

Enumeration of irreducible and extended irreducible Goppa codes

Kondwani Magamba^{1,2} and John A. Ryan³

¹Malawi University of Science and Technology, Malawi

²Mzuzu University, Malawi

³Chombe Boole Research Center, Malawi

Abstract

We obtain upper bounds on the number of irreducible and extended irreducible Goppa codes over \mathbb{F}_p of length q and $q + 1$, respectively defined by polynomials of degree r , where $q = p^t$ and $r \geq 3$ is a positive integer.

1 Introduction

It is well known that Goppa codes have few invariants and that the number of inequivalent Goppa codes grows exponentially with the length and dimension of the code [13]. These facts led to the exploitation of Goppa codes in the McEliece cryptosystem. There has been research work on the enumeration of extended Goppa codes but most of it has been confined to particular cases. The reference [11] gives an upper bound on the number of inequivalent extended irreducible binary quartic Goppa codes. Recently, an upper bound on the number of inequivalent extended irreducible Goppa codes of degree r and length $q^n + 1$, where $q = p^t$ with the restriction that n and r be primes was found in [7]. Also, in 1978, Chen [3] gave upper bounds on the number of inequivalent irreducible and extended irreducible Goppa codes of length $q^n + 1$ which are not tight. In this paper we derive upper bounds on the number of irreducible and extended irreducible Goppa codes which are tighter than the bounds found in [3]. Our approach takes advantage of recent work by various researchers on the action of $PGL(2, q)$ and $GL(2, q)$ on the set of irreducible polynomials in $\mathbb{F}_q[x]$, see [10] and [4]. This work sheds more light on the structure of Goppa codes and the strength of the McEliece cryptosystem.

2 Preliminaries

2.1 Irreducible and extended irreducible Goppa Codes

We begin by defining an irreducible Goppa code.

Definition 2.1. *Let n be a positive integer, q be a power of a prime number p and $g(z) \in \mathbb{F}_{q^n}[z]$ be irreducible of degree r . Let $L = \mathbb{F}_{q^n} = \{\zeta_i : 0 \leq i \leq q^n - 1\}$. Then an irreducible Goppa code $\Gamma(L, g)$ is defined as the set of all vectors $\underline{c} = (c_0, c_1, \dots, c_{q^n-1})$ with components in \mathbb{F}_q which satisfy the condition*

$$\sum_{i=0}^{q^n-1} \frac{c_i}{z - \zeta_i} \equiv 0 \pmod{g(z)}. \quad (1)$$

The polynomial $g(z)$ is called the Goppa polynomial. Since $g(z)$ is irreducible and of degree r over \mathbb{F}_{q^n} , $g(z)$ does not have any root in L and the code is called an irreducible Goppa code of degree r . In this paper $g(z)$ is always irreducible of degree r over \mathbb{F}_{q^n} .

It can be shown, see [3], that if α is any root of the Goppa polynomial $g(z)$ then $\Gamma(L, g)$ is completely described α and a parity check matrix $\mathbf{H}(\alpha)$ is given by

$$\mathbf{H}(\alpha) = \left(\frac{1}{\alpha - \zeta_0} \frac{1}{\alpha - \zeta_1} \cdots \frac{1}{\alpha - \zeta_{q^n-1}} \right), \quad (2)$$

where $L = \mathbb{F}_{q^n} = \{\zeta_i : 0 \leq i \leq q^n - 1\}$.

Next we give the definition of an irreducible Goppa code extended with an overall parity check.

Definition 2.2. Let $\Gamma(L, g)$ be an irreducible Goppa code of length q^n . Then the extended code $\overline{\Gamma(L, g)}$ is defined by $\overline{\Gamma(L, g)} = \{(c_0, c_1, \dots, c_{q^n}) : (c_0, c_1, \dots, c_{q^n-1}) \in \Gamma(L, g) \text{ and } \sum_{i=0}^{q^n} c_i = 0\}$.

In this paper we take $n = 1$. That is, we consider irreducible and extended irreducible Goppa codes of length q and $q + 1$, respectively.

2.2 Matrices of a given order in $GL(2, q)$

Let $A \in GL(2, q)$ be of order D . We obtain a characterization of the elements of $GL(2, q)$ based on minimal polynomials, conjugacy classes and the order of each matrix. We focus our attention on elements of $GL(2, q)$ which fit our purpose. Elements of $GL(2, q)$ of a given order turn out to be useful in the enumeration of irreducible and extended irreducible Goppa codes.

It is well known that if the order of a matrix $A \in GL(2, q)$ is D then $D \mid p(q - 1)$ or $D \mid (q^2 - 1)$ and that the minimal polynomial $m_A(x)$ of A divides $x^D - 1$. Combining these facts, Proposition 4.2.2 in [1] and Lemma 2.1 in [7] we obtain the following theorem.

Theorem 2.1. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, q)$ be of order D and $\mathbb{F}_q = \mathbb{F}_{p^t}$. Denote the minimal polynomial of A by $m_A(x)$. Then

1. If $D = 1$, then $m_A(x) = x - 1$. Thus $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
2. If $p \mid D$ then $m_A(x) = (x - 1)^2$ and A is conjugate with a matrix of the form $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ where $b \in \mathbb{F}_q^*$.
3. If $(p, D) = 1$, $D \mid (q - 1)$ and $m_A(x) = (x - 1)(x - a)$ for some $a \in \mathbb{F}_q - \{0, 1\}$ where A is not a multiple of the identity matrix, then A is conjugate with a matrix of the form $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ where $a \in \mathbb{F}_q - \{0, 1\}$.
4. If $(p, D) = 1$ and $D \mid (q + 1)$ where $D > 2$ and $m_A(x) = x^2 - \xi x - \zeta \in \mathbb{F}_q$ where $m_A(x)$ is irreducible over \mathbb{F}_q , then A is conjugate with a matrix of the form $\begin{pmatrix} 0 & 1 \\ \zeta & \xi \end{pmatrix}$.

2.3 Equivalence Classes

2.3.1 The set \mathbb{S}

An irreducible Goppa code can be defined by any root of its Goppa polynomial. As such the set of all roots of such polynomials is important and we make the following definition.

Definition 2.3. *The set \mathbb{S} is the set of all elements in \mathbb{F}_{q^r} of degree r over \mathbb{F}_q .*

2.3.2 Maps on \mathbb{S}

We define the following maps on \mathbb{S} .

Definition 2.4. *Let $\alpha \in \mathbb{S}$. Mappings of α of Types 1, 2 and 3 are defined as follows:*

Type 1 $\sigma^i : \alpha \mapsto \alpha^{q^i}$ where σ denotes the Frobenius automorphism of \mathbb{F}_{q^r} leaving \mathbb{F}_q fixed and $0 \leq i \leq r$;

Type 2 $\pi_A : \alpha \mapsto a\alpha + b$ where $A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in GL(2, q)$.

Type 3 $\pi_B : \alpha \mapsto \frac{a\alpha+b}{c\alpha+d}$, where $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, q)$.

It has been shown in [2] that the composition of Type 1 and Type 2 sends irreducible Goppa codes into equivalent irreducible Goppa codes and the composition of Type 1 and Type 3 maps sends extended irreducible Goppa codes into equivalent extended irreducible Goppa codes. Note that the “action” of Type 1 and Type 2 on \mathbb{S} was used in [3], Theorem 1, to find bounds on the number of equivalence classes of irreducible Goppa codes.

2.3.3 Groups arising from Type 1, Type 2 and Type 3 maps

In this section we define groups which arise from Type 1, Type 2 and Type 3 maps. The action of these groups on \mathbb{S} will help in counting irreducible and extended irreducible Goppa codes.

Definition 2.5. *Let G denote the set of all maps $\{\sigma^i : 1 \leq i \leq r\}$. G forms a group under the composition of mappings. It is the group of Frobenius automorphisms. It is shown in [12] that G acts on \mathbb{S} .*

Definition 2.6. *Let F denote the set of all maps $\left\{ \pi_A : A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in GL(2, q) \right\}$. F forms a group under the composition of mappings and is isomorphic to the group of affine linear transformations.*

Observe that there is an action of the projective linear group $PGL(2, q)$ on \mathbb{S} via the map $\pi_B(\alpha) = [B](\alpha) = \frac{a\alpha+b}{c\alpha+d}$ where $\alpha \in \mathbb{S}$ and $[B] \in PGL(2, q)$, see [7].

2.3.4 Actions of F , $PGL(2, q)$ and G

We first consider the action of the affine group F on \mathbb{S} . For each $\alpha \in \mathbb{S}$, the action of F on \mathbb{S} induces orbits denoted $A(\alpha)$ where $A(\alpha) = \{a\alpha + b : a \neq 0, b \in \mathbb{F}_q\}$, and called the affine set containing α . We denote the set of all affine sets, $\{A(\alpha) : \alpha \in \mathbb{S}\}$, by \mathbb{A} . Since $|A(\alpha)| = q(q-1)$ then $|\mathbb{A}| = |\mathbb{S}|/q(q-1)$. It can be shown that G acts on the set \mathbb{A} , see [14]. We will then consider the action of G on \mathbb{A} to obtain orbits in \mathbb{S} of FG . The number of orbits in \mathbb{S} under FG will give us an upper bound on the number of irreducible Goppa codes.

Next we consider the action of $PGL(2, q)$ on \mathbb{S} . The action of $PGL(2, q)$ on \mathbb{S} induces orbits denoted by $O(\alpha)$ where $O(\alpha) = \{\frac{a\alpha+b}{c\alpha+d} : a, b, c, d \in \mathbb{F}_q, ad-bc \neq 0\}$. We will refer to $O(\alpha)$ as a projective linear set. By Theorem 2.3 in [7], $|O(\alpha)| = q^3 - q$.

We denote the set of all projective linear sets in \mathbb{S} under the action of $PGL(2, q)$ by \mathbb{O} . That is, $\mathbb{O} = \{O(\alpha) : \alpha \in \mathbb{S}\}$. Observe that \mathbb{O} partitions the set \mathbb{S} and that G acts on the set \mathbb{O} [12].

It is shown in [12] that each projective linear set $O(\alpha)$ in \mathbb{O} can be partitioned into $q+1$ affine sets. See the theorem below.

Theorem 2.2. *For $\alpha \in \mathbb{S}$, $O(\alpha) = A(\alpha) \cup A(\frac{1}{\alpha}) \cup A(\frac{1}{\alpha+1}) \cup A(\frac{1}{\alpha+\xi_1}) \cup A(\frac{1}{\alpha+\xi_2}) \cup \dots \cup A(\frac{1}{\alpha+\xi_{q-2}})$ where $\mathbb{F}_q = \{0, 1, \xi_1, \xi_2, \dots, \xi_{q-2}\}$.*

Observe that the sets \mathbb{O} and \mathbb{A} are different. \mathbb{O} and \mathbb{A} are both partitions of \mathbb{S} but $|\mathbb{A}| = (q+1) \times |\mathbb{O}|$.

We will use the actions of $PGL(2, q)$ and G on \mathbb{S} to find an upper bound on the number of extended irreducible Goppa codes. Firstly, we will apply the action of $PGL(2, q)$ on \mathbb{S} to obtain projective linear sets $O(\alpha)$. Then we will consider the action of G on \mathbb{O} . The number of orbits in \mathbb{O} under the action of G will give an upper bound on the number of extended irreducible Goppa codes. To find the number of orbits we will use the Cauchy-Frobenius counting theorem, see [6].

The group $G = \langle \sigma \rangle$ is cyclic of order r . In analysing the action of G we will make use of the fact that subgroups of G are of the form $\langle \sigma^{r_1} \rangle$ where $r_1 \mid r$. Clearly, $|\langle \sigma^{r_1} \rangle| = \frac{r}{r_1} = \bar{r}_1$.

Next we note that if $r = 3$ then the number of projective linear sets in \mathbb{O} is $|\mathbb{O}| = \frac{|\mathbb{S}|}{q^3 - q} = \frac{q^3 - q}{q^3 - q} = 1$. That is, there is just one projective linear set containing all $q^3 - q$ elements of \mathbb{S} . We put the result in a theorem.

Theorem 2.3. *When $r = 3$ the set \mathbb{S} consists of just one projective linear set, that is, $\mathbb{S} = O(\alpha)$ for any $\alpha \in \mathbb{S}$.*

Corollary 2.1. *All extended irreducible Goppa codes of length $q+1$ with $r = 3$ are equivalent.*

The result in Corollary 2.1 is well known, for example see [3] and [9].

Now, suppose that $[B](\alpha) = \frac{a\alpha+b}{c\alpha+d} = \alpha^{q^{r_1}}$ where $r_1 \mid r$. We see that if D is the smallest positive integer such that $\alpha^{q^{Dr_1}} = \alpha$, then $D \mid r$ since $\alpha \in \mathbb{F}_{q^r}$. Observe that $\alpha^{q^{Dr_1}} = \alpha$ implies that $\alpha^{q^{Dr_1}} = [B^D](\alpha) = [I_2](\alpha) = \alpha$. Thus the order D of $B \in GL(2, q)$ is $D = \frac{r}{r_1} = \bar{r}_1$.

3 Enumeration of irreducible Goppa codes

We count irreducible Goppa codes by using the tools developed in [14] where an upper bound on the number of irreducible Goppa codes of degree r and length q^n is given. The upper bound is found by counting the number of affine sets in \mathbb{A} fixed under the action of subgroups G and then applying the Cauchy-Frobenius Theorem. As opposed to [14], where the upper bound is given in the form of an algorithm, we obtain analytic formulas for the upper bound.

Suppose $A(\alpha)$ is fixed by $\langle \sigma^{r_1} \rangle$. Then $\sigma^{r_1}(A(\alpha)) = A(\alpha)$. So we have $\sigma^{r_1}(\alpha) = \alpha^{q^{r_1}} = \zeta\alpha + \xi$ for some $\zeta \neq 0, \xi \in \mathbb{F}_q$. Thus $\alpha^{q^{r_1}} = [A](\alpha)$ where $A = \begin{pmatrix} \zeta & \xi \\ 0 & 1 \end{pmatrix} \in GL(2, q)$. Now, $\alpha^{q^{r_1 \bar{r}_1}} = [A^{\bar{r}_1}](\alpha) = [I_2](\alpha) = \alpha$ so A is a matrix of order \bar{r}_1 . We divide our analysis according to whether $\bar{r}_1 = 1$, $\gcd(p, \bar{r}_1) = 1$ and $\gcd(p, \bar{r}_1) = p$.

3.1 Affine sets fixed under $\langle \sigma^{r_1} \rangle$ when $\bar{r}_1 = 1$

If $\bar{r}_1 = 1$ then $r_1 = r$ and $\alpha^{q^{r_1}} = [A](\alpha) = [I_2](\alpha) = \alpha$ and $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, see Theorem 2.1. Now $\alpha^{q^{r_1}} = \alpha$ if and only if $\mathbb{F}_{q^{r_1}}$ contains elements of \mathbb{S} . We know that this is true if and only if $r_1 = r$. It is easy to see that every affine set is fixed under $\langle \sigma^r \rangle$. By Corollary 3.5 in [13] the number of affine sets fixed under $\langle \sigma^r \rangle$ is

$$\frac{|\mathbb{S}|}{q^2 - q}.$$

Example 3.1. Let $q = 2^6$ and $r = 3$. There are 17 affine sets in \mathbb{A} and all of them are fixed under $\langle \sigma^3 \rangle$.

3.2 Affine sets fixed under $\langle \sigma^{r_1} \rangle$ when $\gcd(p, \bar{r}_1) = 1$

Now suppose that $A(\alpha) \in \mathbb{A}$ is fixed under $\langle \sigma^{r_1} \rangle$ where $\gcd(p, \bar{r}_1) = 1$. Then we have that $\alpha^{q^{r_1}} = [A](\alpha)$ and by Theorem 2.1, we may take $A = \begin{pmatrix} \zeta & 0 \\ 0 & 1 \end{pmatrix} \in GL(2, q)$ of order \bar{r}_1 . Thus $\alpha^{q^{r_1}} = \zeta\alpha$ and as such α satisfies an equation of the form

$$x^{q^{r_1}} - \zeta x = 0, \tag{3}$$

where ζ is of order \bar{r}_1 .

Next we note that the factorization of $F_{r_1}(x) = x^{q^{r_1}} - \zeta x$ was considered in [4]. Using our notation and Theorem 4 in [4] we obtain the following result.

Theorem 3.1. Let $\bar{r}_1 > 1$ and suppose $(p, \bar{r}_1) = 1$ and that $\bar{r}_1 \mid (q-1)$. Let $r = \bar{r}_1 u$, $u \in \mathbb{N}$ and $T(r)$ be the set of all roots of irreducible factors of degree r in the factorization of $F_{r_1}(x) = x^{q^s-1} - \zeta \in \mathbb{F}_q[x]$, where $\zeta \neq 1 \in \mathbb{F}_q^*$ is of order \bar{r}_1 . If $r \not\equiv 0 \pmod{\bar{r}_1}$ then $|T(r)| = 0$. Otherwise

$$|T(r)| = \sum_{\substack{d|u \\ (d, \bar{r}_1)=1}} \mu(d) \left(q^{\frac{u}{d}} - 1 \right).$$

Observe that since $A = \begin{pmatrix} \zeta & 0 \\ 0 & 1 \end{pmatrix} \in GL(2, q)$ is of order \bar{r}_1 there are $\phi(\bar{r}_1)$ conjugacy classes in $GL(2, q)$ in this case and a polynomial arising from a representative of each conjugacy class contributes $|T(r)|$ roots to \mathbb{S} . Thus there are $\phi(\bar{r}_1)|T(r)|$ roots which lie in \mathbb{S} . Note that this closed formula is a partial answer to Remark 4.5 in [13].

Example 3.2. Let $q = 2^6$ and $r = 6$. There are 672 irreducible factors of degree 6 in the factorization of $F_2(x) = x^{2^{12}} - \varepsilon^{42}x$ where ε is a primitive element of \mathbb{F}_{2^6} . Hence there are 8,064 roots of polynomials of the form $F_2(x)$ which lie in \mathbb{S} where $A = \begin{pmatrix} \varepsilon^{42} & 0 \\ 0 & 1 \end{pmatrix} \in GL(2, 2^6)$ is of order 3.

Next we find the number of affine sets fixed under $\langle \sigma^{r_1} \rangle$. We know that if $\bar{r}_1 > 1$ where $p \nmid \bar{r}_1$ and $\bar{r}_1 \mid (q - 1)$ then there are $\phi(\bar{r}_1)|T(r)|$ roots of the equations of the form $x^{q^{r_1}} - \zeta x = 0$ which lie in \mathbb{S} . By [13, Theorem 4.4], each polynomial $F_{r_1}(x)$ has $q - 1$ roots in exactly one $A(\alpha)$. Thus we have proved the following theorem.

Theorem 3.2. Suppose $\bar{r}_1 > 1$ where $p \nmid \bar{r}_1$ and $\bar{r}_1 \mid (q - 1)$. Then there are $\tau = \frac{\phi(\bar{r}_1)|T(r)|}{q-1}$ affine sets fixed by $\langle \sigma^{r_1} \rangle$.

3.3 Affine sets fixed under $\langle \sigma^{r_1} \rangle$ when $\gcd(p, \bar{r}_1) = p$

Suppose that $A(\alpha) \in \mathbb{A}$ is fixed under $\langle \sigma^{r_1} \rangle$ where $\gcd(p, \bar{r}_1) = p$. Then we have that $\alpha^{q^{r_1}} = [A](\alpha)$ and by Theorem 2.1, we may take $A = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \in GL(2, q)$ where $\beta \in \mathbb{F}_q^*$. Thus $\alpha^{q^{r_1}} = \alpha + \beta$ and as such α satisfies an equation of the form

$$x^{q^{r_1}} - x - \beta = 0. \quad (4)$$

Observe that if $\bar{r}_1 = p$ hence $r_1 = \frac{r}{p}$ then we will take $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ since we can show, by direct computation, that the order of A is p . As such, we have $\alpha^{q^{\frac{r}{p}}} = \alpha + 1$ and we may assume that α satisfies an equation of type

$$x^{q^{\frac{r}{p}}} - x - 1 = 0. \quad (5)$$

Next we note that the factorization of polynomials of the form $F_{r_1}(x) = x^{q^{r_1}} - x - 1$ was considered in [4]. Using our notation and [4, Theorem 2] we obtain the following result.

Theorem 3.3. Suppose $F_{r_1}(x) = x^{q^{r_1}} - x - 1$ where $r_1 = \frac{r}{p}$ and $\bar{r}_1 = p$. Let $r = pu, u \in \mathbb{N}$, and $U(r)$ be the set of roots of irreducible factors of degree r in the factorization of $F_{r_1}(x)$. If $r \not\equiv 0 \pmod{p}$, then $|U(r)| = 0$. Otherwise

$$|U(r)| = \sum_{\substack{d \mid u \\ d \not\equiv 0 \pmod{p}}} \mu(d) q^{u/d}.$$

It is easy to see that if α satisfies Equation 5 then all the q elements of the set $\{\alpha + \xi : \xi \in \mathbb{F}_q\}$ also satisfy 5 while the remaining elements in $A(\alpha)$ do not. Hence if α satisfies equation 5 then $A(\alpha)$ contains precisely q roots of Equation 5. We have proved the following theorem.

Theorem 3.4. *If $\bar{r}_1 = p$ then there are $\frac{|U(r)|}{q}$ affine sets fixed by $\langle \sigma^{r_1} \rangle$ where $r_1 = \frac{r}{p}$.*

Corollary 3.1. *If $r = p$ and $\bar{r}_1 = p$ then $r_1 = 1$ and there is one affine set fixed by $\langle \sigma \rangle$.*

Example 3.3. *Let $q = 2^6$ and $r = 6$. Then $|U(r)| = 262,080$ and there are $\frac{262,080}{64} = 4,095$ affine sets fixed by $\langle \sigma^3 \rangle$.*

Now suppose that $\bar{r}_1 = p^2$. We consider $r_1 = \frac{r}{p^2}$. Thus, we have $\alpha^{q^{r_1}} = [A](\alpha)$. So $\alpha^{q^r} = [A^{p^2}](\alpha) = [I_2](\alpha) = \alpha$ and so the order of A divides p^2 . We know that matrices of order p^2 do not exist. So we consider matrices of order p . We obtain an equation of the form $x^{q^{\frac{r}{p^2}}} - x - 1 = 0$ and all roots of this equation lie in $\mathbb{F}_{q^{\frac{r}{p}}} - \mathbb{F}_{q^{\frac{r}{p^2}}}$ and not in \mathbb{S} . We have the following theorem.

Theorem 3.5. *If $\bar{r}_1 = p^2$ then $p^2 \mid r$ and there is no polynomial of degree r in the factorization of $F_{r_1}(x) = x^{q^{r_1}} - x - 1$ where $r_1 = \frac{r}{p^2}$.*

Next suppose that $\bar{r}_1 = pp_1$ where p_1 is some other divisor of r . Then $\alpha^{q^{r_1}} = [A](\alpha)$ and $\alpha^{q^{r_1 pp_1}} = [A^{pp_1}](\alpha) = [I_2](\alpha) = \alpha$. Then $A^{pp_1} = I_2$. If we take $B = A^p$ of order p_1 then we have $\alpha^{q^{sp_1}} = [B^{p_1}](\alpha)$ then α satisfies Equation 3. Also if we take $B = A^{p_1}$ of order p then we have $\alpha^{q^{r_1 p}} = [B^p](\alpha)$ then α satisfies Equation 5 and this is not possible. So there is no irreducible polynomial of degree r in the factorization of $F_{r_1}(x)$ in this case. We have the following result.

Theorem 3.6. *There is no affine set fixed under $\langle \sigma^{r_1} \rangle$ if $\bar{r}_1 = p^2$ and $p^2 \mid r$ or $\bar{r}_1 = pp_1$ where p_1 is some other divisor of r .*

Example 3.4. *Let $q = 2^4$ and $r = 12$. The subgroups $\langle \sigma^2 \rangle$ and $\langle \sigma^3 \rangle$ where $\bar{r}_1 = 6$ and $\bar{r}_1 = 4$ respectively do not fix any affine set.*

Putting the results together, we have proved the following:

Theorem 3.7. *With the notation we have established:*

1. *There are $\frac{|\mathbb{S}|}{q^2 - q}$ affine sets fixed by $\langle \sigma^r \rangle$.*
2. *There are $\frac{\phi(\bar{r}_1)|T(r)|}{q-1}$ affine sets fixed by $\langle \sigma^{r_1} \rangle$ if $\bar{r}_1 \mid (q-1)$.*
3. *If $(\bar{r}_1, r) = p$ then*
 - (a) *there are $\frac{|U(r)|}{q}$ affine sets fixed by $\langle \sigma^{r_1} \rangle$ if $\bar{r}_1 = p$.*
 - (b) *there is 1 affine set fixed by $\langle \sigma^{r_1} \rangle$ if $\bar{r}_1 = r$.*

Remark 3.1. *This result agrees with [13, Theorem 4.13] for $n = 1$. Our main contribution here is that we have found closed formulas for $|T(r)|$ and $|U(r)|$.*

4 Counting extended irreducible Goppa codes

4.1 Strategy for counting extended irreducible Goppa codes

We will use the actions of $PGL(2, q)$ and G on \mathbb{S} to find the maximum number of extended irreducible Goppa codes. Firstly, we will apply the action of the group $PGL(2, q)$ on \mathbb{S} to obtain projective linear sets $O(\alpha)$. Then we will consider the action of G on \mathbb{O} . The number of orbits in \mathbb{O} under the action of G will give us an upper bound on the number of extended Goppa codes.

Recall that a projective linear set can be decomposed as $O(\alpha) = A(\alpha) \cup A(\frac{1}{\alpha}) \cup A(\frac{1}{\alpha+1}) \cup A(\frac{1}{\alpha+\xi_1}) \cup A(\frac{1}{\alpha+\xi_2}) \cup \dots \cup A(\frac{1}{\alpha+\xi_{q-2}})$ where $\mathbb{F}_{q^n} = \{0, 1, \xi_1, \xi_2, \dots, \xi_{q-2}\}$. Observe that if a projective linear set $O(\alpha) \in \mathbb{O}$ is fixed under $\langle \sigma^{r_1} \rangle$ then $\langle \sigma^{r_1} \rangle$ acts on $O(\alpha) = A(\alpha) \cup A(\frac{1}{\alpha}) \cup A(\frac{1}{\alpha+1}) \cup A(\frac{1}{\alpha+\xi_1}) \cup A(\frac{1}{\alpha+\xi_2}) \cup \dots \cup A(\frac{1}{\alpha+\xi_{q-2}})$ and partitions this set of $q+1$ affine sets. We see that some projective linear sets fixed under $\langle \sigma^{r_1} \rangle$ contain fixed affine sets and there is also a possibility of having a fixed projective linear set that does not contain fixed affine sets. We will consider the following possibilities: $\bar{r}_1 = 1$; $\gcd(p, \bar{r}_1) = 1$ and $\bar{r}_1 \mid (q-1)$; $\gcd(p, \bar{r}_1) = p$; and $\gcd(p, \bar{r}_1) = 1$ where $\bar{r}_1 \mid (q+1)$. We will discuss each of the four cases in separate sections.

4.2 Projective linear sets fixed when $D = 1$

If $\bar{r}_1 = 1$ then $\alpha^{q^{r_1}} = [B](\alpha) = [I_2](\alpha) = \alpha$ and $B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, see Theorem 2.1. Now $\alpha^{q^{r_1}} = \alpha$ if and only if $\mathbb{F}_{q^{r_1}}$ contains elements of \mathbb{S} . That is, $r_1 = r$. By Section 3.1 we know that the number of affine sets fixed under $\langle \sigma^r \rangle$ where $\bar{r}_1 = 1$ is $\frac{|\mathbb{S}|}{q^2 - q}$.

By an argument similar to the one in [7, Section 4.3.2], we find that the number of projective linear sets $O(\alpha)$ fixed under $\langle \sigma^r \rangle$ is $\frac{|\mathbb{S}|}{q^3 - q}$.

4.3 Projective linear sets fixed when $\gcd(p, \bar{r}_1) = 1$ and $\bar{r}_1 \mid (q-1)$

Suppose $\gcd(p, \bar{r}_1) = 1$ and that $\bar{r}_1 \mid (q-1)$. Theorem 3.2 gives the number of affine sets fixed by $\langle \sigma^{r_1} \rangle$ in this case.

Next we find the number of projective linear sets $O(\alpha)$ fixed under $\langle \sigma^{r_1} \rangle$. We will do this by finding how many affine sets fixed under $\langle \sigma^{r_1} \rangle$ lie in each fixed projective linear set.

Suppose $O(\alpha) \in \mathbb{O}$ is fixed under $\langle \sigma^{r_1} \rangle$. Then $\langle \sigma^{r_1} \rangle$ acts on $O(\alpha) = A(\alpha) \cup A(\frac{1}{\alpha}) \cup A(\frac{1}{\alpha+1}) \cup A(\frac{1}{\alpha+\xi_1}) \cup A(\frac{1}{\alpha+\xi_2}) \cup A(\frac{1}{\alpha+\xi_3}) \cup \dots \cup A(\frac{1}{\alpha+\xi_{q-2}})$, a set of $q+1$ affine sets. $\langle \sigma^{r_1} \rangle$ partitions this set of $q+1$ affine sets. The possible lengths of an orbit are 1 and factors of \bar{r}_1 . Now, since $\bar{r}_1 \mid q-1$ then $q+1 = q-1+2 \equiv 2 \pmod{\bar{r}_1}$. We claim that each $O(\alpha)$ fixed under $\langle \sigma^{r_1} \rangle$ contains 2 affine sets which are fixed under $\langle \sigma^{r_1} \rangle$. Observe that if \bar{r}_1 is prime then we are done. So we will suppose that \bar{r}_1 is composite. That is, we can find non-negative integers e_1, e_2, \dots, e_t such that $d_1 e_1 + d_2 e_2 + \dots + d_t e_t = q+1$ where $d_i \mid \bar{r}_1$, $1 \leq i \leq t$, $d_1 = 1$ and $d_t = \bar{r}_1$. Note that we can always choose a factor d_i , $1 < i \leq t$ such that $\langle \sigma^{d_i r_1} \rangle$ is of prime order $\frac{\bar{r}_1}{d_i}$ and fixes $O(\alpha)$. Now, an $O(\alpha)$ fixed under $\langle \sigma^{d_i r_1} \rangle$ contains two fixed affine sets so it follows that an $O(\alpha)$ fixed under $\langle \sigma^{r_1} \rangle$ also contains two fixed affine sets. Thus if $\bar{r}_1 \mid (q-1)$ then each $O(\alpha)$ fixed under $\langle \sigma^{r_1} \rangle$ contains 2 fixed affine sets.

We have the following theorem.

Theorem 4.1. *Let $\gcd(p, \bar{r}_1) = 1$ and $\bar{r}_1 \mid (q-1)$. The number of projective linear sets fixed under $\langle \sigma^{r_1} \rangle$ is $\frac{\tau}{2}$ where τ is defined in Theorem 3.2.*

4.4 Projective linear sets fixed when $\gcd(p, \bar{r}_1) = p$

In this section we obtain the number of projective linear sets fixed when $\gcd(p, \bar{r}_1) = p$. By Theorem 3.4, there are $\frac{|U(r)|}{q}$ affine sets fixed by $\langle \sigma^{r_1} \rangle$ when $\gcd(p, \bar{r}_1) = p$. We will do this by finding how many affine sets fixed under $\langle \sigma^{r_1} \rangle$ lie in a projective linear set fixed under $\langle \sigma^{r_1} \rangle$.

We claim that each of the $O(\alpha)$ in \mathbb{O} fixed under $\langle \sigma^{r_1} \rangle$ contains precisely one affine set which is fixed under $\langle \sigma^{r_1} \rangle$. It suffices to show that $O(\alpha)$ cannot contain two affine sets which are fixed under $\langle \sigma^{r_1} \rangle$. Without loss of generality, suppose $A(\alpha)$ is fixed under $\langle \sigma^{r_1} \rangle$. Recall that $O(\alpha) = A(\alpha) \cup A(\frac{1}{\alpha}) \cup A(\frac{1}{\alpha+1}) \cup A(\frac{1}{\alpha+\xi_1}) \cup A(\frac{1}{\alpha+\xi_2}) \cup A(\frac{1}{\alpha+\xi_3}) \cup \dots \cup A(\frac{1}{\alpha+\xi_{q-2}})$. We show that none of the affine sets after $A(\alpha)$ in the above decomposition of $O(\alpha)$ is fixed under $\langle \sigma^{r_1} \rangle$. This is done by showing that no element in any of these affine sets satisfies Equation 5. It is sufficient to show that no element in $A(\frac{1}{\alpha})$ satisfies $x^{q^{\frac{r}{p}}} - x - 1 = 0 = 0$. A typical element of $A(\frac{1}{\alpha})$ has the form $\frac{\zeta}{\alpha} + \xi$ and substituting this into $x^{q^{\frac{r}{p}}} - x - 1$ we get $(\frac{\zeta}{\alpha} + \xi)^{q^{\frac{r}{p}}} - (\frac{\zeta}{\alpha} + \xi) - 1 = \frac{-\alpha^2 - \alpha - \zeta}{\alpha^2 + \alpha} \neq 0$, since α is an element of degree $r > 3$ over \mathbb{F}_q . We conclude that $A(\frac{1}{\alpha})$ is not fixed under $\langle \sigma^{r_1} \rangle$ and in fact $A(\alpha)$ is the only affine set in $O(\alpha)$ fixed under $\langle \sigma^{r_1} \rangle$. It follows that the number of projective linear sets $O(\alpha)$ in \mathbb{O} which are fixed under $\langle \sigma^{r_1} \rangle$ where $(p, \bar{r}_1) = p$ is $\frac{|U(r)|}{q}$. Thus we have proved the following.

Theorem 4.2. *If $\gcd(p, \bar{r}_1) = p$ and $\bar{r}_1 = p$, then the number of projective linear sets fixed under $\langle \sigma^{r_1} \rangle$ is the same as the number of affine sets fixed under $\langle \sigma^{r_1} \rangle$.*

4.5 Projective linear sets fixed by $\langle \sigma^{r_1} \rangle$ where $\gcd(p, \bar{r}_1) = 1$ and $\bar{r}_1 \mid (q+1)$

Suppose that $O(\alpha) \in \mathbb{O}$ is fixed by $\langle \sigma^{r_1} \rangle$ where $\gcd(p, \bar{r}_1) = 1$, $\bar{r}_1 \mid (q+1)$ and $\bar{r}_1 > 2$. Then we have that $\alpha^{q^{r_1}} = [A](\alpha)$, where $\gcd(p, \bar{r}_1) = 1$ and $\bar{r}_1 \mid (q+1)$. Then, by Theorem 2.1, A is conjugate with a matrix of the form $B = \begin{pmatrix} 0 & 1 \\ \zeta & \xi \end{pmatrix} \in GL(2, q)$ where the minimal polynomial of B , $m_B(x)$, is an irreducible quadratic polynomial over \mathbb{F}_q . Without loss of generality, we will take $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, q)$ where, as above, $m_A(x)$ is an irreducible quadratic polynomial over \mathbb{F}_q .

Now, $\alpha^{q^{r_1}} = [A](\alpha) = \frac{a\alpha+b}{c\alpha+d}$ implies that α satisfies an equation of the form

$$F_{r_1}(x) = cx^{q^{r_1}+1} + dx^{q^{r_1}} - ax - b = 0. \quad (6)$$

It is clear from the foregoing discussion that in order to find the number of projective linear sets fixed under $\langle \sigma^{r_1} \rangle$ we need to find roots of Equation 6 which lie in \mathbb{S} . Observe that in this case there is no affine set fixed in the decomposition of $O(\alpha)$.

Note that there are $\frac{\phi(\bar{r}_1)}{2}$ polynomials of the form $F_{r_1}(x) = cx^{q^{r_1}+1} + dx^{q^{r_1}} - ax - b \in \mathbb{F}_q[x]$ each of which corresponds to a representative of a conjugacy class of matrices of order

\bar{r}_1 where the minimal polynomials of such matrices are irreducible quadratic polynomials over \mathbb{F}_q , see Theorem 2.2 in [7].

We now consider the factorization of $F_{r_1}(x) = cx^{q^{r_1}+1} + dx^{q^{r_1}} - ax - b \in \mathbb{F}_q[x]$. We begin by considering the factorization of $F_{r_1}(x)$ where $\gcd(p, \bar{r}_1) = 1$, $\bar{r}_1 \mid (q+1)$ and $\bar{r}_1 > 2$ is even. Note that the assumption that $\bar{r}_1 \mid (q+1)$ where \bar{r}_1 is even implies that the characteristic of \mathbb{F}_q is odd.

Suppose that α is a root of $F_{r_1}(x)$ where $\bar{r}_1 > 2$ is even. Then $\bar{r}_1 = 2d$ where $d > 1$ is an integer. Thus we have $\alpha^{q^{r_1}} = [A^{\bar{r}_1}](\alpha) = [I_2](\alpha) = \alpha$. So $A^{2d} = (A^d)^2 = B^2 = I_2$, where $B = A^d$. Now, since $B^2 = I_2$, without loss of generality we can take $B = \begin{pmatrix} q-1 & 0 \\ 0 & q-1 \end{pmatrix}$ since the only elements $\zeta \in \mathbb{F}_q$ such that $\zeta^2 = 1$ are $\zeta = 1$ and $\zeta = q-1$. Thus α satisfies an equation of the form $F_{r_1}(x) = (q-1)(x^{q^{r_1}} - x) = 0$. By the argument in Section 4.2 there are no irreducible polynomials of degree r in the factorization of $F_{r_1}(x) = (q-1)(x^{q^{r_1}} - x)$. We have proved the following.

Theorem 4.3. *Suppose $\gcd(p, \bar{r}_1) = 1$, $\bar{r}_1 \mid (q+1)$ and $\bar{r}_1 = 2d$ where $d > 1$ is an integer. Then there is no projective linear set fixed under $\langle \sigma^{r_1} \rangle$.*

Example 4.1. *Consider $q = 3^3$ and $r = 4$. There are no polynomials of degree 4 in the factorization of $F_1(x) = 2x^{28} + 2 \in \mathbb{F}_{3^3}[x]$ where $A = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} \in GL(2, 3^3)$ is of order 4. Hence there is no projective linear set fixed under $\langle \sigma \rangle$.*

Next we consider the factorization of $F_{r_1}(x)$ where $\gcd(p, \bar{r}_1) = 1$, $\bar{r}_1 \mid (q+1)$ and $d \mid \bar{r}_1$ but $d^2 \nmid \bar{r}_1$. Suppose that α is a root of $F_{r_1}(x)$ and that $d \mid \bar{r}_1$ where $1 < d < \bar{r}_1$. We have $\alpha^{q^{r_1}} = [A](\alpha)$ where A is a matrix of order \bar{r}_1 . Now, if $d \mid \bar{r}_1$ then $\alpha^{q^{r_1 d}} = [A^d](\alpha) = [B](\alpha)$, where $B = A^d$ and the order of B is $\frac{\bar{r}_1}{d}$ since $\text{GCD}(\bar{r}_1, d) = d$. We see that for α to satisfy $F_{r_1 d}(x)$, d must divide $\frac{\bar{r}_1}{d}$. That is α satisfies $F_{r_1 d}(x)$ provided $d^2 \mid \bar{r}_1$. We have proved the following theorem.

Theorem 4.4. *Suppose α satisfies $F_{r_1}(x)$ and $d \mid \bar{r}_1$ where $1 < d < \bar{r}_1$. If $d^2 \nmid \bar{r}_1$ then α does not satisfy $F_{r_1 d}(x)$.*

This theorem is significant because it tells us about the existence of an irreducible factor of degree r in the factorization of $F_{r_1}(x)$ by looking at the factorization of $F_{r_1 d}(x)$.

Now we consider when an irreducible quadratic polynomial of the form $cx^2 + (d-a)x - b \in \mathbb{F}_q[x]$ divides $F_{r_1}(x)$.

Proposition 4.1. *If $P(x) = cx^2 + (d-a)x - b \in \mathbb{F}_q[x]$ is irreducible, then $P(x) \mid F_{r_1}(x)$ if and only if $r_1 = 2w$.*

Proof. Suppose $P(x) = cx^2 + (d-a)x - b \in \mathbb{F}_q[x]$ is irreducible and that $P(\alpha) = 0$. Then $\alpha^{q^2} = \alpha$. If r_1 is even then $\gcd(2, r_1) = 2$ and this implies that $\alpha^{q^{r_1}} = \alpha$. Thus $F_{r_1}(\alpha) = c\alpha^{q^{r_1}+1} + d\alpha^{q^{r_1}} - a\alpha - b = c\alpha^2 + d\alpha - a\alpha - b = 0$. So $P(x) \mid F_{r_1}(x)$. If r_1 is odd and $P(\alpha) = 0$ then $\alpha^{q^{r_1}+1} = \alpha^{q+1}$. So $F_{r_1}(\alpha) = c\alpha^{q^{r_1}+1} + d\alpha^{q^{r_1}} - a\alpha - b = c\alpha^{q+1} + d\alpha^q - a\alpha - b = (\alpha^{q-1} - 1)(c\alpha^2 + d\alpha) + c\alpha^2 + d\alpha - a\alpha - b = 0$. We know that $c\alpha^2 + d\alpha - a\alpha - b = 0$ so $F_{r_1}(\alpha) = 0 \Leftrightarrow \alpha^{q-1} - 1 = 0$. This means $\alpha \in \mathbb{F}_q$ and $P(x)$ is reducible. \square

Consequently, the parity of r_1 indicates whether or not there is a quadratic factor in the factorization of $F_{r_1}(x)$. The following theorem, see [10] for its proof, gives the factorization of $F_{r_1}(x) = cx^{q^{r_1}+1} + dx^{q^{r_1}} - ax - b \in \mathbb{F}_q[x]$.

Theorem 4.5. *Let $\gcd(p, \bar{r}_1) = 1$ and $\bar{r}_1 \mid (q+1)$ where $\bar{r}_1 \neq 2t$, $t > 1$. Let $X(r)$ be the set of roots of polynomials of degree $r = \bar{r}_1 u$ in the factorization of $F_{r_1}(x) = cx^{q^{r_1}+1} + dx^{q^{r_1}} - ax - b$ where the minimal polynomial of A is an irreducible quadratic polynomial over \mathbb{F}_q . Then*

$$|X(r)| = \sum_{\substack{d \mid u \\ d \not\equiv 0 \pmod{\bar{r}_1}}} \mu(d) (q^{\frac{u}{d}} - (-1)^{\frac{u}{d}}).$$

Example 4.2. *Consider $q = 2^5$ and $r = 6$. We want to find the number of irreducible polynomials of degree 6 in the factorization of $F_2(x) = x^{2^{10}+1} - x + 1 \in \mathbb{F}_{2^5}[x]$. Using Theorem 4.5, with $r = \bar{r}_1 u = 3 \times 2$ there are $\frac{990}{6} = 165$ polynomials of degree 6 in the factorization of $F_2(x) = x^{2^{10}+1} - x + 1 \in \mathbb{F}_{2^5}[x]$.*

Theorem 4.5 implies that each polynomial $F_{r_1}(x) = cx^{q^{r_1}+1} + dx^{q^{r_1}} - ax - b$ contributes $|X(r)|$ roots to \mathbb{S} . Recall that there are $\frac{\phi(\bar{r}_1)}{2}$ conjugacy classes of matrices of order \bar{r}_1 whose eigenvalues lie in \mathbb{F}_{q^2} hence there are $\frac{\phi(\bar{r}_1)}{2}$ polynomials counting representatives only. If we let \mathbb{S}_F be the set of roots of the $\frac{\phi(\bar{r}_1)}{2}$ polynomials $F_{r_1}(x)$ which lie in \mathbb{S} then $|\mathbb{S}_F| = \frac{\phi(\bar{r}_1)|X(r)|}{2}$.

In the following theorem we count the number of roots of $F_{r_1}(x)$ which lie in $O(\alpha)$.

Theorem 4.6. *If $O(\alpha)$ is a projective linear set fixed by $\langle \sigma^{r_1} \rangle$, then $O(\alpha)$ contains $q+1$ roots of $F_{r_1}(x) = cx^{q^{r_1}+1} + dx^{q^{r_1}} - ax - b$.*

Proof. Suppose $O(\alpha)$ is fixed under $\langle \sigma^{r_1} \rangle$, then $\alpha^{q^{r_1}} = [A](\alpha) = \frac{a\alpha+b}{c\alpha+d}$, where $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, q)$.

Thus we may assume that α satisfies $F_s(x) = cx^{q^{r_1}+1} + dx^{q^{r_1}} - ax - b$.

Recall that $O(\alpha) = A(\alpha) \cup A(\frac{1}{\alpha}) \cup A(\frac{1}{\alpha+1}) \cup A(\frac{1}{\alpha+\nu_1}) \cup A(\frac{1}{\alpha+\nu_2}) \cup \dots \cup A(\frac{1}{\alpha+\nu_{q-2}})$ where $\mathbb{F}_q = \{0, 1, \nu_1, \nu_2, \dots, \nu_{q-2}\}$.

It is easy to see that α is the only element in $A(\alpha)$ which satisfies $F_{r_1}(x)$. Now, let us fix $\nu \in \mathbb{F}_q$, we would like to count how many elements of the affine set $A(\frac{1}{\alpha+\nu})$ satisfy $F_{r_1}(x)$. A typical element of $A(\frac{1}{\alpha+\nu})$ is $\frac{\zeta}{\alpha+\nu} + \xi$ where $\zeta \neq 0, \xi \in \mathbb{F}_q$. If $\frac{\zeta}{\alpha+\nu} + \xi$ is a root of $F_{r_1}(x) = cx^{q^{r_1}+1} + dx^{q^{r_1}} - ax - b$ then

$$c \left(\frac{\zeta}{\alpha+\nu} + \xi \right)^{q^{r_1}+1} + d \left(\frac{\zeta}{\alpha+\nu} + \xi \right)^{q^{r_1}} - a \left(\frac{\zeta}{\alpha+\nu} + \xi \right) - b = 0.$$

From this we obtain

$$\left(\frac{\zeta}{\alpha+\nu} + \xi \right)^{q^{r_1}} = \frac{a \left(\frac{\zeta}{\alpha+\nu} + \xi \right) + b}{c \left(\frac{\zeta}{\alpha+\nu} + \xi \right) + d}. \quad (7)$$

So

$$\frac{\zeta}{\alpha^{q^{r_1}} + \nu} + \xi = \frac{a\zeta + a\xi\alpha + a\xi\nu + b\alpha + b\nu}{c\zeta + c\xi\alpha + c\xi\nu + d\alpha + d\nu}. \quad (8)$$

Thus $\nu \in \mathbb{F}_q$ since $\mathbb{F}_q \cap \mathbb{F}_{q^{r_1}} = \mathbb{F}_q$.

Equation 8 implies

$$\frac{\xi\alpha^{q^{r_1}} + \zeta + \nu\xi}{\alpha^{q^{r_1}} + \nu} = \frac{(a\xi + b)\alpha + a\zeta + a\xi\nu + b\nu}{(c\xi + d)\alpha + c\zeta + c\xi\nu + d\nu}.$$

Recall that $\alpha^{q^{r_1}} = \frac{a\alpha+b}{c\alpha+d}$ so we have,

$$\frac{\xi \left(\frac{a\alpha+b}{c\alpha+d} \right) + \zeta + \nu\xi}{\frac{a\alpha+b}{c\alpha+d} + \nu} = \frac{(a\xi + b)\alpha + a\zeta + a\xi\nu + b\nu}{(c\xi + d)\alpha + c\zeta + c\xi\nu + d\nu}.$$

From this, we obtain

$$\frac{(a\xi + c\xi\nu + c\zeta)\alpha + b\xi + d\nu\xi + d\zeta}{(a + c\nu)\alpha + b + d\nu} = \frac{(a\xi + b)\alpha + a\zeta + a\xi\nu + b\nu}{(c\xi + d)\alpha + c\zeta + c\xi\nu + d\nu}.$$

Comparing coefficients, we get

$$a\xi + c\xi\nu + c\zeta = a\xi + b$$

$$b\xi + d\nu\xi + d\zeta = a\zeta + a\xi\nu + b\nu$$

$$a + c\nu = c\xi + d$$

$$b + d\nu = c\zeta + c\xi\nu + d\nu.$$

Solving these equations we get

$$\xi = \frac{a + c\nu - d}{c} \text{ and } \zeta = \frac{b - c\nu\xi}{c}$$

where $c \neq 0$. That is, for any $\nu \in \mathbb{F}_q$ we get unique values of ζ and ξ . Since ν specifies an affine set, this means that each affine set contains exactly one root of $F_{r_1}(x)$. Hence there are $q + 1$ roots of $F_{r_1}(x)$ in $O(\alpha)$. \square

Note that if $O(\alpha)$ contains a root of any of the polynomials $F_{r_1}(x) = cx^{q^{r_1}+1} + dx^{q^{r_1}} - ax - b$ it contains precisely $q + 1$ roots of the same equation. We know that if $O(\alpha)$ is fixed under $\langle \sigma^{r_1} \rangle$ where $\gcd(p, \bar{r}_1) = 1$ and $\bar{r}_1 \mid (q + 1)$ then either $\bar{r}_1 = 2$ or \bar{r}_1 is odd. The case $\bar{r}_1 = 2$ was addressed in Section 4.3. We have the following lemma.

Lemma 4.1. *Suppose $\gcd(p, \bar{r}_1) = 1$ where \bar{r}_1 is an odd integer. Then there are $\frac{\phi(\bar{r}_1)|X(r)|}{2(q+1)}$ projective linear sets fixed by $\langle \sigma^{r_1} \rangle$ if and only if $\bar{r}_1 \mid (q + 1)$.*

Note that if $\bar{r}_1 = r$ then $u = 1$ and, by Theorem 4.5, all the $q + 1$ roots of $F_{r_1}(x)$ lie in \mathbb{S} . In this case, the number of projective linear sets fixed under $\langle \sigma^{r_1} \rangle$ is $\frac{\phi(\bar{r}_1)}{2}$. We have the following result.

Corollary 4.1. *Suppose $\gcd(p, \bar{r}_1) = 1$ and $\bar{r}_1 = r$. Then there are $\frac{\phi(\bar{r}_1)}{2}$ projective linear sets fixed under $\langle \sigma^{r_1} \rangle$ if and only if $\bar{r}_1 \mid (q+1)$.*

Putting all the results together we have proved the following:

Theorem 4.7. *With the notation we have established:*

1. *There are $\frac{|\mathbb{S}|}{q^3-q}$ projective linear sets fixed by $\langle \sigma^r \rangle$.*
2. *There are $\frac{\phi(\bar{r}_1)|T(r)|}{2(q-1)}$ projective linear sets fixed by $\langle \sigma^{r_1} \rangle$ if $\bar{r}_1 \mid (q-1)$.*
3. *If $\gcd(\bar{r}_1, r) = p$ then*
 - (a) *there are $\frac{|U(r)|}{q}$ projective linear sets fixed by $\langle \sigma^{r_1} \rangle$ if $\bar{r}_1 = p$.*
 - (b) *there is 1 projective linear set fixed by $\langle \sigma^{r_1} \rangle$ if $\bar{r}_1 = r$.*
4. *If $\gcd(\bar{r}_1, p) = 1$ and $\bar{r}_1 \mid (q+1)$ then there are*
 - (a) *$\frac{\phi(\bar{r}_1)}{2}$ projective linear sets fixed by $\langle \sigma^{r_1} \rangle$ if $\bar{r}_1 = r$.*
 - (b) *$\frac{\phi(\bar{r}_1)|X(r)|}{2(q+1)}$ projective linear sets fixed by $\langle \sigma^{r_1} \rangle$ if \bar{r}_1 is an odd integer.*

5 The main theorem

We can use Theorem 3.7 and Theorem 4.7 together with the Cauchy-Frobenius theorem to calculate the average number of affine sets and projective linear sets fixed by an element of G respectively.

Theorem 5.1. *Let $N(q, r)$ (resp. $N_e(q, r)$) denote the number of orbits in \mathbb{S} under the action of the affine group (resp. projective linear group) and the Frobenius automorphism, as derived from Theorem 3.7 (resp. Theorem 4.7). The number of irreducible Goppa codes (resp. extended irreducible Goppa codes) over \mathbb{F}_q of length q (resp. $q+1$) and degree r is at most $N(q, r)$ (resp. $N_e(q, r)$).*

The following table compares $N(q, r)$ and $N_e(q, r)$.

q	r	$N_e(q, r)$	$N(q, r)$
2^5	5	205	6,765
5^2	6	2,667	67,930
2^3	9	29,604	266,304
3^3	7	76,027	2,128,684

References

- [1] Basheer, A.B.M., *Character Tables of the General Linear Group and Some of its Subgroups*, Msc Thesis, University of KwaZulu Natal, (2008).
- [2] Berger, T.P., *On the Cyclicity of Goppa Codes, Parity-Check Subcodes of Goppa Codes, and Extended Goppa Codes*, Finite Fields and Their Applications 6, 255-281 (2000).
- [3] Chen, C.L., *Equivalent irreducible Goppa codes*, IEEE Trans. IT 24, pp 766-769, (1978).
- [4] Garefalakis, T., *On the action of $GL_2(\mathbb{F}_q)$ on irreducible polynomials over F_q* . Journal of Pure and Applied Algebra, 215(8):18351843, (2011).
- [5] Goppa, V.D., *Rational representation of codes and (L, g) codes*, Probl. Peredach. Inform., vol. 7, no. 3, pp. 41-49, Sept. 1971.
- [6] Isaacs, I.M., *Algebra: A Graduate Text*, Brooks/Cole, Pacific Grove, CA, 1994.
- [7] Magamba K., and Ryan, J.A., *Counting Extended Irreducible Codes*, Appl. Algebra Engrg. Comm. Comput. (2018) doi:10.1007/s00200-018-0375-x
- [8] Lidl, R., and Niederreiter, H., *Finite Fields*, Cambridge University Press, (1986).
- [9] Moreno, O., *Symmetries of binary Goppa codes*, IEEE Trans. IT 25, (1979), 609612.
- [10] Reis, L., *Invariant theory of a special group action on irreducible polynomials over finite fields*, arXiv:1708.06862v2 [math.NT].
- [11] Ryan, J.A., *Counting extended irreducible binary quartic Goppa codes of length $2^n + 1$* . IEEE Transactions on Information Theory, 61, No. 3, 1174-1178, (2015).
- [12] Ryan, J.A., *Counting Extended Irreducible Goppa Codes*, Journal of Discrete Mathematics. vol. 2014, Article ID 871871, 4 pages, doi: 10.1155/2014/871871, (2014).
- [13] Ryan, J.A., Fitzpatrick, P., *Enumeration of inequivalent irreducible Goppa codes*. Discrete Applied Mathematics, vol. 154, no. 2, pp. 399412, (2006).
- [14] Ryan, J.A., *Irreducible Goppa codes*. PhD Thesis, University College Cork, (2004).