. L. SHARMA[1], SHABNAM SHARMA[2] AND MANSI REHAN[3]
[1,2,3] Department of Mathematics and Statistics,
Himachal Pradesh University, Shimla - 171005, India
E-mail: [1] plsharma1964@gmail.com

Abstract

We construct infinite sequences of irreducible polynomials over F_2 with three coefficients prescribed. We also show the structures of graphs related to the roots of sequenced irreducible polynomials over finite fields with characteristic 2.

1. Introduction

Irreducible polynomials have various applications in many areas such as design theory[9, 10], combinatorics[7], quantum information theory and cryptography, see [8, 11, 12, 13,14]. Irreducible polynomials are also used to form the generator polynomials which are important in the construction of cyclic codes and BCH codes in coding theory over binary and non-binary finite field, see [1, 3, 4, 6]. The construction of infinite sequences of irreducible polynomials by using different transformations over finite field has been studied by various researchers. The description of the Q-transform that is

---

Key Words : *Irreducible polynomial, Reciprocal polynomial, Q-transform, Finite field.*

AMS Subject Classification : 11T06, 12E05.

$g^Q(x) = x^m g\left(x + \frac{1}{x}\right)$ of an irreducible polynomial is given by R. R. Varshamov et al. in [20]. Ugolini [18, 19] gives the sequences of irreducible polynomials without prescribed coefficients over prime fields and sequences of irreducible polynomials via elliptic curve endomorphisms respectively. Ugolini [16] also describes the structures of graphs associated with the iteration of the map(2.6) over finite field F_2. Sequences of binary irreducible polynomials with two coefficients prescribed are given in [17]. Cohen [2] gives a transformation called R-operator and Sharma et al. [15] give the construction of infinite sequences of irreducible polynomials using Kloosterman sums. In this paper, we construct the sequences of irreducible polynomials over F_2 by prescribing three coefficients.

2. Basic Notations and Backgorund

We use the following notations in the present paper:

- m : positive integer
- F_q : finite field with $q = p^m$ elements
- $Tr(\gamma)$: trace of an element γ
- $g^Q(x)$: Q-transform of the polynomial
- $P^1(F_{2^m})$: projective line overF_{2^m}.

Let F_q be the finite field having $q = 2^m$ elements, where m is a positive integer. If $g(x) \in F_2[x]$ is an irreducible polynomial of degree m, then its Q-transform is given in [5] as

$$g^Q(x) = x^m g\left(x + \frac{1}{x}\right) = x^m \sum_{i=0}^{m} a_m \left(x + \frac{1}{x}\right)^m \tag{2.1}$$

and has degree $2m$. The polynomials $g(x) = \sum_{i=0}^{m} a_i x^i$ and $g^*(x) = \sum_{i=0}^{m} c_i x^i$ are reciprocal of each other, which is defined in [8] as

$$g^*(x) = x^m g\left(\frac{1}{x}\right). \tag{2.2}$$

In other words, $a_i = c_{m-i}$. A polynomial $g(x)$ is self reciprocal if

$$g(x) = g\left(\frac{1}{x}\right) \tag{2.3}$$

and it clearly holds for all $g^Q(x)$. The absolute trace of element $\gamma \in F_{2^m}$ is defined in [8] as

$$Tr_m(\gamma) = \sum_{i=0}^{m-1} \gamma^{2^i}. \tag{2.4}$$

For a positive integer m, the projective line over F_{2^m} is

$$P^1(F_{2^m}) = F_{2^m} \cup \{\infty\}, \tag{2.5}$$

which contains $q+1$ elements. The map v over $P^1(F_{2^m})$ is defined in [17] as

$$v(\gamma) = \begin{cases} \infty & \text{if } \gamma = 0 \text{ or } \infty \\ \gamma + \frac{1}{\gamma} & \text{otherwise.} \end{cases} \tag{2.6}$$

The elements of projective line $P^1(F_{2^m})$ act as the vertices of the graph and two elements $\gamma, \delta \in P^1(F_{2^m})$ are connected by a directed edge if $\gamma = v(\delta)$. The points on the projective line $P^1(F_{2^m})$ can be partitioned into two sets as:

$$\begin{aligned} A_n &= \{\gamma \in F_{2^m}^* : Tr_m(\gamma) = Tr_m(\gamma^{-1})\} \cup \{0, \infty\}, \\ B_n &= \{\gamma \in F_{2^m}^* : Tr_m(\gamma) \neq Tr_m(\gamma^{-1})\}. \end{aligned}$$

If $\gamma \in P^1(F_{2^m})$ and $v^k(\gamma) = \gamma$ for some positive integer k, then γ is said to be v-periodic otherwise pre-periodic.

In this paper, we classify any irreducible polynomial $g(x)$ as follows:

(1) $g(x)$ is of type (A, m) if $a_{m-1} = a_{m-2} = a_1 = 0$.

(2) $g(x)$ is of type (B, m) if $a_{m-1} = 0, a_{m-2} = 0, a_1 = 1$.

(3) $g(x)$ is of type (C, m) if $a_{m-1} = 0, a_{m-2} = 1, a_1 = 0$.

(4) $g(x)$ is of type (D, m) if $a_{m-1} = 1, a_{m-2} = 0, a_1 = 0$.

(5) $g(x)$ is of type (E, m) if $a_{m-1} = 1, a_{m-2} = 1, a_1 = 1$.

(6) $g(x)$ is of type (F, m) if $a_{m-1} = 1, a_{m-2} = 1, a_1 = 0$.

(7) $g(x)$ is of type (G, m) if $a_{m-1} = 1, a_{m-2} = 0, a_1 = 1$.

(8) $g(x)$ is of type (H, m) if $a_{m-1} = 0, a_{m-2} = 1, a_1 = 1$.

Theorem 2.1 [5] : If $g(x)$ is irreducible over F_2, then either $g^Q(x)$ is self-reciprocal irreducible monic polynomial of degree $2m$ or $g^Q(x)$ factors into irreducible reciprocal factors $l(x)$ and $l^*(x)$ of degree m which are not self reciprocal.

Theorem 2.2 [20] : Let $g(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + 1$ be an irreducible polynomial of $F_2[x]$. Then $g^Q(x)$ is irreducible if and only if $a_1 = 1$.

Lemma 2.3 [17] : If $g(x)$ is a binary irreducible polynomial of degree m with a root $\alpha \in F_{2^m}$ and $v(\beta) = \alpha$ for some $\beta \in F_{2^{2m}}$, then β is a root of $g^Q(x)$.

3. Main Results

Lemma 3.1 : Let $g^Q(x) = x^m \sum_{i=0}^{m} b_l \left(x + \frac{1}{x}\right)^i$ be the Q - transform having degree $2m$ of a polynomial $g(x) = \sum_{i=0}^{m} a_i x^i$ with degree m such that $g^Q(x) = l(x) \cdot l^*(x)$, where $l(x) = \sum_{i=0}^{m} c_i x^i, l^*(x) = \sum_{i=0}^{m} c_{m-i} x^i$ are irreducible over F_2. Then the coefficients

$$(c_{m-1}, c_{m-2}, c_1, c_2) = (c_{m-1}, c_{m-2}, c_{m-1} + a_{m-1}, a_{m-2} + c_{m-2} + c_{m-1}(c_{m-1} + a_{m-1}) + b).$$

Proof : On expanding the product of the polynomials $l(x)$ and $l^*(x)$ and comparing the coefficients of the terms having degrees $2m-1$ and $2m-2$ with the coefficients of the terms of $g^Q(x)$ having the same degrees. So on comparing the coefficients, we obtained that

$$b_{m-1} = c_{m-1} + c_1 \tag{3.1}$$

and

$$mb_m + b_{m-2} = c_2 + c_{m-1} + c_{m-2}. \tag{3.2}$$

Solving equations (3.1) and (3.2) for $(c_{m-1}, c_{m-2}, c_1, c_2)$ for given values of b_{m-1}, b_{m-2}, we get

$$(c_{m-1}, c_{m-2}, c_1, c_2) = (c_{m-1}, c_{m-2}, c_{m-1} + b_{m-1}, b_{m-2} + c_{m-2} + c_{m-1}(c_{m-1} + b_{m-1}) + d),$$

where d is 0 if m is even and 1 if m is odd.

Lemma 3.2 : Let $h(x) = g^Q(x) = x^m \sum_{i=0}^{m} b_i \left(x + \frac{1}{x}\right)^i$ be the Qtransform of an irreducible polynomial $g(x) = \sum_{i=0}^{m} a_i x^i$, then the following conditions holds:

(a) If $a_{m-1} = 1, a_{m-2} = 1$ the $b_{2m-1} = 1, b_{2m-2} = 0$ or 1, $b_1 = 1$.

(b) If $a_{m-1} = 1, a_{m-2} = 0$ the $b_{2m-1} = 1, b_{2m-2} = 0$ or 1, $b_1 = 1$.

(c) If $a_{m-1} = 0, a_{m-2} = 1$ the $b_{2m-1} = 0, b_{2m-2} = 0$ or 1, $b_1 = 0$.

(d) If $a_{m-1} = 0, a_{m-2} = 0$ the $b_{2m-1} = 0, b_{2m-2} = 0$ or 1, $b_1 = 0$.

Proof : In the expansion of the term $\left(x + \frac{1}{x}\right)^m$, only terms x^g, with $-m \leq g \leq m$ exists. The coefficients b_{2m-1} and b_1 are affected by the expansion of the terms $\left(x + \frac{1}{x}\right)^{m-1}$ and $\left(x + \frac{1}{x}\right)^m$. Also, the coefficient b_{2m-2} are affected by two factors that is by the expansion of the term $\left(x + \frac{1}{x}\right)^{m-2}$ and by the odd or even values of m.
(a) If $a_{m-1} = 1, a_{m-2} = 1$.
Case 1 : Let m be an odd positive integer, then

$$\begin{aligned} &= x^m \left[x^m + \frac{1}{x^m} + x^{m-2} + \frac{1}{x^{m-2}} + \cdots + x^{m-1} + \frac{1}{x_{m-1}} + \cdots + x^{m-2} \right. \\ &\left. + \frac{1}{x^{m-2}} + \cdots + 1 \right] \\ = \ & [x^{2m} + 1 + x^{2m-1} + x + \cdots + x^m] \\ = \ & [x^{2m} + x^{2m-1} + 0.x^{2m-2} + \cdots + x + 1], \end{aligned}$$

which gives

$$b_{2m-1} = 1, \quad b_{2m-2} = 0, \quad b_1 = 1.$$

Case 2 : Let m be an even positive integer, then

$$\begin{aligned} h(x) &= x^m[(x + /x^{-1})^m + 1.(x + x^{-1})^{m-1} + 1.(x + x^{-1})^{m-2} + \cdots + 1] \\ &= x^m \left[x^m + \frac{1}{x^m} + \cdots + x^{m-1} + \frac{1}{x^{m-1}} + x^{m-3} + \frac{1}{x_{m-3}} + \cdots + x^{m-2} \right. \\ &\left. + \frac{1}{x^{m-2}} + \cdots + 1 \right] \\ &= [x^{2m} + 1 + x^{2m-1} + x + x^{2m-2} + x^2 + \cdots + x^m] \\ &= [x^{2m} + x^{2m-1} + x^{2m-2} + \cdots + x + 1]. \end{aligned}$$

This gives,

$$b_{2m-1} = 1, \quad b_{2m-2} = 1, \ b_1 = 1.$$

Similarly, we can prove the parts (b), (c) and (d).
Theorem 3.3 : If $g(x)$ is a polynomial of the type (A, m), then $g^Q(x)$ can be factored into the product of a reciprocal pair of irreducible polynomials $l(x)$ and $l^*(x)$ of degree

m, where $l(x)$ is of type (A, m) and $l^*(x)$ is of type (C, m) or $l(x)$ is of type (G, m) and $l^*(x)$ is of type(E, m) or both are of same type (C, m) or (A, m) or (E, m) or (G, m).

Proof : Let $g(x) = \sum_{i=0}^{m} a_i x^i$ be a polynomial of type (A, m) i.e,

$$a_{m-1} = a_{m-2} = a_1 = 0,$$

where $m > 4$. Since $a_1 = 0$, therefore $g^Q(x)$ is reducible over F_2 by Theorem 2.1. Thus, it can be factored into a reciprocal pair of irreducible polynomials say $l(x)$ and $l^*(x)$. The Q-transform of $g(x)$ is

$$h(x) = g^Q(x) = x^m \sum_{i=0}^{m} a_m \left(x + \frac{1}{x}\right)^m.$$

Since $a_{m-1} = 0, a_{m-2} = 0$, therefore by Lemma 3.2,

$$b_{2m-1} = b_{2m-2} = b_1 = 0 \quad \text{or} \quad b_{2m-1} = 0, b_{2m-2} = 1, \quad b_1 = 0.$$

If

$$b_{2m-1} = b_{2m-2} = b_1 = 0,$$

then from Lemma 3.1, $l(x)$ and $l^*(x)$ are of type (A, m) or (C, m); $l(x)$ is of type (G, m) and $l^*(x)$ is of type (E, m). If

$$b_{2m-1} = 0, b_{2m-2} = 1, b_1 = 0,$$

then $l(x)$ is of type (C, m) and $l^*(x)$ is of type (A, m) or both are of type (G, m) or (E, m), which proves the result.

Theorem 3.4 : Let $g(x)$ be a polynomial of type (C, m), then $g^Q(x)$ can be factored into a reciprocal pair of irreducible polynomials $l(x)$ and $l^*(x)$ of degree m, which are of type (G, m) or (E, m) or (A, m) or (C, m); $l(x)$ is of type (G, m) and $l^*(x)$ is of type (E, m) or $l(x)$ is of type (A, m) and $l^*(x)$ is of type (C, m).

Proof : The polynomial $g(x)$ is of type (C, m) with degree $m > 4$. In polynomial of type (C, m), coefficient of $x = 0$, therefore By Theorem 2.1, $g^Q(x)$ is reducible. Thus By Theorem 2.2, it can be factored into reciprocal pair of irreducible polynomials.

Since $a_{m-1} = 0, a_{m-2} = 1$, therefore by Lemma 3.2,

$$b_{2m-1} = b_{2m-2} = b_1 = 0 \quad \text{or} \quad b_{2m-1} = 0, b_{2m-2} = 1, b_1 = 0.$$

If

$$b_{2m-1} = b_{2m-2} = b_1 = 0,$$

then by Lemma 3.1, $l(x)$ and $l^*(x)$ are of type (A, m) or (C, m); $l^*(x)$ is of type (G, m) and $l^*(x)$ is of type (E, m). If

$$b_{2m-1} = 0, \quad b_{2m-2} = 1, b_1 = 0,$$

then $l(x)$ and $l^*(x)$ are of type (G, m) or (E, m); $l(x)$ is of type (A, m) and $l^*(x)$ is of type (C, m). This proves the theorem.

Theorem 3.5 : Let $g(x)$ be a polynomial of type (D, m), then $g^Q(x)$ can be factored into reciprocal pair of distinct irreducible polynomials $l(x)$ and $l^*(x)$ of degree m; $l(x)$ is of type (B, m) and $l^*(x)$ is of type (D, m) or $l(x)$ is of type (H, m) and $l^*(x)$ is of type (F, m) or $l(x)$ is of type (H, m) and $l^*(x)$ is of type (D, m) or $l(x)$ is of type (B, m) and $l^*(x)$ is of type (F, m).

Proof : The polynomial $g(x)$ is of type (D, m) with degree $m \geq 4$. In polynomial of type $(D, m), a_1 = 0$, therefore $g^Q(x)$ is reducible. Thus, it can be written into the product of two irreducible polynomials. Since $a_{m-1} = 1, a_{m-2} = 0$, therefore by Lemma 3.2,

$$b_{2m-1} = b_{2m-2} = b_1 = 1 \quad \text{or} \quad b_{2m-1} = 1, \quad b_{2m-2} = 0, \quad b_1 = 1.$$

If

$$b_{2m-1} = b_{2m-2} = b_1 = 1,$$

then by Lemma 3.1, $l(x)$ is of type (H, m) and $l^*(x)$ is of type (D, m) or $l(x)$ is of type (B, m) and $l^*(x)$ is of type (F, m). If

$$b_{2m-1} = 1, \quad b_{2m-2} = 0, b_1 = 1,$$

then by Lemma 3.1, $l(x)$ is of type (B, m) and $l^*(x)$ is of type (D, m) or $l(x)$ is of type (H, m) and $l^*(x)$ is of type (F, m) which completes the proof of the theorem.

Theorem 3.6 : Let $g(x)$ be a polynomial of type (F, m), then $g^Q(x)$ can be factored into a reciprocal pair of distinct irreducible polynomials $l(x)$ and $l^*(x)$ of degree m, where $l(x)$ is of type (H, m) and $l^*(x)$ is of type (F, m) or $l(x)$ is of type (B, m) and $l^*(x)$ is of type (D, m) or $l(x)$ is of type (H, m) and $l^*(x)$ is of type (D, m) or $l(x)$ is of type (B, m) and $l^*(x)$ is of type (F, m).

Proof : Let $g(x)$ be a polynomial of type (F, m), where $m > 4$, since $a_1 = 0$, therefore $g^Q(x)$ is reducible over F_2. Since, $a_{m-1} = 1, a_{m-2} = 1$, therefore, by Lemma 3.2,

$$b_{2m-1} = b_{2m-2} = b_1 = 1 \quad \text{or} \quad b_{2m-1} = 1, b_{2m-2}, b_1 = 1.$$

So by Lemma 3.1, $l(x)$ is of type (H, m) and $l^*(x)$ is of type (F, m) or $l(x)$ is of type (B, m) and $l^*(x)$ is of type (D, m) or (l, x) is of type (H, m) and $l^*(x)$ is of type (D, m) or $l(x)$ is of type (B, m) and $l^*(x)$ is of type (F, m).

Theorem 3.7 : Let $g(x)$ be a polynomial of type (B, m) or (H, m) then Qtransform of this polynomial is either of the type $(A, 2m)$ or $(C, 2m)$.

Proof : If $g(x)$ is a polynomial of type (B, m) or (H, m) then $g^Q(x)$ is irreducible. Since $a_{m-1} = 0, a_{m-2} = 0$ or 1, therefore by Lemma 3.2, $g^Q(x)$ is either of type $(A, 2m)$ or $(C, 2m)$.

4. Procedure to Construct an Infinite Sequence of Irreducible Polynomials

Let $g_0(x)$ be an irreducible polynomial over F_2 of degree $m = 2^q \cdot p$, where p is odd and q is a non negative integer, then the following cases arise:

4.1 (a) If $g_0(x)$ is of type (A, m) or (C, m) then $g_0^Q(x)$ splits into two irreducible factors, say $l(x)$ and $l^*(x)$ that is, $g_0^Q(x) = l(x) \cdot l^*(x)$ which are of the type (G, m) or (E, m); $l(x)$ is of type (G, m) and $l^*(x)$ is of type (E, m). We set

$$h_0 = l(x) \quad \text{or} \quad h_0 = l^*(x),$$

and construct a finite sequence $h_0, h_1, h_2, \cdots, h_s$ for $s \leq q + 1$. Let

$$g_i = h_{i-1} \quad \text{for} \quad 1 \leq i \leq s + 1 \leq q + 1,$$

then an infinite sequence of irreducible polynomials can be formed by setting

$$g_{i+1} = g_i^Q \qquad \text{for} \quad i \geq s.$$

(b) If $l(x)$ and $l^*(x)$ are not of the type (G, m) or (E, m) as discussed in 4.1 (a), then set $h_0 = l(x)$ and its Q-transform factored into two factors say $l_1(x)$ and $l_2(x)$ that is, $l(x) = l_1(x) \cdot l_2(x)$. If $l_1(x)$ and $l_2(x)$ are of type (G, m) or (E, m) then repeat as in part 4.1(a) but if not then we set $h_0(x) = l^*(x)$ and repeat the same process. Let

$$g_i = h_{i-1} \quad \text{for} \quad 1 \leq i \leq s + 1 \leq q + 3,$$

then an infinite sequence of irreducible polynomials can be formed by setting

$$g_{i+1} = g_i^Q \quad \text{for} \quad i \geq s.$$

4.2 If $g_0(x)$ is of type (B, m) then by Theorem 3.7, $g_0^Q(x)$ is of type $(A, 2m)$ or $(C, 2m)$. Let $m' = 2m$ and $q' = q + 1, h_0 = g_0^Q(x)$, then a finite sequence $h_0, h_1, h_2, \cdots, h_{s'}$ can be constructed where $s' \leq q = q + 1$ and $h_{s'}$ is either of type $(G, 2m)$ or $(E, 2m)$. Let

$$g_i = h_{i-1} \quad \text{for} \quad 1 \leq i \leq s' + 1 \leq q + 2,$$

then an infinite sequence of irreducible polynomials can be formed by setting

$$g_{i+1} = g_i^Q \quad \text{for} \quad i \geq s'.$$

4.3 If $g_0(x)$ is of type (D, m) and (F, m) then it is possible to construct a polynomial $g_1(x)$ of type (B, m) or (H, m). According to Theorem 3.7, $g_1^Q(x)$ is either of type $(C, 2m)$ or $(A, 2m)$. We set

$$h_0(x) = g_1^Q(x), \quad m' = 2m \quad \text{and} \quad q' = q + 1,$$

so it is possible to construct a finite sequence $h_0, h_1, h_2, \cdots, h_{s'}$, where $s' \leq q' = q + 1$. Let

$$g_i = h_{i-2} \quad \text{for} \quad 2 \leq i \leq s' + 1 \leq q + 3,$$

then an infinite sequence of irreducible polynomials can be formed by setting

$$g_{i+1} = g_i^Q \quad \text{for} \quad i \geq s'.$$

4.4 If $g_0(x)$ is a polynomial of type (H, m) then it is possible to construct a polynomial $g_1(x) = g_0^Q(x)$ of type $(A, 2m)$ or $(C, 2m)$. We set

$$h_0 = g_0^Q, \quad m' = 2m, \quad q' = q + 1.$$

Let

$$g_i = h_{i-1} \quad \text{for} \quad 1 \leq i \leq s' + 1 \leq q + 2,$$

then an infinite sequence of irreducible polynomials can be formed by setting

$$g_{i+1} = g_i^Q \quad \text{for} \quad i \geq s'.$$

4.5 If $g_0(x)$ is a polynomial of type (G, m) or (E, m), then $g_0^Q(x)$ is irreducible, see [5]. Therefore, an infinite sequence of binary irreducible polynomials can be formed by setting

$$g_{i+1} = g_i^Q \quad \text{for} \quad i \geq 0.$$

Remark : Let $g_0(x)$ be an irreducible polynomial of any one of the type from (A, m) to (H, m). If $g_0^Q(x)$ is reducible, then it can be factored into the product of two irreducible polynomials $l(x)$ and $l^*(x)$.

5. Examples

5.1 We construct a sequence of irreducible polynomials starting from an irreducible polynomial of degree 4. Let α be a root of the Conway polynomial

$$x^4 + x + 1,$$

which is primitive polynomial in $F_2[x]$. The illustration of the construction of binary irreducible polynomials is as follows:
We take a binary polynomial of type $(D, 4)$ as

$$g_0(x) = x^4 + x^3 + 1$$

and notice that α^{13} is one of the roots of this polynomial, which is v-periodic. By Lemma 3.1, the Q-transform $g_0^Q(x)$ splits into the product of two irreducible factors say $l(x)$ and $l^*(x)$ of degree 4, where $l(x)$ is of type $(B, 4)$ and $l^*(x)$ is of type $(D, 4)$. Therefore,

$$g_0^Q(x) = (x^4 + x + 1)(x^4 + x^3 + 1).$$

One of the factor $l(x)$ and $l^*(x)$ has a root α which is not v-periodic and rooted in α^{13}. Therefore, We set

$$g_1(x) = x^4 + x + 1.$$

The polynomial $g_1(x)$ is of type $(B, 4)$ and α^4 is the root of this polynomial which is rooted in α^{13}. Also there is no element γ such that $v(\gamma) = \alpha^4$. Such an element γ exists in F_{2^s} and $g_1^Q(\gamma) = 0$. Let

$$h_0(x) = g_2(x) = g_1^Q(x) = x^8 + x^5 + x^4 + x^3 + 1,$$

which is of type $(A, 2m)$.
Again, taking Qtransform of the polynomial $h_0(x)$ and factoring, we get

$$h_0^Q(x) = (x^8 + x^6 + x^3 + x^2 + 1)(x^8 + x^6 + x^5 + x^2 + 1).$$

We set

$$h_1(x) = x^8 + x^6 + x^3 + x^2 + 1,$$

which is of type $(C, 8)$. We factor $h_1^0(x)$ and get

$$h_1^Q(x) = (x^8 + x^5 + x^3 + x^2 + 1)(x^8 + x^6 + x^5 + x^3 + 1).$$

Again, the factors of $h_1^Q(x)$ are not of type $(G, 8)$ or $(E, 8)$, so further let

$$h_2(x) = x^8 + x^5 + x^3 + x^2 + 1,$$

which is of type $(A, 8)$, we factor $h_2^Q(x)$ and get

$$h_2^Q(x) = (x^8 + x^7 + x^2 + x + 1)(x^8 + x^7 + x^6 + x + 1).$$

We set

$$h_3(x) = x^8 + x^7 + x^2 + x + 1,$$

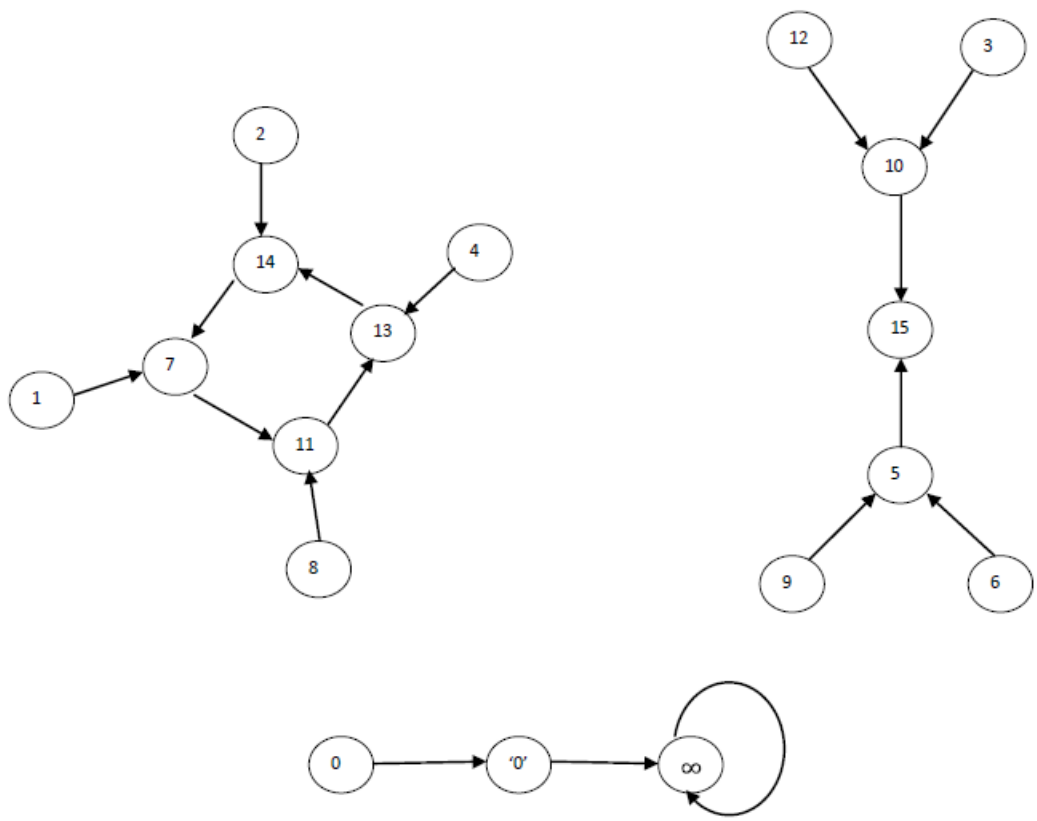
which is of type $(G, 8)$. Hence, we construct a finite sequence h_0, h_1, h_2, h_3 of irreducible polynomials.
Now, on setting

$$h_0 = g_2, \quad h_1 = g_3, \quad h_2 = g_4, \quad h_3 = g_5$$

and

$$g_{i+1} = g_i^Q$$

for any integer $i \geq 5$, we get an infinite sequence of irreducible polynomials. We also present a graph Gr_4 having three connected components. The labels of the vertices are $\infty, `0'$ (the zero of F_2) and the exponent j is the power of α for$0 \leq j \leq 14$.



Structure of the Graph Associated with the Map $v(x) = x + \frac{1}{x}$ over F_{2^4}

5.2 In this example, we construct an infinite sequence of irreducible polynomials starting from an irreducible polynomial of degree 7 over F_2. Let α be the root of the Conway polynomial

$$x^7 + x + 1.$$

The explanation of the sequence of binary irreducible polynomials is as follows: Let us start with the polynomial of type $(A, 7)$

$$g_0(x) = x^7 + x^3 + 1$$

and α^{11} is one the roots of $g_0(x)$. Now, $g_0^Q(x)$ factors as

$$g^Q(x) = (x^7 + x^4 + x^3 + x^2 + 1)(x^7 + x^5 + x^4 + x^3 + 1).$$

Here, first irreducible factor is of type $(A, 7)$ and the second one is of type $(C, 7)$. One of the factor $l(x)$ and $l^*(x)$ has a root α which is not v-periodic and rooted in α^{11}. We set

$$g_1(x) = (x^7 + x^4 + x^3 + x^2 + 1)$$

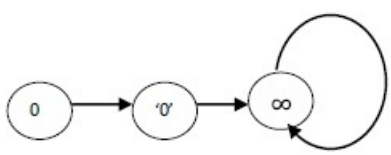
and α^{93} is the root of $g_1(x)$, which is rooted in α^{11}. These roots are connected by the map (2.6). Again, taking Qtransform of $g_1(x)$ and split it into two irreducible factors, which are of type $(G, 7)$. Therefore,

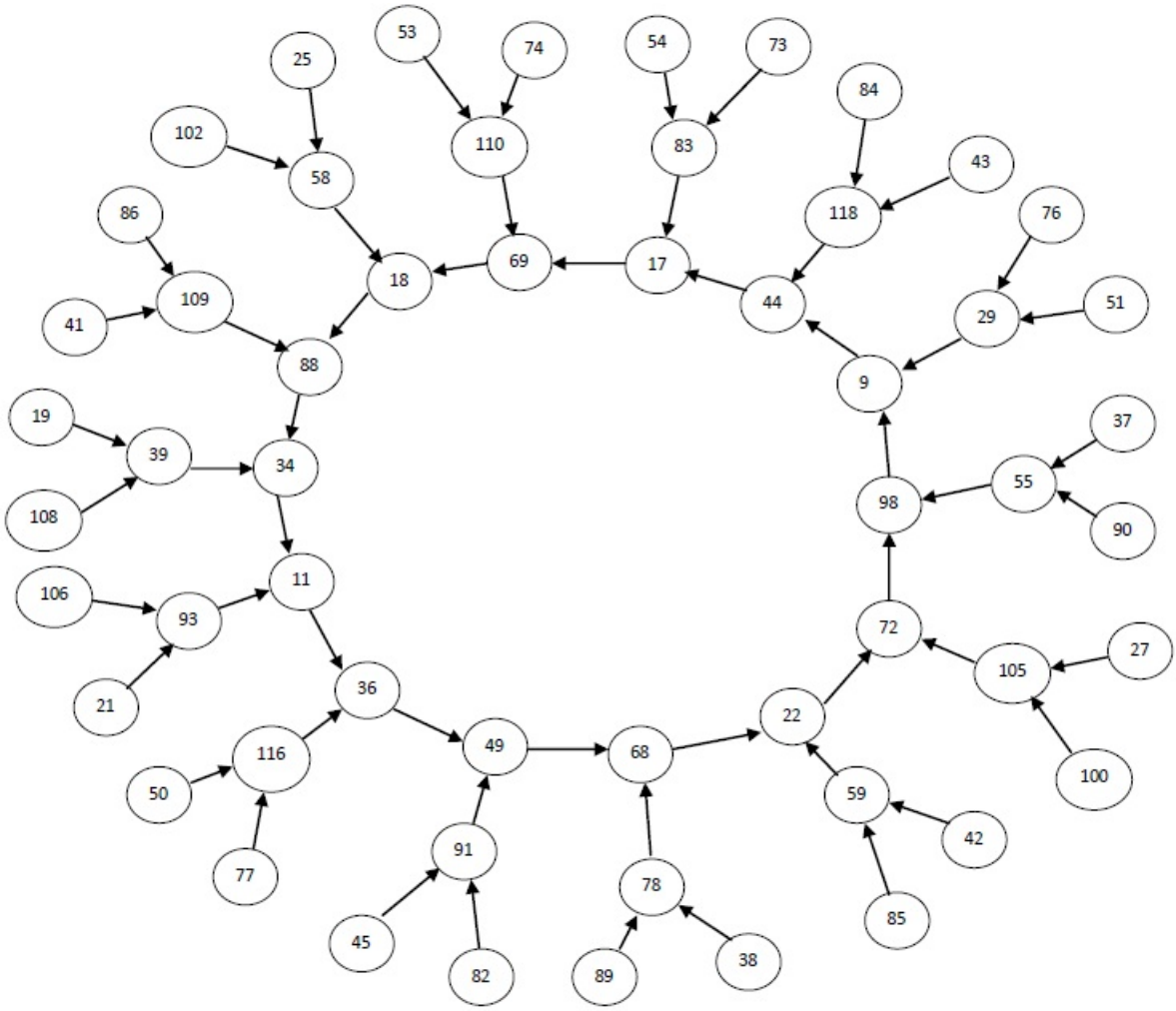
$$g_1^Q(x) = (x^7 + x^6 + x^3 + x + 1)(x^7 + x^6 + x^4 + x + 1).$$

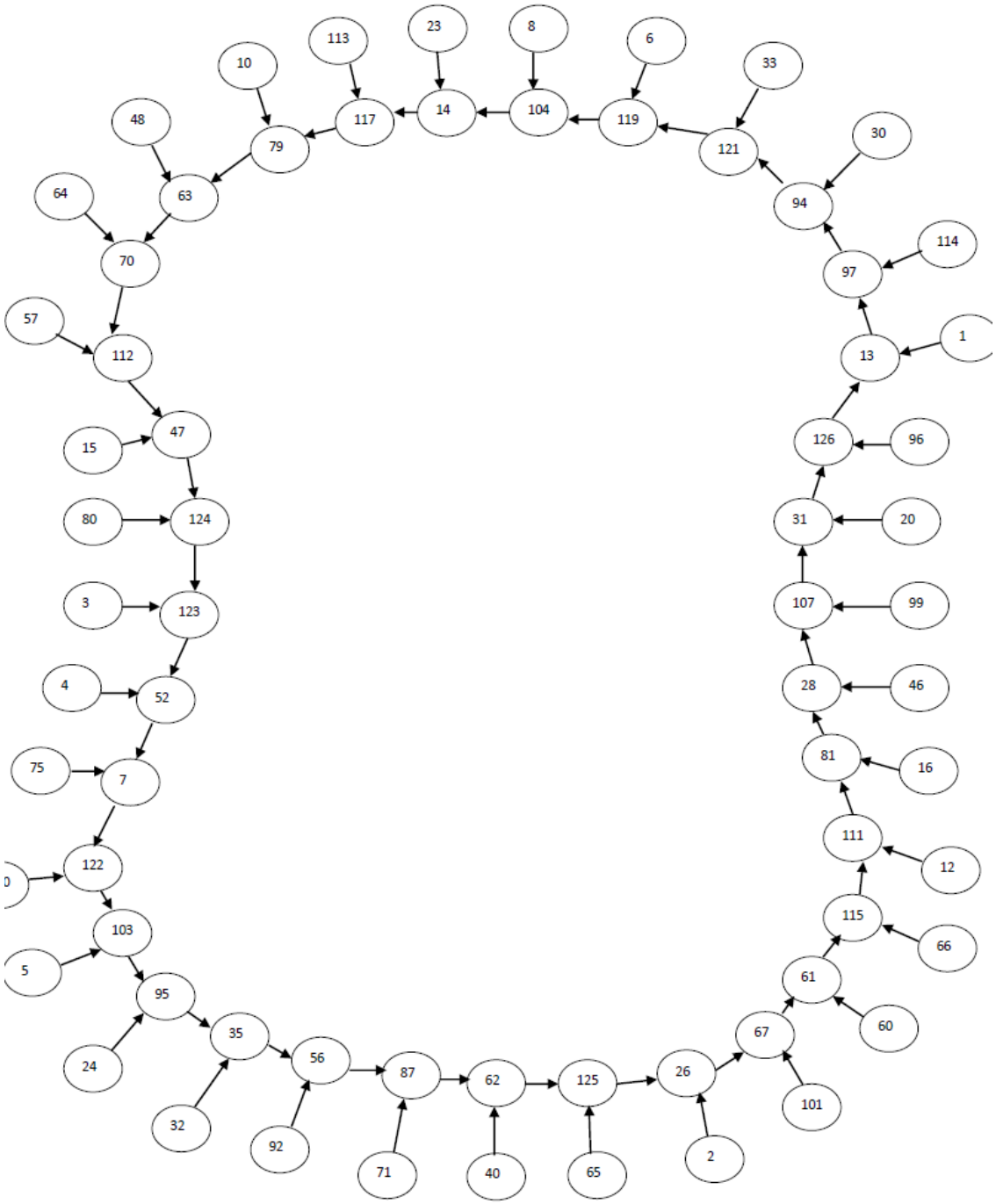
The first and second irreducible factors of $g_1^Q(x)$ has α^{21} and α^{106} respectively as one of their roots. These two roots are connected to α^{93} by the map (2.6), which is a root of $g_1(x)$. Also there is no element γ such that $v(\gamma) = \alpha^{21}$ or α^{106}. Such an element γ exists in $F_{2^{14}}$ and $g_2^Q(\gamma) = 0$. We Set

$$g_{i+1} = g_i^Q \quad \text{for} \quad i \geq 2$$

and obtain an infinite sequence of irreducible polynomials. We present the graph Gr_7, having 3 connected components. The exponents j are the powers of α, where $0 \leq j \leq 126$.




53
74
54
73
25
84
102
110
83
58
43
118
86
76
69
17
18
44
109
51
41
29
88
9
19
37
39
34
55
98
108
90
11
106
93
72
27
105
36
21
22
116
49
68
100
50
59
42
91
77
78
85
45
82
89
38



Structure of the Graph Associated with the Map $v(x) = x + \frac{1}{x}$ over F_{2^7}

6. Conclusion

We classified the irreducible polynomials of degree m over F_2 on the basis of their coefficients and constructed an infinite sequence of irreducible polynomials by using the Q-transform repeatedly starting from an irreducible polynomial of degree m. We also shown the structure of graphs by using the map $x \to x + \frac{1}{x}$ over finite fields F_{2^4} and F_{2^7}.

Acknowledgement

Authors acknowledge the support of UGC-SAP.

References

[1] Ashikhmin A. E. and Litsyn S. N., Fast decoding of non-binary first order Reed-Mullar codes, AAECC, 7 (1996), 299-308.

[2] Cohen S. D., The explicit construction of irreducible polynomials over finite field, 2 (1992), 169-174.

[3] Charpin P., Tietäväinen A. and Zinoviev V., On binary cyclic codes with minimum distance three, Problems of Information Transmission, 33 (1997), 314.

[4] Geer G. V. D., Schoof R. and Vlugt M. V. D., Weight formulas for ternary Melas codes, Mathematics of Computation, 58(198) (1992), 781-792.

[5] Meyn H., On the construction of irreducible self-reciprocal polynomials over finite fields, Appl. Algebra Eng. Comm. Comput., 1(1) (1990), 43-53.

[6] MacWilliams F. J. and Sloane N. J. A., The Theory of Error-Correcting Codes, North-Holland, New York, (1986).

[7] Mullen G. L. and Panario D., Handbook of Finite Fields, CRC Press, (2013).

[8] Lidl R. and Niederreiter H., Finite Fields, Cambridge University Press, (1983).

[9] Sharma P. L. and Kumar S., Balanced incomplete block design (BIBD) using Hadamard Rhotrices, International Journal of Technology, 4(1) (2014), 62-66.

[10] Sharma P. L. and Kumar S., Some applications of Hadamard Rhotrices to design balanced incomplete block, International J. of Math Sci. and Engg Appls, 8(II) (2014), 389-404.

[11] Sharma P. L. and Kumar S., On construction of MDS Rhotrices from companion Rhotrices over finite field, International Journal of Mathematical Sciences, 12(3-4) (2013), 271-286.

[12] Sharma P. L. and Rehan M., On security of Hill Cipher using finite fields, International Journal of Computer Applications, 71(4) (2013), 30-33.

[13] Sharma P. L. and Rehan M., Modified Hill Cipher using Vandermonde matrix and finite field, International Journal of Technology, 4(1) (2014), 252- 256.

[14] Sharma P. L., Kumar S. and Rehan M., On Hadamard Rhotrix over finite field, Bulletin of Pure and Applied Sciences, 32E(2) (2013), 181-190.

[15] Sharma P. L., Sharma Shabnam and Dhiman Neetu, Construction of infinite sequences of irreducible polynomials using Kloosterman sums, Bulletin of Pure and Applied Sciences, 33E(2)P. (Math. and Stat.), (2014), 161-168.

[16] Ugolini S., Graphs associated with the map $x \to x + x^{-1}$ in finite fields of characteristic two, in: Theory and Applications of Finite Fields, in: Contemp. Math., Amer. Math. Soc., Providence, RI, 579 (2012).

[17] Ugolini S., Sequences of binary irreducible polynomials, Discrete Mathematics, 313 (2013), 2656-2662.

[18] Ugolini S., Sequences of irreducible polynomials without prescribed coefficients over odd prime fields, arxiv: 1207. 6959v5 (2013).

[19] Ugolini S., Sequences of irreducible polynomials over odd prime fields via elliptic curve endomorphisms, arxiv: 1308.6723v3 (2014).

[20] Varshamov R. R. and Garakov G. A., On the theory of self-dual polynomials over a Galois field, Bull. Math. Soc. Sci. Math. R. S. Roumanie (N.S.), 13 (1969), 403-415 (in Russian).