Open Journal of
Discrete Applied Mathematics

PSR Press

Article

The number of extended irreducible binary Goppa codes of degree $(2\ell)^m$ and length $2^n + 1$

Augustine Musukwa[1,2,*]

[1] Department of Mathematics, University of Trento, Via Sommarive, 14, 38123 Povo TN, Italy.
[2] Department of Mathematics and Statistics, Mzuzu University, P/Bag 201, Mzuzu 2, Malawi.
[*] Correspondence: augustinemusukwa@gmail.com

Received: 19 November 2018; Accepted: 31 December 2018; Published: 24 February 2019.

Abstract: Let n and ℓ be odd prime numbers such that $\ell \neq n$ and $(\ell, 2^n \pm 1) = 1$. We produce an upper bound on the number of inequivalent extended irreducible binary Goppa codes of degree $(2\ell)^m$, with $m \geq 1$ and length $2^n + 1$.

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

MSC: 11T71, 68R99.

1. Introduction

In this paper we consider Goppa codes which form a subclass of alternant codes. This family of codes was named after V.D. Goppa who described it in the early 1970's. These codes have an interesting algebraic structure and contain good parameters. Goppa codes are believed to have high practical value. Some of the examples which are mostly named as direct application of Goppa codes are the McEliece and Niederreiter cyptosystems.

The McEliece cryptosystem is believed to be a cryptosystem which may have potential to withstand attack by quantum computers [1,2]. However, what could be worrisome about this cryptosystem is that it chooses a Goppa code at random as its key yet the exact number of these codes for given parameters is not known. Can't a brutal-force search, via equivalence of codes, be mounted by an adversary so as to find the key? This simply tells us how important the knowledge of the number of inequivalent Goppa codes for fixed parameters could facilitate in the evaluation of the security of such a cryptosystem. We find the best upper bound, available today, on the number of inequivalent irreducible Goppa codes in [3]. Our concern is to find an upper bound on the number of inequivalent extended irreducible Goppa codes. Some recent attempts to count inequivalent extended irreducible Goppa codes can be found in [4–7]. In particular, this paper seeks to find a tight upper bound on the number of inequivalent extended irreducible binary Goppa codes of degree $(2\ell)^m$ and length $2^n + 1$ where n and ℓ are odd prime numbers such that $\ell \neq n$, $(\ell, 2^n \pm 1) = 1$ and $m \geq 1$ is a positive integer. The tools which were used to count the non-extended versions (see [3]) are recalled in this paper.

2. Preliminaries

We encourage the reader, whether familiar with the content presented or not, to go through this section for the sake of acquaintance with the notation used. 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 [8] 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 [8].)

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, [3]): 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 1. 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 9. 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 10. 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 11. *(Berger, [9]): If $\pi_{\zeta_1,\zeta_2,\xi_1,\xi_2,i}(\alpha) = \beta$ then $\overline{C}(\alpha)$ is equivalent to $\overline{C}(\beta)$.*

We also break up the map in Definition 10 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 12. 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 and it acts on $\mathbb{S}$.

Definition 13. 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 [6] and we state it as follow:

Theorem 14. *For any $\alpha \in \mathbb{S}$, $|O(\alpha)| = q^{3n} - q^n = q^n(q^n - 1)(q^n + 1)$.*

Definition 15. 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 $\mathbb{S}$.

G acts on the set $\mathbb{O}_F$ (see [7]). The sets $O(\alpha)$ in $\mathbb{O}_F$ can be partitioned into $q^n + 1$ sets. The theorem below provides more details.

Theorem 16. $O(\alpha) = A(\alpha) \cup A(\frac{1}{\alpha}) \cup A(\frac{1}{\alpha+1}) \cup A(\frac{1}{\alpha+\xi_1}) \cup A(\frac{1}{\alpha+\xi_2}) \cup \cdots \cup A(\frac{1}{\alpha+\xi_{q^n-2}})$ *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., $|\mathbb{A}| = (q^n + 1) \times |\mathbb{O}_F|$. It is worth mentioning that G also acts on $\mathbb{A} = \{A(\alpha) : \alpha \in \mathbb{S}\}$ (see [6]).

3. Main results

3.1. Technique of counting extended irreducible binary Goppa codes

We are going to produce an upper bound on the number of inequivalent extended irreducible binary Goppa codes of degree $(2\ell)^m$ and length 2^n+1 where $m \geq 1$, $\ell \neq n$ and $(\ell, 2^n \pm 1) = 1$. We consider the tools, in [3], employed to count the non-extended irreducible binary Goppa codes and those used to count the extended irreducible binary Goppa codes of degrees 4, 2^m and $2p$ (with $m \geq 1$ and p odd prime) in [4–6], respectively.

In counting the non-extended irreducible Goppa codes the action of H on $\mathbb{S}$ is considered. This induces orbits in $\mathbb{S}$ which are denoted by $A(\alpha)$ as seen in previous section. We then consider the action of G on the set $\mathbb{A}$ (recall that $\mathbb{A} = \{A(\alpha) : \alpha \in \mathbb{S}\}$) and the number of orbits induced gives us an upper bound on the number of inequivalent irreducible Goppa codes.

To count extended irreducible Goppa codes the action of F on $\mathbb{S}$ is considered. This action induces orbits in $\mathbb{S}$ denoted by $O(\alpha)$. The action of G on $\mathbb{O}_F = \{O(\alpha) : \alpha \in \mathbb{S}\}$ is then considered and the number of orbits induced gives us an upper bound on the number of inequivalent extended irreducible Goppa codes. It is worth pointing out that the action of G on $\mathbb{O}_F$ largely depends on the results found when acting G on $\mathbb{A}$.

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 [10]. Since the Cauchy Frobenius Theorem is central in this paper we state it as follows:

Theorem 17 (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 elements in $\mathbb{S}$. Since we are considering the binary case then from now onwards $q = 2$. We consider the degree $r = (2\ell)^m$ where $m \geq 1$ and $\ell \nmid (2^n \pm 1)$. To count elements in $\mathbb{S}$, the set of all elements of degree $(2\ell)^m$ in $\mathbb{F}_{2^{(2\ell)^m n}}$, we use the principle of inclusion-exclusion as explained in [11]. That is we simply exclude elements in the subfields $\mathbb{F}_{2^{(2^{m-1}\ell^m)n}}$ and $\mathbb{F}_{2^{(2^m\ell^{m-1})n}}$. Since $\mathbb{F}_{2^{(2^{m-1}\ell^m)n}} \cap \mathbb{F}_{2^{(2^m\ell^{m-1})n}} = \mathbb{F}_{2^{(2^{m-1}\ell^{m-1})n}}$ then we have $|\mathbb{S}| = 2^{(2\ell)^m n} - 2^{2^{m-1}\ell^m n} - 2^{2^m\ell^{m-1}n} + 2^{(2\ell)^{m-1}n}$.

For the sake of our main result, it is pertinent to factorize $|\mathbb{S}|$ to some form which will make sense later. Let $\gamma = 2^n$ and $\lambda = (2\ell)^{m-1}$. We have

$$\begin{aligned} |\mathbb{S}| &= \gamma^{2\ell\lambda} - \gamma^{\ell\lambda} - \gamma^{2\lambda} + \gamma^{\lambda} = (\gamma^{2\ell\lambda} - \gamma^{\ell\lambda}) - (\gamma^{2\lambda} - \gamma^{\lambda}) \\ &= (\gamma^{2\lambda} - \gamma^{\lambda})(\gamma^{(2\ell-2)\lambda} + \gamma^{(2\ell-3)\lambda} + \cdots + \gamma^{\ell\lambda} + \gamma^{(\ell-1)\lambda} - 1) \end{aligned} \tag{1}$$

Observe that $\ell - 1$ is even since ℓ is an old prime and $\lambda = 1$ if $m = 1$. In this case, by Equation 1, we have

$$\begin{aligned} |\mathbb{S}| &= (\gamma^2 - \gamma)(\gamma^{(2\ell-2)} + \gamma^{(2\ell-3)} + \cdots + \gamma^{(\ell-1)} - 1) \\ &= \gamma(\gamma-1)(\gamma+1)\left(\sum_{i=1}^{(\ell-1)/2}\gamma^{2(\ell-i)-1} + \sum_{i=0}^{\ell-2}(-1)^{i+1}\gamma^i\right) \end{aligned} \tag{2}$$

For $m > 1$, we have $\lambda > 1$ even. By Equation 1, we have

$$
\begin{aligned}
|\mathbb{S}| &= (\gamma^{2\lambda}-\gamma^{\lambda})\left(\left(\sum_{i=0}^{\ell-1}\gamma^{(\ell-1+i)\lambda}\right)-1\right)\\
&= \gamma^{\lambda}(\gamma^{\lambda}-1)\left(\left(\sum_{i=0}^{\ell-1}\gamma^{(\ell-1+i)\lambda}\right)-1\right)\\
&= \gamma^{\lambda}(\gamma^{2}-1)\left(\sum_{i=0}^{(\lambda-2)/2}\gamma^{2i}\right)\left(\left(\sum_{i=0}^{\ell-1}\gamma^{(\ell-1+i)\lambda}\right)-1\right)\\
&= \gamma(\gamma-1)(\gamma+1)\gamma^{\lambda-1}\left(\sum_{i=0}^{(\lambda-2)/2}\gamma^{2i}\right)\left(\left(\sum_{i=0}^{\ell-1}\gamma^{(\ell-1+i)\lambda}\right)-1\right). \qquad (3)
\end{aligned}
$$

3.3. The number of fixed affine sets in $\mathbb{A}$

Observe that the group G in Definition 7 is a cyclic group of order $(2\ell)^m n$, where $n>2$ is prime, and it's subgroups are all of the form $\langle\sigma^h\rangle$, where h is a factor of $(2\ell)^m n$. In this section, we determine the G-orbits of this action.

We first need to know the number of affine sets $A(\alpha)$ which are in $\mathbb{A}$. By Section 3.2, $|\mathbb{S}| = 2^{(2\ell)^m)n} - 2^{(2^{m-1}\ell^m)n} - 2^{(2^m\ell^{m-1})n} + 2^{(2\ell)^{m-1}n}$. Since $|A(\alpha)| = 2^n(2^n-1)$ then $|\mathbb{A}| = |\mathbb{S}|/(2^n(2^n-1))$.

The expected length of orbits in $\mathbb{A}$ under the action of G are all factors of $(2\ell)^m n$. For our convenience in factorizing $(2\ell)^m n$, we write it as $2^m\ell^k n$ where $m=k$. The trivial subgroup $\langle\sigma^{2^m\ell^k n}\rangle$, containing the identity, fixes every affine set in $\mathbb{A}$. In the following subsections, we separately consider the remaining subgroups of G, i.e., $\langle\sigma^{2^{m-1}\ell^k n}\rangle$, $\langle\sigma^{2^m\ell^k}\rangle$, $\langle\sigma^{2^{m-1}\ell^k}\rangle$, $\langle\sigma^{2^s\ell^d n}\rangle$ and $\langle\sigma^{2^s\ell^d}\rangle$, with $0\le s\le m$ and $0\le d\le k$, while avoiding the combinations (i) $s=m$ and $d=k$, (ii) $s=m-1$ and $d=k$ (these combinations have been considered already in other subgroups).

The approach we apply in the subsequent subsections in this section generalises the one used in [4] when considering the action of G on $\mathbb{A}$.

3.3.1. $\langle\sigma^{2^{m-1}\ell^k n}\rangle$ a subgroup of G of order 2

Suppose the orbit in $\mathbb{A}$ under the action of G containing $A(\alpha)$ contains $2^{m-1}\ell^k n$ affine sets, i.e,

$$\{A(\alpha), \sigma(A(\alpha)), \sigma^2(A(\alpha)), ..., \sigma^{2^{m-1}\ell^k n-1}(A(\alpha))\}.$$

Then $A(\alpha)$ is fixed by $\langle\sigma^{2^{m-1}\ell^k n}\rangle$. That is, $\sigma^{2^{m-1}\ell^k n}(A(\alpha)) = A(\alpha)$. So we have $\sigma^{2^{m-1}\ell^k n}(\alpha) = \alpha^{2^{2^{m-1}\ell^k n}} = \zeta\alpha+\xi$ for some $\zeta\neq 0, \xi\in\mathbb{F}_{2^n}$. So applying $\sigma^{2^{m-1}\ell^k n}$ for the second time we get $\alpha = \sigma^{2^m\ell^k n}(\alpha) = \sigma^{2^m\ell^k n}(\zeta\alpha+\xi) = \zeta^{2^{2^{m-1}\ell^k n}}\alpha^{2^{2^{m-1}\ell^k n}} + \xi^{2^{m-1}\ell^k n} = \zeta\alpha^{2^{2^{m-1}\ell^k n}} + \xi = \zeta(\zeta\alpha+\xi)+\xi = \zeta^2\alpha + (\zeta+1)\xi$. We conclude that $\zeta^2 = 1$ otherwise $(1-\zeta^2)\alpha\in\mathbb{F}_{2^n}$, contradicting the fact that $\alpha\in\mathbb{S}$. Since $2\nmid(2^n-1)$ then $\zeta^2=1$ implies $\zeta=1$

Hence, we have $\alpha^{2^{2^{m-1}\ell^k n}} = \alpha+\xi$ for some $\xi\neq 0\in\mathbb{F}_{2^n}$. Multiplying both sides by ξ^{-1} we get $(\xi^{-1}\alpha)^{2^{2^{m-1}\ell^k n}} = (\xi^{-1}\alpha)+1$. We may assume that α satisfies the equation

$$x^{2^{2^{m-1}\ell^k n}} - x - 1 = 0. \qquad (4)$$

If α satisfies (4) then certainly all the 2^n elements in the set $\{\alpha+\xi : \xi\in\mathbb{F}_{2^n}\}$ also satisfy (4) while the remaining elements in $A(\alpha)$ do not satisfy (4). This follows from the fact that the equation $(\zeta\alpha+\xi)^{2^{2^{m-1}\ell^k n}} = \zeta\alpha^{2^{2^{m-1}\ell^k n}} + \xi = \zeta(\alpha+1)+\xi = \zeta\alpha+\zeta+\xi = (\zeta\alpha+\xi)+1$ holds if and only if $\zeta=1$. Hence if α satisfies (4) then $A(\alpha)$ contains precisely 2^n roots of (4).

We now find the number of elements of $\mathbb{S}$ which satisfy (4). We know that

$$x^{2^{2^{m-1}\ell^k n}} - x - 1 = \prod_{i=1}^{2^{2^{m-1}\ell^k n-1}}(x^2-x-\beta_i), \qquad (5)$$

where β_i denotes all the elements of $\mathbb{F}_{2^{2^{m-1}\ell^k n}}$ which have trace 1 over $\mathbb{F}_2$ [12]. We know that there are precisely $2^{2^{m-1}\ell^k n-1}$ such β_i's. Note that the trace function we are dealing with is from the field $\mathbb{F}_{2^{(2^{m-1}\ell^k)n}}$ to $\mathbb{F}_2$. Note that if an element is in a subfield $\mathbb{F}_{2^{(2^{m-2}\ell^k)n}}$ of $\mathbb{F}_{2^{(2^{m-1}\ell^k)n}}$, in calculating its trace we regard it as an element of $\mathbb{F}_{2^{(2^{m-1}\ell^k)n}}$. Observe that if $\beta \in \mathbb{F}_{2^{(2^{m-2}\ell^k)n}}$, then $Trace_{\mathbb{F}_{2^{(2^{m-1}\ell^k)n}}|\mathbb{F}_2}(\beta) = 2 \cdot Trace_{\mathbb{F}_{2^{(2^{m-2}\ell^k)n}}|\mathbb{F}_2}(\beta)$. Since the characteristic is 2, then we conclude that none of the β_i in the decomposition of $x^{2^{2^{m-1}\ell^k n}} - x - 1$ in (5) lie in $\mathbb{F}_{2^{(2^{m-2}\ell^k)n}}$. However, $2^{2^{m-1}\ell^{k-1}n-1}$ of the β_i lie in $\mathbb{F}_{2^{(2^{m-1}\ell^{k-1})n}}$, $2^{2^{m-1}\ell^k-1}$ of the β_i lie in $\mathbb{F}_{2^{2^{m-1}\ell^k}}$ and the remaining $2^{2^{m-1}\ell^k n-1} - 2^{2^{m-1}\ell^{k-1}n-1} - 2^{2^{m-1}\ell^k-1}$ lie in $\mathbb{F}_{2^{(2^{m-1}\ell^k)n}}$. Furthermore, all the quadratic factors on the right hand side of (5) are irreducible over $\mathbb{F}_{2^{(2^{m-1}\ell^k)n}}$. This is as a result of linearity of the trace function and the fact that $Trace(\beta_i) = 1$ for each β_i. The $2^{2^{m-1}\ell^k-1}$ quadratic equations corresponding to the β_i in $\mathbb{F}_{2^{2^{m-1}\ell^k}}$ have $\mathbb{F}_{2^{2^m\ell^k}}$ as their splitting field, $2^{2^{m-1}\ell^{k-1}n-1}$ quadratic equations corresponding to the β_i in $\mathbb{F}_{2^{(2^{m-1}\ell^{k-1})n}}$ have $\mathbb{F}_{2^{(2^m\ell^{k-1})n}}$ as their splitting field and the remaining $2^{2^{m-1}\ell^k n-1} - 2^{2^{m-1}\ell^{k-1}n-1} - 2^{2^{m-1}\ell^k-1}$ quadratic equations have $\mathbb{F}_{2^{(2^m\ell^k)n}}$ as their splitting field. Hence we have $2^{2^{m-1}\ell^k n} - 2^{2^{m-1}\ell^{k-1}n}$ roots lie in $\mathbb{S}$.

Conversely if $\alpha \in \mathbb{S}$ satisfies (4) then $A(\alpha)$ is fixed under $\langle\sigma^{2^{m-1}\ell^k n}\rangle$. We may conclude that there are precisely $\frac{2^{2^{m-1}\ell^k n}-2^{2^{m-1}\ell^{k-1}n}}{2^n} = 2^{(2^{m-1}\ell^k-1)n} - 2^{(2^{m-1}\ell^{k-1}-1)n}$ affine sets $A(\alpha)$ fixed under $\langle\sigma^{2^{m-1}\ell^k n}\rangle$.

3.3.2. $\langle\sigma^{2^s\ell^d n}\rangle$ a subgroup of G of order $2^{m-s}\ell^{k-d}$

Suppose the orbit in $\mathbb{A}$ under the action of G containing $A(\alpha)$ contains $2^s\ell^d n$ affine sets where $0 \le s \le m$ and $0 \le d \le k$ while avoiding the combinations: (i) $s = m$ and $d = k$, (ii) $s = m-1$ and $d = k$. As in Subsection 3.3.1, then $\sigma^{2^s\ell^d n}(\alpha) = \alpha^{2^{2^s\ell^d n}} = \zeta\alpha + \xi$ for some $\zeta \ne 0, \xi \in \mathbb{F}_{2^n}$. Applying $\sigma^{2^s\ell^d n}$ for $2^{m-s}\ell^{m-d}$ times to α we obtain $\alpha = \sigma^{2^m\ell^k n}(\alpha) = \zeta^{2^{m-s}\ell^{k-d}}\alpha + (\zeta^{2^{m-s}\ell^{k-d}-1} + \zeta^{2^{m-s}\ell^{k-d}-2} + \cdots + \zeta^2 + \zeta + 1)\xi$. We conclude that $\zeta^{2^{m-s}\ell^{k-d}} = 1$ otherwise $(1 - \zeta^{2^{m-s}\ell^{k-d}})\alpha \in \mathbb{F}_{2^n}$, contradicting the fact that $\alpha \in \mathbb{S}$. The possibilities are that $\zeta^{2^h} = 1$ where h is a factor of $2^{m-s}\ell^{k-d}$. Since $2 \nmid (2^n - 1)$ and $\ell \nmid (2^n - 1)$ (by assumption) then, for all $h \ne 1$, $h \nmid (2^n - 1)$. Hence the only possibility left is that $\zeta = 1$.

So $\alpha^{2^{2^s\ell^d n}} = \alpha + \xi$ for some $\xi \ne 0 \in \mathbb{F}_{2^n}$. If we multiply both sides by ξ^{-1} we obtain $(\xi^{-1}\alpha)^{2^{2^s\ell^d n}} = (\xi^{-1}\alpha) + 1$. We assume that α satisfies the equation $x^{2^{2^s\ell^d n}} - x - 1 = 0$. Using similar argument to the one in Subsection 3.3.1, all roots of $x^{2^{2^s\ell^d n}} - x - 1 = 0$ lie in $\mathbb{F}_{2^{2^{s+1}\ell^d}}$, $\mathbb{F}_{2^{(2^{s+1}\ell^{d-1})n}}$ and $\mathbb{F}_{2^{(2^{s+1}\ell^d n)}}$ (none is in $\mathbb{S}$). We conclude that there is no affine set $A(\alpha)$ fixed under $\langle\sigma^{2^s\ell^d n}\rangle$.

3.3.3. $\langle\sigma^{2^m\ell^k}\rangle$ a subgroup of G of order n

Suppose the orbit in $\mathbb{A}$ under the action of G containing $A(\alpha)$ contains 2^m affine sets. Then $A(\alpha)$ is fixed under $\langle\sigma^{2^m\ell^k}\rangle$. It is proved in [3] that if r is the degree of irreducible Goppa codes then the number of affine sets fixed by $\langle\sigma^r\rangle$ is $|\mathbb{S}(1,r)|/(q(q-1))$. Also note that if an affine set $A(\alpha)$ is fixed under $\langle\sigma^r\rangle$ then it contains some fixed points, that is, some elements in $A(\alpha)$ satisfy the equation $x^{2^r} = x$. In our case, we have $q = 2$ and $r = 2^m\ell^k$. Hence the number of affine sets fixed by $\langle\sigma^{2^m\ell^k}\rangle$ is $|\mathbb{S}(1,2^m)|/(2(2-1)) = (2^{2^m\ell^k} - 2^{2^{m-1}\ell^k} - 2^{2^m\ell^{k-1}} + 2^{2^{m-1}\ell^{k-1}})/2 = 2^{2^m\ell^k-1} - 2^{2^{m-1}\ell^k-1} - 2^{2^m\ell^{k-1}-1} + 2^{2^{m-1}\ell^{k-1}-1}$.

3.3.4. $\langle\sigma^{2^{m-1}\ell^k}\rangle$ **a subgroup of** G **of order** $2n$

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

We now show that $2^{2^{m-1}\ell^k} + 1$ is relatively prime to $2^n - 1$. Let $e = 2^{m-1}\ell^k$. It suffices to show that $(2^e + 1, 2^n - 1) = 1$. We show this by contradiction. Assume that $(2^e + 1, 2^n - 1) \ne 1$. That is there must

be some odd prime p which divides both 2^e+1 and 2^n-1. This implies that $2^n \equiv 1 \pmod{p}$ and $2^e \equiv -1 \pmod{p}$. So $2^e \equiv -1 \pmod{p}$ implies $2^{2e} \equiv (-1)^2 = 1 \equiv 2^n \pmod{p}$. Thus $n \equiv 2e \pmod{(p-1)}$. Since $p-1$ is even then n is also even. This establishes a contradiction since n is an odd prime. Hence $(2^e+1, 2^n-1) = 1$ for odd n.

Since $(2^{2^{m-1}\ell^k}+1, 2^n-1) = 1$ then we conclude that $\zeta^{2^{2^{m-1}\ell^k}+1} = 1$ implies $\zeta = 1$. So the equation $\alpha = \zeta^{2^{2^{m-1}\ell^k}+1}\alpha + \zeta^{2^{2^{m-1}\ell^k}}\xi + \xi^{2^{2^{m-1}\ell^k}}$ implies $\alpha = \alpha + \xi + \xi^{2^{2^{m-1}\ell^k}}$. Clearly, ξ is in the intersection of the fields of order $2^{2^{m-1}\ell^k}$ and 2^n. Since $(2^{m-1}\ell^k, n) = 1$ then either ξ is 0 or 1. But $\xi = 0$ is impossible since this would mean that $\alpha \in \mathbb{F}_{2^{2^{m-1}\ell^k}}$. So ξ must be 1.

So $\alpha^{2^{2^{m-1}\ell^k}} = \alpha + 1$. Clearly α satisfies the equation

$$x^{2^{2^{m-1}\ell^k}} - x - 1 = 0. \tag{6}$$

Observe that $\alpha+1$ also satisfies (6) and one can easily check that these are the only elements in $A(\alpha)$ which satisfy (6). Using an argument similar to the one in Subsection 3.3.1, $2^{2^{m-1}\ell^{k-1}}$ roots of (6) lie in $\mathbb{F}_{2^{2^{m}\ell^{k-1}}}$ (not in $\mathbb{S}$) while the remaining $2^{2^{m-1}\ell^k} - 2^{2^{m-1}\ell^{k-1}}$ roots lie in $\mathbb{F}_{2^{2^m\ell^k}}$ (in $\mathbb{S}$). Since in each fixed affine set under $\langle\sigma^{2^{m-1}\ell^k}\rangle$ there are two elements, α and $\alpha+1$, which satisfy (6) then we conclude that there are $\frac{2^{2^{m-1}\ell^k} - 2^{2^{m-1}\ell^{k-1}}}{2} = 2^{2^{m-1}\ell^k - 1} - 2^{2^{m-1}\ell^{k-1}-1}$ affine sets fixed under $\langle\sigma^{2^{m-1}\ell^k}\rangle$.

3.3.5. $\langle\sigma^{2^s\ell^d}\rangle$ a subgroup of G of order $2^{m-s}\ell k-d n$

Suppose the orbit in $\mathbb{A}$ under the action of G containing $A(\alpha)$ contains $2^s\ell^d$ affine sets where $0 \le s \le m$ and $0 \le d \le k$ while avoiding the combinations: (i) $s = m$ and $d = k$, (ii) $s = m-1$ and $d = k$. Then $\sigma^{2^s}(\alpha) = \alpha^{2^{2^s\ell^d}} = \zeta\alpha + \xi$ for some $\zeta \neq 0, \xi \in \mathbb{F}_{2^n}$. As in Subsection 3.3.4, if $A(\alpha)$ is fixed under $\langle\sigma^{2^s\ell^d}\rangle$ then it is also fixed under $\langle\sigma^{2^m\ell^k}\rangle$ since $\langle\sigma^{2^m\ell^k}\rangle \subset \langle\sigma^{2^s\ell^d}\rangle$. Assume $\alpha \in \mathbb{F}_{2^{2^m\ell^k}} \setminus (\mathbb{F}_{2^{2^{m-1}\ell^k}} \cup \mathbb{F}_{2^{2^m\ell^{k-1}}})$ then applying $\sigma^{2^s\ell^d}$ to α for $2^{m-s}\ell^{k-d}$ times we obtain

$$\begin{aligned}
\alpha &= \alpha^{2^{2^m}} \\
&= \zeta^{2^{\overline{n}\cdot 2^s\ell^d} + 2^{(\overline{n}-1)\cdot 2^s\ell^d} + \cdots + 2^{3\cdot 2^s\ell^d} + 2^{2\cdot 2^s\ell^d} + 2^{2^s\ell^d} + 1}\alpha \\
&+ \zeta^{2^{\overline{n}\cdot 2^s\ell^d} + 2^{(\overline{n}-1)\cdot 2^s\ell^d} + \cdots + 2^{3\cdot 2^s\ell^d} + 2^{2\cdot 2^s\ell^d} + 2^{2^s\ell^d}}\xi \\
&+ \zeta^{2^{\overline{n}\cdot 2^s\ell^d} + 2^{(\overline{n}-1)\cdot 2^s\ell^d} + \cdots + 2^{3\cdot 2^s\ell^d} + 2^{2\cdot 2^s\ell^d}}\xi^{2^{2^s\ell^d}} \\
&+ \zeta^{2^{\overline{n}\cdot 2^s\ell^d} + 2^{(\overline{n}-1)\cdot 2^s\ell^d} + \cdots + 2^{3\cdot 2^s\ell^d}}\xi^{2^{2\cdot 2^s\ell^d}} \\
&\vdots \\
&+ \zeta^{2^{\overline{n}\cdot 2^s\ell^d} + 2^{(\overline{n}-1)\cdot 2^s\ell^k}}\xi^{2^{(\overline{n}-2)\cdot 2^s\ell^d}} \\
&+ \zeta^{2^{\overline{n}\cdot 2^s\ell^d}}\xi^{2^{(\overline{n}-1)\cdot 2^s\ell^d}} \\
&+ \xi^{2^{\overline{n}\cdot 2^s\ell^d}}
\end{aligned} \tag{7}$$

where $\overline{n} = 2^{m-s}\ell^{k-d} - 1$. Observe that $\zeta^{2^{\overline{n}\cdot 2^s\ell^d} + 2^{(\overline{n}-1)\cdot 2^s\ell^d} + \cdots + 2^{3\cdot 2^s\ell^d} + 2^{2\cdot 2^s\ell^d} + 2^{2^s\ell^d} + 1}$ must be equal to 1 otherwise $(1 - \zeta^{2^{\overline{n}\cdot 2^s} + 2^{(\overline{n}-1)\cdot 2^s} + \cdots + 2^{3\cdot 2^s} + 2^{2\cdot 2^s} + 2^{2^s} + 1})\alpha \in \mathbb{F}_{2^n}$, contradicting the fact that α is of degree $2^m\ell^k$.

We now show that $2^{\overline{n}\cdot 2^s\ell^d} + 2^{(\overline{n}-1)\cdot 2^s\ell^d} + \cdots + 2^{3\cdot 2^s\ell^d} + 2^{2\cdot 2^s\ell^d} + 2^{2^s\ell^d} + 1$ and $2^n - 1$ are coprime. First observe that $2^{\overline{n}\cdot 2^s\ell^d} + 2^{(\overline{n}-1)\cdot 2^s\ell^d} + \cdots + 2^{3\cdot 2^s\ell^d} + 2^{2\cdot 2^s\ell^d} + 2^{2^s\ell^d} + 1 = (2^{2^s\ell^d(\overline{n}+1)} - 1)/(2^{2^s\ell^d} - 1) = (2^{2^m\ell^k} - 1)/(2^{2^s\ell^d} - 1)$. But we have $(2^m\ell^k, n) = 1$, so $(2^{2^m\ell^k} - 1, 2^n - 1) = 1$ from which we conclude that $2^{\overline{n}\cdot 2^s\ell^d} + 2^{(\overline{n}-1)\cdot 2^s\ell^d} + \cdots + 2^{3\cdot 2^s\ell^d} + 2^{2\cdot 2^s\ell^d} + 2^{2^s\ell^d} + 1$ and $2^n - 1$ are coprime.

Hence $\zeta^{2^{\overline{n}\cdot 2^s\ell^d} + 2^{(\overline{n}-1)\cdot 2^s\ell^d} + \cdots + 2^{3\cdot 2^s\ell^d} + 2^{2\cdot 2^s\ell^d} + 2^{2^s\ell^d} + 1} = 1$ implies $\zeta = 1$. Since $\zeta = 1$ then (7) becomes $\alpha = \alpha + \xi + \xi^{2^{2^s l^d}} + \xi^{2^{2\cdot 2^s\ell^d}} + \cdots + \xi^{2^{(\overline{n}-2)2^s\ell^d}} + \xi^{2^{(\overline{n}-1)2^s\ell^d}} + \xi^{2^{\overline{n}\cdot 2^s\ell^d}}$. It is clear that ξ is in the intersection of the fields of order $2^{2^s\ell^d}$ and 2^n. Since $(2^s\ell^d, n) = 1$ then ξ is either 0 or 1. But $\xi = 0$ is impossible since this would mean that $\alpha \in \mathbb{F}_{2^{2^s}}$. So ξ must be 1.

So we have $\alpha^{2^{2^s\ell^d}} = \alpha + 1$. Clearly α satisfies the equation $x^{2^{2^s\ell^d}} - x - 1 = 0$. Observe that $\alpha + 1$ also satisfies the equation $x^{2^{2^s\ell^k}} - x - 1 = 0$ and one can easily check that these are the only elements in $A(\alpha)$ which satisfy $x^{2^{2^s\ell^k}} - x - 1 = 0$. Using similar argument to the one in Subsection 3.3.1, all the $2^{2^s\ell^k}$ roots of $x^{2^{2^s\ell^d}} - x - 1$ lie in $\mathbb{F}_{2^{(2^{s+1}\ell^{d-1})}}$ and $\mathbb{F}_{2^{(2^{s+1}\ell^d)}}$ (not in $\mathbb{S}$). Hence we conclude that there is no affine set fixed under $\langle\sigma^{2^s\ell^d}\rangle$.

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 4 subgroups of G and the other subgroups which do not fix any affine set are left out. The subgroups are listed in ascending order of the number of elements in the subgroup. So the first row is the subgroup $\langle\sigma^{2^m\ell^k n}\rangle$ 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.

Table 1. Number of fixed affine sets under the action of 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
$\langle\sigma^{2^m\ell^k n}\rangle$	1	1	$\frac{\lvert\mathbb{S}(n,2^m\ell^k)\rvert}{2^n(2^n-1)}$	$\frac{\lvert\mathbb{S}(n,2^m\ell^k)\rvert}{2^n(2^n-1)}$
$\langle\sigma^{2^{m-1}\ell^k n}\rangle$	2	1	$2^{(2^{m-1}\ell^k-1)n} - 2^{(2^{m-1}\ell^{k-1}-1)n}$	$2^{(2^{m-1}\ell^k-1)n} - 2^{(2^{m-1}\ell^{k-1}-1)n}$
$\langle\sigma^{2^m\ell^k}\rangle$	n	$n-1$	$\lvert\mathbb{S}(1,2^m\ell^k)\rvert$	$(n-1)\lvert\mathbb{S}(1,2^m\ell^k)\rvert$
$\langle\sigma^{2^{m-1}\ell^k}\rangle$	$2n$	$n-1$	$2^{2^{m-1}\ell^k-1} - 2^{2^{m-1}\ell^{k-1}-1}$	$(n-1)(2^{2^{m-1}\ell^k-1} - 2^{2^{m-1}\ell^{k-1}-1})$

Remark 2. The number of orbits in $\mathbb{A}$ under the action of G gives us an upper bound on the number of irreducible Goppa codes. By the Cauchy Frobenius Theorem, the number of orbits in $\mathbb{A}$ under the action of G is

$$\frac{2^{(2^{m-1}\ell^k-1)n} - 2^{(2^{m-1}\ell^{k-1}-1)n} + (n-1)\lvert\mathbb{S}(1,2^m\ell^k)\rvert + (n-1)(2^{2^{m-1}\ell^k-1} - 2^{2^{m-1}\ell^{k-1}-1}) + \delta}{n(2^m\ell^k)}$$

where $\delta = \lvert\mathbb{S}(n,2^m\ell^k)\rvert/(2^n(2^n-1))$.

3.5. The number of fixed $O(\alpha)$ in $\mathbb{O}_F$

We are going to consider the action of G on $\mathbb{O}_F$ so that we find the number of $O(\alpha)$ which are fixed in $\mathbb{O}_F$. This is done by acting all subgroups of G on $\mathbb{O}_F$.

We begin by finding the number of elements in $\mathbb{O}_F$. In Section 3.2, we saw that $\lvert\mathbb{S}\rvert = 2^{(2^m\ell^k)n} - 2^{(2^{m-1}\ell^k)n} - 2^{(2^m\ell^{k-1})n} + 2^{(2^{m-1}\ell^{k-1})n}$. Since $\lvert O(\alpha)\rvert = 2^n(2^n-1)(2^n+1)$ then $\lvert\mathbb{O}_F\rvert = \frac{\lvert\mathbb{S}\rvert}{2^n(2^n-1)(2^n+1)}$.

Since G acts on $\mathbb{O}_F$ and its cardinality is $2^m\ell^k n$ then the expected lengths for the orbits in $\mathbb{O}_F$ under the action of G are all the factors of $2^m\ell^k n$. Every $O(\alpha)$ in $\mathbb{O}_F$ is fixed by a trivial subgroup $\langle\sigma^{2^m\ell^k n}\rangle$ containing the identity. As in Section 3.3, we consider the remaining subgroups of G, i.e., $\langle\sigma^{2^{m-1}\ell^k n}\rangle$, $\langle\sigma^{2^m\ell^k}\rangle$,$\langle\sigma^{2^{m-1}\ell^k}\rangle$, $\langle\sigma^{2^s\ell^d}\rangle$ and $\langle\sigma^{2^s\ell^d n}\rangle$ where $0 \le s \le m$ and $0 \le d \le k$ while avoiding the combinations: (i) $s = m$ and $d = k$, (ii) $s = m-1$ and $d = k$.

3.5.1. $\langle\sigma^{2^{m-1}\ell^k n}\rangle$ a subgroup of G of order 2

Suppose $O(\alpha) \in \mathbb{O}_F$ is fixed under $\langle\sigma^{2^{m-1}\ell^k n}\rangle$. Then $\langle\sigma^{2^{m-1}\ell^k n}\rangle$ acts on $O(\alpha) = A(\alpha) \cup A(\frac{1}{\alpha}) \cup A(\frac{1}{\alpha+1}) \cup A(\frac{1}{\alpha+\tilde{\zeta}_1}) \cup A(\frac{1}{\alpha+\tilde{\zeta}_2}) \cup A(\frac{1}{\alpha+\tilde{\zeta}_2}) \cup \cdots \cup A(\frac{1}{\alpha+\tilde{\zeta}_{2^n-2}})$. We can consider $O(\alpha)$ as a set of 2^n+1 affine sets. $\langle\sigma^{2^{m-1}\ell^k n}\rangle$ 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 $\langle\sigma^{2^{m-1}\ell^k n}\rangle$. By Subsection 3.3.1, there are $2^{(2^{m-1}\ell^k-1)n} - 2^{(2^{m-1}\ell^{k-1}-1)n}$ such affine sets. We claim that any fixed $O(\alpha)$ in $\mathbb{O}_F$ contains precisely one affine set which is fixed under $\langle\sigma^{2^{m-1}\ell^k n}\rangle$. It suffices to show that $O(\alpha)$ cannot contain two affine sets which are fixed under $\langle\sigma^{2^{m-1}\ell^k n}\rangle$. Without loss of generality, suppose $A(\alpha)$ is fixed under $\langle\sigma^{2^{m-1}\ell^k n}\rangle$. Recall that $O(\alpha) = A(\alpha) \cup A(\frac{1}{\alpha}) \cup A(\frac{1}{\alpha+1}) \cup A(\frac{1}{\alpha+\xi_1}) \cup A(\frac{1}{\alpha+\xi_2}) \cup A(\frac{1}{\alpha+\xi_3}) \cup \cdots \cup A(\frac{1}{\alpha+\xi_{2^n-2}})$. We show that none of the affine sets after $A(\alpha)$ in the above decomposition of $O(\alpha)$ is fixed under $\langle\sigma^{2^{m-1}\ell^k n}\rangle$. This is done by showing that no element in any of these affine sets satisfies the equation $x^{2^{2^{m-1}\ell^k n}} - x - 1 = 0$ (see Equation 4 in Subsection 3.3.1). By Subsection 3.3.1, the 2^n elements in the set $\{\alpha + \xi : \xi \in \mathbb{F}_{2^n}\}$ satisfy the equation $x^{2^{2^{m-1}\ell^k n}} - x - 1 = 0$ from which we see that $\alpha^{2^{2^{m-1}\ell^k n}} = \alpha + 1$. It is sufficient to show that no element in $A(\frac{1}{\alpha})$ satisfies $x^{2^{2^{m-1}\ell^k n}} - x - 1 = 0$. A typical element in $A(\frac{1}{\alpha})$ has the form $\frac{\zeta}{\alpha} + \xi$ and substituting this in $x^{2^{2^{m-1}\ell^k n}} - x - 1$ we get $(\frac{\zeta}{\alpha} + \xi)^{2^{2^{m-1}\ell^k n}} - (\frac{\zeta}{\alpha} + \xi) - 1 = \frac{\alpha^2+\alpha+\zeta}{\alpha^2+\alpha} \neq 0$, since α is an element of degree $2^m\ell^k$ over $\mathbb{F}_{2^n}$. We conclude that $A(\frac{1}{\alpha})$ is not fixed under $\langle\sigma^{2^{m-1}\ell^k n}\rangle$ and in fact $A(\alpha)$ is the only affine set in $O(\alpha)$ fixed under $\langle\sigma^{2^{m-1}\ell^k n}\rangle$. It follows that the number of $O(\alpha)$'s in $\mathbb{O}_F$ which are fixed under $\langle\sigma^{2^{m-1}\ell^k n}\rangle$ is $2^{(2^{m-1}\ell^k-1)n} - 2^{(2^{m-1}\ell^{k-1}-1)n}$.

3.5.2. $\langle\sigma^{2^s\ell^d n}\rangle$ a subgroup of G of order $2^{m-s}\ell^{k-d}$

Suppose $O(\alpha) \in \mathbb{O}_F$ is fixed under $\langle\sigma^{2^s\ell^d n}\rangle$ where $0 \leq s \leq m$ and $0 \leq d \leq k$ while avoiding the combinations: (i) $s = m$ and $d = k$, (ii) $s = m-1$ and $d = k$. Then $\langle\sigma^{2^s\ell^d n}\rangle$ acts on $O(\alpha)$. We can consider $O(\alpha)$ as a set of $2^n + 1$ affine sets. $\langle\sigma^{2^s\ell^d n}\rangle$ partitions this set of $2^n + 1$ affine sets. The possible orbit lengths are all factors of $2^{m-s}\ell^{k-d}$. By Subsection 3.3.2, there is no affine set fixed under $\langle\sigma^{2^s\ell^d}\rangle$. So we preclude the possibility of length 1. Since $O(\alpha)$ contains an odd number of affine sets then all orbits cannot have even length. And, by assumption, $\ell \nmid (2^n - 1)$ so we preclude the possibility that all orbits have length of multiples of ℓ. The only possibility we remain to check is that the orbit lengths are both 2^i and multiples of ℓ. Since if $s = m$ then the order of $\langle\sigma^{2^s\ell^d n}\rangle$ is ℓ^d and also $d = k$ implies $\langle\sigma^{2^s\ell^d n}\rangle$ has 2^s, we only check when $s < m$ and $d < k$. We observe that $\langle\sigma^{2^{s+i}\ell^d n}\rangle \subset \langle\sigma^{2^s\ell^d n}\rangle$, so a length of 2^i under $\langle\sigma^{2^s\ell^d n}\rangle$ would mean that 2^i affine sets are fixed in each fixed $O(\alpha)$ under $\langle\sigma^{2^{s+i}\ell^d n}\rangle$ which is a contradiction as there is no affine set fixed under $\langle\sigma^{2^{s+1}\ell^d n}\rangle$ where $s < m$ and $d < k$ (see Subsection 3.3.2). Hence we conclude that no $O(\alpha)$ in $\mathbb{O}_F$ is fixed under $\langle\sigma^{2^s\ell^d n}\rangle$.

3.5.3. $\langle\sigma^{2^m\ell^k}\rangle$ a subgroup of G of order n

Suppose $O(\alpha) \in \mathbb{O}_F$ is fixed under $\langle\sigma^{2^m\ell^k}\rangle$. Then $\langle\sigma^{2^m\ell^k}\rangle$ acts on $O(\alpha)$ which is seen as a set of $2^n + 1$ affine sets. $\langle\sigma^{2^m\ell^k}\rangle$ partitions this set of $2^n + 1$ affine sets. The only possible orbit lengths are 1 and n. Since $2^n + 1 \equiv 2 + 1 = 3 \pmod{n}$ (by Fermat Little Theorem) then n does not divide $2^n + 1$. So there must be at least three affine sets in $O(\alpha)$ fixed under $\langle\sigma^{2^m\ell^k}\rangle$. We claim that there are precisely three affine sets in $O(\alpha)$ which are fixed under $\langle\sigma^{2^m\ell^k}\rangle$. 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 $\langle\sigma^{2^m\ell^k}\rangle$. So, by Subsection 3.3.3, $A(\alpha)$ contains a fixed point, i.e., some elements of $A(\alpha)$ satisfy the equation $x^{2^{2^m\ell^k}} = x$. It is clear that α and $\alpha + 1$ in $A(\alpha)$ are the only elements that satisfy the equation $x^{2^{2^m\ell^k}} = x$. Since $(\frac{1}{\alpha})^{2^{2^m\ell^k}} = \frac{1}{\alpha}$ and $(\frac{1}{\alpha+1})^{2^{2^m\ell^k}} = \frac{1}{\alpha+1}$ 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 $\langle\sigma^{2^m\ell^k}\rangle$. First observe that, for $\nu \in \mathbb{F}_{2^n} \setminus \{0, 1\}$, we have $\nu^{2^{2^m\ell^k}} \neq \nu$ since $(2^m\ell^k, n) = 1$. So $(\frac{1}{\alpha+\nu})^{2^{2^m\ell^k}} = \frac{1}{\alpha+\nu^{2^{2^m\ell^k}}} = \frac{1}{\alpha+\eta}$ implies that $\sigma^{2^m\ell^k}(A(\frac{1}{\alpha+\nu})) = A(\frac{1}{\alpha+\eta})$ as required. Therefore $A(\alpha)$, $A(\frac{1}{\alpha})$ and $A(\frac{1}{\alpha+1})$ are the only affine sets fixed under $\langle\sigma^{2^m\ell^k}\rangle$. By Subsection 3.3.3, there are $2^{2^m\ell^k-1} - 2^{2^{m-1}\ell^k-1} - 2^{2^m\ell^{k-1}-1} + 2^{2^{m-1}\ell^{k-1}-1}$ affine sets which are fixed under $\langle\sigma^{2^m}\rangle$. Hence the number of $O(\alpha)$ in $\mathbb{O}_F$ which are fixed under $\langle\sigma^{2^m l^k}\rangle$ is $(2^{2^m\ell^k-1} - 2^{2^{m-1}\ell^k-1} - 2^{2^m\ell^{k-1}-1} + 2^{2^{m-1}\ell^{k-1}-1})/3$.

3.5.4. $\langle \sigma^{2^{m-1}\ell^k} \rangle$ a subgroup of G of order $2n$

Suppose $O(\alpha) \in \mathbb{O}_F$ is fixed under $\langle \sigma^{2^{m-1}\ell^k} \rangle$. Then $\langle \sigma^{2^{m-1}\ell^k} \rangle$ acts on $O(\alpha)$ which is seen as a set of 2^n+1 affine sets. $\langle \sigma^{2^{m-1}\ell^k} \rangle$ partitions this set of 2^n+1 affine sets. $O(\alpha) = A(\alpha) \cup A(\frac{1}{\alpha}) \cup A(\frac{1}{\alpha+1}) \cup A(\frac{1}{\alpha+\xi_1}) \cup A(\frac{1}{\alpha+\xi_2}) \cup A(\frac{1}{\alpha+\xi_3}) \cup \cdots \cup A(\frac{1}{\alpha+\xi_{2^n-2}})$. The possible lengths of orbits are all factors of $2n$. But the possibility that all orbits are of even length is precluded since the $O(\alpha)$ contains odd number of affine sets. It is also not possible to have length n for all orbits since $n \nmid (2^n+1)$ (see Subsection 3.5.3). So there must be at least one affine set fixed under $\langle \sigma^{2^{m-1}\ell^k} \rangle$. We claim that any $O(\alpha)$ fixed under $\langle \sigma^{2^{m-1}\ell^k} \rangle$ contains precisely one affine set fixed under $\langle \sigma^{2^{m-1}\ell^k} \rangle$. By Subsection 3.3.4, an affine set fixed under $\langle \sigma^{2^{m-1}\ell^k} \rangle$ contains some elements which satisfy the equation $x^{2^{2^{m-1}\ell^k}} + x + 1 = 0$. Without loss of generality, suppose $A(\alpha)$ is fixed under $\langle \sigma^{2^{m-1}\ell^k} \rangle$. It is clear that α and $\alpha+1$ satisfy $x^{2^{2^{m-1}\ell^k}} - x - 1 = 0$. We also observe that $(\frac{1}{\alpha})^{2^{2^{m-1}\ell^k}} = \frac{1}{\alpha+1}$ and $(\frac{1}{\alpha+1})^{2^{2^{m-1}\ell^k}} = \frac{1}{\alpha}$ which imply that $\sigma^{2^{m-1}\ell^k}(A(\frac{1}{\alpha})) = A(\frac{1}{\alpha+1})$ and $\sigma^{2^{m-1}\ell^k}(A(\frac{1}{\alpha+1})) = A(\frac{1}{\alpha})$. We can conclude that $A(\frac{1}{\alpha})$ and $A(\frac{1}{\alpha+1})$ form an orbit of length 2. Since $\langle \sigma^{2^m\ell^k} \rangle \subset \langle \sigma^{2^{m-1}\ell^k} \rangle$ then any $O(\alpha)$ or affine set fixed under $\langle \sigma^{2^{m-1}l^k} \rangle$ is also fixed under $\langle \sigma^{2^m l^k} \rangle$. By Subsection 3.3.3, no affine set after $A(\frac{1}{\alpha+1})$ in the decomposition of $O(\alpha)$ is fixed under $\langle \sigma^{2^m\ell^k} \rangle$. So we conclude that $\langle \sigma^{2^{m-1}l\ell^k} \rangle$ does not fix any affine set after $A(\frac{1}{\alpha+1})$ in the decomposition of $O(\alpha)$ as otherwise it would mean that it is also fixed under $\langle \sigma^{2^m\ell^k} \rangle$. So it follows that we only have $A(\alpha)$ fixed in any fixed $O(\alpha)$ under $\langle \sigma^{2^{m-1}\ell^k} \rangle$. By Subsection 3.3.4, there are $2^{2^{m-1}\ell^k-1} - 2^{2^{m-1}\ell^{k-1}-1}$ affine sets fixed under $\langle \sigma^{2^{m-1}\ell^k} \rangle$. So we conclude that the number of $O(\alpha)$ in $\mathbb{O}_F$ which are fixed under $\langle \sigma^{2^{m-1}\ell^k} \rangle$ is $2^{2^{m-1}\ell^k-1} - 2^{2^{m-1}\ell^{k-1}-1}$.

3.5.5. $\langle \sigma^{2^s\ell^d} \rangle$ a subgroup of G of order $2^{m-s}\ell^{k-d}n$

Suppose $O(\alpha) \in \mathbb{O}_F$ is fixed under $\langle \sigma^{2^s\ell^d} \rangle$ where $0 \leq s \leq m$ and $0 \leq d \leq k$ while avoiding the combinations: (i) $s = m$ and $d = k$, (i) $s = m-1$ and $d = k$. Then $\langle \sigma^{2^s\ell^d} \rangle$ acts on $O(\alpha)$ which is seen as a set of 2^n+1 affine sets. $\langle \sigma^{2^s\ell^d} \rangle$ partitions this set of 2^n+1 affine sets. The possible lengths of orbits are all factors of $2^{m-s}\ell^{k-d}n$. By Subsection 3.3.5, no affine set is fixed under $\langle \sigma^{2^s\ell^d} \rangle$, so no orbits of length one are expected. Since $O(\alpha)$ contains an odd number of affine sets then the possibility that all orbits are of even length is precluded. Since $2^n+1 \equiv 3 \pmod{n}$ (see Subsection 3.5.3) we also preclude the possibility that all orbits are of length n. Also, by assumption, $\ell \nmid (2^n+1)$ so we cannot have all orbits of length ℓ.

We now consider the possibility of x affine sets partitioned in orbits of length 2^i, with $1 \leq i \leq m-s$ and 2^n+1-x affine sets partitioned in orbits of length multiples of n, i.e., $2^n+1-x \equiv 0 \pmod{n}$. Since $2^n+1 \equiv 3 \pmod{n}$, x has the form $jn+3$ where j is an odd integer. Since $2|x$ then j is non zero. So there are $jn+3 > 3$ affine sets permuted in orbits of length 2^i under $\langle \sigma^{2^s\ell^d} \rangle$. Since $\langle \sigma^{2^{s+i}\ell^d} \rangle \subset \langle \sigma^{2^s\ell^d} \rangle$ it is easy to observe that 2^i affine sets that form an orbit under $\langle \sigma^{2^s\ell^d} \rangle$ are fixed under $\langle \sigma^{2^{s+i}\ell^d} \rangle$. If $s = m-2$ and $d = k$ (recall that we cannot have $s = m-1, m$ and $d = k$ here) then it would mean that there exist a fixed $O(\alpha)$ under $\langle \sigma^{2^{m-2+i}\ell^k} \rangle$, with $i = 1$ or $i = 2$, which contains more than 3 affine sets fixed under $\langle \sigma^{2^{m-2+i}\ell^k} \rangle$, contradicting Subsections 3.5.3 and 3.5.4. Also note that, by excluding the combinations we just considered (i.e., $s+i = m-1, m$ and $d = k$), no affine set is fixed under $\langle \sigma^{2^{s+i}\ell^d} \rangle$ (see Subsection 3.3.5) so it would be a contradiction to say that more than 3 affine sets in each fixed $O(\alpha)$ are fixed under $\langle \sigma^{2^{s+i}l^d} \rangle$. A similar argument can be used to show that orbit lengths of 2^i and multiples of ℓ are also not possible.

Next, we check the possibility of orbit lengths of multiples of ℓ and n. If x affine sets are partitioned into orbits of length multiples of ℓ then 2^n+1-x affine sets are partitioned into orbits of length multiples of n. So $2^n+1-x \equiv 0 \pmod{n}$ and hence x must be of the $hn+3$ because $2^n+1 \equiv 3 \pmod{n}$. Observe that since $3 \mid 2^n+1$ (because $2^n+1 = 2^{2t+1}+1 = 2 \cdot 2^{2t}+1 \equiv 3 \equiv 0 \pmod{3}$) then $\ell \neq 3$. So there are $hn+3 > 3$ affine sets permuted in orbits of length multiples of ℓ under $\langle \sigma^{2^s\ell^d} \rangle$. Note that since $\langle \sigma^{2^s\ell^{d+1}} \rangle \subset \langle \sigma^{2^s\ell^d} \rangle$ so an orbit of length ℓ under $\langle \sigma^{2^s\ell^d} \rangle$ is fixed under $\langle \sigma^{2^s\ell^{d+1}} \rangle$. An argument similar to the one above shows that the orbit lengths of ℓ and n are impossible.

What about the possibility of orbit lengths of 2^i, ℓ and n? Again, if x is the number of affine sets partitioned in orbits of length 2^i and multiples of ℓ then 2^n+1-x is the number of affine sets partitioned in orbits of length n. Since $2^n+1 \equiv 3 \pmod{n}$ then the form of x, the number of affine sets partitioned in orbits of length 2^i and ℓ, is $hn+3$ for some integer h. Since $(n,\ell) = 1$ then we can write $y\ell = zn+1$ for some integers y and z (by

Bezout's identity). Hence we can write $hn+3=(hn+1)+2=w\ell+2=g\ell+(f\ell+2)$, for some integers w, g and f, where $g\ell$ are affine sets partitioned into orbits of length ℓ and $f\ell+2$ are affine sets partitioned into orbits of length 2^i. Since 2 must divide $f\ell+2$ then f has to be even. It is clear that $f\ell+2\geq 2$. If $f=0$ then it implies that 2 affine sets in a fixed $O(\alpha)$ form an orbit under $\langle\sigma^{2^s\ell^d}\rangle$. If $s=m-2$ and $d=k$ then, since $\langle\sigma^{2^{s+1}\ell^d}\rangle\subset\langle\sigma^{2^s\ell^d}\rangle$, it would mean that $\langle\sigma^{2^{m-1}\ell^k}\rangle$ fixes 2 affine sets in each fixed $O(\alpha)$ which is a contradiction as it only fixes one affine set (see Subsection 3.5.4). For any other combination of s and d it would mean that 2 affine sets are fixed in an $O(\alpha)$ fixed under $\langle\sigma^{2^{s+1}\ell^d}\rangle$ which is again contradiction as in Subsection 3.3.5 it shows that no such subgroup fixes any affine set. Also $f>1$ is impossible as it would mean that four or more affine sets are fixed in some fixed $O(\alpha)$ under some subgroup contained in $\langle\sigma^{2^s\ell^d}\rangle$ which cannot happen by previous subsections. We have exhausted all the possibilities and we thus conclude that there is no $O(\alpha)$ in $\mathbb{O}_F$ which is fixed under $\langle\sigma^{2^s\ell^d}\rangle$.

3.6. Applying the Cauchy Frobenius Theorem

Table 3.6.1 present the results found in Section 3.5 and its structure is similar to Table 3.4.1.

Table 2. Number of fixed $O(\alpha)$ under the action 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
$\langle\sigma^{2^m\ell^k n}\rangle$	1	1	$\frac{\lvert\mathbb{S}\rvert}{2^n(2^n-1)(2^n+1)}$	$\frac{\lvert\mathbb{S}\rvert}{2^n(2^n-1)(2^n+1)}$
$\langle\sigma^{2^{m-1}\ell^k n}\rangle$	2	1	$2^{(2^{m-1}\ell^k-1)n}-2^{(2^{m-1}\ell^{k-1}-1)n}$	$2^{(2^{m-1}\ell^k-1)n}-2^{(2^{m-1}\ell^{k-1}-1)n}$
$\langle\sigma^{2^m\ell^k}\rangle$	n	$n-1$	$\lvert\mathbb{S}(1,2^m\ell^k)\rvert/3$	$(n-1)(\lvert\mathbb{S}(1,2^m\ell^k)\rvert)/3$
$\langle\sigma^{2^{m-1}\ell^k}\rangle$	$2n$	$n-1$	$2^{2^{m-1}\ell^k-1}-2^{2^{m-1}\ell^{k-1}-1}$	$(n-1)(2^{2^{m-1}\ell^k-1}-2^{2^{m-1}\ell^{k-1}-1})$

We know that $\lvert\mathbb{S}(1,2^m\ell^k)\rvert=2^{2^m\ell^k-1}-2^{2^{m-1}\ell^k-1}-2^{2^m\ell^{k-1}-1}+2^{2^{m-1}\ell^{k-1}-1}$ and $\lvert\mathbb{S}(n,2^m\ell^k)\rvert=2^{(2^m\ell^k)n}-2^{(2^{m-1}\ell^k)n}-2^{(2^m\ell^{k-1})n}+2^{(2^{m-1}\ell^{k-1})n}$.

Remark 3. The number of orbits in $\mathbb{O}_F$ under the action of G gives us an upper bound for the number of inequivalent extended irreducible binary Goppa codes. By the Cauchy Frobenius Theorem, the number of orbits in $\mathbb{O}_F$ under the action of G is

$$\frac{2^{(2^{m-1}\ell^k-1)n}-2^{(2^{m-1}\ell^{k-1}-1)n}+(n-1)(\lvert\mathbb{S}(1,2^m\ell^k)\rvert)/3+(n-1)(2^{2^{m-1}\ell^k-1}-2^{2^{m-1}\ell^{k-1}-1})+\Delta}{2^m\ell^k n},$$

where $\Delta=\lvert\mathbb{S}(n,2^m\ell^k)\rvert/(2^n(2^n-1)(2^n+1))$.

Recall that we set $m=k$ and by Equations 2 and 3 the values of $\lvert\mathbb{S}(1,2^m\ell^k)\rvert$ and $\lvert\mathbb{S}(n,2^m\ell^k)\rvert$ are known. Since this is our main result in this paper, we state it in the following theorem.

Theorem 18. *Let n and ℓ be odd prime numbers such that $(\ell,2^n\pm1)=1$ and $\ell\neq n$. The number of inequivalent extended irreducible binary Goppa codes of degree $(2\ell)^m$, with $m\geq1$ and length 2^n+1 is at most*

$$\begin{cases}\dfrac{\left(\sum\limits_{i=1}^{(\ell-1)/2}\gamma^{2(\ell-i)-1}+\sum\limits_{i=0}^{\ell-2}(-1)^{i+1}\gamma^i\right)+(\gamma^{\ell-1}-1)+(n-1)(2^{2\ell-1}+2^\ell-4)/3}{2\ell n} & \text{if } m=1\\[2ex] \dfrac{\gamma^{\lambda-1}\left(\sum\limits_{i=0}^{(\lambda-2)/2}\gamma^{2i}\right)\left(\left(\sum\limits_{i=0}^{\ell-1}\gamma^{(\ell-1+i)\lambda}\right)-1\right)+\gamma^{\ell\lambda-1}-\gamma^{\lambda-1}+(n-1)(2^{2\ell\lambda-1}-2^{2\lambda-1}+2^{\ell\lambda}-2^\lambda)/3}{n(2\ell)^m} & \text{if } m>1\end{cases}$$

where $\lambda=(2\ell)^{m-1}$ and $\gamma=2^n$.

Example 1. The tables below compare the upper bound on the number of extended irreducible binary Goppa codes of degree $(2\ell)^m$ and length 2^n+1 and non-extended versions of length 2^n. The bounds on the number of the two versions of codes are obtained using Remark 2 and Theorem 18.

Table 3. Number of non-extended and extended Goppa codes when $m = 1$, $\ell = 5$ and $n = 7, 11, 13$

r	n	Number of extended irreducible Goppa codes	Number of irreducible Goppa codes
$m = 1, \ell = 5$	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

Table 4. Number of non-extended and extended Goppa codes when $m = 2$, $\ell = 5$ and $n = 7$

	$n = 7, m = 2, \ell = 5$
Non-Ext. Goppa codes	4,622,588,496,158,230,374,051,769,793,025,984,836,851,746,873,965, 809,423,771,689,488,776,657,578,801,416,6,920,445,784,006,149,455, 542,768,623,409,098,875,990,160,540,631, 751,785,597,245,560,480, 490,009,340,223,525,920,966,754,236,069,676,754,557,809,563, 115, 990,501,031,936
Ext. Goppa codes	358,340,193,500,638,013,492,385,255,273,332,157,895,484,253,795, 799,180,137,340,270,447,802,742,646,641,023,601,382,950,503,453, 909,148,362,538, 791,931,238,348,268,716,699,081,713,709,698,766, 594,405,529,127,416,760,975,801,640,365,691,439,359,515,939, 510, 005,752,320

Note that in our example we made sure that the condition $b = 2^n - (2\ell)^m n > 0$, where b represents the lower bound of the dimension of Goppa codes, is met.

4. Conclusion

In this paper we produced an upper bound on the number of extended irreducible binary Goppa codes of degree $(2\ell)^m$ and length $2^n + 1$ where n and ℓ are odd prime numbers not equal. The result is presented in the Theorem 18.

Acknowledgments

The author thanks anonymous reviewers for their thorough review and highly appreciates the comments and suggestions, which significantly contributed to the quality of this work.

Conflicts of Interest: "The author declare no conflict of interest."

References

[1] Dinh, H., Moore, C., & Russell, A. (2010). The mceliece cryptosystem resists quantum fourier sampling attacks. *arXiv preprint arXiv:1008.2390*.

[2] Loidreau, P., & Sendrier, N. (2001). Weak keys in the McEliece public-key cryptosystem. *IEEE Transactions on Information Theory, 47*(3), 1207-1211.

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

[4] Musukwa, A. (2018). Counting extended irreducible binary Goppa codes of degree $2p$ and length $2^n + 1$, *J. Math. Comput. Sci. 8*(1), 1-17.

[5] Musukwa, A., Magamba, K. & Ryan, J.A. (2017). Enumeration of extended irreducible binary Goppa codes of degree 2^m and length $2^n + 1$. *Journal of Algebra Combinatorics Discrete Structures and Applications 4*, 235-246.

[6] Ryan, J.A. (2015). Counting Extended Irreducible Binary Quartic Goppa Codes, *IEEE Transactions on Information Theory, 61*(3), 1-5.

[7] Ryan, J. A. (2014). Counting extended irreducible Goppa codes. *Journal of Discrete Mathematics, 2014.*

[8] Chen, C. L. (1978). Equivalent irreducible Goppa codes (Corresp.). *IEEE Transactions on Information Theory, 24*(6), 766-769.

[9] Berger, T. P. (2000). Goppa and related codes invariant under a prescribed permutation. *IEEE Transactions on Information Theory, 46*(7), 2628-2633.

[10] Isaacs, I. M. (2009). *Algebra: a graduate course* (Vol. 100). American Mathematical Soc..

[11] Magamba, K., & Ryan, J. A. (2014). Counting Irreducible Polynomials of Degree over $\mathbb{F}_{q^n}$ and Generating Goppa Codes Using the Lattice of Subfields of $\mathbb{F}_{q^{nr}}$. *Journal of Discrete Mathematics, 2014*.

[12] Lidl, R., & Niederreiter, H. (1994). *Introduction to finite fields and their applications*. Cambridge university press.