Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 6, pp. 2383–2396
DOI : 10.47974/JDMSC-2308

Some new constructions of irreducible polynomials using composition of polynomials over finite fields

Balkaran Singh [†]
Department of Mathematics & Statistics
Himachal Pradesh University
Shimla 171005
Himachal Pradesh
India

Neetu Dhiman *
University Institute of Technology
Himachal Pradesh University
Shimla 171005
Himachal Pradesh
India

Shalini Gupta [§]
Department of Mathematics & Statistics
Himachal Pradesh University
Shimla 171005
Himachal Pradesh
India

Ashima [‡]
Department of Mathematics
Hansraj College
University of Delhi
Delhi 110007
India

[†] *E-mail:* balkaransingh895@gmail.com
* *E-mail:* dhimanneetu278@gmail.com (Corresponding Author)
[§] *E-mail:* shalini.garga1970@gmail.com
[‡] *E-mail:* ashima@hrc.du.ac.in

Abstract

Construction of irreducible polynomials hold significant importance in coding theory, complexity theory and cryptography. Irreducible polynomials also helps us to generate non-zero elements of finite fields. In the present work, starting from a specified n degree irreducible polynomial, the methods to construct irreducible polynomials with a degree $6n$ over finite field $\mathbb{F}_{3^s}$ are explored. Additionally, a method for generating irreducible polynomial of degree p^2n over finite field $\mathbb{F}_{p^s}$ by polynomial composition under specific constraints related to coefficients and the degree of initial irreducible polynomial is given.

Subject Classification: *11T06, 12E05, 12E20.*

Keywords: *Trace function, Irreducible polynomials, Finite fields.*

1. Introduction

The study of Irreducible Polynomials (IRPs) over finite fields stands as a cornerstone in modern algebra and has far-reaching implications across various fields of mathematics and computer science. These polynomials, which cannot be factored into non-trivial polynomials over a given field have significant applications in cryptography, error-correcting codes and combinatorial designs, among others see [15, 16, 18]. The ability to construct such polynomials efficiently and systematically is therefore of paramount importance.

Finite fields, also known as Galois fields, play a central role in this construction process. These fields consist of a finite number of elements and possess algebraic properties that distinguish them from fields of infinite order. Understanding the structure and properties of finite fields is crucial for devising methods to construct irreducible polynomials within them.

The quest to construct irreducible polynomials over finite fields has spurred considerable research activity, leading to the development of various algorithms and techniques. These methods often leverage insights from algebraic number theory, abstract algebra and computational complexity theory. Many authors have given different algorithms for recursive and recurrent construction of irreducible polynomials over the years, see [1, 3, 11, 19, 22, 23, 25, 5, 12, 7, 24, 9, 20]. While previous research discusses structural properties of polynomials over finite fields, such as matroidal root structure of skew polynomials [26], the search for efficient and versatile algorithms for constructing irreducible polynomials remains an active area of investigation.

In [1] by choosing initial n degree irreducible polynomial $f(x) = d_nx^n + d_{n-1}+\ldots+d_1x + d_0$ over $\mathbb{F}_q$. Irreducibility of composite polynomials $(x^p - lx + m)^n \left(\frac{x^p-lx+k}{x^p-lx+m}\right)$ over finite fields is given for some special cases. Additionally, IRPs sequences of degree of $n2^m$ and $np^m, m \in \mathbb{N}$, are constructed over $\mathbb{F}_{2^k}$ and $\mathbb{F}_{p^k}$ respectively. Kim and Son [11] used the transformation $x \to \frac{x^p-x^{p-1}+1}{-x^{p-1}+1}$ to construct infinite sequences of irreducible polynomials over $\mathbb{F}_q$ having characteristic p. Also, using iterations for this transformation authors constructed k-normal polynomials having degree np^k in $\mathbb{F}_q[x]$ taking an initial n degree k-normal polynomial. These methods not only provide theoretical insights into the structure of finite fields but also facilitate efficient computation in applied fields such as cryptography and coding theory, see [2, 4, 6, 10, 13, 14, 17, 18, 21]. The present work is motivated by the results given by Sharma et al. [19], where the authors constructed IRPs of degree $4n$ over the finite field $\mathbb{F}_{2^m}$ for an initial n degree IRP. In addition to this, IRPs of degree p^2n are constructed for a given n degree IRPs by taking some constraints and using composition method.

In this paper, we embark on an exploration of the construction of irreducible polynomials over finite fields. We delve into the fundamental concepts underlying finite fields and irreducible polynomials, laying the groundwork for understanding the intricacies involved in their construction. Furthermore, we present novel approaches, refinements aimed at enhancing the efficiency and applicability of irreducible polynomial construction for algorithms. Leveraging recent advancements in computational techniques and mathematical insights, we propose innovative strategies for generating irreducible polynomials over finite fields, contributing to the ongoing discourse in this field.

In the second section, the preliminaries related to research work are discussed. In the third section, our primary findings are given, where IRPs of degree $6n$, $9n$ and p^2n are constructed. In the fourth section, we conclude our results.

2. Preliminaries

Definition 2.1: [15] For $\gamma \in \mathbb{F}_{q^n}$, the trace $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\gamma)$ of γ over $\mathbb{F}_q$ is defined as

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\gamma) = \gamma + \gamma^q + \gamma^{q^2} + \cdots + \gamma^{q^{n-1}}.$$

Definition 2.2: [15] The polynomial $f^*(x) = x^n f\left(\frac{1}{x}\right)$ is known as the reciprocal polynomial of any polynomial $f(x)$.

Proposition 2.1: [8] Let $P(x) \in \mathbb{F}_q[x]$ be an n degree IRP and $r(x), s(x) \in F_q[x]$ are two coprime polynomials, then the composition

$$H(x) = P\left(\frac{r(x)}{s(x)}\right) s^n(x)$$

is an IRP if and only if $r(x) - \gamma s(x)$ is an IRP over $\mathbb{F}_{q^n}$, where $\gamma \in \mathbb{F}_{q^n}$ is any root of $P(x)$.

Proposition 2.2: [18] In $\mathbb{F}_q[x]$, $x^s - x - l$ is an irreducible trinomial if and only if $Tr_{\mathbb{F}q/\mathbb{F}p}(l) \neq 0$, where s is the characteristic of $\mathbb{F}_q$ and $l \in \mathbb{F}_q$.

Proposition 2.3: [18] For $l, m \in \mathbb{F}_q^*$, $x^p - lx - m$ is an irreducible trinomial over $\mathbb{F}_q$ if and only if $l = B^{p-1}$ for some $B \in \mathbb{F}_q$ and $Tr_{\mathbb{F}_q/\mathbb{F}_p}(m/B^p) \neq 0$.

Proposition 2.4: [20] For an n degree IRP $L(x) = \sum_{i=0}^{n} l_i x^i$ over $\mathbb{F}_q$, the polynomial

$$H(x) = L\left(\frac{x^p - x^{p-1} + 1}{x^p}\right) \cdot (x^p)^n$$

of degree pn over $\mathbb{F}_q$ is an IRP if and only if

$$Tr_{\mathbb{F}_q/\mathbb{F}_p}\left(n + \frac{L^{*\prime}(0)}{L^*(0)}\right) \neq 0.$$

Theorem 2.1: [1] *Let* $x^p - lx + m$ *and* $x^p - lx + k \in \mathbb{F}_q$ *be two coprime polynomials and* $L(x) = \sum_{i=0}^{n} c_i x^i$ *is a* n *degree IRP over* $\mathbb{F}_q$ *such that* $n \geq 2$ *and let* $l \in \mathbb{F}_q^*, m, k \in \mathbb{F}_q, (m, k) \neq (0,0)$. *Then,*

$$H(x) = L\left(\frac{x^p - lx + m}{x^p - lx + k}\right) \cdot (x^p - lx + k)^n$$

is an IRP of degree pn *over* $\mathbb{F}_q$ *if,*

$$N_{\mathbb{F}_q/\mathbb{F}_p}(l) = 1$$

and

$$Tr_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{1}{B^p}\left(\frac{(m-k)L'(1)}{L(1)} + kn\right)\right) \neq 0,$$

where $B^{p-1} = l, B \in \mathbb{F}_{q^n}$.

3. Main Results

This section presents the constructions of IRPs of degree $6n$ and $p^2 n$ by using an IRP of degree n over $\mathbb{F}_q$, applying composition method for irreducibility of polynomials [8]. Further, an IRP of degree $9n$ is constructed for an initially defined IRP of degree n with the help of Corollary 1.

Lemma 3.1: *For any IRP,* $L(x) = \sum_{i=0}^{n} l_i x^i$ *over* $\mathbb{F}_q$ *of degree* n, *the polynomial*

$$H(x) = L\left(\frac{x^p - x^{p-1} + 1}{x^{p-1} - 1}\right) \cdot (x^{p-1} - 1)^n$$

over $\mathbb{F}_q$ *is a* pn *degree IRP if and only if*

$$Tr_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{L'(1)}{L(1)}\right) \neq 0.$$

Proof: By applying Proposition 2.3, $H(x)$ over $\mathbb{F}_q$ is an IRP if and only if $(x^p - x^{p-1} + 1) - \gamma(x^{p-1} - 1)$ is an IRP over $\mathbb{F}_{q^n}$, where $\gamma \in \mathbb{F}_q$ is a root of $L(x)$. Precisely, $H(x)$ is an IRP if and only if $x^p - x - \left(\frac{-1}{\gamma+1}\right)$ is an IRP over $\mathbb{F}_{q^n}$. Also, using Proposition 2.4, $x^p - x - \left(\frac{-1}{\gamma+1}\right)$ is irreducible if and only if $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_p}\left(\frac{-1}{\gamma+1}\right) \neq 0$.

Given that,

$$L(x) = \sum_{i=0}^{n} l_i x^i = l_0 + l_1 x + l_2 x^2 + l_3 x^3 + \ldots\ldots + l_n x^n. \tag{1}$$

Therefore,

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_p}(\gamma) = -Tr_{\mathbb{F}_{q^n}/\mathbb{F}_p}\left(\frac{x+1}{x}\right).$$

Now,

$$L\left(\frac{x+1}{x}\right) = l_0 + l_1\left(\frac{x+1}{x}\right) + l_2\left(\frac{x+1}{x}\right)^2 + l_3\left(\frac{x+1}{x}\right)^3 + \ldots\ldots + l_n\left(\frac{x+1}{x}\right)^n. \tag{2}$$

Since,

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_p}\left(\frac{-1}{\gamma+1}\right) = Tr_{\mathbb{F}_q/\mathbb{F}_p}\left(Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left(\frac{-1}{\gamma+1}\right)\right)$$

and

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left(\frac{-1}{\gamma+1}\right) = \frac{L\prime(1)}{L(1)}.$$

Therefore,

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_p}\left(\frac{-1}{\gamma+1}\right) = -Tr_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{L\prime(1)}{L(1)}\right).$$

Hence, $H(x)$ is an IRP over $\mathbb{F}_q$ if and only if

$$Tr_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{L\prime(1)}{L(1)}\right) \neq 0.$$

Theorem 3.1: *For $q = 3^k$ and $L(x) = \sum_{i=0}^{n} l_i x^i$ be an IRP of degree n over $\mathbb{F}_q$. Assume that $Tr_{\mathbb{F}_q/\mathbb{F}_3}\left(\frac{L^*\prime(0)}{L^*(0)}\right) \neq 0$ and $Tr_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{L\prime(0)}{L(0)}\right) \neq 0$. Then, $6n$ degree IRP over $\mathbb{F}_q$ is defined as*

$$t(x) = L\left(\frac{x^9+2x^7+2x^5+2x^3}{(x^2-1)^3}\right) \cdot (x^2-1)^{3n}.$$

Proof: For a root γ of $L(x)$ over $\mathbb{F}_{q^n}$,

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_3}(\gamma) = Tr_{\mathbb{F}_q/\mathbb{F}_3}(Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\gamma))$$

$$= Tr_{\mathbb{F}_q/\mathbb{F}_3}\left(\frac{-l_{n-1}}{l_n}\right) = -Tr_{\mathbb{F}_q/\mathbb{F}_3}\left(\frac{l_{n-1}}{l_n}\right)$$

$$= -Tr_{\mathbb{F}_q/\mathbb{F}_3}\left(\frac{L^*\prime(0)}{L^*(0)}\right)$$

By assumption,

$$Tr_{\mathbb{F}_q/\mathbb{F}_3}\left(\frac{L^*\prime(0)}{L^*(0)}\right) \neq 0.$$

Now, $f(x) = x^3 - x - \gamma$ in $\mathbb{F}_{q^n}[x]$ is irreducible according to Proposition 2.2. Using Lemma 3.1, polynomial $H(x)$ is defined as

$$H(x) = f\left(\frac{x^3-x^2+1}{x^2-1}\right) \cdot (x^2-1)^3$$

is an IRP if and only if $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_p}\left(\frac{f\prime(1)}{f(1)}\right) \neq 0$.

This gives,

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_p}\left(\frac{-2}{\gamma}\right) \neq 0.$$

So,

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_p}\left(\frac{1}{\gamma}\right) \neq 0.$$

That is,

$$Tr_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{-l_1}{l_0}\right) = -Tr_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{-l_1}{l_0}\right) \neq 0.$$

So,

$$Tr_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{L\prime(0)}{L(0)}\right) \neq 0.$$

Thus,

$$\begin{aligned} H(x) &= f\left(\frac{x^3-x^2+1}{x^2-1}\right)\cdot(x^2-1)^3 \\ &= \left(\left(\frac{x^3-x^2+1}{x^2-1}\right)^3 - \left(\frac{x^3-x^2+1}{x^2-1}\right) - \gamma\right)\cdot(x^2-1)^3 \\ &= (x^9+2x^7+2x^5+2x^3) - \gamma(x^2-1)^3 \end{aligned}$$

is an IRP over $\mathbb{F}_{q^n}$. Therefore, according to the Proposition 2.1, IRP of degree $6n$ over $\mathbb{F}_q$ denoted as $t(x)$ is given by

$$t(x) = L\left(\frac{x^9+2x^7+2x^5+2x^3}{(x^2-1)^3}\right)\cdot(x^2-1)^{3n}.$$

Example 3.1: Let $l(x) = x^3+x^2+x+2$ be an IRP over $\mathbb{F}_3$. Now, $Tr_{3/3}(1) \neq 0$ and $Tr_{3/3}(\frac{1}{2}) \neq 0$. Here, all the assumptions of the above theorem are satisfied, therefore the polynomial

$$\begin{aligned} H(x) &= l\left(\frac{x^9+2x^7+2x^5+2x^3}{(x^2-1)^3}\right)\cdot(x^2-1)^9 \\ &= \left(\left(\frac{x^9+2x^7+2x^5+2x^3}{(x^2-1)^3}\right)^3 + \left(\frac{x^9+2x^7+2x^5+2x^3}{(x^2-1)^3}\right)^2 \right. \\ &\quad \left. + \left(\frac{x^9+2x^7+2x^5+2x^3}{(x^2-1)^3}\right) + 2\right)\cdot(x^2-1)^9 \\ &= x^{27}+x^{24}+x^{22}+2x^{20}+2x^{19}+x^{18}+2x^{17}+2x^{16}+2x^{15} \\ &\quad +2x^{13}+x^{12}+2x^{11}+2x^9+x^8+2x^7+2x^6+2x^5+2x^3+1 \end{aligned}$$

is an IRP of degree 27 over $\mathbb{F}_3$.

Theorem 3.2: *Let $L(x) = \sum_{i=0}^{n} l_i x^i$ be an n degree IRP over $\mathbb{F}_q$, $q = p^k$. Assume that $Tr_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{L^*\prime(0)}{L^*(0)}\right) \neq 0$ and $Tr_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{L\prime(0)}{L(0)}\right) \neq 0$. Then,*

$$t(x) = L\left(\frac{(x^p-x^{p-1}+1)^p-(x^{p-1}-1)^{p-1}(x^p-x^{p-1}+1)}{(x^{p-1}-1)^p}\right)\cdot(x^{p-1}-1)^{pn}$$

is an IRP having degree p^2n over $\mathbb{F}_q$.

Proof: Consider a root $\gamma \in \mathbb{F}_{q^n}$ of $L(x)$. As $Tr_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{L^{*\prime}(0)}{L^*(0)}\right) \neq 0$, the polynomial, $f(x) = x^p - x - \gamma$ in $\mathbb{F}_{q^n}[x]$ is irreducible, as stated in Proposition 2.2. Further, by Lemma 3.1 the polynomial

$$H(x) = f\left(\frac{x^p - x^{p-1} + 1}{x^{p-1} - 1}\right) \cdot (x^{p-1} - 1)^p$$

over $\mathbb{F}_{q^n}$ is irreducible if and only if $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_p}\left(\frac{f'(1)}{f(1)}\right) \neq 0$. That is, $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_p}\left(\frac{1}{\gamma}\right) \neq 0$.

Since,

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_p}\left(\frac{1}{\gamma}\right) = Tr_{\mathbb{F}_q/\mathbb{F}_p}\left(Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left(\frac{1}{\gamma}\right)\right)$$
$$= -Tr_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{l_1}{l_0}\right) \neq 0.$$

Therefore,

$$Tr_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{l_1}{l_0}\right) = Tr_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{L'(0)}{L(0)}\right) \neq 0.$$

Thus,

$$H(x) = f\left(\frac{x^p - x^{p-1} + 1}{x^{p-1} - 1}\right) \cdot (x^{p-1} - 1)^p$$

over $\mathbb{F}_{q^n}$ is an IRP. As $f(x) = x^p - x - \gamma$, so

$$H(x) = \left(\left(\frac{x^p - x^{p-1} + 1}{x^{p-1} - 1}\right)^p - \left(\frac{x^p - x^{p-1} + 1}{x^{p-1} - 1}\right) - \gamma\right) \cdot (x^{p-1} - 1)^p$$
$$= ((x^p - x^{p-1} + 1)^p - (x^p - x^{p-1} + 1)(x^{p-1} - 1)^{p-1} - \gamma(x^{p-1} - 1)^p)$$

over $\mathbb{F}_{q^n}$ is an IRP. Hence, the obtained IRP over $\mathbb{F}_q$ of degree $p^2 n$ is

$$t(x) = L\left(\frac{(x^p - x^{p-1} + 1)^p - (x^p - x^{p-1} + 1)(x^{p-1} - 1)^{p-1}}{(x^{p-1} - 1)^p}\right) \cdot (x^{p-1} - 1)^{pn}.$$

Example 3.2: Let $\mathbb{F}_{3^3} = \mathbb{F}_3(\gamma)$, where γ is a root of a IRP $x^3 + 2x + 1$ over $\mathbb{F}_3$. Consider the polynomial $L(x) = (\gamma + 1)x^3 + (\gamma^2 + 1)x^2 + \gamma x + (\gamma^2 + 1)$ which is irreducible over $\mathbb{F}_{3^3}$. It follows that, $Tr_{3^3/3}\left(\frac{\gamma^2 + 1}{\gamma + 1}\right) = 2 \neq 0$ and $Tr_{3^3/3}\left(\frac{\gamma}{\gamma^2 + 1}\right) = 2 \neq 0$. Since assumptions of Theorem 3.2 are met, so the polynomial

$$H(x) = L\left(\frac{x^9 + 2x^7 + 2x^5 + 2x^3}{(x^2 - 1)^3}\right) \cdot (x^2 - 1)^9$$
$$= \left((\gamma + 1)\left(\frac{x^9 + 2x^7 + 2x^5 + 2x^3}{(x^2 - 1)^3}\right)^3 + (\gamma^2 + 1)\left(\frac{x^9 + 2x^7 + 2x^5 + 2x^3}{(x^2 - 1)^3}\right)^2\right.$$
$$\left. + \gamma\left(\frac{x^9 + 2x^7 + 2x^5 + 2x^3}{(x^2 - 1)^3}\right) + (\gamma^2 + 1)\right) \cdot (x^2 - 1)^9$$
$$= (1 + \gamma)x^{27} + (1 + \gamma^2)x^{24} + (\gamma^2 + 1)x^{22} + 2x^{21} + (2 + 2\gamma^2)x^{20}$$
$$+ 2\gamma x^{19} + 2\gamma x^{17} + (2 + 2\gamma^2)x^{16} + (2 + 2\gamma)x^{15} + 2\gamma x^{13}$$

$$+(1+\gamma^2)x^{12} + 2\gamma x^{11} + (2+2\gamma)x^9 + (1+\gamma^2)x^8 + 2\gamma x^7$$
$$+(2+2\gamma^2)x^6 + \gamma x^5 + 2x^3\gamma + 2 + 2\gamma$$

is an IRP over $\mathbb{F}_{3^3}$.

Theorem 3.3: *Let $L(x) = \sum_{i=0}^{n} l_i x^i$ be an n degree IRP over $\mathbb{F}_q$, $q = p^k$. Consider that $Tr_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{L^{*\prime}(0)}{L^*(0)}\right) \neq 0$ and $Tr_{\mathbb{F}_q/\mathbb{F}_p}(n) \neq 0$. Then, the polynomial*

$$t(x) = L\left(\frac{(x^p - x^{p-1}+1)^p - (x^p - x^{p-1}+1)x^{p-1}}{(x^p)^p}\right) \cdot (x^p)^{pn}$$

over $\mathbb{F}_q$ is an IRP having degree $p^2 n$.

Proof: Consider a root $\gamma \in \mathbb{F}_{q^n}$ of $L(x)$. As $Tr_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{L^{*\prime}(0)}{L^*(0)}\right) \neq 0$ the polynomial, $f(x) = x^p - x - \gamma$ in $\mathbb{F}_{q^n}[x]$ is irreducible, as stated in Proposition 2.2. Furthermore, applying Proposotion 2.4, the polynomial

$$H(x) = f\left(\frac{x^p - x^{p-1}+1}{x^p}\right) \cdot (x^p)^p$$

over $\mathbb{F}_{q^n}$ is an IRP if and only if $Tr_{q/p}(n + \frac{f^{*\prime}(0)}{f^*(0)}) \neq 0.$

Let

$$f(x) = x^p - x - \gamma.$$

Then, the reciprocal polynomial of $f(x)$ using Definition 2.2 is,

$$f^*(x) = -\gamma x^n - x^{n-1} + x^{n-p}.$$

Therefore, $Tr_{\mathbb{F}_q/\mathbb{F}_p}\left(n + \frac{f^{*\prime}(0)}{f^*(0)}\right) = Tr_{\mathbb{F}_q/\mathbb{F}_p}(n).$

By assumption $H(x)$ is irreducible if and only if $Tr_{\mathbb{F}_q/\mathbb{F}_p}(n) \neq 0.$ Thus,

$$H(x) = f\left(\frac{x^p - x^{p-1}+1}{x^p}\right) \cdot (x^p)^p$$

over $\mathbb{F}_{q^n}$ is an IRP. Now,

$$H(x) = \left(\left(\frac{x^p - x^{p-1}+1}{x^p}\right)^p - \left(\frac{x^p - x^{p-1}+1}{x^p}\right) - \gamma\right) \cdot (x^p)^p$$
$$= (x^p - x^{p-1} + 1)^p - (x^p - x^{p-1} + 1)x^{p-1} - \gamma(x^p)^p$$

over $\mathbb{F}_{q^n}$ is an IRP.

Therefore, by applying Proposition 2.1, we get an IRP of degree $p^2 n$ over $\mathbb{F}_q$ denoted by

$$t(x) = L\left(\frac{(x^p - x^{p-1}+1)^p - (x^p - x^{p-1}+1)x^{p-1}}{(x^p)^p}\right) \cdot (x^p)^{pn}.$$

Corollary 1: *Consider an IRP $P(x) = \sum_{i=0}^{2} c_i x^i$ of degree 3 over $\mathbb{F}_q$ with $q = 3^s$ and let $x^3 - lx + m$ and $x^3 - bx + k$ be relatively prime polynomials in $\mathbb{F}_q[x]$. Let $l \in \mathbb{F}_q^*, m, k \in \mathbb{F}_q$ and $(m,k) \neq (0,0)$. Then,*

$$H(x) = P\left(\frac{x^3 - lx + m}{x^3 - lx + k}\right) \cdot (x^3 - lx + k)^3$$

over $\mathbb{F}_q$ is an IRP of degree pn if $N_{\mathbb{F}_q/\mathbb{F}_p} = 1$ and $Tr_{\mathbb{F}_q/\mathbb{F}_p}(\frac{1}{B^p}\frac{(m-k)P\prime(1)}{P(1)} + 3m) \neq 0$.

Proof: An IRP $f(x)$ over $\mathbb{F}_q$, can be expressed over $\mathbb{F}_{q^n}$ as

$$f(x) = c_3 \prod_{u=0}^{2} (x - \gamma^{q^u}), \qquad c_n \in \mathbb{F}_q^* \tag{3}$$

such that, γ is a root of $P(x)$. Multiplying both sides of 3 by $(x^3 - lx + k)$ and subsitituting $x = \left(\frac{x^3-lx+m}{x^3-lx+k}\right)$, we have

$$\begin{aligned} H(x) &= \left(\frac{x^3-lx+m}{x^3-lx+k}\right) \cdot (x^3 - lx + k)^3 \\ &= c_3 \prod_{u=o}^{2} ((x^3 - lx + m) - \gamma^{q^u}(x^3 - lx + k)) \\ &= c_3 \prod_{u=0}^{2} ((1 - \gamma^{q^u})x^3 - (1 - \gamma^{q^u})lx + (m - \gamma^{q^u})) \\ &= c_3 \prod_{u=0}^{2} (1 - \gamma^{q^u}) \left(x^3 - lx + \frac{m-\gamma^{q^u}k}{1-\gamma^{q^u}}\right) \\ &= c_3(1 - \gamma)^{\left(\frac{q^3-1}{q-1}\right)} \prod_{u=0}^{2} \left(x^3 - lx + \frac{m-\gamma^{q^u}h}{1-\gamma^{q^u}}\right). \end{aligned}$$

Using Theorem 2.1, the polynomial $(x^3 - lx + m) - \gamma(x^3 - lx + k)$ or $\left(x^3 - lx - \frac{m-\gamma k}{\gamma-1}\right)$ is irreducible over $\mathbb{F}_q$ if and only if $l = B^{(p-1)}$ for some $B \in \mathbb{F}_{q^n}$. Also, $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_3}\left(\frac{m-\gamma k}{B^p(\gamma-1)}\right) \neq 0$ by the Proposition 2.3. It is obvious that $N_{\mathbb{F}_q/\mathbb{F}_3}(l) = 1$, so there always exists $B \in \mathbb{F}_q^*$ such that $B^{p-1} = l$.

Now, calculating the trace,

$$Tr_{\mathbb{F}_{q^3}/\mathbb{F}_3}\left(\frac{m-\gamma k}{B^p(\gamma-1)}\right) = Tr_{\mathbb{F}_q/\mathbb{F}_3}\left(\frac{1}{B^p} Tr_{\mathbb{F}_{q^3}/\mathbb{F}_q}\left(\frac{m-\gamma k}{\gamma-1}\right)\right).$$

Here,

$$\begin{aligned} Tr_{\mathbb{F}_{q^3}/\mathbb{F}_q}\left(\frac{m-k\gamma}{\gamma-1}\right) &= Tr_{\mathbb{F}_{q^3}/\mathbb{F}_q}\left(\frac{m}{\gamma-1}\right) - kTr_{\mathbb{F}_{q^3}/\mathbb{F}_q}\left(\frac{\gamma-1+1}{\gamma-1}\right) \\ &= mTr_{\mathbb{F}_{q^3}/\mathbb{F}_q}\left(\frac{1}{\gamma-1}\right) - k\left(Tr_{\mathbb{F}_{q^3}/\mathbb{F}_q}(1) + Tr_{\mathbb{F}_{q^3}/\mathbb{F}_q}\left(\frac{1}{\gamma-1}\right)\right). \end{aligned}$$

Now, to find $Tr_{\mathbb{F}_{q^3}/\mathbb{F}_q}\left(\frac{m-k\gamma}{\gamma-1}\right)$, we firstly calculate $Tr_{\mathbb{F}_{q^3}/\mathbb{F}_q}\left(\frac{1}{\gamma-1}\right)$.

Since,

$$P(x) = c_0 + c_1x + c_2x^2 + c_3x^3.$$

Therefore,

$$P(x + 1) = c_0 + c_1(x + 1) + c_2(x + 1)^2 + c_3(x + 1)^3 = \sum_{i=0}^{3} d_i x^i$$

and

$$Tr_{\mathbb{F}_{q^3}/\mathbb{F}_q}\left(\frac{1}{\gamma-1}\right) = -\frac{d_1}{d_0} = \frac{P\prime(1)}{P(1)}.$$

$$Tr_{\mathbb{F}_{q^3}/\mathbb{F}_q}\left(\frac{m-\gamma k}{B^p(\gamma-1)}\right) = Tr_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{1}{B^p}\left(\frac{mP\prime(1)}{P(1)} - k\left(3 - \frac{P\prime(1)}{P(1)}\right)\right)\right)$$

$$= -Tr_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{1}{B^p}\frac{(m-k)P\prime(1)}{P(1)} + 3k\right).$$

Hence, by assumption $Tr_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{1}{B^p}\frac{(m-k)P\prime(1)}{P(1)} + 3k\right) \neq 0$. Therefore,

$$H(x) = P\left(\frac{x^3-lx+m}{x^3-lx+k}\right)\cdot(x^3-lx+k)^3$$

is an IRP of degree pn over $\mathbb{F}_q$.

Theorem 3.4: *Let $L(x) = \sum_{i=0}^{n} l_i x^i$ be an n degree IRP over $\mathbb{F}_q$, $q = 3^s$. Consider that $Tr_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{L^*\prime(0)}{L^*(0)}\right) \neq 0$ and $Tr_{\mathbb{F}_q/\mathbb{F}_q}\left(\frac{(c+h)}{B^p}\left(\frac{L\prime(0)}{L(0)}\right)\right) \neq 0$, where $l \in \mathbb{F}_q^*$ and $m,k \in \mathbb{F}_q$, $(m,k) \neq (0,0)$. Then, an IRP $h(x)$ of degree $9n$ over $\mathbb{F}_q$ is defined as*

$$h(x) = L\left(\frac{(m-k)(x^3-lx+m)(2x^3-2lx+m+k)}{(x^3-lx+k)}\right)\cdot(x^3-lx+k)^{3n}.$$

Proof: Consider a root $\gamma \in \mathbb{F}_{q^n}$ of $L(x)$. As $Tr_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{L^*\prime(0)}{L^*(0)}\right) \neq 0$, the polynomial $f(x) = x^3 - x - \gamma$ in $\mathbb{F}_{q^n}[x]$ is irreducible, as stated in Proposition 2.2. Now, using Corollary 1, the polynomial

$$H(x) = f\left(\frac{x^3-lx+m}{x^3-lx+k}\right)\cdot(x^3-lx+k)^3$$

is irreducible over $\mathbb{F}_{q^n}$ if

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_3}\left(\frac{1}{B^p}\left(\frac{(m-k)f\prime(1)}{f(1)} + 3k\right)\right) \neq 0.$$

That is, $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_3}\left(\frac{(m-k)}{B^p}\left(\frac{-2}{\gamma}\right)\right) \neq 0$. Equivalently, $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_3}\left(\frac{(m-k)}{B^p\gamma}\right) \neq 0$.

Here,

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_3}\left(\frac{(m-k)}{B^p\gamma}\right) = Tr_{\mathbb{F}_q/\mathbb{F}_3}\left(Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left(\frac{(m-k)}{B^p\gamma}\right)\right).$$

Firstly, we need to calculate $\left(Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left(\frac{(m-k)}{B^p\gamma}\right)\right)$. That is,

$$\left(Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left(\frac{(m-k)}{B^p\gamma}\right)\right) = \frac{m+k}{B^p} Tr_{q^n/q}\left(\frac{1}{\gamma}\right)$$
$$= -\left(\frac{m+k}{B^p}\left(\frac{l_1}{l_o}\right)\right).$$

So,

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_3}\left(\frac{m+k}{B^p\gamma}\right) = -Tr_{\mathbb{F}_q/\mathbb{F}_3}\left(\frac{(m+k)}{B^p}\left(\frac{L\prime(0)}{L(0)}\right)\right) \neq 0.$$

That is,

$$Tr_{\mathbb{F}_q/\mathbb{F}_3}\left(\frac{(m+k)}{B^p}\left(\frac{L\prime(0)}{L(0)}\right)\right) \neq 0.$$

Thus,

$$H(x) = f\left(\frac{x^3-lx+m}{x^3-lx+k}\right) \cdot (x^3 - lx + k)^3$$

over $\mathbb{F}_{q^n}$ is an IRP. That is,

$$H(x) = \left(\frac{x^3-bx+c}{x^3-bx+h}\right)^3 - \left(\left(\frac{x^3-bx+c}{x^3-bx+h}\right) - \gamma\right) \cdot (x^3 - bx + h)$$
$$= (c-h)(x^3 - lx + m)(2x^3 - 2lx + m + k) - \gamma(x^3 - lx + k)^3$$

is an IRP over $\mathbb{F}_{q^n}$. Hence, By Proposition 2.1, IRP having degree $9n$ over $\mathbb{F}_q$ is :

$$t(x) = L\left(\frac{(m-k)(x^3-lx+m)(2x^3-2lx+m+k)}{(x^3-lx+k)}\right) \cdot (x^3 - lx + k)^{3n}.$$

4. Conclusion

The paper explores techniques for constructing irreducible polynomials of specific degrees $6n$ over $\mathbb{F}_{3^s}$ and p^2n over $\mathbb{F}_{p^s}$. It employs results and methods tailored for these constructions within the framework of finite fields and the composition method. This work is valuable for applications in coding theory, cryptography and other fields where finite fields and polynomial constructions play a crucial role.

Acknowledgement

The first author fully acknowledge the financial assistance of CSIR.

Conflict of Interest

There are no conflicts of interest declared by the authors.

References

[1] S. Abrahamyan, M. Alizadeh and M. K. Kyuregyan, "Recursive constructions of irreducible polynomials over finite fields," *Finite Fields and its Applications,* vol. 18, no. 4, pp. 738-745 (2012).

[2] M. Alan and B. Duman, "A note on construction of irreducible polynomials over finite fields with characteristic 2," *International Journal of Pure and Applied Mathematics,* vol. 115, no. 3, pp. 529-532 (2017).

[3] M. Alizadeh, "Constructing methods for irreducible polynomials," *Mathematical Problems of Computer Sciences*, vol. 35, pp. 26-32 (2011).

[4] M. Alizadeh, "Some algorithms for normality testing irreducible polynomials and computing complexity of the normal polynomials over finite fields," *Applied Mathematical Sciences*, vol. 6, no. 40, pp. 1997-2003 (2012).

[5] M. Alizadeh, S. Abrahamyan, S. Mehrabi and M. K. Kyuregyan, "Constructing of N-polynomials over finite fields," *International Journal of Algebra,* vol. 5, no. 29, pp. 1437-1442 (2011).

[6] M. Alizadeh, M. R. Darafsheh and S. Mehrabi, "On the k-normal elements and polynomials over finite fields," I*talian Journal of Pure and Applied Mathematics,* vol. 39, pp. 451-464 (2018).

[7] M. Alizadeh and S. Mehrabi, "Construction of self-reciprocal normal polynomials over finite fields of even characteristic," *Turkish Journal of Mathematics,* vol. 39, no. 2, pp. 259-267 (2015).

[8] S. D. Cohen, "On irreducible polynomials of certain types in finite fields," In *Mathematical Proceedings of the Cambridge Philosophical Society,* vol. 66, no. 2, pp. 335-344 (1969).

[9] S. Huczynska, G. L. Mullen, D. Panario, and D. Thomson, "Existence and properties of k-normal elements over finite fields," *Finite Fields and Their Applications,* vol. 24, pp. 170-183 (2013).

[10] X. D. Hou, "A criterion for the normality of polynomials over finite fields based on their coefficients," *Finite Fields and Their Applications,* vol. 93, pp. 102313 (2024).

[11] R. Kim and H. S. Son, "Recursive constructions of k-normal polynomials using some rational transformations over finite fields," *Journal of Algebra and its Applications,* vol. 19, no. 11, pp. 2050210 (2020).

[12] M. K. Kyuregyan, "Recurrent methods for constructing irreducible polynomials over GF(2^s)," *Finite Fields and its Applications*, vol. 8, no. 1, pp. 52-68 (2002).

[13] M. K., Kyuregyan, "Recursive constructions of N-polynomials over GF (2^s)," *Discrete Applied Mathematics,* vol. 156, no. 9, pp. 1554-1559 (2008).

[14] M. K. Kyuregyan, "Iterated constructions of irreducible polynomials over finite fields with linearly independent roots'', *Finite fields and their applications,* vol. 10, no. 3, pp. 323-341 (2004).

[15] R. Lidl and H. Niederreiter, Introduction to finite fields and their applications, Cambridge University Press, Cambridge (1986).

[16] A. J. Menezes, I. F. Blake, X. Gao, R. C. Mullin, S. A. Vanstone and T. Yaghoobian, Applications of Finite Fields, Kluwer Academic Publishers, Boston, Dordrecht, Lancaster (1993).

[17] H. Meyn, "Explicit n-polynomials of 2-power degree over finite fields," *I Designs, Codes and Cryptography*, vol. 6, no. 2, pp. 107-116 (1995).

[18] G. L. Mullen and D. Panario, Handbook of Finite Fields, Discrete Mathematics and its Applications, CRC Press, Taylor & Francis Group (2013).

[19] P. L. Sharma, Ashima and A. K. Sharma, "Recursive construction of normal polynomials over finite fields'', *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 8, pp. 2645-2660 (2021).

[20] P. L. Sharma and Ashima, "Construction of irreducible polynomials over finite fields," *Asian-European Journal of Mathematics*, vol. 15, no. 7, pp. 2250130 (2022).

[21] P. L. Sharma, S. Sharma and N. Dhiman, "Construction of infinite sequences of irreducible polynomials using Kloosterman sums," *Bulletin of Pure and Applied Sciences,* vol. 33, no. 2, pp. 161-168 (2014).

[22] P. L. Sharma, S. Sharma and M. Rehan, "Construction of infinite sequences of irreducible polynomials over $\mathbb{F}_2$," *International Journal of Mathematical Sciences and Engineering Applications,* vol. 9, no. 3, pp. 19-35 (2015).

[23] P. L. Sharma, S. Sharma and M. Rehan, "On construction of irreducible polynomials over $\mathbb{F}_3$," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 18, no. 4, pp. 335-347 (2015).

[24] Å . Schwarz, "Irreducible polynomials over finite fields with linearly independent roots," *Mathematica Slovaca*, vol. 38 no. 2, pp. 147-158 (1988).

[25] R. R. Varshamov, "A general method of synthesizing irreducible polynomials over Galois Fields," *Soviet Math. Dokl*, vol. 29, pp. 334-336 (1984).

[26] T. Baumbaugh and F. Manganiello, "Matroidal root structure of skew polynomials over finite fields," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 22, no. 3, pp. 377-389 (2019).

Received September, 2024