Available online at http://scik.org
J. Math. Comput. Sci. 8 (2018), No. 1, 1-17
https://doi.org/10.28919/jmcs/3442
ISSN: 1927-5307

COUNTING EXTENDED IRREDUCIBLE BINARY GOPPA CODES OF DEGREE $2p$ AND LENGTH 2^n+1

AUGUSTINE MUSUKWA

Department of Mathematics, Mzuzu University, P/Bag 201, Mzuzu 2, Malawi

Abstract. Let n and p be odd primes such that $p \neq n$ and $p \nmid (2^n \pm 1)$. An upper bound on the number of inequivalent extended irreducible binary Goppa codes of degree $2p$ and length 2^n+1 is produced.

Keywords: Goppa codes; extended codes; irreducible Goppa codes; equivalent codes.

2010 AMS Subject Classification: 11T71, 68R99.

1. Introduction

Goppa codes form a subclass of alternant codes and it was V.D. Goppa who, in the early 1970's, described this family of codes. These codes are said to have an interesting algebraic structure and contain good parameters. For these reasons, Goppa codes are of high practical value. The McEliece and Niederreiter cyptosystems are examples of public-key cryptosystems in cryptography which make use of Goppa codes.

The McEliece cryptosystem is believed to be a cryptosystem which may have potential to withstand attack by quantum computers [3, 4]. As this cryptosystem chooses a Goppa code at

E-mail address: augulela@yahoo.com

Received: July 28, 2017

random as its key, knowledge of the number of inequivalent Goppa codes for fixed parameters may facilitate in the evaluation of the security of such a cryptosystem. In [11], we find the best upper bound, available today, on the number of inequivalent irreducible Goppa codes. Some recent attempts to count inequivalent extended irreducible Goppa codes can be found in [7, 8, 9]. This paper seeks to find a tight upper bound on the number of inequivalent extended irreducible binary Goppa codes of degree $2p$. The count employs the tools which were used to count the non-extended versions (see [11]).

2. Preliminaries

The reader is encouraged to read the work we reproduce in this section since it is a prerequisite for the subsequent sections of this article. We begin by giving the definition of irreducible Goppa codes.

Definition 1. Let q be a power of a prime number 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 $\underline{c} = (c_0, c_1, ..., c_{q^n-1})$ with components in $\mathbb{F}_q$ which satisfy the condition

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

The set L is called the *defining set* and its cardinality defines the length of $\Gamma(L, g)$. The polynomial $g(z)$ is called the *Goppa polynomial.* If the degree of $g(z)$ is r then the code is called an *irreducible Goppa code of degree r.*

The roots of $g(z)$ are contained in $\mathbb{F}_{q^{nr}} \setminus \mathbb{F}_{q^n}$. If α is any root of $g(z)$ then it completely describes $\Gamma(L, g)$. Chen in [2] described a parity check matrix $\mathbf{H}(\alpha)$ for $\Gamma(L, g)$ which is given by

$$\mathbf{H}(\alpha) = \begin{pmatrix} \frac{1}{\alpha - \zeta_0} & \frac{1}{\alpha - \zeta_1} & \cdots & \frac{1}{\alpha - \zeta_{q^n-1}} \end{pmatrix}.$$

We will sometimes denote this code by $C(\alpha)$.

We next give the definition of extended irreducible Goppa codes.

Definition 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 $\overline{\Gamma(L,g)} = \{(c_0,c_1,...,c_{q^n}) : (c_0,c_1,...,c_{q^n-1}) \in \Gamma(L,g) \text{ and } \sum_{i=0}^{q^n} c_i = 0\}$.

Next we define the set which contains all the roots of all possible $g(z)$ of degree r.

Definition 3. We define the set $\mathbb{S} = \mathbb{S}(n,r)$ as the set of all elements in $\mathbb{F}_{q^{nr}}$ of degree r over $\mathbb{F}_{q^n}$.

Any irreducible Goppa code can be defined by an element in $\mathbb{S}$. The converse is also true, that is, any element in $\mathbb{S}$ defines an irreducible Goppa code. Since an irreducible Goppa code $\Gamma(L,g)$ is determined uniquely by the Goppa polynomial $g(z)$, or by a root α of $g(z)$, we define the mapping below. (For further details, see [2].)

Definition 4. The relation $\pi_{\zeta,\xi,i}$ defined on $\mathbb{S}$ by

$$\pi_{\zeta,\xi,i} : \alpha \mapsto \zeta\alpha^{q^i} + \xi$$

for fixed i, ζ, ξ where $1 \leq i \leq nr$, $\zeta \neq 0, \xi \in \mathbb{F}_{q^n}$ is a mapping on $\mathbb{S}$.

This map sends irreducible Goppa codes into equivalent codes and we generalise this as follows:

Theorem 5. (Ryan, [11]): *If α and β are related by an equation of the form $\alpha = \zeta\beta^{q^i} + \xi$ for some $\zeta \neq 0, \xi \in \mathbb{F}_{q^n}$, then the codes $C(\alpha)$ and $C(\beta)$ are equivalent.*

The map in Definition 4 can be broken up into the composition of two maps as follows:

1. $\pi_{\zeta,\xi}$ defined on $\mathbb{S}$ by $\pi_{\zeta,\xi} : \alpha \mapsto \zeta\alpha + \xi$ and
2. the map $\sigma^i : \alpha \mapsto \alpha^{q^i}$, where σ denotes the Frobenius automorphism of $\mathbb{F}_{q^{nr}}$ leaving $\mathbb{F}_q$ fixed.

From these two maps we define the following sets of mappings.

Definition 6. Let H denote the set of all maps $\{\pi_{\zeta,\xi} : \zeta \neq 0, \xi \in \mathbb{F}_{q^n}\}$.

Definition 7. Let G denote the set of all maps $\{\sigma^i : 1 \leq i \leq nr\}$.

The sets of maps H and G together with the operation *composition of maps* both form groups which act on $\mathbb{S}$.

Definition 8. The action of H on $\mathbb{S}$ induces orbits denoted by $A(\alpha)$ where $A(\alpha) = \{\zeta\alpha + \xi : \zeta \neq 0, \xi \in \mathbb{F}_{q^n}\}$.

Remark 9. We refer to $A(\alpha)$ as an *affine set* containing α where α is an element of degree r over $\mathbb{F}_{q^n}$ and $\zeta, \xi \in \mathbb{F}_{q^n}$. Since $\zeta \neq 0, \xi \in \mathbb{F}_{q^n}$ then to form the set $A(\alpha)$ the number of choices for ζ is $q^n - 1$ and ξ has q^n choices and so $|A(\alpha)| = q^n(q^n - 1)$.

Definition 10. Let $\mathbb{A}$ denote set of all affine sets, i.e., $\mathbb{A} = \{A(\alpha) : \alpha \in \mathbb{S}\}$.

Next, we define a mapping on $\mathbb{S}$ which sends extended irreducible Goppa codes into equivalent extended irreducible Goppa codes.

Definition 11. The relation $\pi_{\zeta_1,\zeta_2,\xi_1,\xi_2,i}$ defined on $\mathbb{S}$ by

$$\pi_{\zeta_1,\zeta_2,\xi_1,\xi_2,i} : \alpha \mapsto \frac{\zeta_1\alpha^{q^i} + \xi_1}{\zeta_2\alpha^{q^i} + \xi_2}$$

fixed i, ζ_j, ξ_j where $0 \leq i \leq nr$, $\zeta_j, \xi_j \in \mathbb{F}_{q^n}$, $j = 1, 2$ and $\zeta_1\xi_2 \neq \zeta_2\xi_1$ is a mapping on $\mathbb{S}$.

Since the scalars ζ_j and ξ_j are defined up to scalar multiplication, we may assume that $\zeta_2 = 1$ or $\xi_2 = 1$ if $\zeta_2 = 0$.

We have the following generalisation:

Theorem 12. (Berger, [1]): *If $\pi_{\zeta_1,\zeta_2,\xi_1,\xi_2,i}(\alpha) = \beta$ then $\overline{C}(\alpha)$ is equivalent to $\overline{C}(\beta)$.*

The map in Definition 11 can be broken up into the composition of two maps as follows:

1. the map $\pi_{\zeta_1,\zeta_2,\xi_1,\xi_2}$ defined on $\mathbb{S}$ by $\pi_{\zeta_1,\zeta_2,\xi_1,\xi_2} : \alpha \mapsto \frac{\zeta_1\alpha+\xi_1}{\zeta_2\alpha+\xi_2}$, and
2. the map $\sigma^i : \alpha \mapsto \alpha^{q^i}$, where σ denotes the Frobenius automorphism of $\mathbb{F}_{q^{nr}}$ leaving $\mathbb{F}_q$ fixed.

From these two maps we give the following two definitions.

Definition 13. Let F denote the set of all maps $\{\pi_{\zeta_1,\zeta_2,\xi_1,\xi_2} : \zeta_j, \xi_j \in \mathbb{F}_{q^n},\ j = 1, 2 \text{ and } \zeta_1\xi_2 \neq \zeta_2\xi_1\}$.

F forms a group under the operation of composition of maps which acts on $\mathbb{S}$.

Definition 14. Let $\alpha \in \mathbb{S}$. Then the *orbit* in $\mathbb{S}$ containing α under the action of F is $O(\alpha) = \{\frac{\zeta_1\alpha+\xi_1}{\zeta_2\alpha+\xi_2} : \zeta_j, \xi_j \in \mathbb{F}_{q^n}, j = 1,2 \text{ and } \zeta_1\xi_2 - \zeta_2\xi_1 \neq 0\}$.

The cardinality of $O(\alpha)$ is found in [8] and we state it in the theorem:

Theorem 15. *For any* $\alpha \in \mathbb{S}$, $|O(\alpha)| = q^{3n} - q^n = (q^n - 1)(q^n)(q^n + 1)$.

Definition 16. Let $\mathbb{O}_F$ denote the set of all orbits in $\mathbb{S}$ under the action of F, i.e., $\mathbb{O}_F = \{O(\alpha) : \alpha \in \mathbb{S}\}$. Observe that $\mathbb{O}_F$ is a partition of the set $\mathbb{S}$.

Note that G acts on the set $\mathbb{O}_F$.

It is shown in [10] that each of the sets $O(\alpha)$ in $\mathbb{O}_F$ can be partitioned into $q^n + 1$ sets. The theorem below provides more details.

Theorem 17. $O(\alpha) = A(\alpha) \cup A(\frac{1}{\alpha}) \cup A(\frac{1}{\alpha+1}) \cup A(\frac{1}{\alpha+\xi_1}) \cup A(\frac{1}{\alpha+\xi_2}) \cup \cdots \cup A(\frac{1}{\alpha+\xi_{q^n-2}})$ *where* $\mathbb{F}_{q^n} = \{0, 1, \xi_1, \xi_2, ..., \xi_{q^n-2}\}$.

Observe that the sets $\mathbb{O}_F$ and $\mathbb{A}$ are different. $\mathbb{O}_F$ is a partition on $\mathbb{S}$ and also $\mathbb{A}$ is a partition on $\mathbb{S}$. The number of elements in $\mathbb{A}$ is $q^n + 1$ times the number of elements in $\mathbb{O}_F$, i.e., $|\mathbb{A}| = (q^n + 1) \times |\mathbb{O}_F|$.

G also acts on $\mathbb{A} = \{A(\alpha) : \alpha \in \mathbb{S}\}$.

3. Main results

3.1. **Technique of counting extended irreducible binary Goppa codes:** We wish to produce an upper bound on the number of inequivalent extended irreducible binary Goppa codes of degree $2p$ and length $2^n + 1$. We intend to achieve this by employing the tools developed for counting the non-extended versions.

In counting the non-extended irreducible Goppa codes we consider the action of H on $\mathbb{S}$. This gives orbits in $\mathbb{S}$ denoted by $A(\alpha)$ called affine sets. We then consider the action of G on the set $\mathbb{A}$ where $\mathbb{A} = \{A(\alpha) : \alpha \in \mathbb{S}\}$. The number of orbits in $\mathbb{A}$ under G gives us an upper bound on the number of inequivalent irreducible Goppa codes.

Now to count extended irreducible Goppa codes we consider the action of F on $\mathbb{S}$. This action induces orbits in $\mathbb{S}$ denoted by $O(\alpha)$. Next we consider the action of G on $\mathbb{O}_F = \{O(\alpha) : \alpha \in \mathbb{S}\}$. The number of orbits in $\mathbb{O}_F$ under G gives us an upper bound on the number of inequivalent extended irreducible Goppa codes.

To find the number of orbits in $\mathbb{A}$ and $\mathbb{O}_F$ we use the Cauchy Frobenius Theorem whose proof can be found in [5]. Since the Cauchy Frobenius Theorem is central in this paper we state it as follows.

Theorem 18 (Cauchy Frobenius Theorem)**.** *Let E be a finite group acting on a set X. For any $e \in E$, let X_e denote the set of elements of X fixed by e. Then the number of orbits in X under the action of E is $\frac{1}{|E|}\sum_{e\in H}|X_e|$.*

3.2. **The cardinality of $\mathbb{S}$:** We begin by counting the number of elements in $\mathbb{S}$. Since we are considering the binary case then from now on ward $q = 2$. We use the lattice of subfields of $\mathbb{F}_{2^{2pn}}$ as done in [6]. **Fig 3.1** shows the lattice of subfields of $\mathbb{F}_{2^{2pn}}$.

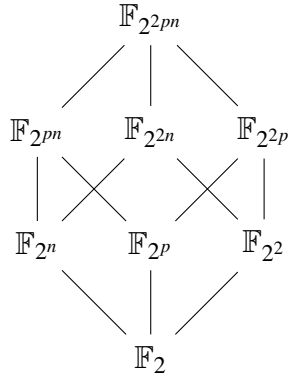

Fig 3.1: Lattice of subfields of $\mathbb{F}_{2^{2pn}}$

Remark 19. The elements of degree $2p$ over $\mathbb{F}_{2^n}$ lie in $\mathbb{F}_{2^{2p}}$ and $\mathbb{F}_{2^{2pn}}$.

To find the number of elements of degree $2p$ in $\mathbb{F}_{2^{2pn}}$ we therefore exclude $\mathbb{F}_{2^{2n}}$ and $\mathbb{F}_{2^{pn}}$ so that, for $\lambda = \frac{p-1}{2}$, we have

$$|\mathbb{S}| = 2^{2pn} - 2^{pn} - 2^{2n} + 2^n = 2^n(2^{\lambda n} - 1)(2^{\lambda n} + 1)(2^{pn} + 2^n - 1)$$

$$= 2^n(2^n-1)(2^n+1)\left[\left(\frac{2^{\lambda n}-1}{2^n-1}\right)\left(\frac{2^{\lambda n}+1}{2^n+1}\right)(2^{pn}+2^n-1)\right]$$
$$= 2^n(2^n-1)(2^n+1)\left[\left(\frac{2^{2\lambda n}-1}{2^{2n}-1}\right)(2^{pn}+2^n-1)\right]$$
$$= 2^n(2^n-1)(2^n+1)\left[\left(\frac{2^{(p-1)n}-1}{2^{2n}-1}\right)(2^{pn}+2^n-1)\right].$$

3.3. **The Action of G on $\mathbb{A}$:** The number of orbits in $\mathbb{A}$ under the action G is found by first counting the number of affine sets in $\mathbb{A}$ which are fixed by the subgroups of G and Cauchy Frobenius Theorem is then applied.

Since we are acting G on $\mathbb{A}$ then it necessary to find the number of elements (affine sets) which are in $\mathbb{A}$. In Section 3.2 we found that $|\mathbb{S}|$ and by Remark 9 $|A(\alpha)| = 2^n(2^n-1)$. So $|\mathbb{A}| = |\mathbb{S}|/(2^n(2^n-1))$.

The cardinality of G is $2pn$. Since G acts on $\mathbb{A}$ then we expect the orbits in $\mathbb{A}$ under the action of the group G to have the length 1, 2, p, $2p$, n, $2n$, pn or $2pn$. Note that every element (affine set) in $\mathbb{A}$ is fixed under $\langle\sigma^{2pn}\rangle$, i.e., σ^{2pn} is the identity in G. We only need to consider the remaining subgroups of G. We begin with the subgroup $\langle\sigma^{pn}\rangle$.

3.3.1. $\langle\sigma^{pn}\rangle$ **is a subgroup of G of order 2:** Suppose the orbit in $\mathbb{A}$ under the action of G containing $A(\alpha)$ contains pn affine sets, i.e, $\{A(\alpha), \sigma(A(\alpha)), \sigma^2(A(\alpha)), ..., \sigma^{pn-1}(A(\alpha))\}$. Then $A(\alpha)$ is fixed by $\langle\sigma^{pn}\rangle$. That is we have $\sigma^{pn}(A(\alpha)) = A(\alpha)$. So we must have $\sigma^{pn}(\alpha) = \alpha^{2^{pn}} = \zeta\alpha + \xi$ for some $\zeta \neq 0, \xi \in \mathbb{F}_{2^n}$. When we apply σ^{pn} twice we obtain $\alpha = \sigma^{2pn}(\alpha) = \sigma^{pn}(\zeta\alpha+\xi) = \zeta^{2^{pn}}\alpha^{2^{pn}} + \xi^{2^{pn}} = \zeta\alpha^{2^{pn}} + \xi = \zeta(\zeta\alpha+\xi)+\xi = \zeta^2\alpha + (\zeta+1)\xi$. We conclude that $\zeta^2 = 1$ otherwise $\zeta^2 \neq 1$ would mean $(1-\zeta^2)\alpha \in \mathbb{F}_{2^n}$ contradicting the fact that $\alpha \in \mathbb{S}$. Since $2 \nmid 2^n - 1$ then $\zeta^2 = 1$ implies $\zeta = 1$.

So consider $\alpha^{2^{pn}} = \alpha + \xi$ for some $\xi \neq 0 \in \mathbb{F}_{2^n}$. If we multiply both sides by ξ^{-1} we get $(\xi^{-1}\alpha)^{2^{pn}} = (\xi^{-1}\alpha) + 1$. Without loss of generality, we may assume that α satisfies the equation

$$x^{2^{pn}} - x - 1 = 0. \tag{1}$$

If α satisfies (1) we observe that all the 2^n elements in the set $\{\alpha+\xi : \xi \in \mathbb{F}_{2^n}\}$ also satisfy (1) while the remaining elements in $A(\alpha)$ do not satisfy. This is so because the equation $(\zeta\alpha+\xi)^{2^{pn}} = \zeta\alpha^{2^{pn}}+\xi = \zeta(\alpha+1)+\xi = \zeta\alpha+\zeta+\xi = (\zeta\alpha+\xi)+1$ holds if and only if $\zeta = 1$. We conclude that if α satisfies (1) then $A(\alpha)$ contains precisely 2^n roots of (1).

We now calculate the number of elements of $\mathbb{S}$ which satisfy (1). We note that

$$x^{2^{pn}} - x - 1 = \prod_{i=1}^{2^{pn-1}} (x^2 - x - \beta_i) \tag{2}$$

where β_i denote all the elements of $\mathbb{F}_{2^{pn}}$ which have trace 1 over $\mathbb{F}_2$. We know that there are precisely 2^{pn-1} such β_i. Some of the β_i's lie in $\mathbb{F}_{2^p}$ and $\mathbb{F}_{2^n}$. The number of β_i's in $\mathbb{F}_{2^p}$ with trace 1 are 2^{p-1}. So the 2^{p-1} quadratic equations corresponding to the $\beta_i \in \mathbb{F}_{2^p}$ have $\mathbb{F}_{2^{2p}}$ as their splitting field. The number of β_i's in $\mathbb{F}_{2^n}$ with trace 1 are 2^{n-1}. So the 2^{n-1} quadratic equations corresponding to the $\beta_i \in \mathbb{F}_{2^n}$ have $\mathbb{F}_{2^{2n}}$ as their splitting field while the remaining $2^{pn-1} - 2^{n-1} - 2^{p-1}$ quadratic equations have $\mathbb{F}_{2^{2pn}}$ as their splitting field. So there are 2^n roots which are in $\mathbb{F}_{2^{2n}}$ (not in $\mathbb{S}$) whereas $2^{pn} - 2^n$ roots lie in $\mathbb{S}$.

Conversely if $\alpha \in \mathbb{S}$ satisfies (1) then $A(\alpha)$ is fixed under $\langle\sigma^{pn}\rangle$. We may conclude that there are precisely $\frac{2^{pn}-2^n}{2^n} = 2^{(p-1)n} - 1$ sets of $A(\alpha)$ fixed under $\langle\sigma^{pn}\rangle$.

3.3.2. $\langle\sigma^{2n}\rangle$ **a subgroup of** G **of order** p**:** Suppose the orbit in $\mathbb{A}$ under the action of G containing $A(\alpha)$ contains $2n$ affine sets. As in Subsection 3.3.1, we have $A(\alpha)$ fixed by $\langle\sigma^{2n}\rangle$ and $\sigma^{2n}(\alpha) = \alpha^{2^{2n}} = \zeta\alpha+\xi$ for some $\zeta \neq 0, \xi \in \mathbb{F}_{2^n}$. Applying σ^{2n} for p times to α we obtain $\alpha = \sigma^{2pn}(\alpha) = \zeta^p\alpha + (\zeta^{p-1}+\zeta^{p-2}+\cdots+\zeta+1)\xi$. We conclude that $\zeta^p = 1$ otherwise $\zeta^p \neq 1$ would mean $(1-\zeta^p)\alpha \in \mathbb{F}_{2^n}$ contradicting the fact that $\alpha \in \mathbb{S}$. Since by assumption $(2^n \pm 1, p) = 1$ then $\zeta^p = 1$ implies $\zeta = 1$.

Now we have $\alpha^{2^{2n}} = \alpha+\xi$ for some $\xi \neq 0 \in \mathbb{F}_{2^n}$. If we multiply both sides by ξ^{-1} we get $(\xi^{-1}\alpha)^{2^{2n}} = \xi^{-1}\alpha + 1$. We assume that α satisfies the equation $x^{2^{2n}} - x - 1 = 0$. Using an argument similar to the one in Subsection 3.3.1, we find all roots of $x^{2^{2n}} - x - 1 = 0$ in $\mathbb{F}_{2^4}$, $\mathbb{F}_{2^{2n}}$, $\mathbb{F}_{2^{4n}}$ and not in $\mathbb{S}$. We conclude that there is no affine set $A(\alpha)$ fixed under $\langle\sigma^{2n}\rangle$.

3.3.3. $\langle\sigma^{n}\rangle$ **a subgroup of** G **of order** $2p$**:** Suppose the orbit in $\mathbb{A}$ under the action of G containing $A(\alpha)$ contains n elements (affine sets). Then, as in Subsection 3.3.1, $A(\alpha)$ is fixed by

$\langle\sigma^n\rangle$ and $\sigma^n(\alpha)=\alpha^{2^n}=\zeta\alpha+\xi$ for some $\zeta\neq 0,\xi\in\mathbb{F}_{2^n}$. When we apply σ^n to α for $2p$ times we have $\alpha=\alpha^{2^{2pn}}=\zeta^{2p}\alpha+(\zeta^{2p-1}+\zeta^{2p-2}+\zeta^{2p-3}+\cdots+\zeta^2+\zeta+1)\xi$. We conclude that $\zeta^{2p}=1$ otherwise $\zeta^{2p}\neq 1$ would mean $(1-\zeta^{2p})\alpha\in\mathbb{F}_{2^n}$ contradicting the fact that $\alpha\in\mathbb{S}$. The possibilities are that $\zeta^{2p}=1$, $\zeta^p=1$ or $\zeta^2=1$. It is clear that $2\nmid(2^n-1)$. Also by assumption $p\nmid(2^n-1)$. So all the three possibilities are impossible since 2, p and $2p$ do not divide 2^n-1. We conclude that $\zeta=1$.

So we have $\alpha^{2^n}=\alpha+\xi$ for some $\xi\neq 0\in\mathbb{F}_{2^n}$. Multiplying both sides by ξ^{-1} we get $(\xi^{-1}\alpha)^{2^n}=\xi^{-1}\alpha+1$. We assume that α satisfies the equation $x^{2^n}-x-1=0$. However, using an argument as the one in Subsection 3.3.1, all roots of $x^{2^n}-x-1$ lie in $\mathbb{F}_{2^2}$, $\mathbb{F}_{2^{2n}}$ and not in $\mathbb{S}$. We conclude that there is no affine set $A(\alpha)$ fixed under $\langle\sigma^n\rangle$.

3.3.4. $\langle\sigma^{2p}\rangle$ **a subgroup of** G **of order** n**:** Suppose the orbit in $\mathbb{A}$ under the action of G containing $A(\alpha)$ contains $2p$ affine sets. Then $A(\alpha)$ is fixed under $\langle\sigma^{2p}\rangle$ and contains some elements which satisfy the equation $x^{2^{2p}}=x$. In [11], it is proved that the number of affine sets fixed by $\langle\sigma^{n_1 r}\rangle$ where n_1 is a divisor of n is $|\mathbb{S}(n_1,r)|/(q^{n_1}(q^{n_1}-1))$. Hence the number of affine sets fixed by $\langle\sigma^{2p}\rangle$ is $|\mathbb{S}(1,2p)|/(2(2-1))=(2^{2p}-2^p-2^2+2)/2=(2^{2p}-2^p-2)/2=2^{2p-1}-2^{p-1}-1$.

3.3.5. $\langle\sigma^p\rangle$ **a subgroup of** G **of order** $2n$**:** Suppose the orbit in $\mathbb{A}$ under the action of G containing $A(\alpha)$ contains p elements (affine sets). Then $A(\alpha)$ is fixed by $\langle\sigma^p\rangle$. So we must have $\sigma^p(\alpha)=\alpha^{2^p}=\zeta\alpha+\xi$ for some $\zeta\neq 0,\xi\in\mathbb{F}_{2^n}$. But if $A(\alpha)$ is fixed under $\langle\sigma\rangle$ then it is also fixed under $\langle\sigma^p\rangle$ since $\langle\sigma^{2p}\rangle\subset\langle\sigma^p\rangle$. So $A(\alpha)$ contains some elements which satisfy $x^{2^{2p}}=x$ and these elements are in $\mathbb{F}_{2^{2p}}\setminus(\mathbb{F}_{2^p}\cup\mathbb{F}_{2^2})$. So assume $\alpha\in\mathbb{F}_{2^{2p}}\setminus(\mathbb{F}_{2^p}\cup\mathbb{F}_{2^2})$ then applying σ^p twice to α we obtain $\alpha=\alpha^{2^{2p}}=\zeta^{2^p}(\zeta\alpha+\xi)+\xi^{2^p}=\zeta^{2^p+1}\alpha+\zeta^{2^p}\xi+\xi^{2^p}$. We conclude that $\zeta^{2^p+1}=1$ otherwise $\zeta^{2^p+1}\neq 1$ would mean $(1-\zeta^{2^p+1})\alpha\in\mathbb{F}_{2^n}$ contradicting the fact that α is of degree $2p$.

We show that 2^p+1 is relatively prime to 2^n-1. That is it suffices to show that $(2^p+1,2^n-1)=1$. We show this by contradiction. Assume that $(2^p+1,2^n-1)\neq 1$. That is there must be some odd prime l which divides both 2^p+1 and 2^n-1. This implies that $2^n\equiv 1\pmod{l}$ and $2^p\equiv -1\pmod{l}$. So $2^p\equiv -1\pmod{l}$ implies $2^{2p}\equiv 1\equiv 2^n\pmod{l}$. Thus $n\equiv 2p$

$(\text{mod } (l-1))$. Since $l-1$ is even then n is also even. This establishes a contradiction since n is an odd prime. Hence $(2^p+1, 2^n-1) = 1$ for odd n.

It is now clear that $\zeta^{2^p+1} = 1$ implies $\zeta = 1$. So we have $\alpha = \alpha + \xi + \xi^{2^p}$. Clearly ξ is in the intersection of the fields of order 2^p and 2^n. Since $(p,n) = 1$ then ξ is 0 or 1. But $\xi = 0$ is impossible since this would mean that α is in $\mathbb{F}_{2^p}$. So ξ must be 1.

Now we have $\alpha^{2^p} = \alpha + 1$. Clearly α satisfies the equation $x^{2^p} - x - 1 = 0$. Observe that $\alpha + 1$ also satisfies the equation $x^{2^p} - x - 1 = 0$ and it is not hard to see that these are the only elements in $A(\alpha)$ which satisfy $x^{2^p} - x - 1 = 0$. Using an argument similar to the one in Subsection 3.3.1 we find $2^p - 2$ roots of $x^{2^p} - x - 1$ in $\mathbb{F}_{2^{2p}} \setminus (\mathbb{F}_{2^p} \cup \mathbb{F}_{2^2})$ and 2 roots in $\mathbb{F}_{2^2}$. Hence we conclude that there are $2^{p-1} - 1$ affine sets fixed under $\langle \sigma^p \rangle$.

3.3.6. $\langle \sigma^2 \rangle$ **a subgroup of** G **of order** pn**:** Suppose the orbit in $\mathbb{A}$ under the action of G containing $A(\alpha)$ contains 2 elements (affine sets). Then $A(\alpha)$ is fixed by $\langle \sigma^2 \rangle$. That is we must have $\sigma^2(\alpha) = \alpha^{2^2} = \zeta\alpha + \xi$ for some $\zeta \neq 0, \xi \in \mathbb{F}_{2^n}$. But $\alpha^4 = \zeta\alpha + \xi$ implies that α is a root of an equation of degree 4 contradicting the fact that α is of degree $2p$ over $\mathbb{F}_{2^n}$ (recall that p is odd prime). Hence we conclude that there is no affine set fixed under $\langle \sigma^2 \rangle$.

3.3.7. $\langle \sigma \rangle$ **a subgroup of** G **of order** $2pn$**:** Suppose the orbit in $\mathbb{A}$ under the action of G containing $A(\alpha)$ contains 1 element (affine set). Then $A(\alpha)$ is fixed by $\langle \sigma \rangle$. That is we must have $\sigma(\alpha) = \alpha^2 = \zeta\alpha + \xi$ for some $\zeta \neq 0, \xi \in \mathbb{F}_{2^n}$. But $\alpha^2 = \zeta\alpha + \xi$ implies that α is a root of an equation of degree 2 contradicting the fact that α is of degree $2p$ over $\mathbb{F}_{2^n}$. Hence we conclude that there is no affine set fixed under $\langle \sigma \rangle$.

3.4. **Applying the Cauchy Frobenius Theorem:** We use Table **3.4.1** to present the information in Section 3.3 . This table shows the number of affine sets which are fixed under the action of various subgroups of G. The subgroups are listed in ascending order of the number of elements in the subgroup. Only subgroups which fix some elements have been included. So the first row is the subgroup $\langle \sigma^{2pn} \rangle$ which is merely the trivial subgroup containing the identity. Column 3 lists the number of elements in subgroup which are not already counted in subgroups in the rows above it in the table. This is to avoid repetition when we multiply column 3 by

column 4 in order to get the total number of fixed affine sets by the elements in G.

Subgroup of G	Order of Subgroup	No. of elements not in previous subgroup	No. of fixed affine sets	Product of columns 3 and 4
$\langle\sigma^{2pn}\rangle$	1	1	$\lvert\mathbb{S}\rvert/(2^n(2^n-1))$	$\lvert\mathbb{S}\rvert/(2^n(2^n-1))$
$\langle\sigma^{pn}\rangle$	2	1	$2^{(p-1)n}-1$	$2^{(p-1)n}-1$
$\langle\sigma^{2p}\rangle$	n	$n-1$	$2^{2p-1}-2^{p-1}-1$	$(n-1)(2^{2p-1}-2^{p-1}-1)$
$\langle\sigma^{p}\rangle$	$2n$	$n-1$	$2^{p-1}-1$	$(n-1)(2^{p-1}-1)$

Table **3.4.1**

Remark 20. The total number of fixed affine sets is the sum of the column which gives us $|\mathbb{S}|/(2^n(2^n-1))+(2^{(p-1)n}-1)+(n-1)(2^{2p-1}-2)$. By the Cauchy Frobenius Theorem, the number of orbits in $\mathbb{A}$ under the action of G is

$$\frac{|\mathbb{S}|/(2^n(2^n-1))+(2^{(p-1)n}-1)+(n-1)(2^{2p-1}-2)}{2pn}$$

Remark 21. The number of orbits in $\mathbb{A}$ under the action of G gives us an upper bound on the number of irreducible Goppa codes.

3.5. **The Action of G on $\mathbb{O}_F$:** To find the number of orbits in $\mathbb{O}_F$ under the action of G we count the number of elements in $\mathbb{O}_F$ which are fixed by the various subgroups of G and then apply Cauchy Frobenius Theorem.

Since we are dealing with the action of G on $\mathbb{O}_F$ then it is crucial that we find the number of elements which are in $\mathbb{O}_F$. In Section 3.2, we found that $|\mathbb{S}|=2^n(2^n-1)(2^n+1)\left[\left(\frac{2^{(p-1)n}-1}{2^{2n}-1}\right)(2^{pn}+2^n-1)\right]$ and by Theorem 15, $|O(\alpha)|=2^n(2^n-1)(2^n+1)$. So $|\mathbb{O}_F|=|\mathbb{S}|/(2^n(2^n-1)(2^n+1))$.

As in Section 3.3, the orbits in $\mathbb{O}_F$ under the action of G are expected to have the length 1, 2, p, $2p$, n, $2n$, pn or $2pn$. Note that every $O(\alpha)$ in $\mathbb{O}_F$ is fixed under $\langle\sigma^{2pn}\rangle$. We only need to consider the remaining subgroups of G. We start with the subgroup $\langle\sigma^{pn}\rangle$.

3.5.1. $\langle\sigma^{pn}\rangle$ **a subgroup of G of order 2:** Suppose $O(\alpha)\in\mathbb{O}_F$ is fixed under $\langle\sigma^{pn}\rangle$. Then $\langle\sigma^{pn}\rangle$ acts on $O(\alpha)=A(\alpha)\cup A(\frac{1}{\alpha})\cup A(\frac{1}{\alpha+1})\cup A(\frac{1}{\alpha+\xi_1})\cup A(\frac{1}{\alpha+\xi_2})\cup\cdots\cup A(\frac{1}{\alpha+\xi_{2^n-2}})$. $O(\alpha)$ is

considered as a set of 2^n+1 affine sets. $\langle\sigma^{pn}\rangle$ partitions this set of 2^n+1 affine sets. The only possibility are orbits of length 1 or 2. Since $O(\alpha)$ contains an odd number of affine sets then the possibility that all orbits are of length 2 is excluded. So there has to be at least one orbit of length 1, i.e., $O(\alpha)$ must contain an affine set which is fixed under $\langle\sigma^{pn}\rangle$. By Subsection 3.3.1, there are $2^{(p-1)n}-1$ such affine sets. We claim that each of $O(\alpha)$ fixed under $\langle\sigma^{pn}\rangle$ in $\mathbb{O}_F$ contains precisely one affine set which is fixed under $\langle\sigma^{pn}\rangle$. It suffices to show that $O(\alpha)$ cannot contain two affine sets which are fixed under $\langle\sigma^{pn}\rangle$. Without loss of generality, suppose $A(\alpha)$ is fixed under $\langle\sigma^{pn}\rangle$. We show that none of the affine sets after $A(\alpha)$ in the above decomposition of $O(\alpha)$ is fixed under $\langle\sigma^{pn}\rangle$. This is done by showing that no element in any of these affine sets satisfies the equation $x^{2^{pn}}-x-1=0$ (see Equation (1) in Subsection 3.3.1). It is sufficient to show that no element in $A(\frac{1}{\alpha})$ satisfies $x^{2^{pn}}-x-1=0$. A typical element in $A(\frac{1}{\alpha})$ has the form $\frac{\zeta}{\alpha}+\xi$ and substituting this in $x^{2^{pn}}-x-1$ we get $(\frac{\zeta}{\alpha}+\xi)^{2^{pn}}-(\frac{\zeta}{\alpha}+\xi)-1=\frac{\alpha^2+\alpha+\zeta}{\alpha^2+\alpha}\neq 0$, since α is an element of degree $2p$ over $\mathbb{F}_{2^n}$. We conclude that $A(\frac{1}{\alpha})$ is not fixed under $\langle\sigma^{pn}\rangle$ and in fact $A(\alpha)$ is the only affine set in $O(\alpha)$ fixed under $\langle\sigma^{pn}\rangle$. It follows that the number of $O(\alpha)$ in $\mathbb{O}_F$ which are fixed under $\langle\sigma^{pn}\rangle$ is $2^{(p-1)n}-1$.

3.5.2. $\langle\sigma^{2n}\rangle$ **a subgroup of** G **of order** p**:** Suppose $O(\alpha)\in\mathbb{O}_F$ is fixed under $\langle\sigma^{2n}\rangle$. Then $\langle\sigma^{2n}\rangle$ acts on $O(\alpha)=A(\alpha)\cup A(\frac{1}{\alpha})\cup A(\frac{1}{\alpha+1})\cup A(\frac{1}{\alpha+\xi_1})\cup A(\frac{1}{\alpha+\xi_2})\cup\cdots\cup A(\frac{1}{\alpha+\xi_{2^n-2}})$. $O(\alpha)$ is considered as the set of 2^n+1 affine sets. $\langle\sigma^{2n}\rangle$ partitions this set of 2^n+1 affine sets. The only possibility are orbits of length 1 or p. By Subsection 3.3.2, no affine set is fixed under $\langle\sigma^{2n}\rangle$ so we preclude the possibility of length 1. We remain to show the possibility of length p. Since by assumption $(2^n\pm 1,p)=1$ then we also preclude the possibility of all orbits to have length p. Hence it follows that $\langle\sigma^{2n}\rangle$ does not fix any $O(\alpha)$ in $\mathbb{O}_F$.

3.5.3. $\langle\sigma^{n}\rangle$ **a subgroup of** G **of order** $2p$**:** Suppose $O(\alpha)\in\mathbb{O}_F$ is fixed under $\langle\sigma^{n}\rangle$. Then $\langle\sigma^{n}\rangle$ acts on $O(\alpha)$ which is considered as a set of 2^n+1 affine sets. $\langle\sigma^{n}\rangle$ partitions this set of 2^n+1 affine sets. The only possibility are orbits of length 1, 2, p or $2p$. By Subsection 3.3.3, no affine set is fixed under $\langle\sigma^{n}\rangle$ so the possibility of length 1 is precluded. Since $O(\alpha)$ contains an odd number of affine sets then the possibility that all orbits are of even length is also precluded. Orbits of the lengths 2 and p or 2, p and $2p$ in each $O(\alpha)$ are also possible. We claim that none of these possibilities is true. Suppose $O(\alpha)$ is fixed under the action of $\langle\sigma^{n}\rangle$ and contains an

orbit of length p. This implies that $\langle\sigma^{pn}\rangle$ fixes p affine sets in $O(\alpha)$ since $\langle\sigma^{pn}\rangle \subset \langle\sigma^{n}\rangle$. But this is a contradiction since by Subsection 3.3.1 only one affine set is fixed in each $O(\alpha)$ fixed under $\langle\sigma^{pn}\rangle$. Hence we conclude that no $O(\alpha)$ is fixed under $\langle\sigma^{n}\rangle$.

3.5.4. $\langle\sigma^{2p}\rangle$ **a subgroup of** G **of order** n**:** Suppose $O(\alpha) \in \mathbb{O}_F$ is fixed under $\langle\sigma^{2p}\rangle$. Then $\langle\sigma^{2p}\rangle$ acts on $O(\alpha)$ which is seen as a set of 2^n+1 affine sets. $\langle\sigma^{2p}\rangle$ partitions this set of 2^n+1 affine sets. The only possibility are orbits of length 1 or n. Since $2^n+1 \equiv 2+1 = 3 \pmod{n}$ (by Fermat Little Theorem) then $n \nmid 2^n+1$ and the possibility that all orbits are of length n is precluded. So there must be at least three affine sets in $O(\alpha)$ fixed under $\langle\sigma^{2p}\rangle$. We claim that there are exactly three affine sets in $O(\alpha)$ which are fixed under $\langle\sigma^{2p}\rangle$. Recall that $O(\alpha) = A(\alpha) \cup A(\frac{1}{\alpha}) \cup A(\frac{1}{\alpha+1}) \cup A(\frac{1}{\alpha+\xi_1}) \cup A(\frac{1}{\alpha+\xi_2}) \cup A(\frac{1}{\alpha+\xi_3}) \cup \cdots \cup A(\frac{1}{\alpha+\xi_{2^n-2}})$. Without loss of generality, suppose $A(\alpha)$ in $O(\alpha)$ is fixed under $\langle\sigma^{2p}\rangle$. So, by Subsection 3.3.4, $A(\alpha)$ contains a fixed point, i.e., some elements of $A(\alpha)$ satisfy the equation $x^{2^{2p}} = x$. Assume that α satisfies $x^{2^{2p}} = x$. It is clear that $\alpha+1$ in $A(\alpha)$ also satisfies $x^{2^{2p}} = x$. Since $(\frac{1}{\alpha})^{2^{2p}} = \frac{1}{\alpha}$ and $(\frac{1}{\alpha+1})^{2^{2p}} = \frac{1}{\alpha+1}$ it is clear that $A(\frac{1}{\alpha})$ and $A(\frac{1}{\alpha+1})$ also contain fixed points, i.e., $A(\frac{1}{\alpha})$ and $A(\frac{1}{\alpha+1})$ are also fixed. We now show that no affine set after $A(\frac{1}{\alpha+1})$ in the decomposition of $O(\alpha)$ is fixed under $\langle\sigma^{2p}\rangle$. It is sufficient to show that an arbitrary affine set after $A(\frac{1}{\alpha+1})$ in the decomposition of $O(\alpha)$ is not fixed under $\langle\sigma^{2p}\rangle$. First observe that, for $\nu \in \mathbb{F}_{2^n} \setminus \{0,1\}$, we have $\nu^{2^{2p}} \neq \nu$ since $(2p,n) = 1$. Furthermore observe that, for $\frac{\zeta}{\alpha+\nu} + \xi \in A(\frac{1}{\alpha+\nu})$ where $\nu \in \mathbb{F}_{2^n} \setminus \{0,1\}$, we have $(\frac{\zeta}{\alpha+\nu} + \xi)^{2^{2p}} = \frac{\zeta^{2^{2p}}}{\alpha+\nu^{2^{2p}}} + \xi^{2^{2p}} = \frac{\zeta^{2^{2p}}}{\alpha+\eta} + \xi^{2^{2p}} \in A(\frac{1}{\alpha+\eta})$ which implies that $\sigma^{2p}(A(\frac{1}{\alpha+\nu})) = A(\frac{1}{\alpha+\eta})$. It is clear that $A(\frac{1}{\alpha+\nu})$ and $A(\frac{1}{\alpha+\eta})$ are two different affine sets, thus proving that $A(\frac{1}{\alpha+\nu})$ is not fixed under $\langle\sigma^{2p}\rangle$. Therefore $A(\alpha)$, $A(\frac{1}{\alpha})$ and $A(\frac{1}{\alpha+1})$ are the only affine sets fixed under $\langle\sigma^{2p}\rangle$. By Subsection 3.3.4, there are $2^{2p-1} - 2^{p-1} - 1$ affine sets which are fixed under $\langle\sigma^{2p}\rangle$. Hence the number of $O(\alpha)$ in $\mathbb{O}_F$ which are fixed under $\langle\sigma^{2p}\rangle$ is $(2^{2p-1} - 2^{p-1} - 1)/3$.

3.5.5. $\langle\sigma^{p}\rangle$ **a subgroup of** G **of order** $2n$**:** Suppose $O(\alpha) \in \mathbb{O}_F$ is fixed under $\langle\sigma^{p}\rangle$. Then $\langle\sigma^{p}\rangle$ acts on $O(\alpha)$ which is seen as a set of 2^n+1 affine sets. $\langle\sigma^{p}\rangle$ partitions this set of 2^n+1 affine sets. The only possibility are orbits of length 1, 2, n or $2n$. We first consider the possibility of a fixed $O(\alpha)$ under $\langle\sigma^{p}\rangle$ with no affine set fixed under $\langle\sigma^{p}\rangle$, i.e., the possibility that $O(\alpha)$ contains orbits of length 2, n or $2n$. Since $2^n+1 \equiv 3 \pmod{n}$ then the possibility that all orbits

are of length n or $2n$ is excluded. The fact that $O(\alpha)$ contains an odd number of affine sets precludes the possibility that all orbits are of even length. We now consider the possibility of x affine sets partitioned in orbits of length 2 and 2^n+1-x affine sets partitioned in orbits of length n or $2n$, i.e., $2^n+1-x \equiv 0 \pmod{n}$. Since when we divide n into 2^n+1 the remainder is 3 then the only possible values of x are of the form $kn+3$ where k is an odd positive integer. The least value of k such that $2 \mid (kn+3)$ is clearly $k=1$. But the possibility of $n+3$ affine sets partitioned in orbits of length 2 would mean that there exist a fixed $O(\alpha)$ under the action of $\langle\sigma^{2p}\rangle$ which contains $n+3$ affine sets fixed under $\langle\sigma^{2p}\rangle$ contradicting Subsection 3.5.4 which says that every fixed $O(\alpha)$ under $\langle\sigma^{2p}\rangle$ contains three fixed affine sets under $\langle\sigma^{2p}\rangle$. Using a similar argument, it is not hard to see that for any value of k it is impossible for an $O(\alpha)$ fixed under $\langle\sigma^{p}\rangle$ to have orbit lengths of 2, n and $2n$. So there must be at least an affine set in $O(\alpha)$ fixed under $\langle\sigma^{p}\rangle$. We claim that there is only one affine set in $O(\alpha)$ fixed under $\langle\sigma^{p}\rangle$. By Subsection 3.3.5, there are 3 affine sets fixed under $\langle\sigma^{p}\rangle$. Each of these affine sets fixed under $\langle\sigma^{p}\rangle$ contains some elements which satisfy the equation $x^{2^p}-x-1=0$. We know that $O(\alpha)=A(\alpha)\cup A(\frac{1}{\alpha})\cup A(\frac{1}{\alpha+1})\cup A(\frac{1}{\alpha+\xi_1})\cup A(\frac{1}{\alpha+\xi_2})\cup A(\frac{1}{\alpha+\xi_3})\cup\cdots\cup A(\frac{1}{\alpha+\xi_{2^n-2}})$. Without loss of generality, suppose $A(\alpha)$ is fixed under $\langle\sigma^{p}\rangle$. Assume that α satisfies $x^{2^p}-x-1=0$. It is clear that $\alpha+1$ also satisfies the equation $x^{2^p}-x-1=0$. Observe that, for $\frac{\zeta}{\alpha}+\xi \in A(\frac{1}{\alpha})$, we have $(\frac{\zeta}{\alpha}+\xi)^{2^p}=\frac{\zeta^{2^p}}{\alpha+1}+\xi^{2^p}\in A(\frac{1}{\alpha+1})$ and similarly $(\frac{\zeta}{\alpha+1}+\xi)^{2^p}=\frac{\zeta^{2^p}}{\alpha}+\xi^{2^p}\in A(\frac{1}{\alpha})$ which imply that $\sigma^p(A(\frac{1}{\alpha}))=A(\frac{1}{\alpha+1})$ and $\sigma^p(A(\frac{1}{\alpha+1}))=A(\frac{1}{\alpha})$. We conclude that $A(\frac{1}{\alpha})$ and $A(\frac{1}{\alpha+1})$ form an orbit of length 2. We remain to show that no affine set after $A(\frac{1}{\alpha+1})$ in the decomposition of $O(\alpha)$ is fixed under $\langle\sigma^{p}\rangle$. Since $\langle\sigma^{2p}\rangle$ does not fix any affine set after $A(\frac{1}{\alpha+1})$ in the decomposition of $O(\alpha)$ (by Subsection 3.5.4) then we conclude that $\langle\sigma^{p}\rangle$ does not also fix any of these affine sets. Therefore $A(\alpha)$ is the only affine set fixed in $O(\alpha)$ under $\langle\sigma^{p}\rangle$. Hence the number of $O(\alpha)$ in $\mathbb{O}_F$ which are fixed under $\langle\sigma^{p}\rangle$ is $2^{p-1}-1$.

3.5.6. $\langle\sigma^2\rangle$ **a subgroup of** G **of order** pn**:** Suppose $O(\alpha)\in\mathbb{O}_F$ is fixed under $\langle\sigma^2\rangle$. That is we have $\sigma^2(O(\alpha))=O(\alpha)$. So we must have $\sigma^2(\alpha)=\alpha^{2^2}=\frac{\zeta_1\alpha+\xi_1}{\zeta_2\alpha+\xi_2}$ where $\zeta_j,\xi_j\in\mathbb{F}_{q^n}$, $j=1,2$ and $\zeta_1\xi_2\neq\zeta_2\xi_1$. But $\alpha^{2^2}=\frac{\zeta_1\alpha+\xi_1}{\zeta_2\alpha+\xi_2}$ implies that α is a root of an equation of degree 5 which contradicts the fact that α is of degree $2p$ over $\mathbb{F}_{2^n}$. So we conclude that there is no $O(\alpha)$ in $\mathbb{O}_F$ fixed under $\langle\sigma^2\rangle$.

3.5.7. $\langle\sigma\rangle$ **a subgroup of** G **of order** $2pn$**:** Suppose $O(\alpha) \in \mathbb{O}_F$ is fixed under $\langle\sigma\rangle$. That is we have $\sigma(O(\alpha)) = O(\alpha)$. So we must have $\sigma(\alpha) = \alpha^2 = \frac{\zeta_1\alpha+\xi_1}{\zeta_2\alpha+\xi_2}$ where $\zeta_j, \xi_j \in \mathbb{F}_{q^n}$, $j = 1,2$ and $\zeta_1\xi_2 \neq \zeta_2\xi_1$. But $\alpha^2 = \frac{\zeta_1\alpha+\xi_1}{\zeta_2\alpha+\xi_2}$ implies that α is a root of an equation of degree 3 contradicting the fact that α is of degree $2p$ over $\mathbb{F}_{2^n}$. So we conclude that there is no $O(\alpha)$ in $\mathbb{O}_F$ fixed under $\langle\sigma\rangle$.

3.6. **Applying the Cauchy Frobenius Theorem:** As in Section 3.4 we present the information on the action of G on $\mathbb{O}_F$ in Table **3.6.1** which gives the number of $O(\alpha)$ in $\mathbb{O}_F$ fixed under various subgroups of G.

Subgroup of G	Order of Subgroup	No. of elements not in previous subgroup	No. of fixed $O(\alpha)$	Product of columns 3 and 4
$\langle\sigma^{2pn}\rangle$	1	1	$\lvert\mathbb{S}\rvert/(2^n(2^n-1)(2^n+1))$	$\lvert\mathbb{S}\rvert/(2^n(2^n-1)(2^n+1))$
$\langle\sigma^{pn}\rangle$	2	1	$2^{(p-1)n}-1$	$2^{(p-1)n}-1$
$\langle\sigma^{2p}\rangle$	n	$n-1$	$(2^{2p-1}-2^{p-1}-1)/3$	$(n-1)(2^{2p-1}-2^{p-1}-1)/3$
$\langle\sigma^{p}\rangle$	$2n$	$n-1$	$(2^{p-1}-1)$	$(n-1)(2^{p-1}-1)$

Table **3.6.1**

Remark 22. The total number of fixed $O(\alpha)$ is the sum of the column which gives us $|\mathbb{S}|/(2^n(2^n-1)(2^n+1)+(2^{(p-1)n}-1)+(n-1)(2^{2p-1}+2^p-4)/3$. By Section 3.2, $|\mathbb{S}| = 2^n(2^n-1)(2^n+1)\left[\left(\frac{2^{(p-1)n}-1}{2^{2n}-1}\right)(2^{pn}+2^n-1)\right]$. So applying the Cauchy Frobenius Theorem, the number of orbits in $\mathbb{A}$ under the action of G is

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

Since our goal in this paper was to obtain this main result then we state it in the theorem as follows:

Theorem 23. *Let n and p be odd primes such that and $p \neq n$ and $(2^n \pm 1, p) = 1$. Then the number of inequivalent extended irreducible binary Goppa codes of degree $2p$ and length 2^n+1*

is at most

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

Example 24. The table below compares the upper bound on the number of extended irreducible binary Goppa codes of degree $2p$ and length 2^n+1 and non-extended versions of length 2^n, respectively. The bounds on the number of the two versions of codes are obtained using Remark 20 and Theorem 23.

r	n	Number of extended irreducible Goppa codes	Number of irreducible Goppa codes
10	7	8,042,636,909,673	1,037,499,670,492,467
	11	1,373,779,668,165,694,887,189	2,814,874,539,743,974,305,462,579
	13	19,045,231,657,451,944,973,334,135	156,037,582,969,219,989,103,853,977,395

Conflict of Interests

The author declares that there is no conflict of interests.

REFERENCES

[1] P. Berger, Goppa and related Codes Invariant under a Prescribed Permutation, *IEEE Trans. IT* 46 (2000) 2628-2633.

[2] C.L. Chen, Equivalent irreducible Goppa codes, *IEEE Trans. IT* 24 (1978) 766-769.

[3] H. Dinh, C. Moore, A. Russell, *The McEliece Cryptosystem Resists Quantum Fourier Sampling Attacks;* arXiv:1008.2390 [cs.CR], (2010).

[4] P. Loidreau, N. Sendrier, Weak keys in the McEliece public-key cryptosystem, *IEEE Transactions on Information Theory*, pp. 1207-1211, available at http://perso.univ-rennes1.fr/pierre.loidreau/articles/ieee-it/Cles_Faibles.pdf, (2001).

[5] I.M. Isaacs, *Algebra: A Graduate Text*, Brooks/Cole, Pacific Grove, CA., (1994).

[6] K. Magamba, J.A. Ryan, Counting Irreducible Polynomials of degree r over $\mathbb{F}_{q^n}$ and Generating Goppa Codes using the Lattice of Subfields of $\mathbb{F}_{q^{nr}}$, *J. Discrete Math.*, 2014 (2014), Article ID 263179, 4 pages.

[7] A. Musukwa, K. Magamba, J.A. Ryan, Enumeration of extended irreducible binary Goppa codes of degree 2^m and length 2^n+1. *J. Algebra Comb. Discrete Struct. Appl.* 4 (2017), 235-246.

[8] J.A. Ryan, Counting Extended Irreducible Binary Quartic Goppa Codes, *IEEE Trans. IT*, 61 (3) (2015), 1-5.

[9] J.A. Ryan, Counting Extended Irreducible Goppa Codes, *J. Discrete Math.*, 2014 (2014), Article ID 871871, 4 pages.

[10] J.A. Ryan, A New Connection between Irreducible and Extended Irreducible Goppa Codes, *SAMSA 2012 Proceedings*, (2012) pp 152-154.

[11] J.A. Ryan, *Irreducible Goppa Codes,* Phd Dissertation, University College Cork, (2004).