The Number of Extended Irreducible Binary Goppa Codes

Bocong Chen and Guanghui Zhang

Abstract—Goppa, in the 1970s, discovered the relation between algebraic geometry and codes, which led to the family of Goppa codes. As one of the most interesting subclasses of linear codes, the family of Goppa codes is often chosen as a key in the McEliece cryptosystem. Knowledge of the number of inequivalent binary Goppa codes for fixed parameters may facilitate the evaluation of the security of such a cryptosystem. Let $n \geq 5$ be an odd prime number, let $q = 2^n$ and let $r \geq 3$ be a positive integer satisfying $\gcd(r, n) = 1$. The purpose of this paper is to establish an upper bound on the number of inequivalent extended irreducible binary Goppa codes of length $q + 1$ and degree $r$. A potential mathematical object for this purpose is to count the number of orbits of the projective semi-linear group $\text{PGL}_2(F_q) \rtimes \text{Gal}(F_q^n/F_2)$ on the set $\mathcal{I}_r$ of all monic irreducible polynomials of degree $r$ over the finite field $F_q$. An explicit formula for the number of orbits of $\text{PGL}_2(F_q) \rtimes \text{Gal}(F_q^n/F_2)$ on $\mathcal{I}_r$ is given, and consequently, an upper bound for the number of inequivalent extended irreducible binary Goppa codes of length $q + 1$ and degree $r$ is derived. Our main result naturally contains the main results of Ryan (IEEE-TIT 2015), Huang and Yue (IEEE-TIT, 2022) and, Chen and Zhang (IEEE-TIT, 2022), which considered the cases $r = 4$, $r = 6$ and $\gcd(r, q^n - q) = 1$ respectively.

Index Terms—Binary Goppa codes, extended Goppa codes, inequivalent codes, group actions.

I. INTRODUCTION

THE progress of cryptography is closely related with the development of coding theory. Analogous to the RSA, coding theory started shaping public key cryptography in the late 1970s. McEliece introduced a public-key cryptosystem based upon encoding the plaintext as codewords of an error-correcting code from the family of Goppa codes in 1978, see [17]. In the McEliece public-key encryption scheme the main practical limitation is probably the size of its key. In order to overcome this practical limitation, the McEliece cryptosystem often chooses a random Goppa code as its key, see [13].

Manuscript received 30 March 2022; accepted 5 September 2023. Date of publication 19 September 2023; date of current version 22 November 2023. The work of Bocong Chen was supported in part by the National Natural Science Foundation of China under Grant 11971175, Grant 12171162, and Grant 12371521; and in part by the Guangdong Basic and Applied Basic Research Foundation under Grant 2023A1515010284. The work of Guanghui Zhang was supported by the Open Research Fund of Key Laboratory of Nonlinear Analysis and Applications, Central China Normal University, Ministry of Education, China. (Corresponding author: Guanghui Zhang.)

Bocong Chen is with the School of Mathematics, South China University of Technology, Guangzhou, Guangdong 510641, China (e-mail: bocongchen@foxmail.com).

Guanghui Zhang is with the Department of Mathematics, Suqian University, Suqian, Jiangsu 223800, China (e-mail: 23175@suq.edu.cn). Communicated by M. Schwartz, Associate Editor for Coding and Decoding, Digital Object Identifier 10.1109/TIT.2023.3317290

and [17]. In the originally proposed system, a codeword is generated from plaintext message bits by using a permuted and scrambled generator matrix of a Goppa code. This matrix is the public key. In this system, the ciphertext is formed by adding a randomly chosen error vector to each codeword of perturbed code. The unperturbed Goppa code together with scrambler and permutation matrices form the private key. On reception, the associated private key is used to invoke an error-correcting decoder based upon the underlying Goppa code to correct the garbled bits in the codeword.

One of the reasons why Goppa codes receive interest from cryptographers may be that Goppa codes have few invariants and the number of inequivalent codes grows exponentially with the length and dimension of the code, which makes it possible to resist to any structural attack. When we give the assessment of the security of this cryptosystem against the enumerative attack, it is important for us to know the number of Goppa codes for any given set of parameters. An enumerative attack in the McEliece cryptosystem is to find all Goppa codes for a given set of parameters and to test their equivalences with the public codes [13]. Thus one of the key issues for the McEliece cryptosystem is the enumeration of inequivalent Goppa codes for a given set of parameters. Knowledge of the number of inequivalent Goppa codes for fixed parameters may facilitate in the evaluation of the security of such a cryptosystem.

A. Known Results

Some significant research efforts have been put in developing the enumeration of (extended) Goppa codes. Based on the invariant property under the group of transformations, Moreno [19] classified cubic and quartic irreducible Goppa codes; in the same paper, it was showed that there are four inequivalent quartic Goppa codes of length 33 and there is only one inequivalent extended irreducible binary Goppa code with any length and degree 3. Berger [1], [2] studied Goppa codes that are invariant under a prescribed permutation. Ryan and Fitzpatrick [28] obtained an upper bound on the number of inequivalent irreducible Goppa codes of length $q^n$ over $\mathbb{F}_q$. Ryan [26] produced an upper bound on the number of inequivalent extended irreducible Goppa codes over $\mathbb{F}_q$ of degree $r$ and length $q^n + 1$.

In a subsequent paper [27], Ryan made a great improvement on giving a much tighter upper bound than that of [26] on the number of inequivalent extended irreducible binary quartic Goppa codes of length $2n^2 + 1$, where $n > 3$ is a prime number. It was shown in [27] that the problem of giving an upper
bound for the number of inequivalent extended irreducible binary Goppa codes of degree $r$ can be transformed into that of finding the number of orbits of the projective semi-linear group $\text{PTL} = \text{PGL}_2(\mathbb{F}_q) \rtimes \text{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_2)$ on the set of elements in $\mathbb{F}_{q^r}$ of degree $r$ over $\mathbb{F}_q$ (which is denoted by $\mathcal{S}$). The objective of the paper [27] is then to find such number of orbits. Following that line of research, Musukwa et al. [21] gave an upper bound on the number of inequivalent extended irreducible binary Goppa codes of degree $2p$ and length $2^n+1$, where $n$ is an odd prime and $m > 1$ is a positive integer. Musukwa produced [20] 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 distinct odd primes such that $p$ does not divide $2^n \pm 1$. Magamba and Ryan [15] obtained an upper bound on the number of inequivalent extended irreducible $q$-ary Goppa codes of degree $r$ and length $q^n + 1$, where $q = p^i$, $n$ and $r > 2$ are both prime numbers. Recently, Huang and Yue [7] obtained an upper bound on the number of extended irreducible binary Goppa codes of degree $6$ and length $2^n + 1$, where $n > 3$ is a prime number. Note that the degrees of the Goppa codes mentioned above are small or have at most two prime divisors. Chen and Zhang [3] presented a new approach to calculate the number of orbits of the projective semi-linear group on $\mathcal{S}$ yielding an upper bound on the number of extended irreducible binary Goppa codes of degree $r$ and length $2^n + 1$, where $n > 3$ is a prime number with $\gcd(r, n) = 1$ and $\gcd(r, q^3 - q) = 1$. In particular, the degree $r$ of the Goppa code considered in [3] can have arbitrary many prime divisors.

B. Our Main Results and Contributions

In this paper, we further explore the ideas in [3] to establish an upper bound on the number of inequivalent extended irreducible binary Goppa codes of length $q+1$ and degree $r$, where $q = 2^n$ and $n \geq 5$ is a prime number satisfying $\gcd(r, n) = 1$. In a word, we settle a much more general case by dropping the assumption $\gcd(r, q^3 - q) = 1$ in [3]; consequently, our main results in the current paper naturally contain the main results of [3], [7], [20], [21], and [27]. A potential mathematical object for this purpose is to count the number of orbits of $\text{PTL} = \text{PGL}_2(\mathbb{F}_q) \rtimes \text{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_2)$ on $\mathcal{S}$ (see Lemma 2.3 in Section II). We first use a strategy exhibited in [3] to count the number of orbits of $\text{PGL}_2(\mathbb{F}_q)$ on $\mathcal{I}_r$, where $\mathcal{I}_r$ denotes the set of monic irreducible polynomials over $\mathbb{F}_q$ of degree $r$ (see Lemmas 2.4 and 2.6 in Section II). By virtue of a result in [27], the number of inequivalent extended irreducible binary Goppa codes of length $q+1$ and degree $r$ is less than or equal to the number of orbits of $\text{PGL}_2(\mathbb{F}_q)$ on $\mathcal{S}$. We finally determine the exact value of the number of orbits of $\text{PTL}$ on $\mathcal{I}_r$ (or equivalently PTL on $\mathcal{S}$), see Theorem 4.21 in Section IV. Comparing to [3], without the assumption $\gcd(r, q^3 - q) = 1$, we have to get around several difficulties in connecting the orbits of PTL on $\mathcal{I}_r$ and that on $\mathcal{S}$ (see Lemmas 4.2-4.6 in Section IV) and establish some new results (see Lemmas 4.8-4.20). The auxiliary results may be interested in their own right.

C. Organization of This Paper

The paper is organized as follows. In Section II, we review some definitions and basic results about extended irreducible Goppa codes, some matrix groups and group actions. In Section III, we study the number of orbits of PTL on $\mathcal{I}_r$. In Section IV, we find an explicit formula for the number of orbits of PTL on the set $\mathcal{I}_r$, which naturally gives an upper bound for the number of inequivalent extended irreducible Goppa codes of length $2^n+1$ and degree $r$, where $n \geq 5$ is a prime number satisfying $\gcd(r, n) = 1$. In Section V, as corollaries of our main results, we apply our main result to some special cases, including $r = 4$, $r = 2p$ ($p \geq 3$ is a prime number) and $\gcd(r, q^3 - q) = 1$.

II. Preliminaries

Starting from this section till the end of this paper, we assume that $n \geq 5$ is an odd prime number and $r \geq 3$ is a positive integer relatively prime to $n$. Let $\mathbb{F}_q$ be the finite field with $q = 2^n$ elements and let $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ be the multiplicative group of the finite field $\mathbb{F}_q$. Suppose $x$ is an indeterminate over $\mathbb{F}_q$ and let $\mathbb{F}_q[x]$ be the polynomial ring in variable $x$ with coefficients in $\mathbb{F}_q$. As usual, for a polynomial $f(x) \in \mathbb{F}_q[x]$ (or simply denoted by $f$), $\deg f$ is the degree of $f$; for a finite set $X$, let $|X|$ denote the number of elements of $X$. Given two integers $a$ and $b$, if $a$ is a divisor of $b$, we write $a \mid b$; otherwise, we write $a \nmid b$. We use $\gcd(a, b)$ to denote the greatest common divisor of $a$ and $b$. In particular, when $a$ and $b$ are relatively prime, we have $\gcd(a, b) = 1$.

We begin with recalling the notion of irreducible binary Goppa codes of length $q$. For the general definition and more detail information about Goppa codes, readers may refer to [12] or [14].

A. Extended Irreducible Goppa Codes

Definition 2.1: Let $g(x)$ be a polynomial in $\mathbb{F}_q[x]$ of degree $r$ and let $L = \mathbb{F}_q = \{\alpha_0, \alpha_1, \ldots, \alpha_{q-1}\}$ satisfy $g(\alpha_j) \neq 0$ for any $0 \leq j < q - 1$. The binary Goppa code $\Gamma(L, g)$ of length $q$ and degree $r$ is defined as

$$\Gamma(L, g) = \left\{ c = (c_0, c_1, \ldots, c_{q-1}) \in \mathbb{F}_2^q \mid \sum_{i=0}^{q-1} c_i (x - \alpha_i) \equiv 0 \pmod{g(x)} \right\}.$$ 

The polynomial $g(x)$ is called the Goppa polynomial. When $g(x)$ is irreducible, $\Gamma(L, g)$ is called an irreducible binary Goppa code of degree $r$. The Goppa code of length $q$ can be extended to a code of length $q+1$ by appending a coordinate in the set $L = \mathbb{F}_q$. In this paper, we mainly consider extended irreducible binary Goppa codes. The definition of extended irreducible binary Goppa codes of length $q+1$ and degree $r$ is given below.

Definition 2.2: For a given monic irreducible polynomial $g(x)$ of degree $r$, let $\Gamma(L, g)$ be an irreducible binary Goppa code of length $q$ as given in Definition 2.1. The extended...
Goppa code $\Gamma(L, g)$ of length $q + 1$ is defined as
$$\Gamma(L, g) = \left\{(c_0, \cdots, c_q) \in \mathbb{F}_2^{q+1} \mid (c_0, \cdots, c_{q-1}) \in \Gamma(L, g) \right\},$$
and
$$c_i = 0.$$  

Chen [4] showed that the irreducible binary Goppa code $\Gamma(L, g)$ is completely determined by any root of the Goppa polynomial $g(x)$; more precisely, if $\alpha$ is a root of $g(x)$ in some extension field over $\mathbb{F}_q$, then
$$H(\alpha) = \left(\frac{1}{\alpha - \alpha_0}, \frac{1}{\alpha - \alpha_1}, \cdots, \frac{1}{\alpha - \alpha_{q-1}}\right)$$
can be served as a parity-check matrix for $\Gamma(L, g)$. As such, let $C(\alpha)$ denote the code $\Gamma(L, g)$ and let $C(\alpha)$ denote the code $\Gamma(L, g)$. Therefore, every extended irreducible binary Goppa code of length $q + 1$ and degree $r$ can be described as $C(\alpha)$ for some $\alpha \in \mathbb{F}_{q^r}$.

**B. Equivalent Extended Irreducible Goppa Codes**

In this paper, we aim to give an upper bound for the number of inequivalent extended irreducible binary Goppa codes of length $q + 1$ and degree $r$. This problem can be reduced to that of counting the number of orbits of the projective semi-linear group action on some subset of $\mathbb{F}_q^r$ (see [1], [7] or [27]). To state this result clearly, we need the notions of group actions (for example, see [9] or [25]) and some matrix groups. In the following, we collect the matrix groups that we will use later, and fix the notations.

1. The general linear group of degree 2 over $\mathbb{F}_q$

$$\text{GL} = \text{GL}_2(\mathbb{F}_q) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{F}_q, \ ad - bc \neq 0 \right\}.$$  

2. The affine general linear group of degree 2 over $\mathbb{F}_q$

$$\text{AGL} = \text{AGL}_2(\mathbb{F}_q) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{F}_q^*, \ b \in \mathbb{F}_q \right\}.$$  

3. The projective general linear group of degree 2 over $\mathbb{F}_q$

$$\text{PGL} = \text{PGL}_2(\mathbb{F}_q) = \text{GL}/Z,$$

where $Z$ is the center of $\text{GL}$ consisting of the multiples of the identity matrix by elements of $\mathbb{F}_q^*$.

4. The projective semi-linear group

$$\text{PTL} = \text{PTL}_2(\mathbb{F}_q) = \text{PGL} \rtimes \text{Gal},$$

where $\text{Gal} = \text{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q) = \text{Gal}(\mathbb{F}_{q^{rn}}/\mathbb{F}_q) = \langle \sigma \rangle$ is the Galois group of order $rn$ generated by $\sigma$ ($\sigma$ sends each $\alpha \in \mathbb{F}_{q^r}$ to $\alpha^2$). The operation “$\circ$” is defined as follows:

$$A \sigma^i \cdot B \sigma^j = A \sigma^i(B) \sigma^{i+j}, \quad 0 \leq i, j \leq rn - 1,$$

where $\sigma^i(B) = \left(\begin{array}{cc} a^t & b^t \\ a^v & b^v \end{array}\right)$ for $B = \left(\begin{array}{cc} t & u \\ v & w \end{array}\right) \in \text{PGL}$. ($\sigma^i a$ means $\sigma^i a = a^{2^i}$ for $a \in \mathbb{F}_q$). It is clear that $E_2 \sigma^0$ is the identity element of $\text{PTL}$, where $E_2 = \left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array}\right)$ is the identity matrix.

Now it is the turn of group actions. For a general group $H$ acting on a finite set $X$, let $H(x)$ denote the orbit containing $x \in X$, namely $H(x) = \{h \cdot x \mid h \in H\}$; let $\text{Stab}_H(x)$ be the stabilizer of the point $x \in X$ in $H$, namely $\text{Stab}_H(x) = \{h \in H \mid h \cdot x = x\}$. Then the cardinality of the orbit $H(x)$ is equal to the index of $\text{Stab}_H(x)$ in $H$ and is written
$$|H(x)| = [H : \text{Stab}_H(x)].$$

Now let $S = S(r, n)$ denote the set of elements in $\mathbb{F}_{q^r}$ of degree $r$ over $\mathbb{F}_q$; in other words, $S$ consists of elements $\alpha \in \mathbb{F}_{q^r}$ such that there exists a monic irreducible polynomial $f$ of degree $r$ over $\mathbb{F}_q$ satisfying $f(\alpha) = 0$.

It is known that $\text{PGL}$ and $\text{PTL}$ can act on the set $S$ in the following ways (see [7] or [27]):

- The action of the projective general linear group on $S$:

$$\text{PGL} \times S \rightarrow S$$
$$\left(A, \alpha\right) \mapsto A\alpha = \frac{aa + b}{ca + d},$$

where $A = \left(\begin{array}{cc} a & b \\ c & d \end{array}\right) \in \text{PGL}$.

- The action of the projective semi-linear group on $S$:

$$\text{PTL} \times S \rightarrow S$$
$$\left(A\sigma^i, \alpha\right) \mapsto (A\sigma^i)\alpha,$$

where $(A\sigma^i)\alpha = A(\sigma^i(\alpha)) = \frac{aa^2 + b}{ca^2 + d}$.

We are ready to state a sufficient condition which guarantees two extended irreducible Goppa codes to be equivalent; thus, in particular, it gives an upper bound for the number of inequivalent codes in
$$\left\{ C(\alpha) \mid \alpha \in S \right\},$$
see [1], [7] or [27].

**Lemma 2.3:** Let $\alpha, \beta \in S$ and $\beta \in S$. If $\alpha, \beta$ lie in the same $\text{PTL}$-orbit, namely $\alpha = A\sigma^i\beta$ for some $A\sigma^i \in \text{PTL}$, then the extended Goppa code $C(\alpha)$ is (permutation) equivalent to the extended Goppa code $C(\beta)$. In particular, the number of inequivalent extended irreducible binary Goppa codes of length $q + 1$ and degree $r$ is less than or equal to the number of orbits of $\text{PTL}$ on $S$.

With the help of Lemma 2.3, we only need to count the number of orbits of $\text{PTL}$ on $S$.

**C. The Action of $\text{PTL}$ on $I_r$**

In this subsection, we introduce another group action: The group $\text{PTL}$ can act on the set of all monic irreducible polynomials of degree $r$ over $\mathbb{F}_q$. Let $I_r$ be the set of all monic irreducible polynomials of degree $r$ over $\mathbb{F}_q$. It has been shown that the number of orbits of $\text{PTL}$ on $S$ is equal to the number of orbits of $\text{PTL}$ on $I_r$, see [3].

Let $A = \left(\begin{array}{cc} a & b \\ c & d \end{array}\right) \in \text{PGL}$, $\alpha \in \mathbb{F}_q$, and $f(x) = a_0 + a_1x + \cdots + a_rx^r \in \mathbb{F}_q[x]$ with $a_r \neq 0$. We make the following
The group $PGL$ can act on the set $I_r$, as restated below.

**Lemma 2.4** [3, Lemma 3.1]: With notation given above, we have a group action $PTL$ on the set $I_r$ defined by

$$PTL \times I_r \rightarrow I_r$$

$$(A \sigma^i, f) \rightarrow (A \sigma^i)(f) = (A(\sigma^i f))^*.$$

**Remark 2.5:** Many authors have studied the action of $PGL$ on $I_r$, focusing on the characterization and enumeration of $A$-invariants where $A \in PGL$ (for example, see [5], [22], [23], [24], [29]). The paper [16] considered an action of the group $A$ on $I_r$ and our definition of $PTL$ is different from that of [16].

The next result reveals that the problem of counting the number of orbits of $PTL$ on $S$ can be completely converted to that of counting the number of orbits of $PTL$ on $I_r$.

**Lemma 2.6:** (3, Lemma 3.3) The number of orbits of $PTL$ on $S$ is equal to the number of orbits of $PTL$ on $I_r$.

By Lemma 2.6, our ultimate aim is to find the number of orbits of $PTL = PGL \times Gal$ on the set $I_r$. We will repeatedly use the following fact to achieve this goal (for example, see [9, Pages 35-36]):

**Lemma 2.7:** Let $G$ be a finite group acting on a finite set $X$ and let $N$ be a normal subgroup of $G$. It is clear that $N$ naturally acts on $X$. Suppose the set of $N$-orbits are denoted by $N \backslash X = \{N(x) | x \in X\}$. Then the factor group $G/N$ acts on $N \backslash X$ and the number of orbits of $G$ on $X$ is equal to the number of orbits of $G/N$ on $N \backslash X$.

### III. The Number of Orbits of $PTL$ on $I_r$

In this section we analyze the orbits of $PTL$ on $I_r$. As $PGL$ is a normal subgroup of $PTL$, by virtue of Lemma 2.7, we first count the number of orbits of $PGL$ on the set $I_r$. According to the Cauchy-Frobenius Theorem (or named Burnside’s Lemma, see [25, Theorem 2.113]), we have

$$|PGL \backslash I_r| = \left| \frac{1}{|PGL|} \sum_{A \in PGL} |\text{Fix}(A)| \right| = \frac{1}{q(q^2-1)} \sum_{A \in PGL} |\text{Fix}(A)|,$$

where $\text{Fix}(A) = \{f \in I_r | Af = f\}$ is the number of fixed points of $A \in PGL$ in $I_r$. To find the exact value of $|PGL \backslash I_r|$, it is enough to determine the number of elements of $\text{Fix}(A)$, for each $A \in PGL$. To this end, in order to use some known results in the literature, we need to consider another action of the group $PGL$ on the set $I_r$ defined by

$$PGL \times I_r \rightarrow I_r$$

$$(A, f) \rightarrow A \circ f = \left((bx + d)r f(\frac{ax + c}{bx + d})\right)^*,$$

where $A = \left(\begin{array}{cc} a & b \\ c & d \end{array}\right) \in PGL$, see [23]. Define

$$\text{Fix}(A, o) = \{f \in I_r | A \circ f = f\}.$$

It follows that for every $A \in PGL$,

$$\text{Fix}(A) = \text{Fix}((A^T)^{-1}, o),$$

where $A^T$ denotes the transpose of the matrix $A$. Therefore, the number of orbits of $PGL$ on the set $I_r$ is equal to

$$|PGL \backslash I_r| = \frac{1}{q(q^2-1)} \sum_{A \in PGL} |\text{Fix}(A)| = \frac{1}{q(q^2-1)} \sum_{A \in PGL} |\text{Fix}((A^T)^{-1}, o)| = \frac{1}{q(q^2-1)} \sum_{A \in PGL} |\text{Fix}(A, o)|.$$
The set of all orbits of $\mathbb{PGL}_2$ have $q$ elements. We have

(4) The matrices $V_{\gamma_i} = \begin{pmatrix} 0 & 1 \\ \gamma_i & \gamma_i + 1 \end{pmatrix}$

give $\frac{q}{2}$ conjugacy classes, where $\gamma_i = \xi^{(q-1)i}$ for $i = 1, 2, \ldots, \frac{q}{2}$. Each conjugacy class contains $q(q-1)$ elements.

**Proof:** Its proof is somewhat long, involving some routine and tedious computations, and is deferred to the Appendix.

By [23, Lemma 4.1] and [23, Theorem 4.7], we immediately have

**Lemma 3.2:** Let notation be the same as in Lemma 3.1. We have

(1) If $r$ is even, then

$$|\text{Fix}(U_1, \circ)| = \frac{1}{r} \sum_{d|r} \mu(d)q^{\frac{2}{d}}.$$

If $r$ is odd, then

$$|\text{Fix}(U_1, \circ)| = 0.$$

(2) Let $a \in S$ with $D = \text{ord}(a)$, where $\text{ord}(a)$ is the order of the element $a$ in the multiplicative group $\mathbb{F}_q^*$. If $r$ is divisible by $D$, say $r = Dm$, then

$$|\text{Fix}(D_{1,a}, \circ)| = \frac{\varphi(D)}{r} \sum_{d|\text{gcd}(D,D)} \mu(d)(q^{\frac{2}{d}} - 1),$$

where $\varphi$ is the Euler's Totient function and $\mu$ is the Möbius function.

If $r$ is not divisible by $D$, then

$$|\text{Fix}(D_{1,a}, \circ)| = 0.$$

(3) Let $D = \text{ord}(V_{\gamma_i})$, where $\text{ord}(V_{\gamma_i})$ is the order of the element $V_{\gamma_i}$ in the group PGL. If $r$ is divisible by $D$, say $r = Dm$, then

$$|\text{Fix}(V_{\gamma_i}, \circ)| = \frac{\varphi(D)}{r} \sum_{d|\text{gcd}(D,D)} \mu(d)(q^{\frac{2}{d}} + (-1)^{q^{\frac{2}{d}+1}}).$$

If $r$ is not divisible by $D$, then

$$|\text{Fix}(V_{\gamma_i}, \circ)| = 0.$$

By virtue of Lemmas 3.1 and 3.2, we are ready to obtain the number of orbits of PGL on $\mathcal{I}_r$, which is the main result of this section.

**Theorem 3.3:** Let $\varphi$ and $\mu$ denote the Euler's Totient function and the Möbius function, respectively. Let $\text{PGL} \setminus \mathcal{I}_r$ be the set of all orbits of PGL on $\mathcal{I}_r$. Then

$$|\text{PGL} \setminus \mathcal{I}_r| = \frac{1}{q(q^2 - 1)} (N_0 + N_1 + N_2 + N_3),$$

where

$$N_0 = \frac{1}{r} \sum_{d|r} \mu(d)q^{\frac{2}{d}},$$

$$N_1 = \begin{cases} \frac{q^2 - 1}{r} \sum_{d|\frac{r}{d}} \mu(d)q^{\frac{2}{d}}, & 2 \mid r, \\ 0, & 2 \nmid r \end{cases},$$

$$N_2 = q(q+1) \cdot \sum_{d|\text{gcd}(D,q-1)} \frac{\varphi^2(D)}{r} \sum_{d|\frac{D}{d}} \mu(d)(q^{\frac{2}{d}} - 1)$$

and

$$N_3 = \frac{q(q-1)}{2} \cdot \sum_{d|\text{gcd}(D,q+1)} \frac{\varphi^2(D)}{r} \sum_{d|\frac{D}{d}} \mu(d)(q^{\frac{2}{d}} + (-1)^{q^{\frac{2}{d}+1}}).$$

**Proof:** According to the discussions at the beginning of this section, the number of orbits of PGL on the set $\mathcal{I}_r$ is equal to

$$|\text{PGL} \setminus \mathcal{I}_r| = \frac{1}{q(q^2 - 1)} \sum_{A \in \text{PGL}} |\text{Fix}(A, \circ)|.$$

By Lemma 3.1, the value of $|\text{PGL} \setminus \mathcal{I}_r|$ is equal to

$$\frac{1}{q(q^2 - 1)} \left( |\text{Fix}(E_2, \circ)| + (q^2 - 1) |\text{Fix}(U_1, \circ)| + q(q+1) \sum_{a \in S} |\text{Fix}(D_{1,a}, \circ)| + q(q-1) \sum_{i=1}^{\frac{q}{2}} |\text{Fix}(V_{\xi^{(q-1)i}}, \circ)| \right).$$

Assume that $N_0 = |\text{Fix}(E_2, \circ)|$, $N_1 = (q^2 - 1) \cdot |\text{Fix}(U_1, \circ)|$, $N_2 = q(q+1) \cdot \sum_{a \in S} |\text{Fix}(D_{1,a}, \circ)|$ and $N_3 = q(q-1) \cdot \sum_{i=1}^{\frac{q}{2}} |\text{Fix}(V_{\xi^{(q-1)i}}, \circ)|$. Note that an enumerative formula for the size of $\mathcal{I}_r$ (see [11, Theorem 3.25]) is given by

$$|\mathcal{I}_r| = \frac{1}{r} \sum_{d|r} \mu(d)q^{\frac{2}{d}}.$$

Then

$$N_0 = |\text{Fix}(E_2, \circ)| = |\mathcal{I}_r| = \frac{1}{r} \sum_{d|r} \mu(d)q^{\frac{2}{d}}.$$

In addition, by Lemma 3.2, one has

$$N_1 = (q^2 - 1) \cdot |\text{Fix}(U_1, \circ)| = \begin{cases} 0, & 2 \mid r, \\ \frac{q^2 - 1}{r} \sum_{d|\frac{r}{d}} \mu(d)q^{\frac{2}{d}}, & 2 \nmid r, \end{cases}$$

$$N_2 = q(q+1) \cdot \sum_{d|\text{gcd}(D,q-1)} \frac{\varphi^2(D)}{r} \sum_{d|\frac{D}{d}} \mu(d)(q^{\frac{2}{d}} - 1)$$

and

$$N_3 = \frac{q(q-1)}{2} \cdot \sum_{d|\text{gcd}(D,q+1)} \frac{\varphi^2(D)}{r} \sum_{d|\frac{D}{d}} \mu(d)(q^{\frac{2}{d}} + (-1)^{q^{\frac{2}{d}+1}}).$$
the value of \( N_2 \) is equal to
\[
q(q+1) \cdot \sum_{\sigma \in S} |\text{Fix}(D_1,a,\sigma)|
\]
\[
= q(q+1) \cdot \sum_{D \in \langle q-1 \rangle} \frac{\varphi^2(D)}{r} \sum_{d \mid D, \gcd(d,D)=1} \mu(d) (q^{\frac{r}{m}} - 1)
\]
\[
= q(q+1) \cdot \sum_{D \mid (q-1)} \frac{\varphi^2(D)}{r} \sum_{d \mid D, \gcd(d,D)=1} \mu(d) (q^{\frac{r}{m}} - 1)
\]

and the value of \( N_3 \) is equal to
\[
q(q-1) \cdot \sum_{i=1}^{2} |\text{Fix}(V_\xi(q-1),\sigma)|
\]
\[
= \frac{q(q-1)}{2} \cdot \sum_{i=1}^{q} |\text{Fix}(V_\xi(q-1),\sigma)|
\]
\[
= \frac{q(q-1)}{2} \cdot \sum_{D \mid (q-1)} \frac{\varphi^2(D)}{r} \sum_{d \mid D, \gcd(d,D)=1} \mu(d) (q^{\frac{r}{m}} + (-1)^{\frac{r}{m}+1})
\]
\[
= \frac{q(q-1)}{2} \cdot \sum_{D \mid (q-1)} \frac{\varphi^2(D)}{r} \sum_{d \mid D, \gcd(d,D)=1} \mu(d) (q^{\frac{r}{m}} + (-1)^{\frac{r}{m}+1}).
\]

We are done.

IV. THE NUMBER OF ORBITS OF \( \text{Gal} \) ON PGL\( \backslash I_r \)

In order to get the number of orbits of PGL\( \backslash I_r \), by Lemma 27 and Theorem 3.3, we are left to count the number of orbits of \( \text{Gal} \) on PGL\( \backslash I_r \). Recall that the Galois group \( \text{Gal} = \text{Gal}(\mathbb{F}_q^r/\mathbb{F}_2) = \text{Gal}(\mathbb{F}_{2^n}/\mathbb{F}_2) = \langle \sigma \rangle \) is the cyclic group of order \( r n \) generated by \( \sigma \). The action of \( \text{Gal} \) on PGL\( \backslash I_r \) is given by
\[
\text{Gal} \times \text{PGL} \backslash I_r \rightarrow \text{PGL} \backslash I_r
\]
\[
\langle \sigma \rangle, \text{PGL}(f) \quad \mapsto \quad \sigma \langle \text{PGL}(f) \rangle = \text{PGL}(\sigma f).
\]
Recall also that \( n \geq 5 \) is a prime number, \( q = 2^n \) and \( r \geq 3 \) is a positive integer relatively prime to \( n \). Thus \( \text{Gal} = \langle \sigma \rangle \) has the following decomposition into direct products:
\[
\text{Gal} = \langle \sigma \rangle \times \langle \sigma^n \rangle.
\]
In order to count the number of orbits of \( \text{Gal} \) on PGL\( \backslash I_r \), using Lemma 27 again, we first consider the action of \( \langle \sigma^n \rangle \) on PGL\( \backslash I_r \). Clearly, the action of \( \langle \sigma^n \rangle \) on PGL\( \backslash I_r \) is given by
\[
\langle \sigma^n \rangle \times \text{PGL} \backslash I_r \rightarrow \text{PGL} \backslash I_r
\]
\[
\langle \sigma^n \rangle, \text{PGL}(f) \quad \mapsto \quad \sigma^n \langle \text{PGL}(f) \rangle = \text{PGL}(\sigma^n f).
\]
Observe that \( \sigma^n a = a^{2^n} = a^q = a \) for any \( a \in \mathbb{F}_q \), which gives
\[
\text{PGL}(\sigma^n f) = \text{PGL}(f) \quad \text{for any} \quad f \in I_r.
\]
This means that \( \langle \sigma^n \rangle \) fixes each PGL\( (f) \) in PGL\( \backslash I_r \); in other words, the set of orbits of \( \langle \sigma^n \rangle \) on PGL\( \backslash I_r \) remains PGL\( \backslash I_r \). By Lemma 27, the number of orbits of \( \text{Gal} \) on PGL\( \backslash I_r \) is equal to the number of orbits of \( \langle \sigma^n \rangle \) on PGL\( \backslash I_r \). Since \( \sigma^n \) is of prime order \( n \), the size of every orbit of \( \langle \sigma^n \rangle \) on PGL\( \backslash I_r \) is equal to \( 1 \) or \( n \). Thus it is enough to determine the number of orbits of \( \langle \sigma^n \rangle \) on PGL\( \backslash I_r \) with size \( 1 \).

A. The Orbits of \( \langle \sigma^n \rangle \) ON PGL\( \backslash I_r \) WITH SIZE \( 1 \)

In this subsection we will characterize the orbits of \( \langle \sigma^n \rangle \) on PGL\( \backslash I_r \) with size \( 1 \). First note that if \( a \) is a root of \( f(x) \in I_r \), then \( a^\sigma \) is a root of \( f(x) \) and \( A \alpha = A \) is a root of \( Af(x) \), where \( A \in \text{PGL} \) or \( A \in \text{GL} \). Please keep these facts in mind and we shall use them frequently during the following discussions.

**Lemma 4.1:** Let \( f \in I_r \) and let \( \alpha \) be a root of \( f(x) \). Define a map \( \tau \) as follows:
\[
\tau : \text{PGL} \rightarrow \text{PGL}(\alpha)
\]
\[
A \mapsto A\alpha,
\]
then \( \tau \) is a bijection between PGL and PGL\( (\alpha) \). In particular, PGL and PGL\( (\alpha) \) have the same size, i.e., \( |\text{PGL}| = |\text{PGL}(\alpha)| \).

**Proof:** It is clear that the map \( \tau \) is well-defined and surjective. Assume that \( A\alpha = B\alpha \), where \( A, B \in \text{PGL} \). Then \( A^{-1}B = A^{-1}B = (\alpha)^{-1}(a, b, c, d) \), which leads to \( \frac{a+b+c+d}{ca+db} = \alpha \), or equivalently \( ca^2 + (a+d)\alpha + b = 0 \). Since \( r \geq 3 \), we obtain \( c = 0, a + d = 0 \) and \( b = 0 \), yielding \( A^{-1}B = aE_2 = E_2 \) in PGL and \( A = B \). It follows that \( \tau \) is injective. Therefore \( \tau \) is a bijection between PGL and PGL\( (\alpha) \), which implies that \( |\text{PGL}| = |\text{PGL}(\alpha)| \).

The next result improves [3, Lemma 3.6] by removing the numerical condition \( \gcd(r, q^3 - q) = 1 \), which is one of the key steps in this paper.

**Lemma 4.2:** Let \( f \in I_r \) and let \( \alpha \) be a root of \( f(x) \). Then PGL\( (\sigma^r f) = \text{PGL}(f) \) if and only if PGL\( (\sigma^r \alpha) = \text{PGL}(\alpha) \).

**Proof:** Suppose PGL\( (\sigma^r f) = \text{PGL}(f) \) and let
\[
Q = \{ \text{PGL}(\alpha^i) \mid 0 \leq i \leq r - 1 \}.
\]

**Claim 1:** There is a group action \( \langle \sigma^r \rangle \) on the set \( Q \) defined by
\[
\langle \sigma^r \rangle \times Q \rightarrow Q
\]
\[
\langle \sigma^r, \text{PGL}(\alpha^i) \rangle \quad \mapsto \quad \sigma^r \text{PGL}(\alpha^i) = \text{PGL}(\sigma^r \alpha^i).
\]
Since PGL\( (\sigma^r f) = \text{PGL}(f) \), then there exists an element \( A \in \text{PGL} \) such that \( \sigma^r f = Af \). For any fixed \( 0 \leq j \leq r - 1 \), we have
\[
\sigma^r f = (\sigma^r)^{(j-1)}(\sigma^r f) = \sigma^r(\sigma^{r-j-1}) Af
\]
\[
= \sigma^r(\sigma^{-j-1}) Af
\]
\[
= \sigma^r((\sigma^{r-j-2}) Af)
\]
\[
= \cdots
\]
\[
= \sigma^r(\sigma^{-1})(A) \cdots \sigma^r(\sigma A) \sigma^r f
\]
\[
= \sigma^r(\sigma^{-1})(A) \cdots \sigma^r(\sigma A) \sigma^r A f
\]
\[
\in \text{PGL}(f).
\]
Hence
\[ \text{PGL}(\sigma^{r_j}f) = \text{PGL}(f), \]
yielding that there exists \( B \in \text{PGL} \) such that \( B(\sigma^{r_j}f) = f \). Consequently, \( B(\sigma^{r_j}\alpha^q) \) is a root of \( f \), giving \( B(\sigma^{r_j}\alpha^q) = \alpha^q \), where \( 0 \leq s \leq r - 1 \). Therefore \( \text{PGL}(\sigma^{r_j}\alpha^q) \in \mathcal{Q} \).

On the other hand, it is easy to see that for \( 0 \leq i \leq r - 1 \), we have \( \alpha^i \text{PGL}(\alpha^q) = \text{PGL}(\alpha^q) \) and
\[
(\sigma^{r_1}\sigma^{r_2})\text{PGL}(\alpha^q) = \text{PGL}((\sigma^{r_1}\sigma^{r_2})\alpha^q) = \text{PGL}(\sigma^{r_1}(\sigma^{r_2}\alpha^q)) = \sigma^{r_1}\text{PGL}(\sigma^{r_2}\alpha^q) = \sigma^{r_1}(\sigma^{r_2}\text{PGL}(\alpha^q)),
\]
where \( j_1, j_2 \) are two positive integers satisfying \( 0 \leq j_1, j_2 \leq n - 1 \). Claim 1 is thus proved.

**Claim 2:** \( |\mathcal{Q}| \) is a divisor of \( r \), i.e., \( |\mathcal{Q}| \mid r \). To this end, let
\[ \mathcal{Q} = \left\{ A(\alpha^q) \mid A \in \text{PGL}, \ 0 \leq i \leq r - 1 \right\}. \]
Then \( \mathcal{Q} \) is the set of all roots of the polynomials in \( \text{PGL}(f) \), so
\[ |\mathcal{Q}| = r \cdot |\text{PGL}(g)| = r \cdot |\text{PGL} : \text{Stab}_{\text{PGL}}(f)|. \]
In addition, the set \( \mathcal{Q} \) can be rewritten as
\[
\mathcal{Q} = \{ \text{PGL}(\alpha^{q^{i_1}}), \text{PGL}(\alpha^{q^{i_2}}), \ldots, \text{PGL}(\alpha^{q^{i_{|\mathcal{Q}|}}}) \}\.
\]
Using Lemma 4.1, we have
\[
|\mathcal{Q}| = |\text{PGL}(\alpha^{q^{i_1}})| + \cdots + |\text{PGL}(\alpha^{q^{i_{|\mathcal{Q}|}}})| = \frac{|\text{PGL}| + \cdots + |\text{PGL}|}{|\mathcal{Q}| \text{ times}} = |\text{PGL}| \cdot |\mathcal{Q}|.
\]
Thus,
\[ |\mathcal{Q}| = r \cdot |\text{PGL} : \text{Stab}_{\text{PGL}}(f)| = |\text{PGL}| \cdot |\mathcal{Q}|. \]
That is to say,
\[ r = |\mathcal{Q}| \cdot \frac{|\text{PGL}|}{|\text{PGL} : \text{Stab}_{\text{PGL}}(f)|} = |\mathcal{Q}| \cdot |\text{Stab}_{\text{PGL}}(f)|,
\]
which shows \( |\mathcal{Q}| \mid r \). The proof of Claim 2 is completed.

According to the two claims above, there is a group action \( \langle \sigma^r \rangle \) on the set \( \mathcal{Q} \) and the size of \( \mathcal{Q} \) is a divisor of \( r \). Since \( \langle \sigma^r \rangle \) is of prime order \( n \), every orbit of \( \langle \sigma^r \rangle \) on \( \mathcal{Q} \) is equal to \( 1 \) or \( n \). From \( \gcd(r, n) = 1 \) and \( |\mathcal{Q}| \mid r \) we obtain \( \gcd(|\mathcal{Q}|, n) = 1 \), i.e., \( n \mid |\mathcal{Q}| \). It follows that there exists an orbit of \( \langle \sigma^r \rangle \) on \( \mathcal{Q} \) with size \( 1 \). Suppose that this orbit with size \( 1 \) is \( \text{PGL}(\alpha^{q^t}) \) with \( 0 \leq t \leq r - 1 \). Then
\[ \sigma^r \text{PGL}(\alpha^{q^t}) = \text{PGL}(\sigma^r \alpha^{q^t}) = \text{PGL}(\alpha^{q^t}). \]
Hence, there exists \( D \in \text{PGL} \) satisfying \( D(\sigma^r \alpha^{q^t}) = \alpha^{q^t} \), implying \( (D\sigma^r)\alpha^{q^t} = \alpha^{q^t} \). Therefore \( D\sigma^r = \alpha \), which implies that \( \text{PGL}(\sigma^r) = \text{PGL}(\alpha) \).

Conversely, suppose that \( \text{PGL}(\sigma^r) = \text{PGL}(\alpha) \). Then there is a matrix \( A \in \text{PGL} \) such that \( A(\sigma^r) = \alpha \). Note that \( A(\sigma^r) \) is a root of \( A(\sigma^r f) \), and then we obtain \( A(\sigma^r f) = f \), which implies that \( \text{PGL}(\sigma^r f) = \text{PGL}(f) \). We are done. 

To count the number of \( \text{PGL}(f) \in \text{PGL} \setminus \mathcal{I}_r \) that are fixed by \( \langle \sigma^r \rangle \), we need to use the affine general linear group \( \text{AGL} \). The affine general linear group \( \text{AGL} \) can be viewed naturally as a subgroup of \( \text{PGL} \). Hence, the group \( \text{AGL} \) acts on the set \( \mathcal{S} \) naturally. Let
\[ \text{AGL} \setminus \mathcal{S} = \{ \text{AGL}(\alpha) \mid \alpha \in \mathcal{S} \} \]
be the set of all orbits of \( \text{AGL} \) on \( \mathcal{S} \). Then the cyclic group \( \langle \sigma^r \rangle \) acts on \( \text{AGL} \setminus \mathcal{S} \) in the following way:
\[
\langle \sigma^r \rangle \times \text{AGL} \setminus \mathcal{S} \longrightarrow \text{AGL} \setminus \mathcal{S},
\]
with \( \langle \sigma^r, \text{AGL}(\alpha) \rangle \mapsto \sigma^r(\text{AGL}(\alpha)) = \text{AGL}(\sigma^r \alpha) \). It is not hard to verify that this is indeed a group action. We now turn to consider the orbit \( \text{PGL}(\alpha) \) where \( \alpha \in \mathcal{S} \). There is an action of \( \text{AGL} \) on \( \text{PGL}(\alpha) \):
\[ \text{AGL} \times \text{PGL}(\alpha) \longrightarrow \text{PGL}(\alpha), \]
\[ (C, A\alpha) \mapsto C A\alpha. \]
Therefore, \( \text{PGL}(\alpha) \) is the disjoint union of \( \text{AGL} \)-orbits. Indeed, one can easily check that there are exactly \( q + 1 \) right cosets of \( \text{AGL} \) in \( \text{PGL} \) and,
\[ t_0 = E_2 = \left( \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right), \quad t_1 = \left( \begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \right) \]
and
\[ t_\gamma = \left( \begin{array}{cc} 0 & 1 \\ 1 & \gamma \end{array} \right) \quad \text{for any } \gamma \in \mathbb{F}_q^* \]
consists of a right coset representative of \( \text{AGL} \) in \( \text{PGL} \). The coset decomposition
\[ \text{PGL} = \text{AGL} t_0 \bigcup \text{AGL} t_1 \bigcup \bigcup_{\gamma \in \mathbb{F}_q^*} \text{AGL} t_\gamma \]
gives rise to the orbit decomposition of \( \text{PGL}(\alpha) \) into \( \text{AGL} \)-orbits
\[ \text{PGL}(\alpha) = \text{AGL}(t_0 \alpha) \bigcup \text{AGL}(t_1 \alpha) \bigcup \bigcup_{\gamma \in \mathbb{F}_q^*} \text{AGL}(t_\gamma \alpha). \]
We have arrived at the following result (which has been appeared previously in [3]).

**Lemma 4.3:** Let \( \alpha \in \mathcal{S} \). Then
\[ \text{PGL}(\alpha) = \bigcup_{\gamma \in \mathbb{F}_q^*} \text{AGL} \left( \frac{1}{\alpha + \gamma} \right) \bigcup \text{AGL}(\alpha), \]
is a partition of \( \text{PGL}(\alpha) \) into \( \text{AGL} \)-orbits.Lemma 4.3 implies that
\[
\text{PGL}(\sigma^r(\alpha)) = \bigcup_{\gamma \in \mathbb{F}_q^*} \text{AGL} \left( \frac{1}{\sigma^r(\alpha) + \gamma} \right) \bigcup \text{AGL}(\sigma^r(\alpha))
\]
\[
= \bigcup_{\gamma \in \mathbb{F}_q^*} \text{AGL} \left( \frac{1}{\sigma^r(\alpha) + \gamma} \right) \bigcup \text{AGL}(\sigma^r(\alpha))
\]
\[
= \bigcup_{\gamma \in \mathbb{F}_q^*} \text{AGL} \left( \frac{1}{\alpha + \gamma} \right) \bigcup \text{AGL}(\sigma^r(\alpha)).
\]
Suppose now that PGL(α) is fixed by the cyclic group ⟨σr⟩, i.e., PGL(σrα) = PGL(α). In this case, the cyclic group ⟨σr⟩ acts on the set of AGL-orbits

\[
\text{AGL}/\text{PGL}(\alpha) = \left\{ \text{AGL}(\alpha), \text{AGL}\left( \frac{1}{\alpha + \gamma} \right) \mid \gamma \in \mathbb{F}_q \right\}
\]

in the way given in (IV.1).

**Lemma 4.4** [3, Lemma 3.8]: Let \( n \geq 5 \) be a prime number. If PGL(σrα) = PGL(α), then there exists a fixed point of ⟨σr⟩ on AGL/PGL(α). In other words, either AGL(σrα) = AGL(α) or AGL(σr(1/α+rα)) = AGL(1/α+rα) for some \( \gamma \in \mathbb{F}_q \).

By Lemma 4.2, we derive the next result which is crucial to our enumeration.

**Lemma 4.5**: Let \( x \in \mathcal{I}_r \). Then PGL(σr,f) = PGL(f) if and only if there is a polynomial \( g(x) \in \text{PGL}(f) \) such that \( g(x) \) divides \( x^{2\beta} + x \).

**Proof**: The proof is essentially the same as that given in [3, Lemma 3.9], since we have established Lemma 4.2. ⊙

**B. The Number of Orbits of ⟨σr⟩ on PGL/Ir With Size 1**

Now we are in a position to determine the number of orbits of ⟨σr⟩ on PGL/Ir with size 1. For convenience, we adopt the following notation throughout this subsection.

\[
\begin{align*}
A_1 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \\
A_4 &= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad A_5 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad A_6 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}
\end{align*}
\]

\[
G = \left\{ A_1, A_2, A_3, A_4, A_5, A_6 \right\}
\]

\[
\mathcal{X} = \left\{ f(x) \in \mathcal{I}_r \mid f(x) \text{ divides } x^{2r} + x \right\}
\]

\[
\Delta_i = \left\{ h(x) \in \mathcal{X} \mid A_i h(x) = h(x) \right\} \quad \text{for } 2 \leq i \leq 6.
\]

\[
\Delta_7 = \left\{ h(x) \in \mathcal{X} \mid A_7 h(x) \neq h(x), \text{ for any } 2 \leq i \leq 6 \right\}
\]

\[
\mathcal{G}_f = \left\{ A_1 f = f, A_2 f, A_3 f, A_4 f, A_5 f, A_6 f \right\}, \quad f \in \mathcal{X}
\]

The following result reveals that if PGL(f) contains a polynomial that divides \( x^{2r} + x \), then PGL(f) contains 2, 3 or 6 such polynomials.

**Lemma 4.6**: Suppose that \( f(x) \in \mathcal{I}_r \) such that \( f(x) \) divides \( x^{2r} + x \). Then

\[
\left\{ h(x) \mid h(x) \in \text{PGL}(f), \ h(x) \text{ divides } x^{2r} + x \right\} = \mathcal{G}_f;
\]

in particular,

\[
\left| \left\{ h(x) \mid h(x) \in \text{PGL}(f), \ h(x) \text{ divides } x^{2r} + x \right\} \right| = \left| \mathcal{G}_f \right|.
\]

**Proof**: For simplifying notation, let \( \Delta = \left\{ h(x) \mid h(x) \in \text{PGL}(f), \ h(x) \text{ divides } x^{2r} + x \right\} \). Let \( \alpha \) be a root of \( f(x) \), which gives \( \alpha^{2r} = \alpha \) since \( f(x) \) divides \( x^{2r} + x \). Observe that

\[
\Delta = \left\{ h(x) \mid h(x) \in \text{PGL}(f), \ h(x) \text{ divides } x^{2r} + x \right\} = \langle A \rangle^{2r} + A \alpha = 0
\]

Assume that \( A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \). Then

\[
(A \alpha)^2 + A \alpha = 0 \iff \begin{pmatrix} a \alpha + b \\ c \alpha + d \end{pmatrix} + \begin{pmatrix} a \alpha + b \end{pmatrix} = 0
\]

\[
\iff a^2 \alpha^2 + b^2 \alpha^2 + c^2 \alpha + d \alpha + a \alpha + b = 0
\]

\[
\iff a^2 \alpha + b^2 \alpha + a \alpha + b = 0
\]

\[
\iff d a^2 + c b^2 = 0.
\]

We have to consider three cases separately.

Case 1: \( a \neq 0, c = 0 \). Since \( A \) is invertible, one must have \( d \neq 0 \). From the second equality we have \( a = d \). If \( b \neq 0 \), then \( b = d \). Hence, there are two cases:

\[
b = c = 0, \quad a = d \neq 0 \quad \text{and} \quad c = 0, \quad a = b = d \neq 0.
\]

Therefore in this case

\[
A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.
\]

Case 2: \( c \neq 0, a = 0 \). Since \( A \) is invertible, \( b \neq 0 \) and \( c \neq 0 \).

By the second equality we obtain \( b = c \). If \( d \neq 0 \), then \( b = d \).

Hence, there are two cases:

\[
b = c \neq 0, \quad a = d = 0 \quad \text{and} \quad c = 0, \quad b = c = d \neq 0.
\]

Therefore

\[
A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.
\]

Case 3: \( c \neq 0, a \neq 0 \). From the first equality we get \( a = c \).

We consider three subcases separately.

Subcase 3.1: \( b = 0, d \neq 0 \). From the second equality, we have \( a = d \).

Subcase 3.2: \( b \neq 0, d = 0 \). From the second equality, we have \( b = c \).

Subcase 3.3: \( b \neq 0, d \neq 0 \). From the last equality, we have \( b = d \). However, the determinate of \( A \) is \( ad - bc = 0 \). This is impossible.

Hence, there are two cases:

\[
b = 0, \quad a = c = d \neq 0 \quad \text{and} \quad d = 0, \quad a = b = c \neq 0.
\]

Therefore in this case \( A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \).

In conclusion, we have

\[
\Delta = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} f(x), \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} f(x), \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} f(x), \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} f(x) \right\}
\]

\[
= \left\{ A_1 f = f, A_2 f, A_3 f, A_4 f, A_5 f, A_6 f \right\} = \mathcal{G}_f.
\]

Hence we get at once that \( |\Delta| = |\mathcal{G}_f| \), which is the required result. ⊙
We now provide some properties of the sets $G, \mathcal{X}$ and $\Delta_i$ ($i = 2, 3, \cdots, 7$). We first observe that $G$ is a group of order 6 and this group is isomorphism to the symmetric group $S_3$ of degree 3. Since $r \geq 3$, $f(x) \in I_r$ divides $x^2 + x$ if and only if $f(x) \in I_r$ divides $x^{r-1} - 1$.

The size of $\mathcal{X}$ has been determined explicitly in [3, Lemma 3.10] in terms of the Möbius function.

**Lemma 4.7:** With notation as given above, we have

$$|\mathcal{X}| = \left\{ f(x) \in I_r \mid f(x) \text{ divides } x^2 + x \right\} = \frac{1}{r} \sum_{d \mid r} (2^\frac{r}{d} - 1) \mu(d),$$

where $\mu$ is the Möbius function.

Let $M$ be a subgroup of PGL and $f(x) \in I_r$. If $A \circ f(x) = f(x)$ for any $A \in M$, then according to [23, Theorem 1.3] we see that $M$ must be a cyclic subgroup of PGL. Naturally, we have an analogous result about the group action involved.

**Lemma 4.8:** Let $M$ be a subgroup of PGL and $f(x) \in I_r$. If $A \circ f(x) = f(x)$ for any $A \in M$, then $M$ is a cyclic subgroup of PGL.

**Proof:** Assume that $M_0 = \{(A^T)^{-1} \mid A \in M\}$. Then $M_0$ is a subgroup of PGL, which is isomorphic to $M$. For any $B \in M_0$, there exists a matrix $A \in M$ such that $B = (A^T)^{-1}$. Thus $B \circ f(x) = Af(x) = f(x)$.

It follows from [23, Theorem 1.3] that $M_0$ is cyclic, which implies that $M$ also cyclic.

**Lemma 4.9:** With notation as given above, we have

1. $\Delta_5 = \Delta_6$.
2. $|\Delta_2| = |\Delta_3| = |\Delta_4|$.
3. $\Delta_i \cap \Delta_j = \emptyset$ for any $i, j \in \{2, 3, 4, 5, 7\}$ with $i \neq j$.
4. $\mathcal{X} = \Delta_2 \cup \Delta_3 \cup \Delta_4 \cup \Delta_5 \cup \Delta_7$. In particular, $|\mathcal{X}| = 3|\Delta_2| + |\Delta_3| + |\Delta_4| + |\Delta_5| + |\Delta_7|$.

**Proof:** (1) Since $A_3^3 = A_6$ and $A_5^3 = A_5$, it is easy to see that if $A_3 f = f$ then $A_6 f = A_2 f = f$; if $A_6 f = f$ then $A_5 f = A_2 f = f$. This shows that $\Delta_5 = \Delta_6$.

(2) Note that $G$ is a group of order 6 and this group is isomorphism to the symmetric group of degree 3. Then $G$ has three conjugacy classes given as follows:

$$\{A_1\}, \{A_2, A_3, A_4\}, \{A_5, A_6\}.$$ 

Additionally, there is a group action $G$ on the set $\mathcal{X}$:

$$G \times \mathcal{X} \rightarrow \mathcal{X}$$

$$(A_i, f) \mapsto A_i f.$$ 

Thus for $i = 1, 2, \cdots, 6$,

$$\text{Fix}(A_i) = \{f \in \mathcal{X} \mid A_i f = f\} = \Delta_i.$$ 

Assume that two matrices $A_i$ and $A_j$ of $G$ belong to the same conjugacy class, i.e., there exists a matrix $A_k \in G$ such that $A_k^{-1} A_i A_k = A_j$, where $1 \leq i, j, k \leq 6$. Then

$$\text{Fix}(A_j) = A_k \text{Fix}(A_i) = \Delta_j = A_k \Delta_i,$$

which implies that $|\Delta_i| = |\Delta_j|$. Therefore we have $|\Delta_2| = |\Delta_3| = |\Delta_4|$. 

(3) Suppose that $f \in \Delta_i \cap \Delta_j$ with $i, j \in \{2, 3, 4, 5, 7\}$ and $i \neq j$. Then $A_i f = A_j f = f$. Let $\langle A_i, A_j \rangle$ be the subgroup of $G$ generated by $A_i, A_j$ (which is the smallest subgroup of $G$ containing $A_i$ and $A_j$). Thus the following holds:

$$Af = f, \text{ for any } A \in \langle A_i, A_j \rangle.$$ 

Since $r \geq 3$, according to Lemma 4.8, the subgroup $\langle A_i, A_j \rangle$ is a cyclic subgroup of $G$. Observe that for any $i, j \in \{2, 3, 4, 5, 7\}$ with $i \neq j$, $\langle A_i, A_j \rangle$ cannot be a cyclic subgroup of $G$. We have obtained a contradiction. Hence $\Delta_i \cap \Delta_j = \emptyset$ for any $i, j \in \{2, 3, 4, 5, 7\}$ with $i \neq j$.

(4) It follows from (3) that there is a decomposition of $\mathcal{X}$,

$$\mathcal{X} = \Delta_2 \cup \Delta_3 \cup \Delta_4 \cup \Delta_5 \cup \Delta_7,$$

and by (1) and (2) we get

$$|\mathcal{X}| = 3|\Delta_2| + |\Delta_3| + |\Delta_4| + |\Delta_5| + |\Delta_7|.$$ 

We have seen that the number of monic irreducible polynomials of degree $r$ over $\mathbb{F}_q$ that divide $x^2 + x$ is equal to $\frac{1}{r} \sum_{d \mid r} (2^\frac{r}{d} - 1) \mu(d)$. Our next goals are to determine the number $|\mathcal{G}_f|$ and obtain the number of orbits with size 1.

**Lemma 4.10:** With notation as given above, we then have

1. If $f \in \Delta_2$, then

$$\mathcal{G}_f = \{f, A_3 f, A_4 f\},$$ 

where $A_3 f \in \Delta_4$, $A_4 f \in \Delta_3$. In particular, $|\mathcal{G}_f| = 3$.

2. If $f \in \Delta_3$, then

$$\mathcal{G}_f = \{f, A_2 f, A_4 f\},$$ 

where $A_2 f \in \Delta_4$, $A_4 f \in \Delta_2$. In particular, $|\mathcal{G}_f| = 3$.

3. If $f \in \Delta_4$, then

$$\mathcal{G}_f = \{f, A_2 f, A_3 f\},$$ 

where $A_2 f \in \Delta_3$, $A_3 f \in \Delta_2$. In particular, $|\mathcal{G}_f| = 3$.

4. If $f \in \Delta_5$, then

$$\mathcal{G}_f = \{f, A_2 f\},$$ 

where $A_2 f \in \Delta_5$. In particular, $|\mathcal{G}_f| = 2$.

5. If $f \in \Delta_7$, then

$$\mathcal{G}_f = \{A_1 f = f, A_2 f, A_3 f, A_4 f, A_5 f, A_6 f\}.$$ 

In particular, $|\mathcal{G}_f| = 6$.

6. If $g \notin \text{PGL}(f)$, then

$$\mathcal{G}_f \cap \mathcal{G}_g = \emptyset.$$ 

**Proof:** (1) By straightforward calculations we have

$$(A_3^{-1} A_5) f = (A_3 A_5) f = A_2 f = f$$

and

$$(A_4^{-1} A_6) f = (A_4 A_6) f = A_2 f = f,$$

which implies $A_3 f = A_5 f$ and $A_4 f = A_6 f$. On the other hand, by

$$A_4 (A_3 f) = (A_4 A_3) f = A_5 f = A_3 f$$
and \[ A_3(A_4 f) = (A_3 A_4) f = A_6 f = A_4 f, \]
we obtain \[ A_3 f = A_5 f \in \Delta_4 \text{ and } A_4 f = A_6 f \in \Delta_3. \]
Since the intersection of any two of \( \Delta_2, \Delta_3, \Delta_4 \) is empty, we get \( A_3 f \neq f, \ A_3 f \neq A_4 f \) and \( A_4 f \neq f \). Thus
\[
G_f = \{ f, A_3 f, A_4 f \}.
\]
(2) and (3). By the method analogous to that used in the proof of (1), we obtain the desired results.
(4). Clearly, \( A_6 f = A_5^2 f = A_5 f = f \). In addition,
\[
(A_2^{-1} A_4) f = (A_2 A_4) f = A_5 f = f
\]
and
\[
(A_4^{-1} A_3) f = (A_4 A_3) f = A_5 f = f,
\]
which yields \( A_2 f = A_3 f = A_4 f \). Then from \( A_3(A_2 f) = (A_3 A_2) f = A_4 f = A_5 f \) we obtain \( A_2 f \in \Delta_5 \). Since \( A_2 f \neq f \), it is easy to see that
\[
G_f = \{ f, A_2 f \}.
\]
(5) and (6). They are obvious by the definition of \( \Delta_7 \) and \( G_f \).

The number of orbits of PGL on \( I_r \) with size 1 can be represented in terms of the values of \( |\mathcal{X}|, |\Delta_2| \) and \( |\Delta_5| \), as we show below.

**Theorem 4.11:** Let \( s_0 \) be the number of orbits of PGL on \( I_r \) with size 1. Then
\[
s_0 = \frac{1}{6} \left( |\mathcal{X}| + 3|\Delta_2| + 2|\Delta_5| \right).
\]
**Proof:** Combining Lemmas 4.6, 4.9 and 4.10, we see that
\[
s_0 = \frac{1}{3} \left( |\Delta_2| + |\Delta_3| + |\Delta_4| \right) + \frac{1}{2} |\Delta_5| + \frac{1}{6} |\Delta_7|
\]
\[
= |\Delta_2| + \frac{1}{2} |\Delta_5| + \frac{1}{6} \left( |\mathcal{X}| - 3|\Delta_2| - |\Delta_5| \right)
\]
\[
= \frac{1}{6} \left( |\mathcal{X}| + 3|\Delta_2| + 2|\Delta_5| \right),
\]
which is our desired result. The proof is complete.

We are left to compute \( |\Delta_2| \) and \( |\Delta_5| \). The following result exhibits the value of \( |\Delta_2| \) explicitly.

**Lemma 4.12:** We have
\[
|\Delta_2| = \begin{cases} 
0, & \text{if } r \text{ is odd,} \\
\frac{1}{r} \sum_{d \mid \Delta_2, d \neq \Delta_2} \mu(d) 2^{\mathcal{X}}, & \text{if } r \text{ is even,}
\end{cases}
\]
where \( \mu \) is the Möbius function.

**Proof:** It is easily seen that the order of \( A_2 \in \text{PGL} \) is equal to two, i.e., \( A_2^2 = E_2 \) (\( E_2 \) is the identity element of the group PGL) and \( A_2 \neq E_2 \). If \( r \) is odd then \( |\Delta_2| = 0 \); this is simply because there is no monic irreducible polynomial \( h(x) \) of odd degree over \( \mathbb{F}_q \) satisfying \( A_2 h(x) = h(x) \).

We assume that \( r = 2r' \), where \( r' > 1 \) is a positive integer. By the very definition of the group action of PGL on \( I_r \), we see that \( A_2 h(x) = h(x) \) is equal to the monic polynomial \( A_2 h(x) = \left( x^r h \left( \frac{1}{x} \right) \right) \). The irreducible polynomials satisfying \( \left( x^r h \left( \frac{1}{x} \right) \right)^* = h(x) \) are termed as self-reciprocal irreducible monic polynomials in the literature, which have been studied extensively. It is known that \( h(x) \in \mathbb{I}_r \) is self-reciprocal (equivalently \( A_2 h(x) = h(x) \)) if and only if \( h(x) \) divides \( x^{q^r} + 1 \) (see [18, Theorem 1] or one can prove this fact easily). Therefore, \( A_2 h(x) = h(x) \) and \( h(x) \) divides \( x^{q^r} + x \) if and only if \( h(x) \) divides \( \gcd \left( x^{q^r} + 1, x^{q^r} + x \right) \). We claim that
\[
\gcd \left( x^{q^r} + 1, x^{q^r} + x \right) = x^{\gcd(q^r+1, 2q^r)} + 1
\]
and
\[
\gcd \left( x^{q^r} - 1, x^{q^r} + 1 \right) = x^{\gcd(q^r-1, 2q^r-1)} + 1.
\]
To prove the claim, it is enough to show that
\[
\gcd (2^{nr} - 1, 2^{r'r} - 1) = 2^{nr - 1} + 1.
\]
Indeed, observing that \( 2^{nr} - 1 = (2^{nr - 1})(2^{nr} + 1) \), \( \gcd(2^{nr} - 1, 2^{nr} + 1) = 1 \) and \( 2^{nr - 1} \) divides \( 2^{nr} - 1 \), we have
\[
2^{nr - 1} = \gcd(2^{nr} - 1, 2^{nr} + 1) = \gcd(2^{nr} - 1)(2^{nr} + 1, 2^{nr} - 1)
\]
and
\[
\gcd \left( x^{q^r} - 1, x^{q^r} + 1 \right) = x^{\gcd(q^r-1, 2q^r-1)} + 1.
\]
We have thus shown that \( \gcd \left( x^{q^r} + 1, x^{q^r} + x \right) = x^{2q^r} + 1 \). This implies that the number of monic irreducible polynomials \( h(x) \) of degree \( r \) over \( \mathbb{F}_q \) that satisfy \( A_2 h(x) = h(x) \) and \( h(x) \mid (x^{q^r} + x) \) (namely the size of \( \Delta_2 \)) is equal to the number of monic irreducible polynomials of degree \( r \) over \( \mathbb{F}_q \) that divide \( x^{2q^r} + 1 \).

It is readily seen that every irreducible factor (except the one \( x+1 \)) of \( x^{2q^r} + 1 \) over \( \mathbb{F}_q \) has even degree. If \( f(x) \) is a monic irreducible polynomial of degree \( 2d \) over \( \mathbb{F}_q \) that divides \( x^{2q^r} + 1 \), we assert that \( d \) is a divisor of \( r' \) and \( r'/d \) is odd. To this end, note, by \( f(x) \mid (x^{2q^r} + 1) \), that \( f(x) \mid (x^{2q^r} + 1) \) and thus \( f(x) \mid (x^{2q^r} + 1) \), which yields \( f(x) \mid (x^{q^r - 1} + 1) \). Since \( f(x) \) is irreducible of degree \( 2d \) over \( \mathbb{F}_q \), we have \( (2d - 1) \mid (q^r - 1) \). We then have that \( 2d \) is a divisor of \( r \), which implies that \( d \) divides \( r' \). Since \( n \) is an odd prime number, it follows that \( x^{2q^r} + 1 \) divides \( x^{2q^r} + 1 = x^{nr} + 1 \). Thus, \( f(x) \) divides \( \gcd(x^{q^r} + 1, x^{q^r} + x) \). If \( r'/d = r'' \) is even, then \( \gcd(q^d + 1, q^{r''} + 1) = 1 \); otherwise, let \( \gcd(q^d + 1, q^{r''} + 1) = \ell \neq 1 \). Then \( q^d \equiv -1 \pmod{\ell} \) and \( (q^d)^{\ell - 1} \equiv -1 \pmod{\ell} \).
It follows that\[ \prod \{ h(x) \mid h(x) \in \mathcal{I}_{2d} \text{ and } h(x) \text{ divides } x^{2^r' + 1} + 1 \}. \]

Let \( H^0_r(x) = \frac{x^{2^r' + 1} + 1}{x^r + 1} \). By the Möbius inversion formula (for example, see [11, Theorem 3.24]), we have
\[ R_r(x) = \prod_{d \mid d_0} H_r^{0\langle d \rangle}(x)^{\mu(d)}. \]

We conclude that
\[ r|\Delta_2| = \sum_{d \mid d_0} \mu(d)2^r. \]

This completes the proof. \( \square \)

We still need to find the value of \(|\Delta_5|\). For this purpose, we first establish several lemmas.

**Lemma 4.13:** Let \( f(x) \in \mathcal{I}_r \). Then \( f(x) \in \mathcal{X} \) and \( A_5f(x) = f(x) \) if and only if
\[ f(x) \mid \gcd\left(x^{q^0 + 1} + x + 1, x^{2^r} + x\right), \]
where \( r_0 = \frac{r}{2} \).

**Proof:** Suppose that \( f(x) \in \mathcal{X} \) and \( A_5f(x) = f(x) \), which gives \( 3 \mid r \). Assume that \( \alpha \in \mathbb{F}_{q^r} \) is a root of \( f(x) \). Then there exists a positive integer \( r_0 \) (\( 1 \leq r_0 \leq r - 1 \)) such that
\[ \frac{\alpha + 1}{\alpha} = A_5\alpha = \alpha^{q^0}, \]
where \( r_0 \) is the least positive integer satisfying the above equality. Thus, \( f(x) \mid \left(x^{q^0 + 1} + x + 1\right) \), which implies that
\[ f(x) \mid \gcd\left(x^{q^0 + 1} + x + 1, x^{2^r} + x\right). \]

Let
\[ \Omega = \{ \alpha, \alpha^{q^0}, \ldots, \alpha^{q^{r-1}} \} \]
be the set of all the roots of \( f(x) \). Then the cyclic group \( \langle A_5 \rangle \) acts on the set \( \Omega \), and \( \Omega \) can be decomposed into disjoint union of orbits:
\[ \Omega = \langle A_5 \rangle(\alpha) \cup \langle A_5 \rangle(\alpha^{q^0}) \cup \cdots \cup \langle A_5 \rangle(\alpha^{q^{r-1}}), \]
Hence we get \( r = 3r_0 \).

On the contrary, let \( \alpha \in \mathbb{F}_{q^r} \) be a root of \( f(x) \). Then \( f(x) \mid \left(x^{q^0 + 1} + x + 1, x^{2^r} + x\right) \), we have \( f(x) \in \mathcal{X} \) and \( A_5\alpha = \alpha^{q^0} = \alpha^{q^0}. \) Hence, \( A_5\alpha \) is a root of \( f(x) \) and \( A_5f(x) = f(x) \).

The next lemma is important in determining the value of \(|\Delta_5|\).

**Lemma 4.14:** Let \( f(x) \in \mathcal{X} \) with \( A_5f(x) = f(x) \) and let \( \alpha \in \mathbb{F}_{q^r} \) be a root of \( f(x) \). Then
\[ x^{q^0 + 1} + x + 1 = (x - \alpha) \prod_{\gamma \in \mathbb{F}_{q^0}} \left(x - \left(\frac{\gamma^2 + \gamma + 1}{\alpha + \gamma} + \gamma + 1\right)\right), \]
where \( r = 3r_0 \).

**Proof:** According to Lemma 4.13, \( \alpha \) is a root of \( x^{q^0 + 1} + x + 1 \) and \( \alpha^{q^0} = \alpha + 1 \). Thus for any \( \gamma \in \mathbb{F}_{q^0}, \)
\[ \left(\frac{\gamma^2 + \gamma + 1}{\alpha + \gamma} + \gamma + 1\right)^{q^0} = \frac{\gamma^2 + \gamma + 1}{\alpha^{q^0} + \gamma} + \gamma + 1 = \frac{\gamma^2 + \gamma + 1}{\alpha + \gamma} + \gamma + 1. \]

We further obtain that
\[ \left(\frac{\gamma^2 + \gamma + 1}{\alpha + \gamma} + \gamma + 1\right)^{q^0 + 1} + \left(\frac{\gamma^2 + \gamma + 1}{\alpha + \gamma} + \gamma + 1\right) = \frac{\gamma^2 + \gamma + 1}{\alpha + \gamma} + \gamma + 1 = \frac{\alpha \gamma + \alpha + 1}{\alpha + \gamma} + \gamma + 1 = 1 + 1 = 0. \]

Therefore \( \alpha \) and \( \gamma^2 + \gamma + 1 + \gamma \) (for any \( \gamma \in \mathbb{F}_{q^0} \)) are the roots of \( x^{q^0 + 1} + x + 1 \). Let \( \theta_\gamma = \frac{\gamma^2 + \gamma + 1}{\alpha + \gamma} + \gamma + 1 \). In the following we check that for any \( \gamma, \gamma' \in \mathbb{F}_{q^0}, \)
\[ \alpha \neq \theta_\gamma \text{ and } \theta_\gamma \neq \theta_{\gamma'} \left( \gamma \neq \gamma' \right), \]
which shows that the roots of \( x^{q^0 + 1} + x + 1 \) are distinct.

Indeed,
\[ \theta_\gamma = \theta_\gamma', \]
\[ \iff \gamma^2 + \gamma + 1 + \gamma + 1 = \frac{\gamma^2 + \gamma + 1}{\alpha + \gamma} + \gamma + 1 \]
\[ \iff \gamma^2 + \gamma + 1 = \frac{\gamma^2 + \gamma + 1}{\alpha + \gamma} + \gamma + \gamma' \]
\[ \iff \alpha \gamma + \gamma' = \alpha \gamma + \gamma + \alpha^2 \gamma + \alpha^2 \gamma' \]
\[ \iff (\gamma + \gamma')(\alpha^2 + \alpha + 1) = 0 \]
\[ \iff \gamma = \gamma'. \]

In the last but one equality \( r \geq 3 \) implies that \( \alpha^2 + \alpha + 1 \neq 0 \). Next, let us verify that for any \( \gamma \in \mathbb{F}_{q^0}, \)
\[ \alpha = \theta_\gamma', \]
\[ \iff \alpha = \frac{\gamma^2 + \gamma + 1}{\alpha + \gamma} + \gamma + 1 \]
\[ \iff \alpha (\alpha + \gamma) = \gamma^2 + \gamma + 1 + (\alpha + \gamma)(\gamma + 1) \]
\[ \iff \alpha^2 + \alpha + 1 = 0. \]

In conclusion, we see that all the roots of \( x^{q^0 + 1} + x + 1 \) are distinct. Note that the degree of this polynomial is \( q^0 + 1 \). We have decomposed completely the polynomial \( x^{q^0 + 1} + x + 1 \) into degree-one factors in \( \mathbb{F}_{q^r} \).

Given a positive integer \( n' \), let \( N_q(n') \) be the number of monic irreducible polynomials in \( \mathbb{F}_q[x] \) of degree \( n' \).
According to \cite[Theorem 3.25]{11}, the number \( N_q(n') \) is given by
\[
N_q(n') = \frac{1}{n'} \sum_{d|n'} \mu(d)q^\frac{n'}{d}.
\]
Thus, a crude estimate yields\]
\[
N_q(n') > 0.
\]
In other words, for every finite field \( \mathbb{F}_q \) and every positive integer \( n' \), there exists an irreducible polynomial in \( \mathbb{F}_q[x] \) of degree \( n' \).
In addition, the Möbius function \( \mu \) satisfies (see \cite[Lemma 3.23]{11})
\[
\sum_{d|n'} \mu(d) = \begin{cases} 
1 & \text{if } n' = 1, \\
0 & \text{if } n' > 1.
\end{cases}
\]
With these known results, we have the following result which guarantees the existence of a monic irreducible polynomial \( f(x) \) of degree \( r \) over \( \mathbb{F}_2 \) satisfying \( A_5 f(x) = f(x) \).

**Lemma 4.15:** Let \( r \) be an integer satisfying \( 3 \mid r \) and \( r \neq 6 \). Then there exists a monic irreducible polynomial \( f(x) \) of degree \( r \) over \( \mathbb{F}_2 \) satisfying \( A_5 f(x) = f(x) \).

**Proof:** According to \cite[Theorem 4.7]{23}, the number \( \mathcal{N}(\mathbb{F}_2, r) \) of monic irreducible polynomials \( f(x) \) of degree \( r \) over \( \mathbb{F}_2 \) satisfying \( A_5 f(x) = f(x) \) is equal to
\[
\mathcal{N}(\mathbb{F}_2, r) = \frac{2}{r} \sum_{\substack{d \mid 2^r \\ \gcd(d, 3) = 1}} \left( \frac{2^\frac{r}{2} - (-1)^{\frac{r}{2}+1}}{ \mu(d) } \right) \mu(d),
\]
where \( \mu \) is the Möbius function. In the following we aim to prove that
\[
\mathcal{N}_0(\mathbb{F}_2, r) = \sum_{\substack{d \mid 2^r \\ \gcd(d, 3) = 1}} \left( \frac{2^\frac{r}{2} - (-1)^{\frac{r}{2}+1}}{ \mu(d) } \right) \mu(d) > 0.
\]
To this end, suppose that \( r = 3m \) and \( m = 2^l 3^k p_1^{l_1} p_2^{l_2} \cdots p_i^{l_i} \), where \( l, k, \) and \( p_i \) are non-negative integers and \( p_i \) are prime numbers with \( p_i \neq 2, 3 \) for \( i = 1, 2, \cdots, t \). Let \( m_0 = 2^t p_1 p_2 p_3 \cdots p_i \). We consider two cases separately.

(1) \( k \geq 1 \). In this case let \( a = 2^k \), then \( a \geq 8 \). Thus,
\[
\mathcal{N}_0(\mathbb{F}_2, r) = \sum_{d | 2^r} \left( \frac{2^\frac{r}{2} - (-1)^{\frac{r}{2}+1}}{ \mu(d) } \right) \mu(d)
\]
\[
= \sum_{d | m_0} \left( \frac{a^{\frac{r}{2}} - (-1)^{\frac{r}{2}+1}}{ \mu(d) } \right) \mu(d)
\]
\[
= \sum_{d | m_0} \left( a^{\frac{r}{2}} - (-1)^{\frac{r}{2}+1} \right) \mu(d)
\]
\[
\geq a^{m_0} - a^{m_0-1} - a^{m_0-2} - a^2 + m_0
\]
\[
= a^{m_0} - a^{m_0-1} - \cdots - a^2 - a - m_0
\]
\[
= a^{m_0} - \frac{a}{a-1} - m_0
\]
\[
> a^{m_0} \frac{a-2}{a-1} - (m_0 - 1)
\]
\[
= a^{m_0-1} \frac{a(a-2)}{a-1} - m_0
\]
\[
> a^{m_0-1} - (m_0 - 1) > 1.
\]

(2) \( k = 0 \). In this case \( m = m_0 = 2^t p_1^{l_1} p_2^{l_2} \cdots p_i^{l_i} \) and we have
\[
\mathcal{N}_0(\mathbb{F}_2, r) = \sum_{d | m_0} \left( \frac{2^\frac{r}{2} - (-1)^{\frac{r}{2}+1}}{ \mu(d) } \right) \mu(d)
\]
\[
= \sum_{d | m_0} \left( 2^\frac{r}{2} - (-1)^{\frac{r}{2}} \right) \mu(d)
\]
\[
= \sum_{d | m_0} \left( 2^{\frac{m_0}{2}} + 1 \right) \mu(d)
\]
\[
= 3 > 0.
\]

(2.2) \( l = 0, t \geq 1 \). In this case we have \( m_0 > 1 \) and \( 2^t \). Thus
\[
\mathcal{N}_0(\mathbb{F}_2, r) = \sum_{d | m_0} \left( 2^{\frac{m_0}{2}} - (-1)^{\frac{m_0}{2}} \right) \mu(d)
\]
\[
= \sum_{d | m_0} \left( 2^{\frac{m_0}{2}} + 1 \right) \mu(d)
\]
\[
= \sum_{d | m_0} \left( 2^{\frac{m_0}{2}} - (-1)^{\frac{m_0}{2}} \right) \mu(d)
\]
\[
= 2^{t-1} > 2.
\]

(2.4) \( l = 1, t \neq 0 \). In this case we have \( m_0 = p_1^{l_1} p_2^{l_2} \cdots p_i^{l_i} \) and then \( m_0 = 2n_0 \) with \( n_0 \geq 5 \) being odd. It follows that
\[
\mathcal{N}_0(\mathbb{F}_2, r) = \sum_{d | m_0} \left( 2^{\frac{m_0}{2}} - (-1)^{\frac{m_0}{2}} \right) \mu(d)
\]
\[
= \sum_{d | n_0} \left( 2^{\frac{m_0}{2}} - (-1)^{\frac{m_0}{2}} \right) \mu(2d)
\]
\[
= \sum_{d | n_0} \left( 2^{\frac{m_0}{2}} - 1 \right) \mu(d) + \sum_{d | n_0} \left( 2^{\frac{m_0}{2}} + 1 \right) \mu(2d)
\]
Then be a monic irreducible polynomial of degree \( r \). That is to say, there is indeed no monic irreducible polynomial of degree \( r \).

Lemma 4.15 says that if \( f \) and only if \( r_0 \) is even; If this is the case, \( x^2 + x + 1 \) is a unique monic irreducible factor of \( F_{r_0}(x) \) over \( \mathbb{F}_q \) with degree 2.

(3) \( F_{r_0}(x) \) has the following decomposition over \( \mathbb{F}_{2^r} \):

\[
F_{r_0}(x) = \gcd \left( x^{q^r - 1} + x + 1, x^{2^r} + x \right)
\]

\[
= (x - \alpha) \prod_{\gamma \in \mathbb{F}_{q^{r_0}}} \left( x - \left( \frac{x^2 + \gamma + 1}{\alpha + \gamma} + \gamma + 1 \right) \right).
\]

Proof: (1) Suppose otherwise that \( F_{r_0}(x) \) has an irreducible factor of degree 1 over \( \mathbb{F}_q \). Then there exists an element \( \beta \in \mathbb{F}_q \) such that \( \beta^2 + \beta = 0 \). Using \( \gcd(r, n) = 1 \), we see that

\[
\beta \in \mathbb{F}_q \cap \mathbb{F}_{2^r} = \mathbb{F}_{2^n} \cap \mathbb{F}_{2^r} = \mathbb{F}_{2^{\gcd(r, n)}} = \mathbb{F}_2.
\]

However, \( \beta^{q^r + 1} + \beta + 1 = 0 \), which is a contradiction. Therefore \( F_{r_0}(x) \) has no irreducible factor of degree 1 over \( \mathbb{F}_q \).

(2) First, suppose that \( F_{r_0}(x) \) has an irreducible factor \( x^2 + ax + b \) of degree 2 over \( \mathbb{F}_q \), where \( a, b \in \mathbb{F}_q \). Since \( (x^2 + ax + b) \mid (x^2 + x) \), we have \( \mathbb{F}_{q^2} \subseteq \mathbb{F}_{2^r} \), i.e., \( \mathbb{F}_{2^n} \subseteq \mathbb{F}_{2^r} \). This leads to \( 2n \mid r \), i.e., \( 2n \mid 3r_0 \). Then \( r_0 \) must be even.

Second, suppose that \( r_0 \) is even. It is easy to see that \( x^2 + x + 1 \) is irreducible over \( \mathbb{F}_2 \). Since \( \gcd(r, n) = 1 \), \( x^2 + x + 1 \) is also irreducible over \( \mathbb{F}_q \). In the following, we aim to show that \( (x^2 + x + 1) \mid F_{r_0}(x) \). Let \( r_0 = 2r_1 \). Thus \( r = 6r_1 \) and further \( 3 \mid (2^{6r_1} - 1) \). We have \( x^3 - 1 \mid \left( \frac{x^{2^{6r_1}} - 1}{x^2 - 1} \right) \) and \( x^3 - 1 = (x - 1)(x^2 + x + 1) \), we obtain \( (x^2 + x + 1) \mid (x^{2^r} - x) \). Assume that \( \theta, \theta^2 \) are all the roots of \( x^2 + x + 1 \), giving \( \theta^2 = \theta + 1 \). Thus,

\[
\gamma^2 = \begin{cases} 
\theta, & 2 \mid l, \\
\theta + 1, & 2 \nmid l.
\end{cases}
\]

Therefore,

\[
\varphi^{q^{r_1} + 1} + \varphi + 1 = \varphi \cdot \varphi^{q^{r_1}} + \varphi + 1 = \varphi^2 + \varphi + 1 = 0
\]

and

\[
(\varphi^2)^{q^{r_1} + 1} + \varphi^2 + 1 = \varphi^2 \cdot (\varphi^2)^{q^{r_1}} + \varphi^2 + 1
\]

\[
= \varphi^2 \cdot \varphi^{2^{q^{r_1} + 1}} + \varphi^2 + 1
\]

\[
= \varphi^2 (\varphi + 1) + \varphi^2 + 1 = 0.
\]

We have shown that \( (x^2 + x + 1) \mid F_{r_0}(x) \). It needs to shows that \( x^2 + x + 1 \) is a unique monic irreducible divisor of \( F_{r_0}(x) \) over \( \mathbb{F}_q \). For this purpose, suppose \( \alpha \) is a root of \( F_{r_0}(x) \) satisfying \( \alpha^{q^r} = \alpha \) and \( \alpha \neq \alpha^q \). Since \( F_{r_0}(x) \) is a divisor of \( x^{q^{r_1} + 1} + x + 1 \) and \( r_0 \) is even, then \( \alpha^{q^{r_1} + 1} + \alpha + 1 = 0 \). We thus have \( \alpha^2 + \alpha + 1 = 0 \), implying that \( \alpha \) is a root of \( x^2 + x + 1 \).

(3) Note, by Lemma 4.14, that

\[
x^{q^{r_1} + 1} + x + 1 = (x - \alpha) \prod_{\gamma \in \mathbb{F}_{q^{r_0}}} \left( x - \left( \frac{2 + \gamma + 1}{\alpha + \gamma} + \gamma + 1 \right) \right).
\]
Since \( \alpha^{2^r} = \alpha \), we have \((x - \alpha) \mid F_{r_0}(x)\). On the other hand, for any \( \theta_i = \frac{\gamma^2 + \gamma + 1}{\alpha + \gamma} + 1 \), we have

\[
\theta_i^r = \theta_i \\
\left( \frac{\gamma^2 + \gamma + 1}{\alpha + \gamma} + 1 \right)^r = \frac{\gamma^2 + \gamma + 1}{\alpha + \gamma} + 1
\]

Thus the irreducible decompositions of \( x^{2^r} - 1 \) over \( \mathbb{F}_q \) and over \( \mathbb{F}_2 \) are the same. By Remark 4.17, there is no monic irreducible polynomial \( f(x) \) of degree 6 over \( \mathbb{F}_2 \) satisfying \( A_5 f(x) = f(x) \). Hence, there is no monic irreducible polynomial \( f(x) \) of degree 6 over \( \mathbb{F}_2 \) satisfying \( A_5 f(x) = f(x) \). Therefore in this case we also have \( |\Delta_5| = 0 \).

In the following we consider the case where \( 3 \mid r \) and \( r \neq 6 \). Assume that \( r = 3r_0 \), where \( r_0 \neq 2 \) is a positive integer. We have shown in Lemma 4.18 that

\[
F_{r_0}(x) = \gcd (x^{q_0 + 1} + x + 1, x^{2r_0} + x)
\]

\[
= (x - \alpha) \prod_{\gamma \in \mathbb{F}_{q_0}} \left( x - \left( \frac{\gamma^2 + \gamma + 1}{\alpha + \gamma} + 1 \right) \right).
\]

We are now in a position to give an enumerating formula for the size of the set \( \Delta_5 \), which is based on the Möbius inversion formula and its generalizations, see [10], Section 5.2.

**Lemma 4.19:** Let \( \chi : \mathbb{N} \to \mathbb{C} \) be a completely multiplicative function, which is, in other words, a homomorphism between the monoids \((\mathbb{N}, \cdot)\) and \((\mathbb{C}, \cdot)\). Let \( F, G : \mathbb{N} \to \mathbb{C} \) be two functions such that

\[
F(n) = \sum_{d \mid n} \chi(d) \cdot G\left( \frac{n}{d} \right), \quad n \in \mathbb{N}.
\]

Then,

\[
G(n) = \sum_{d \mid n} \mu(d) \cdot F\left( \frac{n}{d} \right), \quad n \in \mathbb{N}.
\]

**Lemma 4.20:** The value of \(|\Delta_5|\) is equal to

\[
\begin{cases} 
0, & 3 \mid r, \\
0, & r = 6, \\
\frac{1}{r} \sum_{d \mid r, \gcd(d, 3) = 1} \mu(d)\left( 2 \tilde{m} + (-1)^{\tilde{m} + 1} \right), & 3 \mid r \text{ and } r \neq 6,
\end{cases}
\]

where \( \mu \) is the Möbius function.

**Proof:** If \( 3 \mid r \), it is easy to see that \(|\Delta_5| = 0 \). If \( r = 6 \), we consider the irreducible decomposition of \( x^{2^r} - 1 \) over \( \mathbb{F}_q \) and over \( \mathbb{F}_2 \), respectively. Denote by \( \mathbb{Z}_{2r-1} \) the unit group of the residue ring of integers modulo \( 2^r - 1 \). Since \( \gcd(q, 2^r - 1) = 1 \), we have \( q \in \mathbb{Z}_{2r-1}^\ast \). Let \( \langle q \rangle \) denote the cyclic subgroup of \( \mathbb{Z}_{2r-1} \). Then there is an action of the group \( \langle q \rangle \) on the set \( \mathbb{Z}_{2r-1} \) given as follows:

\[
\langle q \rangle \times \mathbb{Z}_{2r-1} \rightarrow \mathbb{Z}_{2r-1} \\
(q^s, k) \mapsto q^s k.
\]

Let \( s \) be an integer with \( 0 \leq s < n \). Thus the \( q \)-cycloctomic coset of \( s \) modulo \( 2^r - 1 \) is the same as the orbit \( \langle q \rangle s = \{ q^i s \mid i \text{ is an integer} \} \) of \( s \) under this group action. For the same reason, there exists an action of the cyclic subgroup \( \langle 2 \rangle \) on the set \( \mathbb{Z}_{2r-1} \), and the \( 2 \)-cycloctomic coset of \( s \) modulo \( 2^r - 1 \) is the same as the orbit \( \langle 2 \rangle s \) of \( s \) under this group action. Noting that \( \langle q \rangle \subseteq \langle 2 \rangle \) and the order \( \operatorname{ord}_{2^r-1}(q) \) of \( q \) modulo \( 2^r - 1 \) is

\[
\operatorname{ord}_{2^r-1}(q) = \frac{\operatorname{ord}_{2^r-1}(2)}{\gcd(n, \operatorname{ord}_{2^r-1}(2))} = \frac{r}{\gcd(n, r)} = r = \operatorname{ord}_{2^r-1}(2),
\]

we obtain that \( \langle q \rangle s = \langle 2 \rangle s \) for any \( s \) with \( 0 \leq s < n \). It follows that the irreducible decompositions of \( x^{2^r - 1} - 1 \) over \( \mathbb{F}_q \) and \( \mathbb{F}_2 \) are the same by Remark 4.17, there is no monic irreducible polynomial \( f(x) \) of degree 6 over \( \mathbb{F}_q \), satisfying \( A_5 f(x) = f(x) \). Hence, there is no monic irreducible polynomial \( f(x) \) of degree 6 over \( \mathbb{F}_2 \) satisfying \( A_5 f(x) = f(x) \). Therefore in this case we also have \( |\Delta_5| = 0 \).

Let \( f(x) \) be a monic irreducible polynomial of degree 3d over \( \mathbb{F}_q \) dividing \( F_{r_0}(x) \). We assert that \( d \mid r_0 \) and \( \gcd(3, \frac{r}{d}) = 1 \). To this end, note, by \( f(x) \mid (x^{q_0 + 1} + x + 1, x^{2r_0} + x) \), that \( f(x) \mid (x^{q_0 + 1} + 1) \) and thus \( f(x) \mid (x^{2r_0} + 1) \), which yields \( f(x) \mid (x^{q_0 + 1} + 1) \) and so \( f(x) \mid (x^{r_0} + 1) \). Since \( f(x) \) is irreducible of degree 3d over \( \mathbb{F}_q \), 3d is a divisor of \( r \), which implies that \( d \) divides \( r_0 \). It remains to show that \( \gcd(3, \frac{r}{d}) = 1 \). Suppose otherwise that \( \gcd(3, \frac{r}{d}) > 1 \), i.e., \( 3 \mid \frac{r}{d} \), say \( \frac{r}{d} = 3k \) for some integer \( k \geq 1 \). Let \( \alpha \) be a root of \( f(x) \). Since \( f(x) \mid (x^{q_0 + 1} + x + 1) \), we have

\[
\frac{\alpha + 1}{\alpha} = q^{r_0}.
\]

The degree of \( f(x) \) is 3d, which implies that \( f(x) \mid (x^{q_0 + 1} + x) \), yielding \( \alpha^{q_0 + 1} = \alpha \) and

\[
\alpha^{q_0 + 1} = \alpha^{q_0 + 1} = \alpha^{q_0 + 1} = \alpha.
\]

Hence

\[
\frac{\alpha + 1}{\alpha} = \alpha.
\]

This is an equation \( \alpha^2 + \alpha + 1 = 0 \) for \( \alpha \) over \( \mathbb{F}_q \) of degree 2, which contradicts to the assumption \( r \geq 3 \). We thus have proven the assertion. On the other hand, we have shown in Lemma 4.18 that

\[
\begin{cases} 
(x^2 + x + 1) \mid F_{r_0}(x), & 2 \mid r_0, \\
(x^2 + x + 1) \nmid F_{r_0}(x), & 2 \nmid r_0.
\end{cases}
\]

Set \( \varepsilon_{r_0}(x) = \gcd(x^2 + x + 1, F_{r_0}(x)) \) and

\[
\chi_s(t) = \begin{cases} 
1, & \gcd(s, t) = 1, \\
0, & \text{otherwise}.
\end{cases}
\]
Let $R_d(x)$ be the product of all monic irreducible polynomials of degree $3d$ over $\mathbb{F}_q$ which divide $F_{r_0}(x)$, in symbols
\[
R_d(x) = \prod \left\{ h(x) \bigg| h(x) \in \mathcal{I}_{3d} \text{ and } h(x) \text{ divides } F_{r_0}(x) \right\}.
\]
It follows from Lemma 4.18 that
\[
\frac{F_{r_0}(x)}{\varepsilon_{r_0}(x)} = \prod_{d|r_0 \text{ gcd}(3,r_0/d)=1} R_d(x).
\]
Note that $F_{r_0}(x)$ has degree $2^{r_0} + 1$ and the degree of $\varepsilon_{r_0}(x)$ is either 0 if $r_0$ is odd, or 2 if $r_0$ is even. Then, if we set $\varepsilon(r_0) = (-1)^{r_0+1}$, then
\[
2^{r_0} + \varepsilon(r_0) = \sum_{d|r_0 \text{ gcd}(3,r_0/d)=1} 3d|R_d(x)| = \sum_{d|r_0} 3d|R_d(x)| \cdot \chi_3 \left( \frac{r_0}{d} \right).
\]
By Lemma 4.19,
\[
3r_0|R_{r_0}(x)| = \sum_{d|r_0} \chi_3(d) \mu(d) \left( 2^{\frac{r_0}{d}} + \varepsilon \left( \frac{r_0}{d} \right) \right).
\]
We then have
\[
r|\Delta_5| = \sum_{d|\frac{r}{q}} \mu(d) \left( 2^{\frac{r}{d}} + (-1)^{\frac{r}{d}+1} \right),
\]
which implies that
\[
|\Delta_5| = \frac{1}{r} \sum_{d|\frac{r}{q}} \mu(d) \left( 2^{\frac{r}{d}} + (-1)^{\frac{r}{d}+1} \right).
\]
The proof is complete.

C. The Number of Orbits of Gal on $\mathbb{PGL}/\mathcal{I}_r$

Collecting all the results that we have established, we arrive at the following result, which gives the number of orbits of Gal on $\mathbb{PGL}/\mathcal{I}_r$ (or equivalently, the number of orbits of PTL on $\mathcal{I}_r$).

Theorem 4.21: We assume that $n \geq 5$ is an odd prime number, $q = 2^n$ and $r \geq 3$ is a positive integer satisfying $\text{gcd}(r,n) = 1$. The number of orbits of Gal on $\mathbb{PGL}/\mathcal{I}_r$ is given by
\[
\frac{n-1}{6n} (|X| + 3|\Delta_2| + 2|\Delta_5|) + \frac{1}{n q (q^2 - 1)} (N_0 + N_1 + N_2 + N_3),
\]
where the values of $|X|$, $|\Delta_2|$ and $|\Delta_5|$ were explicitly given in Lemmas 4.7, 4.12 and 4.20 respectively, and the values of $N_i$ for $0 \leq i \leq 3$ were explicitly determined in Theorem 3.3.

Proof: Recall, from Theorem 4.11, that $s_0$ denotes the number of orbits of PTL on $\mathcal{I}_r$ with size 1. Let $s$ be the number of orbits of PTL on $\mathcal{I}_r$. Then
\[
s_0 + n (s - s_0) = |\mathbb{PGL}/\mathcal{I}_r|.
\]
Substituting $s_0$ by $\frac{1}{6} (|X| + 3|\Delta_2| + 2|\Delta_5|)$, the value of $|\mathbb{PGL}/\mathcal{I}_r|$ is equal to
\[
\frac{1}{6} (|X| + 3|\Delta_2| + 2|\Delta_5|) + n \left( s - \frac{1}{6} (|X| + 3|\Delta_2| + 2|\Delta_5|) \right),
\]
from which we obtain
\[
s = \frac{n-1}{6n} (|X| + 3|\Delta_2| + 2|\Delta_5|) + \frac{1}{n q (q^2 - 1)} (N_0 + N_1 + N_2 + N_3).
\]
We are done.

D. An Upper Bound for the Number of Extended Goppa Codes

By Lemma 2.3, the number of inequivalent extended irreducible binary Goppa codes of length $q+1$ and degree $r$ is less than or equal to the number of orbits of PTL on $\mathcal{S}$. Lemma 2.6 tells us that the number of orbits of PTL on $\mathcal{S}$ is equal to the number of orbits of PTL on $\mathcal{I}_r$. Lemma 2.7 says that the number of orbits of PTL on $\mathcal{I}_r$ is equal to the number of orbits of Gal on $\mathbb{PGL}/\mathcal{I}_r$. With Theorem 4.21 at hand, we immediately have the following result.

Theorem 4.22: We assume that $n \geq 5$ is an odd prime number, $q = 2^n$ and $r \geq 3$ is a positive integer satisfying $\text{gcd}(r,n) = 1$. The number of inequivalent extended irreducible binary Goppa codes of length $q+1$ and degree $r$ is at most
\[
\frac{n-1}{6n} (|X| + 3|\Delta_2| + 2|\Delta_5|) + \frac{1}{n q (q^2 - 1)} (N_0 + N_1 + N_2 + N_3),
\]
where the values of $|X|$, $|\Delta_2|$ and $|\Delta_5|$ were explicitly given in Lemmas 4.7, 4.12 and 4.20 respectively, and the values of $N_i$ for $0 \leq i \leq 3$ were explicitly determined in Theorem 3.3.

V. Corollaries of Theorem 4.22

In this section, we apply Theorem 4.22 to some special cases, including $r = 4$, $r = 2p$ ($p \geq 3$ is a prime number) and $\text{gcd}(r,q^3 - q) = 1$. Some previously known results in the literature are reobtained directly. Consequently, our main result, Theorem 4.22, naturally contains the main results of [3], [7], and [27].

A. The Case: $r = 4$

We first apply Theorem 4.22 to reobtain the main result of [27], which established an upper bound on the number of extended irreducible binary quartic Goppa codes of length $2^n + 1$ (where $n \geq 3$ is a prime number). By Theorem 3.3 and simple computations, we have $N_2 = N_3 = 0$,
\[
N_0 = \frac{1}{4} \sum_{d|4} \mu(d) q^{\frac{3}{4}} = \frac{1}{4} q^2 (q^2 - 1)
\]
and
\[
N_1 = \frac{q^2 - 1}{4} \sum_{d|2 \text{ gcd}(2,d) = 1} \mu(d) q^{\frac{3}{4}} = \frac{q^2 - 1}{4} \cdot q^2 = \frac{1}{4} q^2 (q^2 - 1).
\]
The number of orbits of PGL on \( \mathcal{I}_r \) is equal to
\[
|\text{PGL}/\mathcal{I}_r| = \frac{1}{q(q^2 - 1)}(N_0 + N_1 + N_2 + N_3)
\]
\[
= \frac{1}{q(q^2 - 1)} \cdot \left( \frac{1}{4} q^2(q^2 - 1) + \frac{1}{4} q^2(q^2 - 1) + 0 + 0 \right)
\]
\[
= \frac{q}{2}
\]
Next, by Lemmas 4.7, 4.12 and 4.20, we have \(|\Delta_5| = 0,\)
\[
|\mathcal{X}| = \frac{1}{4} \sum_{d|4} \mu(d)(2^{\frac{d}{2}} - 1) = 3
\]
and
\[
|\Delta_2| = \frac{1}{r} \sum_{d|2 \atop d \text{ odd}} \mu(d)2^{\frac{d}{2}} = \frac{1}{4} \sum_{d|2} \mu(d)2^{\frac{d}{2}} = 1.
\]
Thus the number \( s_0 \) (\( s_0 \) denotes the number of orbits of PTL on \( \mathcal{I}_r \) with size 1, see Theorem 4.11) is equal to
\[
s_0 = \frac{1}{6} (|\mathcal{X}| + 3|\Delta_2| + 2|\Delta_5|) = 1.
\]
Let \( s \) be the number of orbits of PTL on \( \mathcal{I}_r \). Then
\[
1 + n(s - 1) = |\text{PGL}/\mathcal{I}_r| = \frac{q}{2},
\]
leading to
\[
s = \frac{1}{n} \left( \frac{q}{2} - 1 \right) + 1 = \frac{2^{n-1} - 1}{n} + 1.
\]
As a corollary of Theorem 4.22, we have reobtained the main result of [27].

**Corollary 5.1** [27, Theorem 5.1]: Let \( n > 3 \) be a prime number. The number of extended irreducible binary quartic Goppa codes of length \( 2^n + 1 \) is at most \( \frac{2^{n-1} - 1}{n} + 1 \).

**B. The Case: \( r = 2p, p \geq 3 \) Is a Prime Number**

We now turn to consider the case \( r = 2p \), where \( p \geq 3 \) is a prime number. The particular case \( p = 3 \) was considered in [7]. We need to divide the case into three subcases separately: \( p \mid (q - 1) \), \( p \) \( | \) \( (q + 1) \) and the rest.

- **Subcase 1**: \( p \mid (q - 1) \). In this subcase we must have \( p \not\mid (q + 1) \). Using Theorem 3.3 directly, we have
  \[
  N_0 = \frac{1}{2p} \sum_{d|2p} \mu(d)2^{\frac{d}{2}} = \frac{1}{2p} (q^{2p} - q^p - q^2) + q^2 - q^p + q^2 - q^p + q^2 - q^p + 1,
  \]
  \[
  N_1 = \frac{1}{2p} \sum_{d|p \atop d \text{ odd}} \mu(d)2^{\frac{d}{2}} = \frac{q^2 - 1}{2p} (q^p - q^2),
  \]
  \[
  N_2 = q(q + 1) \cdot \sum_{D \mid \gcd(D, 2p)} \frac{\varphi^2(D)}{2p} \sum_{d|D \atop d \text{ odd}} \mu(d)2^{\frac{d}{2}}(q^{2\frac{D}{d}} - 1)
  \]
  \[
  = q(q + 1) \cdot \sum_{D \mid \gcd(D, 2p)} \frac{\varphi^2(D)}{2p} \sum_{d|D \atop d \text{ odd}} \mu(d)(q^{2\frac{D}{d}} - 1)
  \]
  \[
  = q(q + 1) \cdot \frac{\varphi^2(p)}{2p} \sum_{d|2 \atop \gcd(d, p) = 1} \mu(d)(q^{\frac{d}{2}} - 1)
  \]
  \[
  = q(q + 1) \cdot \frac{(p - 1)^2}{2p} (q^2 - 1 - (q - 1))
  \]
  \[
  = \frac{(p - 1)^2}{2p} \cdot q^2(q^2 - 1),
  \]

and
\[
N_3 = \frac{q(q - 1)}{2} \cdot \sum_{D \mid \gcd(D, 2p, q + 1)} \frac{\varphi^2(D)}{2p} \sum_{d|\frac{D}{2} \atop \gcd(d, D) = 1} \mu(d)(q^{\frac{D}{d}} - 1)^2 = 0.
\]

The number of orbits of PGL on \( \mathcal{I}_r \), denoted by \( |\text{PGL}/\mathcal{I}_r| \), is equal to
\[
\frac{1}{q(q^2 - 1)} (N_0 + N_1 + N_2 + N_3)
\]
\[
= \frac{1}{q(q^2 - 1)} \left( \frac{1}{2p} (q^{2p} - q^p - q^2 + q + (q^2 - 1)(q^p - q)) + \frac{(p - 1)^2}{2p} \cdot q^2(q^2 - 1) \right)
\]
\[
= \frac{1}{2p(q^2 - 1)} (q^{2p-1} + q^{p+1} - 2q^{p-1} - q^2 - q + 2)
\]
\[
+ \frac{q(p - 1)^2}{2p}.
\]

Next, we have \(|\Delta_5| = 0,\)
\[
|\mathcal{X}| = \frac{1}{2p} \sum_{d|2p} \mu(d)(2^{\frac{d}{2}} - 1)
\]
\[
= \frac{1}{2p} (2^{2p} - 2^p - 2^2 - 2) = \frac{1}{2p} (2^{2p} - 2^p - 2),
\]
\[
|\Delta_2| = \frac{1}{r} \sum_{d|2 \atop d \text{ odd}} \mu(d)2^{\frac{d}{2}} = \frac{1}{2p} \sum_{d|p \atop d \text{ odd}} \mu(d)2^{\frac{d}{2}} = \frac{1}{2p} (2^{p} - 2).
\]

Thus the number \( s_0 \) of orbits of PTL on \( \mathcal{I}_r \) with size 1 is
\[
s_0 = \frac{1}{6} (|\mathcal{X}| + 3|\Delta_2| + 2|\Delta_5|) = \frac{1}{12p} (2^{2p} + 2^{p+1} - 8).
\]

Let \( s \) be the number of orbits of PTL on \( \mathcal{I}_r \). Then
\[
s_0 + n(s - s_0) = |\text{PGL}/\mathcal{I}_r|,
\]
yielding
\[
\frac{1}{12p} (2^{2p} + 2^{p+1} - 8) + n(s - s_0)
\]
\[
= \frac{1}{2p(q^2 - 1)} (q^{2p-1} + q^{p+1} - 2q^{p-1} - q^2 - q + 2)
\]
\[
+ \frac{q(p - 1)^2}{2p}.
\]
This implies that

$$2^{2p} + 2^{p+1} - 8 + 12 pn (s - s_0) = \frac{6(q^{2p-1} + q^{p+1} - 2q^{p-1} - q^2 + 2)}{q^2 - 1} + 6p(p - 1)^2.$$ 

After some simple algebraic calculations, we have

$$s = \frac{1}{2pn(q^2 - 1)}(q^{2p-1} + q^{p+1} - 2q^{p-1} - q^2 + 2)$$

$$+ \frac{q(p - 1)^2}{2pm} + \frac{2(n - 1)}{3pn} (2^{2p-3} + 2^{p-2} - 1).$$

Based on the above discussions and Theorem 4.22, we obtain the following result.

**Corollary 5.2:** Let \( n \geq 5 \) be a prime number. Assume that \( r = 2p \), where \( p \geq 3 \) is a prime number satisfying \( p \mid (q - 1) \). Then the number of extended irreducible binary Goppa codes of length \( 2^r + 1 \) is at most

$$\frac{1}{2pn(q^2 - 1)}(q^{2p-1} + q^{p+1} - 2q^{p-1} - q^2 + 2) + \frac{q(p - 1)^2}{2pn}$$

$$+ \frac{2(n - 1)}{3pn} (2^{2p-3} + 2^{p-2} - 1).$$

- **Subcase 2:** \( p \mid (q + 1) \). In this subcase we have \( p \nmid (q - 1) \).

First,

$$N_0 = \frac{1}{2p} \sum_{d \mid 2p} \mu(d) q^{2p} = \frac{1}{2p} (q^{2p} - q^p - q^2 + q),$$

$$N_1 = \frac{q^2 - 1}{2p} \sum_{d \mid 2p \mid (d, D) = 1} \mu(d) q^2 = \frac{q^2 - 1}{2p} (q^p - q),$$

$$N_2 = q(q + 1) \cdot \sum_{D \mid (d, D) = 1} \frac{\varphi^2(D)}{2p} \sum_{a \mid \frac{D}{d}, a \nmid d} \mu(d) (q^\frac{2\varphi(D)}{d} - 1)$$

$$= 0$$

and

$$N_3 = \frac{q(q - 1)}{2} \cdot \sum_{D \mid (d, D) = 1} \frac{\varphi^2(D)}{2p} \sum_{a \mid \frac{D}{d}} \mu(d) (q^\frac{2\varphi(D)}{d} + (-1)^2 \frac{2\varphi(D)}{d} + 1)$$

$$= q(q - 1) \cdot \frac{\varphi^2(p)}{2p} \sum_{a \mid \frac{p}{d}} \mu(d) (q^\frac{2\varphi(p)}{d} + (-1)^2 \frac{2\varphi(p)}{d} + 1)$$

$$= \frac{q(q - 1)}{2} \cdot \frac{\varphi^2(p)}{2p} \sum_{a \mid \frac{p}{d}} \mu(d) (q^\frac{2\varphi(p)}{d} + (-1)^2 \frac{2\varphi(p)}{d} + 1)$$

$$= \frac{q(q - 1)}{2} \cdot \frac{(p - 1)^2}{2p} (q^2 - 1 - (q + 1))$$

$$= \frac{(p - 1)^2}{4p} \cdot q(q - 1)(q^2 - q - 2).$$

Thus the number of orbits of \( \text{PGL} \) on \( I_r \) is equal to

$$\left| \text{PGL \setminus I_r} \right| = \frac{1}{q(q^2 - 1)} (N_0 + N_1 + N_2 + N_3),$$

which is also equal to

$$\frac{1}{q(q^2 - 1)} \left( \frac{1}{2p} (q^{2p} - q^p - q^2 + q + (q - 1)(q^p - q)) \right)$$

$$+ \frac{(p - 1)^2}{4p} \cdot q(q - 2)(q^2 - 1).$$

Next, we have \( \Delta_5 = 0 \).

$$|\lambda| = \frac{1}{2p} \sum_{d \mid 2p} \mu(d) 2^{2\varphi(d)} - 1$$

$$= \frac{1}{2p} (2^{2p} - 2^p - 2^2 + 2)$$

$$= \frac{1}{2p} (2^{2p} - 2^p - 2^2)$$

and

$$|\Delta_2| = \frac{1}{r} \sum_{d \mid (d, D) = 1} \mu(d) 2^{2\varphi(d)} = \frac{1}{2p} \sum_{d \mid (d, D) = 1} \mu(d) 2^{\varphi(d)} = \frac{1}{2p} (2^{2p} - 2^p).$$

Thus the number \( s_0 \) of orbits of \( \text{PTL} \) on \( I_r \) with size 1 is

$$s_0 = \frac{1}{6} (|\lambda| + 3|\Delta_2| + 2|\Delta_3|) = \frac{1}{12p} (2^{2p} + 2^{p+1} - 8).$$

Let \( s \) be the number of orbits of \( \text{PTL} \) on \( I_r \). Then

$$s_0 + (s - s_0) = \left| \text{PGL \setminus I_r} \right|,$$

which leads to

$$\frac{1}{12p} (2^{2p} + 2^{p+1} - 8) + n(s - s_0) = \frac{1}{2p(q^2 - 1)} (q^{2p-1}$$

$$+ q^{p+1} - 2q - q^2 - q + 2) + \frac{(q - 2)(p - 1)^2}{4p}.$$ 

After calculations, we have

$$s = \frac{1}{2pn(q^2 - 1)} (q^{2p-1} + q^{p+1} - 2q^{p-1} - q^2 - q + 2) +$$

$$\frac{(q - 2)(p - 1)^2}{4p} + \frac{2(n - 1)}{3pn} (q^{2p-3} + 2^{p-2} - 1).$$

We have arrived at the following result.

**Corollary 5.3:** Let \( n \geq 5 \) be a prime number. Assume that \( r = 2p \), where \( p \geq 3 \) is a prime number satisfying \( p \mid (q + 1) \).
Then the number of extended irreducible binary Goppa codes of length \(2^n + 1\) is at most
\[
\frac{1}{2pn(q^2 - 1)} \left( q^{2p-1} + q^{p+1} - 2q^{p-1} - q^2 - q + 2 \right) + \frac{(q - 2)(p - 1)^2}{3pn} + \frac{2(n - 1)}{3pn}(2p^2 - 3 + 2p - 2 - 1).
\]

Taking \( p = 3 \) in the above corollary, we immediately reobtain the main result of [7], as given below.

**Corollary 5.4** [7, Theorem 4.8]: Let \( n \geq 5 \) be a prime number. The number of extended irreducible binary sextic Goppa codes of length \(2^n + 1\) is at most
\[
\frac{2^{3n} + 2^{2n} + 3 \cdot 2^n + 12n - 18}{6n}.
\]

**Proof:** Taking \( p = 3 \) in Corollary 5.3, one has \( r = 2p = 6 \). It follows from \( 3 \mid (2^n + 1) \) that \( p \mid (q + 1) \). Using Corollary 5.3, we finally have
\[
s = \frac{2^{3n} + 2^{2n} + 3 \cdot 2^n + 12n - 18}{6n}.
\]

We are done.

Subcase 3: \( p \mid (q + 1) \) and \( p \nmid (q - 1) \). In this subcase, \( \mathcal{N}_2 = \mathcal{N}_3 = 0 \),
\[
\mathcal{N}_0 = \frac{1}{2p} \sum_{d \mid 2p} \mu(d)q^{2d} = \frac{1}{2p}(q^{2p} - q^p - q^2 + q),
\]
\[
\mathcal{N}_1 = \frac{q^2 - 1}{2p} \sum_{\gcd(d,2) = 1} \mu(d)q^d = \frac{q^2 - 1}{2p}(q^p - q).
\]

Thus the number of orbits of PGL on \( \mathcal{I}_r \) is equal to
\[
|\text{PGL}\backslash \mathcal{I}_r| = \frac{1}{q(q^2 - 1)}(\mathcal{N}_0 + \mathcal{N}_1 + \mathcal{N}_2 + \mathcal{N}_3),
\]
which turns out to be
\[
\frac{1}{q(q^2 - 1)} \cdot \frac{1}{2p}(q^{2p} - q^p - q^2 + q + (q^2 - 1)(q^p - q)) = \frac{1}{2pq(q^2 - 1)} \cdot (q^{2p} + q^{p+2} - 2q^{p-2} - q^3 - q^2 + 2q) = \frac{1}{2p(q^2 - 1)} \cdot (q^{2p-1} + q^{p+1} - 2q^{p-1} - q^2 - q + 2).
\]

Next, we have \( |\Delta_5| = 0 \),
\[
|\mathcal{X}| = \frac{1}{2p} \sum_{d \mid 2p} \mu(d)(2d^2 - 1) = \frac{1}{2p}(2^{2p} - 2p^2 + 2) = \frac{1}{2p}(2^{2p} - 2p^2 - 2),
\]
and
\[
|\Delta_2| = \frac{1}{r} \sum_{\alpha \mid d} \mu(d)2^{\alpha} = \frac{1}{2p} \sum_{\alpha \mid d} \mu(d)2^{\alpha} = \frac{1}{2p}(2^{p} - 2).
\]

Thus the number \( s_0 \) of orbits of PTL on \( \mathcal{I}_r \) with size \( 1 \) is
\[
s_0 = \frac{1}{6}(|\mathcal{X}| + 3|\Delta_2| + 2|\Delta_5|) = \frac{1}{12p}(2^{2p} + 2p^2 + 2p - 2).
\]

Let \( s \) be the number of orbits of PTL on \( \mathcal{I}_r \). Then
\[
s_0 + n(s - s_0) = |\text{PGL}\backslash \mathcal{I}_r|,
\]
and thus,
\[
\frac{1}{12p}(2^{2p} + 2p^2 + 2p - 2) + n(s - s_0) = \frac{1}{2p(q^2 - 1)}(q^{2p-1} + q^{p+1} - 2q^{p-1} - q^2 - q + 2).
\]

We finally have
\[
s = \frac{1}{2pn(q^2 - 1)}(q^{2p-1} + q^{p+1} - 2q^{p-1} - q^2 - q + 2) + \frac{2(n - 1)}{3pn}(2p^2 - 3 + 2p - 2 - 1).
\]

We have obtained the following result.

**Theorem 5.5**: Let \( n \geq 5 \) be a prime number. Assume that \( r = 2p \), where \( p \geq 3 \) is a prime number satisfying \( p \nmid (q + 1) \) and \( p \nmid (q - 1) \). Then the number of extended irreducible binary Goppa codes of length \(2^n + 1\) is at most
\[
\frac{1}{2pn(q^2 - 1)}(q^{2p-1} + q^{p+1} - 2q^{p-1} - q^2 - q + 2) + \frac{2(n - 1)}{3pn}(2p^2 - 3 + 2p - 2 - 1).
\]

C. The Case: \( \gcd(r, 2(q^2 - 1)) = 1 \)

In this case we have \( 2 \nmid r, 3 \nmid r, \gcd(r, q - 1) = 1 \) and \( \gcd(r, q + 1) = 1 \). After simple calculations, we have
\[
\mathcal{N}_0 = \frac{1}{r} \sum_{d \mid r} \mu(d)q^{d/2}, \quad \mathcal{N}_1 = \mathcal{N}_2 = \mathcal{N}_3 = 0.
\]

Additionally, we have \( |\Delta_2| = |\Delta_5| = 0 \) and
\[
|\mathcal{X}| = \frac{1}{r} \sum_{d \mid r} (2^{d/2} - 1)\mu(d).
\]

We can give an upper bound for the number of inequivalent extended irreducible binary Goppa codes of length \(2^n + 1\) and degree \( r \) with \( \gcd(r, 2(q^2 - 1)) = 1 \), which is the main result of [3].

**Corollary 5.6** [3, Theorem 3.11]: We assume that \( n \geq 5 \) is an odd prime number, \( q = 2^n \), and \( r \geq 3 \) is a positive integer satisfying \( \gcd(r, n) = 1 \) and \( \gcd(r, q^2 - q) = 1 \). The number of inequivalent extended irreducible binary Goppa codes of length \( q + 1 \) and degree \( r \) is at most
\[
n - 1 \cdot \frac{1}{6rn} \cdot \sum_{d \mid r} (2^{d/2} - 1)\mu(d) + \frac{1}{rnq(q^2 - 1)} \cdot \sum_{d \mid r} \mu(d)q^{d/2},
\]
where \( \mu \) is the Möbius function.

**Appendix**

**Proof of Lemma 3.1**: First, there are four families of conjugacy classes of the general linear group GL whose representatives are given as follows, see [8, pages 324-326].

(i) The matrices
\[
sE_2 = \begin{pmatrix} s & 0 \\ 0 & s \end{pmatrix} (s \in \mathbb{F}_q^*)
\]
belong to the centre of GL. They give \( q - 1 \) conjugacy classes of GL with size 1.

(ii) Consider the matrices
\[
U_s = \begin{pmatrix} s & 1 \\ 0 & s \end{pmatrix} (s \in \mathbb{F}_q^*).
\]
The matrices \( U_s (s \in \mathbb{F}_q^*) \) give \( q - 1 \) conjugacy classes of GL. Each conjugacy class contains \( q^2 - 1 \) elements.

(iii) Let
\[
D_{s,t} = \begin{pmatrix} s & 0 \\ 0 & t \end{pmatrix} (s, t \in \mathbb{F}_q^*, s \neq t).
\]
The matrices \( D_{s,t} (s, t \in \mathbb{F}_q^*, s \neq t) \) give \( \frac{(q-1)(q-2)}{2} \) conjugacy classes of GL (note that \( D_{s,t} \) and \( D_{t,s} \) belong to the same conjugacy class). Each conjugacy class contains \( q(q+1) \) elements.

(iv) Consider
\[
V_\gamma = \begin{pmatrix} 0 & 1 \\ \gamma^{1+q} & \gamma + \gamma^q \end{pmatrix} (\gamma \in \bigcup_{i=1}^{2} \xi((q-1)i) \mathbb{F}_q^*).
\]
The matrices \( V_\gamma (\gamma \in \bigcup_{i=1}^{2} \xi((q-1)i) \mathbb{F}_q^*) \) give \( \frac{q(q-1)}{2} \) conjugacy classes of GL. Each conjugacy class contains \( q(q-1) \) elements.

By this result, we can determine the conjugacy classes of PGL. The representatives of the conjugacy classes of PGL are divided into four cases, as we listed below.

1. \( E_2 \)
2. Note that for each \( s \in \mathbb{F}_q^* \),
\[
s \begin{pmatrix} 1 & 0 \\ 0 & s \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} s & 1 \\ 0 & s \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & s \end{pmatrix}.
\]

For any \( s \in \mathbb{F}_q^* \) it follows that
\[
\begin{pmatrix} s & 1 \\ 0 & s \end{pmatrix} \sim \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}
\]
in PGL.

Thus the elements
\[
U_s = \begin{pmatrix} s & 1 \\ 0 & s \end{pmatrix} (s \in \mathbb{F}_q^*)
\]
provide a conjugacy class with representative
\[
\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}
\]
of the group PGL. Clearly, \( \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \) and \( E_2 \) do not belong to the same conjugacy class.

3. Note that the elements
\[
D_{s,t} = \begin{pmatrix} s & 0 \\ 0 & t \end{pmatrix} (s, t \in \mathbb{F}_q^*, s \neq t)
\]
give \( q - 2 \) elements of PGL as follows:
\[
\begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix} (1 \neq \lambda \in \mathbb{F}_q^*).
\]

Additionally, for \( 1 \neq \lambda \in \mathbb{F}_q^* \),
\[
\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & a-1 \end{pmatrix} \begin{pmatrix} a-1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} = a^{-1} \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}.
\]

This shows that
\[
\begin{pmatrix} 1 & 0 \\ 0 & a^{-1} \end{pmatrix} \sim \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}
\]
in PGL.

Clearly,
\[
\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix},
\]
which implies that
\[
\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}
\]
in PGL.

Hence,
\[
\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & a^{-1} \end{pmatrix}
\]
in PGL.

Let \( S \) be a subset of \( \mathbb{F}_q^* \) such that \( \{1\} \cup S \cup S^{-1} = \mathbb{F}_q^* \), where \( S^{-1} = \{s^{-1} | s \in S\} \). In the following we prove that for any \( a, b \in S \) and \( a \neq b \), \( \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \) and \( \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} \) do not belong to the same conjugacy class. Suppose that \( \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \) and \( \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} \) belong to the same conjugacy class, then there exists \( \lambda \in \mathbb{F}_q^* \), \( P \in \text{GL} \) such that
\[
\lambda \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} = P \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} P^{-1}.
\]

Since the conjugate matrices have the same eigenvalues, we have that
\[
\{\lambda, \lambda a\} = \{1, b\}.
\]
If \( \lambda = 1 \), then \( a = b \); if \( \lambda \neq 1 \), then \( \lambda = b, \lambda a = 1 \) and so \( b = a^{-1} \). In either case we can get a contradiction. Hence for any \( a, b \in S \) and \( a \neq b \), \( \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \) and \( \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} \) do not belong to the same conjugacy class. Thus these \( q - 2 \) elements
\[
\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} (1 \neq a \in \mathbb{F}_q^*)
\]
of PGL provide \( \frac{q-2}{2} \) conjugacy classes with representatives
\[
\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} (a \in S),
\]
where $S \subseteq \mathbb{F}_q^*$ satisfying $\{1\} \cup S \cup S^{-1} = \mathbb{F}_q^*$ and $S^{-1} = \{s^{-1} | s \in S\}$.

In the following it remains to show that $\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} (a \in S)$ cannot conjugate to $E_2$ and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, respectively. Since $a \neq 1$, $\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} (a \in S)$ cannot conjugate to $E_2$. Suppose that $\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} (a \in S)$ conjugates to $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Then there exists $\lambda \in \mathbb{F}_q^*$, $P \in \text{GL}$ such that

$$\lambda \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} = P \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} P^{-1}.$$ 

So $\lambda = \lambda a = 1$, which gets $a = 1$. This is a contradiction. Hence $\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} (a \in S)$ do not conjugate to $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

(4) First we are going to prove that for any $\lambda \in \mathbb{F}_q^*$, $V_\gamma$ and $V_{\lambda \gamma}$ are conjugate in PGL, namely

$$V_\gamma = \begin{pmatrix} 0 & 1 \\ \gamma & \gamma \end{pmatrix} \sim V_{\lambda \gamma} = \begin{pmatrix} 0 & 1 \\ \lambda^2 \gamma & \lambda + \gamma \end{pmatrix}.$$ 

Note that

$$V_\gamma = \begin{pmatrix} 0 & 1 \\ \lambda \gamma & \lambda + \gamma \end{pmatrix} \sim \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \lambda \gamma \gamma \text{ in } \text{GL}_2(\mathbb{F}_q^2),$$

$$V_{\lambda \gamma} = \begin{pmatrix} 1 & 0 \\ \lambda & \lambda + \gamma \end{pmatrix} \sim \begin{pmatrix} 0 & 1 \\ \lambda & \lambda + \gamma \end{pmatrix} \lambda \gamma \gamma \text{ in } \text{GL}_2(\mathbb{F}_q^2).$$

Then, in $\text{GL}_2(\mathbb{F}_q^2)$ we have

$$V_\gamma = \begin{pmatrix} 0 & 1 \\ \gamma & \gamma + 1 \end{pmatrix} \sim V_{\lambda \gamma} = \begin{pmatrix} 0 & 1 \\ \lambda^2 \gamma & \lambda + \gamma \end{pmatrix}.$$ 

Hence, for any $\lambda \in \mathbb{F}_q^*$,

$$V_\gamma = \begin{pmatrix} 0 & 1 \\ \gamma & \gamma + 1 \end{pmatrix} \sim V_{\lambda \gamma} = \begin{pmatrix} 0 & 1 \\ \lambda^2 \gamma & \lambda + \gamma \end{pmatrix}.$$ 

Let $\gamma_1 = \xi(q-1)i_1$, $\gamma_2 = \xi(q-1)i_2$, where $1 \leq i_1, i_2 < \frac{q}{2}$ and $i_1 \neq i_2$. Secondly, we prove that $V_{\gamma_1}$ does not conjugate to $V_{\gamma_2}$. Suppose otherwise that $V_{\gamma_1}$ conjugates to $V_{\gamma_2}$. Then there exists $\lambda_0 \in \mathbb{F}_q^*$, $P \in \text{GL}$ such that

$$\lambda_0 V_{\gamma_1} = PV_{\gamma_2} P^{-1},$$

i.e.,

$$\lambda_0 \begin{pmatrix} 0 & 1 \\ \gamma_1 & \gamma_1 + 1 \end{pmatrix} = P \begin{pmatrix} 0 & 1 \\ \gamma_2 & \gamma_2 + 1 \end{pmatrix} P^{-1},$$

which implies that

$$\{\lambda_0 \gamma_1, \lambda_0 \gamma_2 \} = \{\gamma_2, \gamma_2^3\}.$$ 

Note that if $\lambda_0 \gamma_1 = \gamma_2$, then

$$\lambda_0 = \frac{\gamma_2}{\gamma_1} \Rightarrow \lambda_0 = \xi(q-1)(i_2 - i_1)$$

$$\Rightarrow \xi(q-1)^2(i_2 - i_1) = 1$$

$$\Rightarrow (q - 1)^2(i_2 - i_1) \equiv 0 \text{ (mod}(q^2 - 1))$$

$$\Rightarrow (q - 1)(i_2 - i_1) \equiv 0 \text{ (mod}(q + 1))$$

$$\Rightarrow i_2 - i_1 \equiv 0 \text{ (mod}(q + 1)).$$

Since $1 \leq i_1, i_2 < \frac{q}{2}$ and $i_1 \neq i_2$, this is a contradiction. In addition, if $\lambda_0 \gamma_1 = \gamma_2^2$, then $\lambda_0 \xi(q-1)i_1 = \xi(q-1)i_2$, which implies $i_2 + i_1 \equiv 0 \text{ (mod}(q + 1))$. The same reason shows that this is also a contradiction.

Therefore the matrices

$$V_{\gamma_i} = \begin{pmatrix} 0 & 1 \\ \gamma_i & \gamma_i + 1 \end{pmatrix}$$

give $\frac{q}{2}$ conjugacy classes, where $\gamma_i = \xi(q-1)i_i$, $i = 1, 2, \ldots, \frac{q}{2}$.

Using the same arguments as above, it follows that

$$V_{\gamma_i} = \begin{pmatrix} 0 & 1 \\ \gamma_i & \gamma_i + 1 \end{pmatrix}$$

do not conjugate to $E_2$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $(a \in S)$, respectively.

Lastly, the conjugacy classes we have found account for

$$1 + (q^2 - 1) + q^2 \cdot q(q + 1) + q \cdot q(q - 1)$$

elements altogether. This sum is equal to the order of the group PGL, so we have found all the conjugacy classes. We are done.

**Acknowledgment**

The authors sincerely thank an Associate Editor (Prof. Moshe Schwartz) and the anonymous referees for their carefully reading and helpful suggestions that led to improvements of the article.

**References**

[1] 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.

[2] T. P. Berger, “On the cyclicity of Goppa codes, parity-check subcodes of Goppa codes, and extended Goppa codes,” Finite Fields Their Appl., vol. 6, no. 3, pp. 255–281, Jul. 2000.

[3] B. Chen and G. Zhang, “Enumeration of extended irreducible binary Goppa codes,” IEEE Trans. Inf. Theory, vol. 68, no. 8, pp. 5145–5153, Aug. 2022.

[4] C. L. Chen, “Equivalent irreducible Goppa codes (Corresp.),” IEEE Trans. Inform. Theory, vol. IT-24, no. 6, pp. 766–769, Nov. 1978.

[5] T. Garefalakis, “On the action of $\text{GL}_2(\mathbb{F}_q)$ on irreducible polynomials over $\mathbb{F}_q$,” J. Pure Appl. Algebra, vol. 215, pp. 1835–1843, Aug. 2011.

[6] Groupprops-Subwiki. Accessed: Dec. 2011. [Online]. Available: https://groupprops.subwiki.org/wiki/index.php?title=Projective_general_linear_group_of_degree_two#mobiousactions#toggle_view_desktop

[7] D. Huang and Q. Yue, “Extended irreducible binary sextic Goppa codes,” IEEE Trans. Inf. Theory, vol. 68, no. 1, pp. 230–237, Jan. 2022.

[8] G. James and M. Liebeck, Representations and Characters of Groups. Cambridge, U.K.: Cambridge Univ. Press, 2001.

[9] A. Kerber, Applied Finite Group Actions. Berlin, Germany: Springer-Verlag, 1999.

[10] J. Knopfmacher, Abstract Analytic Number Theory, North-Holland Mathematical Library, vol. 12. Amsterdam, The Netherlands: Elsevier, 1975.

[11] R. Lidl and H. Niederreiter, Finite Fields. Cambridge, U.K.: Cambridge Univ. Press, 2003.

[12] S. Ling and C. Xing, Coding Theory: A First Course. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[13] P. Loidreau and N. Sendrier, “Weak keys in the McEliece public-key cryptosystem,” IEEE Trans. Inf. Theory, vol. 47, no. 3, pp. 1207–1211, Mar. 2001.

[14] F. J. Macwilliams and N. J. A. Sloane, The Theory of Error Correcting Codes. Amsterdam, The Netherlands: North Holland, 1986.

[15] K. Magamba and J. A. Ryan, “Counting extended irreducible Goppa codes,” Appl. Algebra Eng. Commun. Comput., vol. 30, pp. 313–331, Aug. 2019.
CHEN AND ZHANG: NUMBER OF EXTENDED IRREDUCIBLE BINARY GOPPA CODES

[16] F. E. B. Martínez, D. Oliveiram, and L. Reis, “Möbius–Frobenius maps on irreducible polynomials,” Bull. Aust. Math. Soc., vol. 104, pp. 66–77, Aug. 2021.

[17] R. McEliece, “A public-key cryptosystem based on algebraic coding theory,” DSN Progress Report, pp. 114–116, Jan./Feb. 1978.

[18] H. Meyn, “On the construction of irreducible self-reciprocal polynomials over finite fields,” Applicable Algebra Eng., Commun. Comput., vol. 1, no. 1, pp. 43–53, Mar. 1990.

[19] O. Moreno, “Symmetries of binary Goppa codes (Corresp.),” IEEE Trans. Inf. Theory, vol. IT-25, no. 5, pp. 609–612, Sep. 1979.

[20] A. L. Musukwa, “Counting extended irreducible binary Goppa codes of degree $2p$ and length $2^n+1$,” J. Math. Comput. Sci., vol. 8, pp. 1–17, Dec. 2018.

[21] A. L. Musukwa, K. Magamba, and 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, pp. 235–256, Sep. 2017.

[22] L. Reis, “Invariant theory of a special group action on irreducible polynomials over finite fields,” 2017, arXiv:1708.06862.

[23] L. Reis, “On the existence and number of invariant polynomials,” Finite Fields Appl., vol. 61, Jan. 2020, Art. no. 101605.

[24] L. Reis, “The action of $\text{GL}_2(F_q)$ on irreducible polynomials over $\mathbb{F}_q$,” revisited, J. Pure Appl. Algebra, vol. 222, pp. 1087–1094, Aug. 2018.

[25] J. J. Rotman, Advanced Modern Algebra. Upper Saddle River, NJ, USA: Prentice-Hall, 2003.

[26] J. A. Ryan, “Counting extended irreducible Goppa codes,” J. Discrete Math., vol. 2014, Feb. 2014, Art. no. 871871.

[27] J. A. Ryan, “Counting extended irreducible binary quartic Goppa codes of length $2^n+1$,” IEEE Trans. Inform. Theory, vol. 61, no. 3, pp. 1174–1178, Mar. 2015.

[28] J. A. Ryan and P. Fitzpatrick, “Enumeration of inequivalent irreducible Goppa codes,” Discrete Appl. Math., vol. 154, no. 2, pp. 399–412, Feb. 2006.

[29] H. Stichtenoth and A. Topuzoğlu, “Factorization of a class of polynomials over finite fields,” Finite Fields Appl., vol. 18, pp. 108–122, Jan. 2012.

Bocong Chen received the Ph.D. degree in mathematics from Central China Normal University in 2013. From 2013 to 2015, he was a Research Fellow with the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore. He is currently a Full Professor with the School of Mathematics, South China University of Technology, Guangzhou, Guangdong, China. His research interests include classical error-correcting codes and quantum error-correcting codes.

Guanghui Zhang received the B.Sc. degree in mathematics from Henan University in 1996, the M.Sc. degree in pure mathematics from Wuhan University in 2002, and the Ph.D. degree in pure mathematics from Central China Normal University in 2010. From July 2002 to August 2022, he was with Luoyang Normal University, where he was a Lecturer, an Associate Professor, and a Professor. Since September 2022, he has been with the Department of Mathematics, Suqian University, Suqian, Jiangsu, China, as a Professor. His current research area is algebraic coding theory.