

# EXTENDED IRREDUCIBLE BINARY SEXTIC GOPPA CODES

DAITAO HUANG AND QIN YUE

ABSTRACT. Let  $n(> 3)$  be a prime number and  $\mathbb{F}_{2^n}$  a finite field of  $2^n$  elements. Let  $L = \mathbb{F}_{2^n} \cup \{\infty\}$  be the support set and  $g(x)$  an irreducible polynomial of degree 6 over  $\mathbb{F}_{2^n}$ . In this paper, we obtain an upper bound on the number of extended irreducible binary Goppa codes  $\Gamma(L, g)$  of degree 6 and length  $2^n + 1$ .

## 1. INTRODUCTION

Let  $\mathbb{F}_{2^n}$  be an extension of the finite field  $\mathbb{F}_2$ . Many codes defined over  $\mathbb{F}_2$  are subfield subcodes of another code defined over the extension  $\mathbb{F}_{2^n}$ . For instance, Alternant codes are subfield subcodes of Generalized Reed-Solomon codes and classical Goppa codes are a special case of Alternant codes [7].

Goppa codes are particularly appealing for cryptographic applications. McEliece was the first to exploit the potential of Goppa codes for the development of a secure cryptosystem [10]. Goppa codes are especially suited to this purpose because they have few invariants and the number of inequivalent codes grows exponentially with the length and dimension of the code. Indeed, since the introduction of code-based cryptography by McEliece in 1978 [5], Goppa codes still remain among the few families of algebraic codes which resist to any structural attack. This is one of the reasons why every improvement of our knowledge of these codes is of particular interest. In the McEliece cryptosystem, one chooses a random Goppa code as a key hence it is important that we know the number of Goppa codes for any given set of parameters. This will help in the assessment of how secure the McEliece cryptosystem is against an enumerative attack. An enumerative attack on the McEliece cryptosystem finds all Goppa codes for a given set of parameters and tests their equivalence with the public code [6]. There have been many attempts to count the number of Goppa codes.

In [1, 2, 3], it has been shown that two Alternant codes  $\mathcal{A}_k(v, L)$  and  $\mathcal{A}_k(v', L')$  are equal even if the parameters  $(v, L)$  are different from  $(v', L')$ . Based on these result, many extended Goppa codes become equivalent by a parity check in [13, 15]. Moreno [11] proved that there is only one extended irreducible binary degree 3 Goppa code of any length and that there are four quartic Goppa codes of length 33. Ryan [15]

---

2010 *Mathematics Subject Classification.* 94B05.

*Key words and phrases.* Binary Goppa codes, Extended Goppa codes, equivalent, Act on Group;

This work was supported in part by National Natural Science Foundation of China (No. 61772015).

focused on the quartic case of length  $2^n + 1$ , where  $n(> 3)$  is prime, and gave an upper bound on the number of inequivalent irreducible Goppa codes. Some similar topic were investigated in [16, 17, 18]. In [8], Magamba and Ryan obtained an upper bound on the number of extended irreducible  $q$ -ary Goppa codes of degree  $r$  and length  $q^n + 1$ , where  $p, r(> 2)$  are two prime numbers and  $q = p^t$ . In [12], Musukwa gave an upper bound on the number of inequivalent extended irreducible binary Goppa codes of degree  $2p$  and length  $2^n + 1$ , where  $n$  and  $p$  are two odd primes such that  $p \neq n$  and  $p \nmid (2^n \pm 1)$ .

In this paper, we shall investigate extended irreducible binary Goppa codes of degree  $r$ , where  $r$  is a product of two distinct prime numbers. In the case:  $r = 6$ , we obtain upper bound of number of extended irreducible binary sextic Goppa codes of length  $2^n + 1$ , where  $n(> 3)$  is a prime.

The paper is organized as follows. In Section 2, we remind some definitions of Alternant codes, Goppa codes, and extended Goppa codes. Moreover, we recall sufficient condition of equivalent extended Goppa codes by projective linear group acting on the projective line  $\mathbb{F}_{2^n} \cup \{\infty\}$ . In Section 3, we investigate projective semi-linear group acting on the element of degree 6 over  $\mathbb{F}_{2^n}$  with  $n(> 3)$  a prime. In Section 4, we obtain the upper bound on the number of inequivalent extended Goppa codes by applying the Cauchy Frobenius Theorem. We conclude the paper in Section 5.

## 2. PRELIMINARIES

Let  $\mathbb{F}_{2^n}$  be the finite field of order  $2^n$  and  $\overline{\mathbb{F}}_{2^n} = \mathbb{F}_{2^n} \cup \{\infty\}$  a set of coordinates for the projective line. We will introduce some basic knowledge in the following.

**2.1. Alternant code, Goppa Code and extended Goppa Code.** In the subsection, we describe concepts of Alternant codes, Goppa codes, and extended Goppa codes. In detail, see [3, 15].

**Definition 2.1.** Let  $L = (\alpha_0, \dots, \alpha_{m-1})$  be an  $m$ -tuple of distinct elements of  $\mathbb{F}_{2^n}$ ,  $v = (v_0, \dots, v_{m-1})$  an  $m$ -tuple of non-zero elements of  $\mathbb{F}_{2^n}$ , and  $r$  an integer less than  $m$ . The Alternant code  $\mathcal{A}_r(v, L)$  is defined as follows:

$$\mathcal{A}_r(v, L) = \{x = (x_0, \dots, x_{m-1}) \in \mathbb{F}_2^m : H_r(v, L)x^T = 0\},$$

where the parity-check matrix is

$$H_r(v, L) = \begin{pmatrix} v_0 & v_1 & \dots & v_{m-1} \\ v_0\alpha_0 & v_1\alpha_1 & \dots & v_{m-1}\alpha_{m-1} \\ \vdots & \vdots & & \vdots \\ v_0\alpha_0^{r-1} & v_1\alpha_1^{r-1} & \dots & v_{m-1}\alpha_{m-1}^{r-1} \end{pmatrix}.$$

**Definition 2.2.** Let  $L = (\alpha_0, \dots, \alpha_{m-1})$  be an  $m$ -tuple of distinct elements of  $\mathbb{F}_{2^n}$  and  $g(x) \in \mathbb{F}_{2^n}[x]$  a polynomial of degree  $r(< m)$  such that  $g(\alpha_i) \neq 0$  for  $i =$

$0, 1, \dots, m-1$ . The Goppa code  $\Gamma(g, L)$  with the Goppa polynomial  $g(x)$  and the support  $L$  is defined as follows:

$$\Gamma(g, L) = \left\{ x = (x_0, x_2, \dots, x_{m-1}) \in \mathbb{F}_2^m : \sum_{i=0}^{m-1} \frac{x_i}{x - \alpha_i} \equiv 0 \pmod{g(x)} \right\}.$$

If  $g(x)$  is irreducible over  $\mathbb{F}_{2^n}$ ,  $\Gamma(g, L)$  is called irreducible.

**Remark 2.3.** Let  $\Gamma(g, L)$  be the Goppa code in Definition 2.2.

- (1)  $\Gamma(g, L) = \mathcal{A}_r(v_{g,L}, L)$ , where  $v_{g,L} = (g(\alpha_0)^{-1}, g(\alpha_1)^{-1}, \dots, g(\alpha_{m-1})^{-1})$ .
- (2) The expurgated Goppa code  $\tilde{\Gamma}(g, L)$  of  $\Gamma(g, L)$  is defined as follows:

$$\tilde{\Gamma}(g, L) = \left\{ x = (x_0, \dots, x_{m-1}) \in \Gamma(g, L) : \sum_{i=0}^{m-1} x_i = 0 \right\}.$$

In fact,  $\tilde{\Gamma}(g, L) = \mathcal{A}_{r+1}(v_{g,L}, L)$ , where  $v_{g,L} = (g(\alpha_0)^{-1}, g(\alpha_1)^{-1}, \dots, g(\alpha_{m-1})^{-1})$ .

- (3) The extended Goppa code  $\bar{\Gamma}(g, L)$  of  $\Gamma(g, L)$  is defined as follows:

$$\bar{\Gamma}(g, L) = \left\{ x = (x_0, \dots, x_{m-1}, x_m) : (x_0, \dots, x_{m-1}) \in \Gamma(g, L), \sum_{i=0}^m x_i = 0 \right\}.$$

**Definition 2.4.** Let  $L = (\alpha_0, \dots, \alpha_{m-1})$  be an  $m$ -tuple of distinct elements of  $\mathbb{F}_{2^n}$ ,  $\bar{L} = L \cup \{\infty\} = (\alpha_0, \dots, \alpha_{m-1}, \infty)$ ,  $v = (v_0, \dots, v_m)$  an  $(m+1)$ -tuple of non-zero elements of  $\mathbb{F}_{2^n}$ , and  $r$  an integer less than  $m+1$ . The Alternant code  $\mathcal{A}_r(v, \bar{L})$  is defined as follows:

$$\mathcal{A}_r(v, \bar{L}) = \{x = (x_0, \dots, x_m) \in \mathbb{F}_2^{m+1} : H_r(v, \bar{L})x^T = 0\},$$

where the parity-check matrix is

$$H_r(v, \bar{L}) = \begin{pmatrix} v_0 & \dots & v_{m-1} & 0 \\ \vdots & & \vdots & \vdots \\ v_0 \alpha_0^{r-2} & \dots & v_{m-1} \alpha_{m-1}^{r-2} & 0 \\ v_0 \alpha_0^{r-1} & \dots & v_{m-1} \alpha_{m-1}^{r-1} & v_m \end{pmatrix}.$$

**Remark 2.5.** Let  $\Gamma(g, L)$  be the Goppa code in Definition 2.2,  $g(x) = \sum_{i=0}^r g_i x^i$  a polynomial of degree  $r$ , and  $\bar{L} = L \cup \{\infty\}$ . Then the extended Goppa code  $\bar{\Gamma}(g, L)$  of  $\Gamma(g, L)$  is just the Alternant code  $\mathcal{A}_{r+1}(v_{g,\bar{L}}, \bar{L})$ , where  $v_{g,\bar{L}} = (g(\alpha_0)^{-1}, \dots, g(\alpha_{m-1})^{-1}, g(\infty)^{-1})$ ,  $g(\infty) = g_r$ .

**2.2. Action of groups.** We will recall the actions of the projective linear group and the projective semi-linear group on  $\mathbb{F}_{2^n}$  and  $\bar{\mathbb{F}}_{2^n} = \mathbb{F}_{2^n} \cup \{\infty\}$ , respectively.

There are some matrix groups as follows:

- (1) the affine group

$$AGL_2(\mathbb{F}_{2^n}) = \left\{ M = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n} \right\};$$

(2) the general linear group

$$GL_2(\mathbb{F}_{2^n}) = \left\{ M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{F}_{2^n}, ad - bc \neq 0 \right\};$$

(3) the projective linear group

$$PGL_2(\mathbb{F}_{2^n}) = GL_2(\mathbb{F}_{2^n}) / \{aE_2 : a \in \mathbb{F}_{2^n}^*\},$$

where  $E_2$  is the  $2 \times 2$  identity matrix;

(4) the projective semi-linear group

$$P\Gamma L_2(\mathbb{F}_{2^n}) = PGL_2(\mathbb{F}_{2^n}) \times G,$$

where  $G = Gal(\mathbb{F}_{2^{6n}}/\mathbb{F}_2) = \langle \sigma \rangle$  is the Galois group,  $\sigma(x) = x^2$  for  $x \in \mathbb{F}_{2^{6n}}$ , and its operation  $\cdot$  is as follows:

$$(\widetilde{A}, \sigma^i) \cdot (\widetilde{B}, \sigma^j) = (\widetilde{A \cdot \sigma^i(B)}, \sigma^{i+j}), 0 \leq i, j \leq 6n - 1.$$

Let  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{F}_{2^n})$ . Then the projective linear group  $PGL_2(\mathbb{F}_{2^n})$  acts on  $\overline{\mathbb{F}_{2^n}}$  as follows:

$$\begin{aligned} PGL_2(\mathbb{F}_{2^n}) \times \overline{\mathbb{F}_{2^n}} &\rightarrow \overline{\mathbb{F}_{2^n}} \\ (\widetilde{M}, \zeta) &\mapsto \widetilde{M}(\zeta) = M(\zeta) = \frac{a\zeta + b}{c\zeta + d}, \end{aligned}$$

where  $\frac{1}{0} = \infty$  and  $\frac{1}{\infty} = 0$ ; the projective semi-linear group  $P\Gamma L_2(\mathbb{F}_{2^n})$  acts on  $\overline{\mathbb{F}_{2^n}}$  as follows:

$$\begin{aligned} P\Gamma L_2(\mathbb{F}_{2^n}) \times \overline{\mathbb{F}_{2^n}} &\rightarrow \overline{\mathbb{F}_{2^n}} \\ ((\widetilde{M}, \sigma^i), \zeta) &\mapsto (\widetilde{M}, \sigma^i)(\zeta) = M(\sigma^i(\zeta)) = \frac{a\zeta^{2^i} + b}{c\zeta^{2^i} + d}. \end{aligned}$$

In [3], there is a result as follows.

**Lemma 2.6.** *Let  $g(x)$  be a polynomial of degree  $r$  over  $\mathbb{F}_{2^n}$  and  $L = (\alpha_0, \dots, \alpha_{m-1})$  an ordered tuples of  $m$  distinct points in the projective line set  $\overline{\mathbb{F}_{2^n}}$ . Let  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{F}_{2^n})$ ,  $L'' = (M(\alpha_0), \dots, M(\alpha_{m-1}))$ ,  $g'(x) = (-cx + a)^r g(M^{-1}(x))$ ,  $M^{-1}(x) = \frac{dx-b}{-cx+a}$ , and  $g(-\frac{d}{c}) \neq 0$  if  $c \neq 0$ . Then the Alternant code  $\mathcal{A}_{r+1}(v_{g,L}, L)$  is equal to the Alternant code  $\mathcal{A}_{r+1}(v_{g',L''}, L'')$ .*

By Lemma 2.6, we have the following corollary.

**Corollary 2.7.** *Let  $g(x) = \sum_{k=0}^r g_k x^k$  be a polynomial of degree  $r$  over  $\mathbb{F}_{2^n}$  and  $L = (\alpha_0, \dots, \alpha_{m-1})$  an ordered tuples of  $m$  distinct points in the projective line set  $\overline{\mathbb{F}_{2^n}}$ . Let  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{F}_{2^n})$ ,  $\tau \in G = Gal(\mathbb{F}_{2^{6n}}/\mathbb{F}_2)$ ,  $L' = (\tau(\alpha_0), \dots, \tau(\alpha_{m-1}))$ ,  $L'' = (M(\tau(\alpha_0)), \dots, M(\tau(\alpha_{m-1})))$ ,  $\tau g(x) = \sum_{k=0}^r \tau(g_k) x^k$ ,  $(\tau g)'(x) = (-cx + a)^r \cdot$*

$\tau g(M^{-1}(x))$ , and  $(\tau g)(-\frac{d}{c}) \neq 0$  if  $c \neq 0$ . Then the Alternant code  $\mathcal{A}_{r+1}(v_{g,L}, L)$  is equal to the Alternant code  $\mathcal{A}_{r+1}(v_{(\tau g)',L''}, L'')$ .

*Proof.* Since the Alternant code  $\mathcal{A}_{r+1}(v_{g,L}, L)$  is a subfield subcode, the Alternant code is equal to the Alternant code  $\mathcal{A}_{r+1}(v_{\tau g,L'}, L')$ . By Lemma 2.6, the Alternant code  $\mathcal{A}_{r+1}(v_{\tau g,L'}, L')$  is equal to the Alternant code  $\mathcal{A}_{r+1}(v_{(\tau g)',L''}, L'')$ .  $\square$

In Corollary 2.7, if  $\tau$  is equal to the identity transformation, then Lemma 2.6 is direct from Corollary 2.7. If  $g(x)$  is irreducible over  $\mathbb{F}_{2^n}$  and has a root  $\alpha$  in an extension over  $\mathbb{F}_{2^n}$ , then  $(\tau g)'(x) = (-cx + a)^r \cdot \tau g(M^{-1}(x))$  is the irreducible polynomial of degree  $r$  over  $\mathbb{F}_{2^n}$  and has a root  $\beta$  in an extension with

$$\beta = (\widetilde{M}, \tau)\alpha = M(\tau(\alpha)) = \frac{a\tau(\alpha) + b}{c\tau(\alpha) + d}.$$

**2.3. Equivalent extended Goppa codes.** Let  $g(x)$  be irreducible of degree  $r$  over  $\mathbb{F}_{2^n}$  and  $L = (\alpha_0, \dots, \alpha_{2^n-1})$  an ordered subset of  $2^n$  distinct points in  $\mathbb{F}_{2^n}$ . Suppose that  $g(x)$  has a root  $\alpha$  in an extension over  $\mathbb{F}_{2^n}$ . Then

$$\Gamma(g, L) = \{x = (x_0, x_1, \dots, x_{2^n-1}) \in \mathbb{F}_2^{2^n} : H(\alpha)x^T = 0\},$$

where the parity check matrix is

$$H(\alpha) = \left( \frac{1}{\alpha - \alpha_0} \quad \frac{1}{\alpha - \alpha_1} \quad \dots \quad \frac{1}{\alpha - \alpha_{2^n-1}} \right).$$

See more detail in [4].

For convenience, we will denote by

$$C(\alpha) = \Gamma(g, L) \text{ and } \overline{C(\alpha)} = \overline{\Gamma}(g, L),$$

where  $\overline{\Gamma}(g, L)$  is the extended Goppa code of  $\Gamma(g, L)$ .

The following Lemma is similar to that in [15]. For completeness, we give the proof.

**Lemma 2.8.** *Let  $L = (\alpha_0, \dots, \alpha_{2^n-1})$  and  $\overline{L} = (\alpha_0, \dots, \alpha_{2^n-1}, \infty)$  be ordered tuples of  $2^n$  and  $2^n + 1$  distinct points in the projective line  $\overline{\mathbb{F}}_{2^n}$ , respectively. Let  $\alpha$  be a root of an irreducible polynomial  $g(x) = \sum_{i=0}^r g_i x^i$  of degree  $r$  over  $\mathbb{F}_{2^n}$ .*

*Let  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{F}_{2^n})$ ,  $\tau \in G = Gal(\mathbb{F}_{2^{6n}}/\mathbb{F}_2)$ ,  $(\widetilde{M}, \tau) \in PGL_2(\mathbb{F}_{2^n})$ ,  $\overline{L}'' = (M(\tau(\alpha_0)), \dots, M(\tau(\alpha_{2^n-1})), M(\infty))$ ,  $\tau g(x) = \sum_{i=0}^r \tau(g_i)x^i$ , and  $(\tau g)'(x) = (-cx + a)^r \cdot \tau g(M^{-1}(x))$  a root  $\beta = (\widetilde{M}, \tau)\alpha = \frac{a\tau(\alpha)+b}{c\tau(\alpha)+d}$ . Then the Alternant code  $\mathcal{A}_{r+1}(v_{g,\overline{L}}, \overline{L})$  is equal to the Alternant code  $\mathcal{A}_{r+1}(v_{(\tau g)',\overline{L}''}, \overline{L}'')$  and the extended Goppa code  $\overline{C(\alpha)}$  is permutation equivalent to the extended Goppa code  $\overline{C(\beta)}$ , denoted by  $\overline{C(\alpha)} \cong \overline{C(\beta)}$ .*

*Proof.* Let  $\bar{L} = (\alpha_0, \dots, \alpha_{2^n-1}, \infty) = L \cup \{\infty\}$  be an ordered tuple of  $2^n + 1$  distinct points in the projective line  $\bar{\mathbb{F}}_{2^n} = \mathbb{F}_{2^n} \cup \{\infty\}$  and  $g(x)$  irreducible of degree  $r$  over  $\mathbb{F}_{2^n}$ . Then by Remark 2.5,

$$\mathcal{A}_{r+1}(v_{g, \bar{L}}, \bar{L}) = \bar{\Gamma}(g, L),$$

where  $\mathcal{A}_{r+1}(v_{g, \bar{L}}, \bar{L})$  is the Alternant code and  $\bar{\Gamma}(g, L)$  is the extended code of  $\Gamma(g, L)$ .

Let  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{F}_{2^n})$ ,  $\tau \in G = Gal(\mathbb{F}_{2^{6n}}/\mathbb{F}_2)$ ,  $(\widetilde{M}, \tau) \in P\Gamma L_2(\mathbb{F}_{2^n})$ ,  $\tau g(x) = \sum_{k=0}^r \tau(g_k)x^k$ ,  $(\tau g)'(x) = (-cx + a)^r \cdot \tau g(M^{-1}(x))$  a root  $\beta = (\widetilde{M}, \tau)\alpha = \frac{a\tau(\alpha)+b}{c\tau(\alpha)+d}$ , and

$$\bar{L}'' = (\widetilde{M}, \tau)(\bar{L}) = (M(\tau(\alpha_0)), M(\tau(\alpha_1)), \dots, M(\tau(\alpha_{2^n-1}), M(\infty)).$$

Then by Corollary 2.7,

$$\mathcal{A}_{r+1}(v_{g, \bar{L}}, \bar{L}) = \mathcal{A}_{r+1}(v_{(\tau g)', \bar{L}'', \bar{L}''}). \quad (2.1)$$

Let  $g(x)$  have a root  $\alpha$  in an extension over  $\mathbb{F}_{2^n}$ . Then  $(\tau g)'(x)$  is irreducible over  $\mathbb{F}_{2^n}$  and has a root  $\beta = (\widetilde{M}, \tau)\alpha = \frac{a\tau(\alpha)+b}{c\tau(\alpha)+d}$  in an extension over  $\mathbb{F}_{2^n}$ . Note that  $\bar{L}$  and  $\bar{L}''$  arrange in distinct orders of the projective set  $\bar{\mathbb{F}}_{2^n}$ . Hence by Remark 2.5 and (2.1),

$$\bar{\Gamma}(g, L) \cong \bar{\Gamma}((\tau g)', L), \text{ i.e., } \overline{C(\alpha)} \cong \overline{C(\beta)},$$

i.e., the extended Goppa code  $\overline{C(\alpha)}$  is permutation equivalent to the extended Goppa code  $\overline{C(\beta)}$ .  $\square$

In [15], Ryan used Lemma 2.8 to give an upper bound on the number of extended irreducible binary quartic Goppa codes of length  $2^n + 1$ , where  $n(> 3)$  is a prime number. In this paper, we shall obtain an upper bound on the number of extended irreducible binary sextic quatic Goppa codes of length  $2^n + 1$ , where  $n(> 3)$  is a prime number. By  $3|(2^n + 1)$  for any  $n(> 3)$  a prime, we prove that there are orbits of length 3 in Propositions 4.3, which is important and different from [15].

### 3. PRIME $n > 3$

In this section, we investigate irreducible binary sextic Goppa codes over  $\mathbb{F}_{2^n}$ . We always assume that  $n(> 3)$  is a prime number.

**Definition 3.1.** The set  $\mathbb{S} = \mathbb{S}(n, 6)$  is the set of all elements in  $\mathbb{F}_{2^{6n}}$  of degree 6 over  $\mathbb{F}_{2^n}$ .

In fact,  $\mathbb{S} = \mathbb{F}_{2^{6n}} \setminus \{\mathbb{F}_{2^{2n}} \cup \mathbb{F}_{2^{3n}}\}$ , then

$$|\mathbb{S}| = 2^{6n} - 2^{2n} - 2^{3n} + 2^n.$$

**Lemma 3.2.** *The projective semi-linear group  $P\Gamma L_2(\mathbb{F}_{2^n})$  acts on on the set  $\mathbb{S}$ :*

$$\begin{aligned} \pi : P\Gamma L_2(\mathbb{F}_{2^n}) \times \mathbb{S} &\rightarrow \mathbb{S} \\ ((\widetilde{M}, \sigma^i), \alpha) &\mapsto (\widetilde{M}, \sigma^i)(\alpha) = \frac{a\alpha^{2^i} + b}{c\alpha^{2^i} + d} = \beta, \end{aligned}$$

where  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{F}_{2^n})$ ,  $G = Gal(\mathbb{F}_{2^{6n}}/\mathbb{F}_2) = \langle \sigma \rangle$ .

Moreover, by Lemma 2.8 the extended Goppa code  $\overline{C(\alpha)}$  is permutation equivalent to the extended Goppa code  $\overline{C(\beta)}$ , i.e.,  $\overline{C(\alpha)} \cong \overline{C(\beta)}$ .

By Lemma 3.2, there is an equivalent relation  $\sim$  in  $\mathbb{S}$ : for  $\alpha, \beta \in \mathbb{S}$ ,

$$\alpha \sim \beta \iff \exists (\widetilde{M}, \sigma^i) \in P\Gamma L_2(\mathbb{F}_{2^n}), (\widetilde{M}, \sigma^i)\alpha = \beta;$$

moreover, by Lemma 2.8

$$\alpha \sim \beta \implies \overline{C(\alpha)} \cong \overline{C(\beta)}. \quad (3.1)$$

There is an interesting question: does the converse proposition of (3.1) hold?

By Lemma 3.2, the orbit of  $\alpha \in \mathbb{S}$  is

$$\begin{aligned} \Omega_\alpha &= \{\beta \in \mathbb{S} : \alpha \sim \beta\} \\ &= \left\{ (\widetilde{M}, \sigma^i)\alpha = \frac{a\alpha^{2^i} + b}{c\alpha^{2^i} + d} : \forall M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{F}_{2^n}), 0 \leq i \leq 6n - 1 \right\} \\ &= \left\{ \sigma^i(\widetilde{M}(\alpha)) = \left(\frac{a\alpha + b}{c\alpha + d}\right)^{2^i} : \forall M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{F}_{2^n}), 0 \leq i \leq 6n - 1 \right\}. \end{aligned} \quad (3.2)$$

Then the number of different orbits in  $\mathbb{S}$  under the action of the group  $P\Gamma L_2(\mathbb{F}_{2^n})$  is the upper bound of inequivalent extended irreducible binary sextic Goppa codes.

To compute the number of orbits in  $\mathbb{S}$  under the action of the group  $P\Gamma L_2(\mathbb{F}_q)$ , by (3.2) we shall divide the action into two actions.

(1) We consider the projective linear group  $PGL_2(\mathbb{F}_{2^n})$  acting on  $\mathbb{S}$ . Then

$$\mathbb{S} = \bigcup_{\alpha \in I} O_\alpha, \quad \Omega = \{O_\alpha : \alpha \in I\}, \quad (3.3)$$

where  $\Omega$  is the set of all distinct orbits in  $\mathbb{S}$  under the action of the projective linear group  $PGL_2(\mathbb{F}_{2^n})$ . In fact,  $\Omega$  is a partition of  $\mathbb{S}$ .

(2) We consider the Galois group  $G = Gal(\mathbb{F}_{2^{6n}}/\mathbb{F}_2) = \langle \sigma \rangle$  acting on  $\Omega$ . Then there is a partition of  $\Omega$ :

$$\Omega = \bigcup_{\alpha \in J} \Omega_\alpha, \quad (3.4)$$

$$\Omega_\alpha = G(O_\alpha) = \{\sigma^i(O_\alpha) : 0 \leq i \leq 6n - 1\} \subset \Omega,$$

where  $\{\Omega_\alpha : \alpha \in J\}$  is the set of all distinct orbits in  $\mathbb{S}$  under the action of the projective semi-linear group  $P\Gamma L_2(\mathbb{F}_{2^n})$ . In fact,  $|J|$  is just the number of different orbits in  $\mathbb{S}$  under the action of the group  $P\Gamma L_2(\mathbb{F}_{2^n})$ .

In order to count the size of the set  $J$ , we shall use Cauchy Frobenius Theorem about orbits in [9].

**Lemma 3.3.** *Let  $G$  be a finite group acting on a set  $X$ . For any  $g \in G$ , let  $F(g)$  denote the set of elements of  $X$  fixed by  $g$ . Then the number of distinct orbits in  $X$  under the action of the group  $G$  is  $\frac{1}{|G|} \sum_{g \in G} |F(g)|$ .*

We firstly state the main result in the following theorem.

**Theorem 3.4.** *Let  $n > 3$  be a prime number. The number of extended irreducible binary sextic Goppa codes of length  $2^n + 1$  over  $\mathbb{F}_{2^n}$  is at most  $\frac{2^{3n} + 2^{2n} + 3 \cdot 2^n + 12n - 18}{6n}$ .*

To prove Theorem 3.4, we shall show some propositions.

3.1.  $PGL_2(\mathbb{F}_{2^n}) \times \mathbb{S} \rightarrow \mathbb{S}$ . Consider the projective linear group  $PGL_2(\mathbb{F}_{2^n})$  acting on the set  $\mathbb{S}$  as follows:

$$\begin{aligned} PGL(\mathbb{F}_{2^n}) \times \mathbb{S} &\rightarrow \mathbb{S} \\ (\widetilde{M}, \alpha) &\mapsto \widetilde{M}(\alpha) = M(\alpha) = \frac{a\alpha + b}{c\alpha + d}, \end{aligned}$$

where  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(\mathbb{F}_{2^n})$ . Clearly, it is a faithful action. Then

$$\mathbb{S} = \bigcup_{\alpha \in I} O_\alpha, \Omega = \{O_\alpha : \alpha \in I\},$$

where  $\Omega$  is the set of all distinct orbits in  $\mathbb{S}$  under the action of the projective linear group  $PGL_2(\mathbb{F}_{2^n})$ . In fact,  $\Omega$  is a partition of  $\mathbb{S}$ . We shall calculate the size of the set  $I$ .

It is clear that

$$|PGL_2(\mathbb{F}_{2^n})| = \frac{|GL_2(\mathbb{F}_{2^n})|}{|\{aE_2 : a \in \mathbb{F}_{2^n}^*\}|} = 2^{3n} - 2^n.$$

For  $\alpha \in I$ , let  $H_\alpha$  denote the stabilizer of  $\alpha$  under the action of  $PGL_2(\mathbb{F}_{2^n})$ , then

$$H_\alpha = \left\{ \widetilde{M}(\alpha) = \alpha : \widetilde{M} \in PGL_2(\mathbb{F}_{2^n}) \right\} = \left\{ \widetilde{E}_2 \right\}$$

and

$$|O_\alpha| = \frac{|PGL_2(\mathbb{F}_{2^n})|}{|H_\alpha|} = 2^{3n} - 2^n.$$

By  $|\mathbb{S}| = 2^{6n} - 2^{2n} - 2^{3n} + 2^n$ ,

$$|I| = \frac{|\mathbb{S}|}{|O_\alpha|} = 2^{3n} + 2^n - 1.$$

Moreover, we investigate the structure of each orbit  $O_\alpha$ . Note that the projective linear group  $PGL_2(\mathbb{F}_{2^n})$  acts transitively on the orbit  $O_\alpha$ .

Since there is an injective homomorphism of two groups:

$$\begin{aligned} AGL_2(\mathbb{F}_{2^n}) &\rightarrow PGL_2(\mathbb{F}_{2^n}) \\ M = \begin{pmatrix} e & f \\ 0 & 1 \end{pmatrix} &\mapsto \widetilde{M}, \end{aligned}$$

the affine group  $AGL_2(\mathbb{F}_{2^n})$  is viewed as the subgroup of  $PGL_2(\mathbb{F}_{2^n})$ .

Hence there is an action of  $AGL_2(\mathbb{F}_{2^n})$  on  $O_\alpha$ :

$$\begin{aligned} AGL_2(\mathbb{F}_{2^n}) \times O_\alpha &\rightarrow O_\alpha \\ (M, \beta) &\mapsto e\beta + f, \end{aligned}$$

where  $M = \begin{pmatrix} e & f \\ 0 & 1 \end{pmatrix} \in AGL_2(\mathbb{F}_{2^n})$ ,  $\beta = \frac{a\alpha+b}{c\alpha+d} \in O_\alpha$ ,  $a, b, c, d \in \mathbb{F}_{2^n}$ ,  $ad - bc \neq 0$ .

We shall investigate all distinct orbits in  $O_\alpha$  under the action of the affine group  $AGL_2(\mathbb{F}_{2^n})$ .

For  $\beta = \frac{a\alpha+b}{c\alpha+d} \in O_\alpha$ , the orbit of  $\beta$  in  $O_\alpha$  under the action of the affine group  $AGL_2(\mathbb{F}_{2^n})$  is

$$A(\beta) = \left\{ M(\beta) = e\beta + f : M = \begin{pmatrix} e & f \\ 0 & 1 \end{pmatrix} \in AGL_2(\mathbb{F}_{2^n}) \right\}.$$

The following lemma is from [14, 15].

**Lemma 3.5.**

$$O_\alpha = \left( \bigcup_{\gamma \in \mathbb{F}_{2^n}} A\left(\frac{1}{\alpha + \gamma}\right) \right) \bigcup A(\alpha),$$

which are disjoint unions. Moreover, there is a partition of  $O_\alpha$  :

$$\Delta_\alpha = \left\{ A(\alpha), A\left(\frac{1}{\alpha + \gamma}\right) : \gamma \in \mathbb{F}_{2^n} \right\}. \quad (3.5)$$

3.2.  $G \times \Omega \rightarrow \Omega$ . Let  $G = Gal(\mathbb{F}_{2^{6n}}/\mathbb{F}_2) = \langle \sigma \rangle$  be the Galois group of  $\mathbb{F}_{2^{6n}}$  over  $\mathbb{F}_2$  and  $\Omega$  defined as (3.3). Now consider the group  $G$  acting on the set  $\Omega$ :

$$\begin{aligned} \varphi : G \times \Omega &\rightarrow \Omega \\ (\sigma^i, O_\alpha) &\mapsto \sigma^i(O_\alpha) = O_{\sigma^i(\alpha)}. \end{aligned}$$

Now we shall count the number of distinct orbits in  $\Omega$  under the action of  $G$ . By Lemma 3.3, we need to calculate that for  $\sigma^i \in G$ ,  $0 \leq i \leq 6n - 1$ ,

$$|F(\sigma^i)| = |\{O_\alpha \in \Omega : \sigma^i(O_\alpha) = O_\alpha\}|. \quad (3.6)$$

**Remark 3.6.** (1) In fact, for  $0 \leq i \leq 6n - 1$ , let  $d = \gcd(6n, i)$ , then  $\langle \sigma^i \rangle = \langle \sigma^d \rangle$ . Thus,

$$\{O_\alpha \in \Omega : \sigma^i(O_\alpha) = O_\alpha\} = \{O_\alpha \in \Omega : \sigma^d(O_\alpha) = O_\alpha\}$$

and

$$|F(\sigma^i)| = |F(\sigma^d)|.$$

(2) Let  $o(\sigma^i)$  denote the order of  $\sigma^i$  in  $G$ , then  $o(\sigma^i) \mid |G|$ . By  $|G| = 6n$  and  $n$  a prime,

$$o(\sigma^i) \in \{1, 2, 3, 6, n, 2n, 3n, 6n\}.$$

Suppose that  $o(\sigma^i) \in \{6n, 3n\}$  and  $\sigma^i(O_\alpha) = O_\alpha$ . Then  $H = \langle \sigma^i \rangle = \langle \sigma^k \rangle$ ,  $k \in \{1, 2\}$ , and  $\sigma^k(O_\alpha) = O_\alpha$ . Hence  $\frac{a\alpha+b}{c\alpha+d} = \alpha^{2^k}$ , which is impossible by  $\alpha$  of degree 6 over  $\mathbb{F}_{2^n}$ . Therefore

$$|F(\sigma^i)| = 0 \text{ if } o(\sigma^i) \in \{6n, 3n\}.$$

In the next section, we shall discuss other cases.

#### 4. THE ACTION OF $G$ ON $\Omega$

**Proposition 4.1.** *Let  $G = \text{Gal}(\mathbb{F}_{2^{6n}}/\mathbb{F}_2) = \langle \sigma \rangle$ .*

(1) *If  $o(\sigma^i) = 1$ , then  $|F(\sigma^i)| = |\Omega| = 2^{3n} + 2^n - 1$ .*

(2) *If  $o(\sigma^i) = 2$ , then  $|F(\sigma^i)| = 2^{2n} - 1$ .*

*Proof.* (1) If  $o(\sigma^i) = 1$ , then for all  $O_\alpha \in \Omega$ ,  $\sigma^i(O_\alpha) = O_\alpha$  and  $|F(\sigma^i)| = |\Omega| = 2^{3n} + 2^n - 1$ .

(2) By  $o(\sigma^i) = 2$ ,  $H = \langle \sigma^i \rangle = \langle \sigma^{3n} \rangle$ . Suppose that  $\sigma^{3n}(O_\alpha) = O_\alpha$  for  $O_\alpha \in \Omega$ . Then the group  $H$  acts on the partition  $\Delta_\alpha$  of  $O_\alpha$  in (3.5) as follows:

$$\begin{aligned} H \times \Delta_\alpha &\longrightarrow \Delta_\alpha \\ (\sigma^{3ni}, A(\alpha)) &\longmapsto \sigma^{3ni}(A(\alpha)), i = 0, 1. \end{aligned}$$

Denote by  $O_{A(\alpha)}$  the orbit of  $A(\alpha)$  under the action of the subgroup  $H = \langle \sigma^{3n} \rangle$ . Then there is a class equation:

$$2^n + 1 = |\Delta_\alpha| = \sum |O_{A(\alpha)}|.$$

By  $|H| = 2$ , there is  $A(\alpha) \in \Delta_\alpha$  such that  $|O_{A(\alpha)}| = 1$ , i.e.,  $\sigma^{3n}(A(\alpha)) = A(\alpha)$ . Hence

$$\sigma^{3n}(\alpha) = \alpha^{2^{3n}} = c_1\alpha + c_2,$$

with  $c_1 \in \mathbb{F}_{2^n}^*$ ,  $c_2 \in \mathbb{F}_{2^n}$ . Then  $\alpha = \sigma^{6n}(\alpha) = c_1\sigma^{3n}(\alpha) + c_2 = c_1^2\alpha + c_1c_2 + c_2$ . Thus  $c_1 = 1$  and

$$\alpha^{2^{3n}} = \alpha + c_2$$

with  $c_2 \neq 0$  (if  $c_2 = 0$ , then  $\alpha \in \mathbb{F}_{2^{3n}}$  which is contradictory.). Consequently,

$$(c_2^{-1}\alpha)^{2^{3n}} + c_2^{-1}\alpha + 1 = 0.$$

If  $c_2^{-1}\alpha$  is viewed as  $\alpha$  then  $\alpha$  satisfies the equation:

$$x^{2^{3n}} + x + 1 = 0.$$

Hence there is a factorization:

$$x^{2^{3n}} + x + 1 = \prod_{c \in \mathbb{F}_{2^{3n}}} (x + \alpha + c).$$

It is clear that  $\alpha^{2^{6n}} = \alpha$  and  $\alpha^{2^{3n}} = \alpha + 1$ , so all roots  $\alpha + c \in \mathbb{F}_{2^{6n}} \setminus \mathbb{F}_{2^{3n}}$ ,  $c \in \mathbb{F}_{2^{3n}}$ .

Moreover, if  $\alpha$  is a root of the polynomial  $x^{2^{3n}} + x + 1$  and  $\alpha \in \mathbb{F}_{2^{2n}}$ , then  $\alpha$  is a root of the polynomial  $x^{2^n} + x + 1$  and there is a factorization:

$$x^{2^n} + x + 1 = \prod_{c \in \mathbb{F}_{2^n}} (x + \alpha + c)$$

and all roots  $\alpha + c \in \mathbb{F}_{2^{2n}}$ ,  $c \in \mathbb{F}_{2^n}$ .

Hence there are  $2^{3n} - 2^n$  roots of  $x^{2^{3n}} + x + 1$  in  $\mathbb{S}$ .

Conversely, if  $\alpha \in \mathbb{S}$  is a root of  $x^{2^{3n}} + x + 1$ , then  $\sigma^{3n}(A(\alpha)) = A(\alpha)$ .

Therefore  $\alpha \in \mathbb{S}$  is a root of  $x^{2^{3n}} + x + 1 = 0$  if and only if  $\sigma^{3n}(A(\alpha)) = A(\alpha)$ ; moreover,  $A(\alpha)$  has  $2^n$  roots  $\alpha + c, c \in \mathbb{F}_{2^n}$ , of the polynomial  $x^{2^{3n}} + x + 1$ .

Suppose that  $\sigma^{3n}(A(\alpha)) = A(\alpha)$ ,  $\alpha^{2^{3n}} + \alpha + 1 = 0$ , and  $\sigma^{3n}(A(\frac{1}{\alpha+\gamma})) = A(\frac{1}{\alpha+\gamma})$ . Then

$$\left(\frac{1}{\alpha+\gamma}\right)^{2^{3n}} = \frac{1}{\alpha+1+\gamma} = \frac{b_1}{\alpha+\gamma} + b_2, 0 \neq b_1, b_2 \in \mathbb{F}_{2^n},$$

which is contradictory with  $\alpha$  of degree 6 over  $\mathbb{F}_{2^n}$ .

In conclusion,  $\sigma^{3n}(O_\alpha) = O_\alpha$  if and only if  $\sigma^{3n}(A(\alpha)) = A(\alpha)$  if and only if there are  $2^n$  roots of  $x^{2^{3n}} + x + 1$  in  $O_\alpha$ . Then

$$|F(\sigma^{3n})| = \frac{2^{3n} - 2^n}{2^n} = 2^{2n} - 1.$$

□

**Lemma 4.2.**

$$\left| \left\{ \beta \in \mathbb{S} : \beta^{2^{2n}} + \frac{1}{\beta} + 1 = 0 \right\} \right| = 2^{2n} - 2^n - 2.$$

*Proof.* Now we investigate roots of the following equation

$$x^{2^{2n}} + \frac{1}{x} + 1 = 0. \quad (4.1)$$

Suppose that  $\beta$  is a root in (4.1) and

$$B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}. \quad (4.2)$$

Then  $\beta^{2^{2n}} = B(\beta)$ . By  $o(B) = 3$ ,  $\beta^{2^{6n}} = B^3(\beta) = \beta$  and  $\beta \in \mathbb{F}_{2^{6n}}$ . In the following, we shall find all roots  $\beta$  in (4.1) such that  $\beta \in \mathbb{F}_{2^{2n}} \cup \mathbb{F}_{2^{3n}}$ .

It is clear that  $\beta \in \mathbb{F}_{2^{2n}}$  if and only if  $\beta = \frac{1}{\beta} + 1$ , i.e.,  $o(\beta) = 3$  and  $\beta \in \mathbb{F}_4$ . Then

$$\left| \left\{ \beta \in \mathbb{F}_{2^{2n}} : \beta^{2^{2n}} + \frac{1}{\beta} + 1 = 0 \right\} \right| = \left| \left\{ \beta \in \mathbb{F}_{2^{2n}} : \beta + \frac{1}{\beta} + 1 = 0 \right\} \right| = 2.$$

If  $\beta \in \mathbb{F}_{2^{3n}}$ , then  $\beta^{2^n} + \frac{1}{\beta+1} = 0$ . Conversely, if  $\beta^{2^n} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}(\beta)$ , then  $\beta^{2^{3n}} =$

$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^3(\beta) = \beta$  and  $\beta \in \mathbb{F}_{2^{3n}}$ . Hence

$$\left| \left\{ \beta \in \mathbb{F}_{2^{3n}} : \beta^{2^{2n}} + \frac{1}{\beta} + 1 = 0 \right\} \right| = \left| \left\{ \beta \in \mathbb{F}_{2^{3n}} : \beta^{2^n}(\beta + 1) + 1 = 0 \right\} \right| = 2^n + 1.$$

Therefore

$$\left| \left\{ \beta \in \mathbb{S} : \beta^{2^{2n}} + \frac{1}{\beta} + 1 = 0 \right\} \right| = 2^{2n} + 1 - 2 - (2^n + 1) = 2^{2n} - 2^n - 2.$$

□

**Proposition 4.3.** *Let  $G = \text{Gal}(\mathbb{F}_{2^{6n}}/\mathbb{F}_2) = \langle \sigma \rangle$ . If  $o(\sigma^i) = 3$ , then  $|F(\sigma^i)| = 2^n - 2$ .*

*Proof.* By  $o(\sigma^i) = 3$ ,  $H = \langle \sigma^i \rangle = \langle \sigma^{2n} \rangle$ . Suppose that  $\sigma^{2n}(O_\alpha) = O_\alpha$  for  $O_\alpha \in \Omega$ . Then the group  $H$  acts on the partition  $\Delta_\alpha$  of  $O_\alpha$  in (3.5) as follows:

$$\begin{aligned} H \times \Delta_\alpha &\longrightarrow \Delta_\alpha \\ (\sigma^{2ni}, A(\alpha)) &\longmapsto \sigma^{2ni}(A(\alpha)), i = 0, 1, 2. \end{aligned}$$

Denote by  $O_{A(\alpha)}$  the orbit of  $A(\alpha)$  under the action the subgroup  $H = \langle \sigma^{2n} \rangle$ . For  $A(\alpha) \in \Delta_\alpha$ ,  $|O_{A(\alpha)}| = 1$  or  $3$  by  $|H| = 3$ .

Suppose that there is  $A(\alpha) \in \Delta_\alpha$  such that  $|O_{A(\alpha)}| = 1$ . Then  $\sigma^{2n}(A(\alpha)) = A(\alpha)$ . By the proof of Proposition 4.1,  $\alpha$  is a root of  $x^{2^{2n}} + x + 1 = 0$  and  $\alpha^{2^{4n}} = \alpha$ , which is a contradiction with  $\alpha$  of degree 6 over  $\mathbb{F}_{2^n}$ . Hence  $|O_{A(\alpha)}| = 3$  for all  $A(\alpha) \in \Delta_\alpha$ .

Without loss of generality, let  $\sigma^{2n}(A(\alpha)) = A(\frac{1}{\alpha})$ . Then

$$\alpha^{2^{2n}} = \frac{a}{\alpha} + b = B_0(\alpha), \alpha^{2^{6n}} = B_0^3 \alpha = \alpha,$$

where  $B_0 = \begin{pmatrix} b & a \\ 1 & 0 \end{pmatrix} \in GL_2(\mathbb{F}_{2^n})$ . Hence  $B_0^3 = \begin{pmatrix} b^3 & ab^2 + a^2 \\ b^2 + a & ab \end{pmatrix}$  is a scalar matrix and  $a = b^2 \in \mathbb{F}_{2^n}^*$ . If  $\frac{\alpha}{b}$  is viewed as  $\alpha$ , then  $\alpha \in \mathbb{S}$  satisfies the equation (4.1). Hence  $\alpha, \alpha^{2^{2n}} = B(\alpha) = \frac{1}{\alpha} + 1, \alpha^{2^{4n}} = B^2(\alpha) = \frac{1}{\alpha+1}$  are roots of (4.1), where  $B$  is defined as (4.2). So  $\sigma^{2n}(A(\alpha)) = A(\frac{1}{\alpha} + 1) = A(\frac{1}{\alpha}), \sigma^{2n}(A(\frac{1}{\alpha})) = A(\frac{1}{\alpha+1})$ , and  $\sigma^{2n}(A(\frac{1}{\alpha+1})) = A(\alpha)$ .

Suppose that  $\alpha \in A(\alpha)$  is a solution of (4.1) and  $P(\alpha) = c\alpha + d \in A(\alpha)$  is also a solution of (4.1), where  $P = \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix}$ . Then by  $\alpha^{2^{2n}} = B(\alpha)$ ,  $BP(\alpha) = (P(\alpha))^{2^{2n}} = P(\alpha)^{2^{2n}} = PB(\alpha)$  and

$$B^{-1}P^{-1}BP = \frac{1}{a} \begin{pmatrix} c^2 & cd \\ c + c^2 + cd & d + 1 + d^2 + cd \end{pmatrix}$$

is a scalar matrix, i.e.,  $c = 1, d = 0$ . Hence there is a unique solution  $\alpha \in A(\alpha)$  of (4.1), so there are  $2^n + 1$  roots of  $x^{2^{2n}} + x + 1$  in  $O_\alpha$ .

Conversely, if  $\alpha$  is a solution of (4.1), then  $\sigma^{2n}(O_\alpha) = O_\alpha$ .

Consequently, by Lemma 4.2

$$|F(\sigma^{2n})| = \frac{2^{2n} - 2^n - 2}{2^n + 1} = 2^n - 2.$$

□

**Proposition 4.4.** *Let  $G = \text{Gal}(\mathbb{F}_{2^{6n}}/\mathbb{F}_2) = \langle \sigma \rangle$ . If  $o(\sigma^i) = 6$ , then  $|F(\sigma^i)| = 0$ .*

*Proof.* By  $o(\sigma^i) = 6$ ,  $H = \langle \sigma^i \rangle = \langle \sigma^n \rangle$ . Suppose that  $\sigma^n(O_\alpha) = O_\alpha$  for  $O_\alpha \in \Omega$ . Then the group  $H$  acts on the partition  $\Delta_\alpha$  of  $O_\alpha$  in (3.5) as follows:

$$\begin{aligned} H \times \Delta_\alpha &\longrightarrow \Delta_\alpha \\ (\sigma^{ni}, A(\alpha)) &\longmapsto \sigma^{ni}(A(\alpha)), i = 0, 1, \dots, 5. \end{aligned}$$

Denote by  $O_{A(\alpha)}$  the orbit of  $A(\alpha)$  under the action the subgroup  $H = \langle \sigma^n \rangle$ . Then there is a class equation:

$$2^n + 1 = |\Delta_\alpha| = \sum |O_{A(\alpha)}|. \quad (4.3)$$

For  $A(\alpha) \in \Delta_\alpha$ ,  $|O_{A(\alpha)}| \in \{1, 2, 3, 6\}$  by  $|H| = 6$ .

Suppose that there is  $A(\alpha) \in O_\alpha$  such that  $|O_{A(\alpha)}| = 1$ . Then  $\sigma^n(A(\alpha)) = A(\alpha)$  and  $\alpha^{2^n} = a\alpha + b$ . Hence  $\alpha = \alpha^{2^{6n}} = a^6\alpha$ ,  $a = 1$ , and  $\alpha^{2^{2n}} = \alpha$ , which is contradictory.

Suppose that there is  $A(\alpha) \in O_\alpha$  such that  $|O_{A(\alpha)}| = 3$ . Without loss of generality, let  $\sigma^n(A(\alpha)) = A(\frac{1}{\alpha})$ . Then

$$\alpha^{2^n} = \frac{a}{\alpha} + b = B_0(\alpha), \alpha^{2^{6n}} = B_0^6\alpha = \alpha,$$

where  $B_0 = \begin{pmatrix} b & a \\ 1 & 0 \end{pmatrix} \in GL_2(\mathbb{F}_{2^n})$ . Hence

$$B_0^6 = \begin{pmatrix} b^6 + (ab^2 + a^2)(b^2 + a) & (ab^2 + a^2)(b^3 + ab) \\ (b^2 + a)(b^3 + ab) & (b^2 + a)(ab^2 + a^2) + a^2b^2 \end{pmatrix}$$

is a scalar matrix and  $a = b^2 \in \mathbb{F}_{2^n}^*$  or  $b = 0$ .

If  $b = 0$ , then  $B_0^2 = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$  and  $\alpha \in \mathbb{F}_{2^{2n}}$ , which is a contradiction.

If  $a = b^2 \in \mathbb{F}_{2^n}^*$ , then  $(\frac{a}{b})^{2^n} = \frac{b}{a} + 1 = B(\frac{a}{b})$  with  $B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ . Since  $(\frac{a}{b})^{2^{3n}} = B^3(\frac{a}{b}) = \frac{a}{b}$ ,  $\frac{a}{b} \in \mathbb{F}_{2^{3n}}$ , which is a contradiction.

Hence  $|O_{A(\alpha)}|$  can not be 1 and 3.

Suppose that  $|O_{A(\alpha)}| = 2$  or 6 for all  $A(\alpha) \in O_\alpha$ . Then it is a contradiction in (4.3).

Therefore,

$$|F(\sigma^n)| = 0.$$

□

**Lemma 4.5.** *If  $\alpha \in \mathbb{S}$  and  $\alpha^{2^6} = \alpha + b$ ,  $b \in \mathbb{F}_{2^n}$ . Then there is an element  $c \in \mathbb{F}_{2^n}$  such that  $(\alpha + c)^{2^6} = (\alpha + c)$ .*

*Proof.* Let  $T_6^{6n} : \mathbb{F}_{2^{6n}} \rightarrow \mathbb{F}_{2^6}$  and  $T_1^n : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$  be the trace functions, then  $T_6^{6n}(b) = 0$  by  $b = \alpha^{2^6} - \alpha$ . Let  $\mathbb{Z}/(n)$  be the residue class ring modulo  $n$ , then by  $\gcd(n, 6) = 1$   $6 \cdot \mathbb{Z}/(n) = \mathbb{Z}/(n)$  and  $T_1^n(b) = T_6^{6n}(b) = 0$  for  $b \in \mathbb{F}_{2^n}$ . Let  $S = \{c^{2^6} + c : c \in \mathbb{F}_{2^n}\}$ , then  $|S| = 2^{n-1}$  and  $\ker(T_1^n) = S$ . Hence there is an element  $c \in \mathbb{F}_{2^n}$  such that  $b = c^{2^6} + c$ , so  $(\alpha + c)^{2^6} = (\alpha + c)$ . □

**Proposition 4.6.** *Let  $G = \text{Gal}(\mathbb{F}_{2^{6n}}/\mathbb{F}_2) = \langle \sigma \rangle$ . If  $o(\sigma^i) = n$ , then  $|F(\sigma^i)| = 9$ .*

*Proof.* By  $o(\sigma^i) = n$ ,  $H = \langle \sigma^i \rangle = \langle \sigma^6 \rangle$ . Suppose that  $\sigma^6(O_\alpha) = O_\alpha$  for  $O_\alpha \in \Omega$ . Then the group  $H$  acts on the partition  $\Delta_\alpha$  of  $O_\alpha$  in (3.5) as follows:

$$\begin{aligned} H \times \Delta_\alpha &\longrightarrow \Delta_\alpha \\ (\sigma^{6i}, A(\alpha)) &\longmapsto \sigma^{6i}(A(\alpha)), i = 0, 1, \dots, n-1. \end{aligned}$$

Denote by  $O_{A(\alpha)}$  the orbit of  $A(\alpha)$  under the action of the subgroup  $\langle \sigma^n \rangle$ . Then there is a class equation:

$$2^n + 1 = |\Delta_\alpha| = \sum |O_{A(\alpha)}|.$$

For  $A(\alpha) \in \Delta_\alpha$ ,  $|O_{A(\alpha)}| = 1$  or  $n$  by  $|H| = n$ , where  $n$  is a prime number. By  $n \nmid (2^n + 1)$ , there exists  $A(\alpha)$  such that  $|O_{A(\alpha)}| = 1$ .

If  $\sigma^6(A(\alpha)) = A(\alpha)$  for  $A(\alpha) \in \Delta_\alpha$ , then  $\sigma^6(\alpha) = a\alpha + b$ ,  $0 \neq a, b \in \mathbb{F}_{2^n}$ . Hence  $\alpha = \sigma^{6n}(\alpha) = \sigma^{6(n-1)}(a\alpha + b) = a^n\alpha + k$ ,  $k \in \mathbb{F}_{2^n}$ , so  $k = 0$ ,  $a^n = 1$ . Thus  $a = 1$  by  $\gcd(n, 2^n - 1) = 1$  and

$$\alpha^{2^6} = \alpha + b.$$

By Lemma 4.5, there exists an element  $c \in \mathbb{F}_{2^n}$  such that  $(\alpha + c)^{2^6} = \alpha + c$ . If  $\alpha + c$  is viewed as  $\alpha$ , then there are exactly two roots:  $\alpha, \alpha + 1$ , of  $x^{2^6} = x$  in  $A(\alpha)$ .

Moreover, if  $\sigma^6(A(\frac{1}{\alpha+\gamma})) = A(\frac{1}{\alpha+\gamma})$  and  $\alpha^{2^6} = \alpha$ . Then by above,

$$\left(\frac{a}{\alpha + \gamma} + b\right)^{2^6} = \frac{a}{\alpha + \gamma} + b, 0 \neq a, b \in \mathbb{F}_{2^n}.$$

Hence  $a^{2^6} = a, b^{2^6} = b, \gamma^{2^6} = \gamma$ , and  $a = 1, b = 0$  or  $1, \gamma = 0$  or  $1$  by  $n(> 3)$  a prime. So there are exactly six roots:  $\alpha, \alpha + 1, \frac{1}{\alpha}, \frac{1}{\alpha} + 1, \frac{1}{\alpha+1}, \frac{1}{\alpha+1} + 1$ , in  $O_\alpha$  of  $x^{2^6} = x$ .

Conversely, if  $\alpha^{2^6} = \alpha$ , then  $\sigma^6(O_\alpha) = O_\alpha$ . Thus,  $|\mathbb{S} \cap O_\alpha| = 6$ .

Therefore,  $\sigma^6(O_\alpha) = O_\alpha$  if and only if there are exactly six roots in  $O_\alpha$  of  $x^{2^6} = x$ .

On the other hand,  $\mathbb{F}_{2^6} \cap \mathbb{S} = \mathbb{F}_{2^6} \setminus (\mathbb{F}_{2^2} \cup \mathbb{F}_{2^3})$  and  $|\mathbb{F}_{2^6} \cap \mathbb{S}| = 54$ . Then

$$|F(\sigma^6)| = \frac{|\mathbb{F}_{2^6} \cap \mathbb{S}|}{|\mathbb{S} \cap O_\alpha|} = 9.$$

□

**Proposition 4.7.** *Let  $G = \text{Gal}(\mathbb{F}_{2^{6n}}/\mathbb{F}_2) = \langle \sigma \rangle$ . If  $o(\sigma^i) = 2n$ , then  $|F(\sigma^i)| = 3$ .*

*Proof.* By  $o(\sigma^i) = 2n$ ,  $H = \langle \sigma^i \rangle = \langle \sigma^3 \rangle$ . Suppose that  $\sigma^3(O_\alpha) = O_\alpha$ . Then the group  $H$  acts on the partition  $\Delta_\alpha$  of  $O_\alpha$  in (3.5) as follows:

$$\begin{aligned} H \times \Delta_\alpha &\longrightarrow \Delta_\alpha \\ (\sigma^{3i}, A(\alpha)) &\longmapsto \sigma^{3i}(A(\alpha)), i = 0, 1, \dots, 2n-1. \end{aligned}$$

Denote by  $O_{A(\alpha)}$  the orbit of  $A(\alpha)$  under the action of  $\langle \sigma^3 \rangle$ . Then there is a class equation:

$$2^n + 1 = |\Delta_\alpha| = \sum |O_{A(\alpha)}|.$$

For  $A(\alpha) \in \Delta_\alpha$ ,  $|O_{A(\alpha)}| \in \{1, 2, n, 2n\}$  by  $|H| = 2n$ . By  $n \nmid (2^n + 1)$ , there exists  $A(\alpha) \in \Delta_\alpha$  such that  $|O_{A(\alpha)}| = 1$  or  $2$ .

If there is  $A(\alpha) \in \Delta_\alpha$  such that  $|O_{A(\alpha)}| = 2$ , then  $\sigma^3(A(\alpha)) = A(\frac{1}{\alpha+\gamma})$  and  $\sigma^6(A(\alpha)) = A(\alpha)$ . Without loss of generality, let  $\alpha^{2^6} = \alpha$  and  $\alpha^{2^3} = \frac{a}{\alpha+\gamma} + b, 0 \neq a, b \in \mathbb{F}_{2^n}$ . By

$$\alpha = \alpha^{2^6} = \frac{a^{2^3}}{\frac{a}{\alpha+\gamma} + b + \gamma^{2^3}} + b^{2^3},$$

$b = \gamma^{2^3}$ ,  $a = 1$ , and  $(\alpha + \gamma)^{2^3} = \frac{1}{\alpha+\gamma}$ . If  $\alpha + \gamma$  is viewed as  $\alpha$ , then  $\sigma^3(A(\alpha)) = A(\frac{1}{\alpha})$  and  $\alpha^{2^3} = \frac{1}{\alpha}$ . Hence  $(\frac{1}{\alpha+1})^{2^3} = \frac{1}{\alpha+1} + 1$  and  $|O_{A(\frac{1}{\alpha+1})}| = 1$ .

Without loss of generality, let  $A(\alpha) \in \Delta_\alpha$  such that  $|O_{A(\alpha)}| = 1$ . Then  $\sigma^3(A(\alpha)) = A(\alpha)$  and  $\sigma^6(A(\alpha)) = A(\alpha)$ , so  $\alpha^{2^6} = \alpha$  by Proposition 4.6 and  $\alpha^{2^3} = a\alpha + b$ ,  $0 \neq a, b \in \mathbb{F}_{2^n}$ . Then  $\alpha = \alpha^{2^6} = a^{2^3}(a\alpha + b) + b^{2^3}$ , so  $a = 1$  and  $b = 1$  by  $\gcd(2^6 - 1, 2^n - 1) = 1$ . Hence  $\alpha^{2^3} + \alpha + 1 = 0$ .

Suppose that there is also  $A(\frac{1}{\alpha+\gamma})$  such that  $|O_{A(\frac{1}{\alpha+\gamma})}| = 1$ . Then

$$\sigma^3\left(\frac{1}{\alpha+\gamma}\right) = \frac{1}{\alpha+1+\sigma^3(\gamma)} = \frac{a}{\alpha+\gamma} + b, 0 \neq a, b \in \mathbb{F}_{2^n}.$$

Hence  $b = 0$ ,  $a = 1$ , and  $\gamma^8 + \gamma + 1 = 0$ , which is contradictory with  $\gamma \in \mathbb{F}_{2^n}$ .

Hence there is a unique  $A(\alpha) \in O_\alpha$  such that  $|O_\alpha| = 1$  and there are exactly two roots:  $\alpha, \alpha + 1$ , of  $x^{2^3} + x + 1 = 0$  in  $O_\alpha$ .

Conversely, if  $\alpha \in \mathbb{S}$  is a root of  $x^{2^3} + x + 1 = 0$ , then  $\sigma^3(O_\alpha) = O_\alpha$ . Thus,  $|\mathbb{S} \cap O_\alpha| = 2$ .

Moreover, it is clear that

$$\left| \left\{ \alpha \in \mathbb{S} : \alpha^{2^3} + \alpha + 1 = 0 \right\} \right| = \left| \left\{ \alpha \in \mathbb{F}_{2^6} \setminus \{ \mathbb{F}_{2^3} \cup \mathbb{F}_{2^2} \} : \alpha^{2^3} + \alpha + 1 = 0 \right\} \right| = 6.$$

Therefore,

$$|F(\sigma^3)| = \frac{6}{2} = 3.$$

□

By above propositions, we finally give the proof of Theorem 3.4 as follows.

**Proof of Theorem 3.4** For  $i$  an integer, denote by  $\phi(i)$  the Euler function. Then, by Remark 3.6(1)

$$\begin{aligned} \sum_{\sigma^i \in G, i=0, \dots, 6n-1} |F(\sigma^i)| &= \sum_{d|6n} |F(\sigma^d)| \phi\left(\frac{6n}{d}\right) \\ &= |F(\sigma^0)|\phi(1) + |F(\sigma^{3n})|\phi(2) + |F(\sigma^{2n})|\phi(3) + |F(\sigma^6)|\phi(n) + |F(\sigma^3)|\phi(2n) \\ &= 2^{3n} + 2^{2n} + 3 \cdot 2^n + 12n - 18. \end{aligned}$$

By Lemmas 3.3 and 2.8, there are at most  $\frac{2^{3n} + 2^{2n} + 3 \cdot 2^n + 12n - 18}{6n}$  extended irreducible binary sextic Goppa codes of length  $2^n + 1$  over  $\mathbb{F}_{2^n}$ .

## 5. CONCLUSION

In this paper, we have obtained an upper bound on the number of extended irreducible Goppa codes of degree 6 and length  $2^n + 1$  with  $n(> 3)$  a prime number. Our results show that many extended Goppa codes become equivalent and this supports the idea of mounting an enumeration attack on the McEliece cryptosystem using extended Goppa codes.

## REFERENCES

- [1] T. P. Berger, "Cyclic alternant codes induced by an automorphism of a GRS code", in *Finite Field: Theory, Applications and Algorithms* (R. Mullin and G. Mullen Eds.), Contemporary Mathematics, vol. 225, pp. 143-154, Amer. Math. Soc., Providence, 1999.
- [2] T. P. Berger, "Goppa and related codes invariant under a prescribed permutation", *IEEE Trans. Inf. Theory*, vol. 46, no. 7, pp. 2628-2633, Nov. 2000.
- [3] T. P. Berger, "On the cyclicity of Goppa codes, parity-check subcodes of Goppa codes, and extended Goppa codes", *Finite Fields and Their Appl.*, vol. 6, no. 3, pp. 255-281, 2000.
- [4] C.-L. Chen, "Equivalent irreducible Goppa codes (corresp.)", *IEEE Trans. Inf. Theory*, vol. 24, no. 6, pp. 766-769, Nov. 1978.
- [5] V. D. Goppa, "A new class of linear correcting codes", *Probl. Pereda. Inf.*, vol. 6, no. 3, pp. 24-30, 1970.
- [6] P. Loidreau, N. Sendrier, "Weak keys in the McEliece public-key cryptosystem", *IEEE Trans. Inf. Theory*, vol. 47, no. 3, pp. 1207-1211, 2001.
- [7] F. J. Macwilliams, N. J. A. Sloane, "The Theory of Error Correcting Codes", North-Holland, 1986.
- [8] K. Magamba, J. A. Ryan, "Counting extended irreducible Goppa codes", *Appl. Algebra Eng. Commun. Comput.*, vol. 30, no. 4, pp. 313-331, 2019.
- [9] I. Martin Isaacs, *Algebra: A Graduate Text*. Pacific Grove, CA, USA: Brooks/Cole, 1994.
- [10] R. McEliece, "A public-key cryptosystem based on algebraic coding theory", *DSN Progress Report 42-44*, pp. 114-116, 1978.
- [11] O. Moreno, "Symmetries of binary Goppa codes (corresp.)", *IEEE Trans. Inf. Theory*, vol. 25, no. 5, pp. 609-612, Sep. 1979.
- [12] A. L. Musukwa, "Counting extended irreducible binary Goppa codes of degree  $2p$  and length  $2^n + 1$ ", *J. Math. Comput. Sci.* vol. 8, no. 1, pp. 1-17, 2018.
- [13] A. L. Musukwa, K. Magamba, J. A. Ryan, "Enumeration of extended irreducible Goppa codes of degree  $2^m$  and length  $2^n + 1$ ", *J. Algebra Comb. Discrete Struct. Appl.* vol. 4, no. 3, pp. 235-256, 2017.
- [14] J. A. Ryan, "A new connection between irreducible and extended irreducible Goppa codes," in *Proc. SAMSA*, 2012, pp. 152-154.
- [15] J. A. Ryan, "Counting extended irreducible binary quartic goppa codes of length  $2^n + 1$ ", *IEEE Trans. Inf. Theory*, vol. 61, no. 3, pp. 1174-1178, Mar. 2015.
- [16] J. A. Ryan, "Counting extended irreducible Goppa codes", *J. Discrete Math.*, 2014.
- [17] J. A. Ryan, "Irreducible Goppa codes", Ph.D. Thesis, University College Cork (2004).
- [18] J. A. Ryan, P. Fitzpatrick, "Enumeration of inequivalent irreducible Goppa codes", *Discrete Appl. Math.*, vol. 154, no. 2, pp. 399-412, 2006.

College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, 211100, P. R. China

*Email address:* dthuang666@163.com

Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing, 211100, P. R. China

*Email address:* yueqin@nuaa.edu.cn