J. Algebra Comb. Discrete Appl.
4(3) • 235–246

Received: 9 June 2016
Accepted: 7 December 2016

Journal of Algebra Combinatorics Discrete Structures and Applications

Enumeration of extended irreducible binary Goppa codes of degree 2^m and length $2^n + 1$

Research Article

Augustine I. Musukwa, Kondwani Magamba, John A. Ryan

Abstract: Let n be an odd prime and $m > 1$ be a positive integer. We produce an upper bound on the number of inequivalent extended irreducible binary Goppa codes of degree 2^m and length $2^n + 1$. Some examples are given to illustrate our results.

2010 MSC: 11T71, 68R99

Keywords: Goppa codes, Extended codes, Irreducible Goppa codes, Equivalent codes

1. Introduction

This paper focuses on the class of codes called Goppa codes. It was V. D. Goppa who, in the early 1970's, described this class of codes. Goppa codes form a subclass of alternant codes which has an interesting algebraic structure [6]. Goppa codes are said to contain good parameters. This might be the reason why they are of high practical value. The McEliece cryptosystem and the Niederreiter cyptosystem 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]. As this cryptosystem chooses a Goppa code at 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. This paper seeks to find a tight bound on the number of inequivalent extended irreducible binary Goppa codes of degree 2^m. The count employs the tools which were used to count the non-extended versions (see [8]).

Augustine I. Musukwa (Corresponding Author), John A. Ryan; Mzuzu University, P/Bag 201, Luwinga, Mzuzu 2, Malawi (email: augulela@yahoo.com, jar@mzuzu.org).
Kondwani Magamba; Malawi University of Science and Technology, P.O. Box 5196, Limbe, Malawi (email: kmagamba@must.ac.mw).

2. Preliminaries

As this paper is focused on irreducible Goppa codes we begin with the definition of irreducible Goppa codes.

Definition 2.1. *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 2.2. *Let $\Gamma(L, g)$ be an irreducible Goppa code of length q^n. Then the extended code $\overline{\Gamma(L, g)}$ is defined by $\overline{\Gamma(L, g)} = \{(c_0, c_1, ..., c_{q^n}) : (c_0, c_1, ..., c_{q^n-1}) \in \Gamma(L, g)$ 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 2.3. *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 2.4. *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 2.5. (Ryan, [8]): *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 2.4 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 2.6. *Let H denote the set of all maps $\{\pi_{\zeta,\xi} : \zeta \neq 0, \xi \in \mathbb{F}_{q^n}\}$.*

Definition 2.7. *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 2.8. *The action of H on $\mathbb{S}$ induces orbits denoted by $A(\alpha)$ where $A(\alpha) = \{\zeta\alpha + \xi : \zeta \neq 0, \xi \in \mathbb{F}_{q^n}\}$.*

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 2.9. *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 2.10. *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 2.11. (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 2.10 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 2.12. *Let F denote the set of all maps $\{\pi_{\zeta_1,\zeta_2,\xi_1,\xi_2} : \zeta_j, \xi_j \in \mathbb{F}_{q^n}, j = 1, 2$ 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 2.13. *Let $\alpha \in \mathbb{S}$. Then the* orbit *in $\mathbb{S}$ containing α under the action of F is $O(\alpha) = \{\frac{\zeta_1\alpha+\xi_1}{\zeta_2\alpha+\xi_2} : \zeta_j, \xi_j \in \mathbb{F}_{q^n}, j = 1, 2$ and $\zeta_1\xi_2 - \zeta_2\xi_1 \neq 0\}$.*

The cardinality of $O(\alpha)$ is found in [10] and we state it in the theorem:

Theorem 2.14. *For any $\alpha \in \mathbb{S}$, $|O(\alpha)| = q^{3n} - q^n = (q^n - 1)(q^n)(q^n + 1)$.*

Definition 2.15. *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 $\mathbb{S}$.*

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

Remark 2.16. *From now on we take* $q = 2$.

It is shown in [9] that each of the sets $O(\alpha)$ in $\mathbb{O}_F$ can be partitioned into $2^n + 1$ sets. The theorem below provides more details.

Theorem 2.17. $O(\alpha) = A(\alpha) \cup A(\frac{1}{\alpha}) \cup A(\frac{1}{\alpha+1}) \cup A(\frac{1}{\alpha+\xi_1}) \cup A(\frac{1}{\alpha+\xi_2}) \cup \cdots \cup A(\frac{1}{\alpha+\xi_{2^n-2}})$ *where* $\mathbb{F}_{2^n} = \{0, 1, \xi_1, \xi_2, ..., \xi_{2^n-2}\}$.

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 $2^n + 1$ times the number of elements in $\mathbb{O}_F$, i.e., $|\mathbb{A}| = (2^n + 1) \times |\mathbb{O}_F|$.

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

3. Counting extended irreducible binary Goppa codes of degree 2^m

3.1. Technique of counting

We wish to produce an upper bound on the number of inequivalent extended irreducible binary Goppa codes of degree $r = 2^m$. 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 [4]. Since the Cauchy Frobenius Theorem is central in this paper we state it as follows.

Theorem 3.1 (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. Cardinality of $\mathbb{S}$

In order to simplify our notation we denote all the factors of the degree 2^m by 2^i for $0 \leq i \leq m$. Now to find the number of elements in $\mathbb{S}$ we use the lattice of subfields of $\mathbb{F}_{2^{nM}}$, where $M = 2^m$ as done in [7]. Figure 1 shows the lattice of subfields of $\mathbb{F}_{2^{nM}}$.

Remark 3.2. *In Figure 1 observe that the elements of degree* 2^m *over* $\mathbb{F}_{2^n}$ *lie in* $\mathbb{F}_{2^{n(2^m)}}$ *and* $\mathbb{F}_{2^{2^m}}$. *So the number of elements of degree* 2^m *in* $\mathbb{F}_{2^{n(2^m)}}$ *is* $|\mathbb{S}| = 2^{n(2^m)} - 2^{n(2^{m-1})}$.

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

Note that the group G defined in Definition 2.7 is a cyclic group of order $n2^m$, where $n > 2$ is prime, and it's subgroups are all of the form $\langle \sigma^k \rangle$, where k is a factor of $n2^m$. Further, note that G acts on $\mathbb{A}$. In this section, we determine the G-orbits of this action.

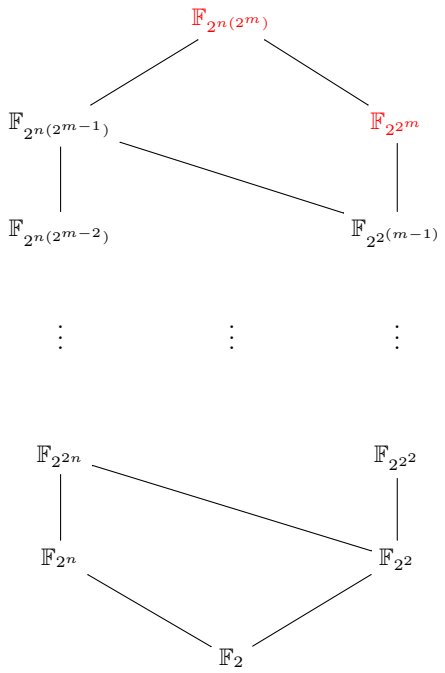

Figure 1.

We first need to know the number of affine sets $A(\alpha)$ which are in $\mathbb{A}$. By Remark 3.2, $|\mathbb{S}| = 2^{n(2^m)} - 2^{n(2^{m-1})}$. 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 $n2^m$. The trivial subgroup $\langle\sigma^{n(2^m)}\rangle$, containing the identity, fixes every affine set in $\mathbb{A}$. In the following subsections, we separately consider the remaining subgroups of G, i.e., $\langle\sigma^{n(2^{m-1})}\rangle$, $\langle\sigma^{2^m}\rangle$, $\langle\sigma^{2^{m-1}}\rangle$, $\langle\sigma^{2^s}\rangle$ and $\langle\sigma^{n(2^s)}\rangle$ where $0 \leq s < m - 1$.

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

Suppose the orbit in $\mathbb{A}$ under the action of G containing $A(\alpha)$ contains $n(2^{m-1})$ affine sets, i.e, $\{A(\alpha), \sigma(A(\alpha)), \sigma^2(A(\alpha)), ..., \sigma^{n(2^{m-1})-1}(A(\alpha))\}$. Then $A(\alpha)$ is fixed by $\langle\sigma^{n(2^{m-1})}\rangle$. That is $\sigma^{n(2^{m-1})}(A(\alpha)) = A(\alpha)$. So we have $\sigma^{n(2^{m-1})}(\alpha) = \alpha^{2^{n(2^{m-1})}} = \zeta\alpha + \xi$ for some $\zeta \neq 0, \xi \in \mathbb{F}_{2^n}$. So applying $\sigma^{n(2^{m-1})}$ for the second time we get $\alpha = \sigma^{n(2^m)}(\alpha) = \sigma^{n(2^{m-1})}(\zeta\alpha + \xi) = \zeta^{2^{n(2^{m-1})}}\alpha^{2^{n(2^{m-1})}} + \xi^{n(2^{m-1})} = \zeta\alpha^{2^{n(2^{m-1})}} + \xi = \zeta(\zeta\alpha + \xi) + \xi = \zeta^2\alpha + (\zeta + 1)\xi$. We conclude that $\zeta = 1$ as otherwise $\zeta \neq 1$ would mean $(1 - \zeta^2)\alpha \in \mathbb{F}_{2^n}$ contradicting the fact that $\alpha \in \mathbb{S}$.

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

$$x^{2^{n(2^{m-1})}} + x + 1 = 0. \tag{1}$$

If α satisfies (1) then certainly 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 (1). This follows because the equation $(\zeta\alpha + \xi)^{2^{n(2^{m-1})}} =$

$\zeta\alpha^{2^{n(2^{m-1})}} + \xi = \zeta(\alpha+1)+\xi = \zeta\alpha+\zeta+\xi = (\zeta\alpha+\xi)+1$ holds if and only if $\zeta = 1$. Hence if α satisfies (1) then $A(\alpha)$ contains precisely 2^n roots of (1).

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

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

where β_i denotes all the elements of $\mathbb{F}_{2^{n(2^{m-1})}}$ which have trace 1 over $\mathbb{F}_2$ [5]. We know that there are precisely $2^{n(2^{m-1})-1}$ such β_i. Note that the trace function we are dealing with is from the field $\mathbb{F}_{2^{n(2^{m-1})}}$ to $\mathbb{F}_2$. So even if an element is in a proper subfield of $\mathbb{F}_{2^{n(2^{m-1})}}$, in calculating its trace we regard it as an element of $\mathbb{F}_{2^{n(2^{m-1})}}$. We further observe that if $\beta \in \mathbb{F}_{2^{n(2^{m-2})}}$, then $Trace_{\mathbb{F}_{2^{n(2^{m-1})}}|\mathbb{F}_2}(\beta) = 2 \cdot Trace_{\mathbb{F}_{2^{n(2^{m-2})}}|\mathbb{F}_2}(\beta)$. Since the characteristic is 2, then we conclude that none of the β_i in the decomposition of $x^{2^{n(2^{m-1})}} + x + 1$ in (2) lie in $\mathbb{F}_{2^{n(2^{m-1})}}$. However $2^{2^{m-1}-1}$ of the β_i lie in $\mathbb{F}_{2^{2^{m-1}}}$ and the remaining $2^{n(2^{m-1})-1} - 2^{2^{m-1}}$ lie in $\mathbb{F}_{2^{2^{m-1}n}}$ (not in any of its subfields). Furthermore, all the quadratic factors on the right hand side of (2) are irreducible over $\mathbb{F}_{2^{n(2^{m-1})}}$. This is due to linearity of the trace function and the fact that $Trace(\beta_i) = 1$ for each β_i. The $2^{2^{m-1}-1}$ quadratic equations corresponding to the β_i in $\mathbb{F}_{2^{2^{m-1}}}$ have $\mathbb{F}_{2^{2^m}}$ as their splitting field while the remaining $2^{n(2^{m-1})-1} - 2^{2^{m-1}-1}$ quadratic equations have $\mathbb{F}_{2^{n(2^m)}}$ as their splitting field. So all the $2^{n(2^{m-1})}$ roots lie in $\mathbb{S}$.

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

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

Suppose the orbit in $\mathbb{A}$ under the action of G containing $A(\alpha)$ contains $n(2^s)$ affine sets where $0 \le s < m-1$. As in Subsection 3.3.1, we have $A(\alpha)$ fixed by $\langle\sigma^{n(2^s)}\rangle$ and $\sigma^{n(2^s)}(\alpha) = \alpha^{2^{n(2^s)}} = \zeta\alpha + \xi$ for some $\zeta \neq 0, \xi \in \mathbb{F}_{2^n}$. Applying $\sigma^{n(2^s)}$ for 2^{m-s} times to α we obtain $\alpha = \sigma^{n(2^m)}(\alpha) = \zeta^{2^{m-s}}\alpha + (\zeta^{2^{m-s}-1} + \zeta^{2^{m-s}-2} + \cdots + \zeta^2 + \zeta + 1)\xi$. We conclude that $\zeta^{2^{m-s}} = 1$ otherwise $\zeta^{2^{m-s}} \neq 1$ would mean $(1-\zeta^{2^{m-s}})\alpha \in \mathbb{F}_{2^n}$ contradicting the fact that $\alpha \in \mathbb{S}$. The possibilities are that $\zeta^{2^{m-s}} = 1$, $\zeta^{2^{m-s-1}} = 1$, $\zeta^{2^{m-s-2}} = 1$, $\cdots$, $\zeta^{2^2} = 1$, $\zeta^2 = 1$ or $\zeta = 1$. Since $2^n - 1$ is odd then it is not divisible by 2^d where $1 \le d \le m-s$. Hence $\zeta^{2^{m-s}} = 1$ implies $\zeta = 1$.

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

3.3.3. $\langle\sigma^{2^m}\rangle$ 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 $\langle\sigma^{2^m}\rangle$. In [8], it is proved that the number of affine sets fixed by $\langle\sigma^r\rangle$ is $|\mathbb{S}(1,r)|/(q(q-1))$. Hence the number of affine sets fixed by $\langle\sigma^{2^m}\rangle$ is $|\mathbb{S}(1,2^m)|/(2(2-1)) = (2^{2^m} - 2^{2^{m-1}})/2 = 2^{2^m-1} - 2^{2^{m-1}-1}$.

3.3.4. $\langle\sigma^{2^{m-1}}\rangle$ 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} affine sets. Then $A(\alpha)$ is fixed by $\langle\sigma^{2^{m-1}}\rangle$. So we have $\sigma^{2^{m-1}}(\alpha) = \alpha^{2^{2^{m-1}}} = \zeta\alpha + \xi$ for some $\zeta \neq 0, \xi \in \mathbb{F}_{2^n}$. But if $A(\alpha)$ is fixed under $\langle\sigma^{2^{m-1}}\rangle$ then it is also fixed under $\langle\sigma^{2^m}\rangle$ since $\langle\sigma^{2^m}\rangle \subset \langle\sigma^{2^{m-1}}\rangle$. So $A(\alpha)$ contains a fixed point. That is $A(\alpha)$ contains some elements which satisfy $x^{2^{2^m}} = x$ and these elements are in

$\mathbb{F}_{2^{2^m}} \setminus \mathbb{F}_{2^{2^{m-1}}}$. Assume $\alpha \in \mathbb{F}_{2^{2^m}} \setminus \mathbb{F}_{2^{2^{m-1}}}$ then applying $\sigma^{2^{m-1}}$ twice to α we obtain $\alpha = \alpha^{2^{2^m}} = \zeta^{2^{2^{m-1}}}(\zeta\alpha+\xi)+\xi^{2^{2^{m-1}}} = \zeta^{2^{2^{m-1}}+1}\alpha+\zeta^{2^{2^{m-1}}}\xi+\xi^{2^{2^{m-1}}} = \zeta^{2^{2^{m-1}}+1}\alpha+\zeta^{2^{2^{m-1}}}\xi+\xi^{2^{2^{m-1}}}$. We conclude that $\zeta^{2^{2^{m-1}}+1} = 1$ otherwise $\zeta^{2^{2^{m-1}}+1} \neq 1$ would mean $(1-\zeta^{2^{2^{m-1}}+1})\alpha \in \mathbb{F}_{2^n}$ contradicting the fact that α is of degree 2^m.

Now we show that $2^{2^{m-1}}+1$ is relatively prime to 2^n-1. We simply show that any number of the form 2^d+1 is relatively prime to 2^n-1. That is it suffices to show that $(2^d+1, 2^n-1) = 1$. We show this by contradiction. Assume that $(2^d+1, 2^n-1) \neq 1$. That is there must be some odd prime p which divides both 2^d+1 and 2^n-1. This implies that $2^n \equiv 1 \pmod{p}$ and $2^d \equiv -1 \pmod{p}$. So $2^d \equiv -1 \pmod{p}$ implies $2^{2d} \equiv (-1)^2 = 1 \equiv 2^n \pmod{p}$. Thus $n \equiv 2d \pmod{(p-1)}$. Since $p-1$ is even then n is also even. This establishes a contradiction since n is an odd prime. Hence $(2^d+1, 2^n-1) = 1$ for odd n.

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

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

$$x^{2^{2^{m-1}}}+x+1 = 0. \tag{3}$$

Observe that $\alpha+1$ also satisfies (3) and one can easily check that these are the only elements in $A(\alpha)$ which satisfy (3). Using an argument similar to the one in Subsection 3.3.1, all the $2^{2^{m-1}}$ roots of $x^{2^{2^{m-1}}}+x+1$ lie in $\mathbb{F}_{2^{2^m}} \setminus \mathbb{F}_{2^{2^{m-1}}}$. Hence we conclude that there are $2^{2^{m-1}-1}$ affine sets fixed under $\langle\sigma^{2^{m-1}}\rangle$.

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

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

$$\begin{aligned}
\alpha &= \alpha^{2^{2^m}} \\
&= \zeta^{2^{\overline{n}\cdot 2^s}+2^{(\overline{n}-1)\cdot 2^s}+\cdots+2^{3\cdot 2^s}+2^{2\cdot 2^s}+2^{2^s}+1}\alpha \\
&+ \zeta^{2^{\overline{n}\cdot 2^s}+2^{(\overline{n}-1)\cdot 2^s}+\cdots+2^{3\cdot 2^s}+2^{2\cdot 2^s}+2^{2^s}}\xi \\
&+ \zeta^{2^{\overline{n}\cdot 2^s}+2^{(\overline{n}-1)\cdot 2^s}+\cdots+2^{3\cdot 2^s}+2^{2\cdot 2^s}}\xi^{2^{2^s}} \\
&+ \zeta^{2^{\overline{n}\cdot 2^s}+2^{(\overline{n}-1)\cdot 2^s}+\cdots+2^{3\cdot 2^s}}\xi^{2^{2\cdot 2^s}} \\
&+ \cdots \\
&+ \zeta^{2^{\overline{n}\cdot 2^s}+2^{(\overline{n}-1)\cdot 2^s}}\xi^{2^{(\overline{n}-2)\cdot 2^s}} \\
&+ \zeta^{2^{\overline{n}\cdot 2^s}}\xi^{2^{(\overline{n}-1)\cdot 2^s}} \\
&+ \xi^{2^{\overline{n}\cdot 2^s}}
\end{aligned} \tag{4}$$

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

We now show that $2^{\overline{n}\cdot 2^s}+2^{(\overline{n}-1)\cdot 2^s}+\cdots+2^{3\cdot 2^s}+2^{2\cdot 2^s}+2^{2^s}+1$ and 2^n-1 are coprime. First observe that

$2^{\overline{n}\cdot 2^s}+2^{(\overline{n}-1)\cdot 2^s}+\cdots+2^{3\cdot 2^s}+2^{2\cdot 2^s}+2^{2^s}+1=(2^{s(\overline{n}+1)}-1)/(2^{2^s}-1)=(2^{2^m}-1)/(2^{2^s}-1)$. But $(2^m,n)=1$ so $(2^{2^m}-1,2^n-1)=1$ from which we conclude that $(2^{\overline{n}\cdot 2^s}+2^{(\overline{n}-1)\cdot 2^s}+\cdots+2^{3\cdot 2^s}+2^{2\cdot 2^s}+2^{2^s}+1,2^n-1)=1$.

We can now conclude that $\zeta^{2^{\overline{n}\cdot 2^s}+2^{(\overline{n}-1)\cdot 2^s}+\cdots+2^{3\cdot 2^s}+2^{2\cdot 2^s}+2^{2^s}+1}=1$ implies $\zeta=1$. Since $\zeta=1$ then (4) becomes $\alpha=\alpha+\xi+\xi^{2^{2^s}}+\xi^{2^{2\cdot 2^s}}+\cdots+\xi^{2^{(\overline{n}-2)2^s}}+\xi^{2^{(\overline{n}-1)2^s}}+\xi^{2^{\overline{n}\cdot 2^s}}$. It is clear that ξ is in the intersection of the fields of order 2^{2^s} and 2^n. Since $(2^s,n)=1$ then ξ is 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 $\alpha^{2^{2^s}}=\alpha+1$. Clearly α satisfies the equation $x^{2^{2^s}}+x+1=0$. Observe that $\alpha+1$ also satisfies the equation $x^{2^{2^s}}+x+1=0$ and one can easily check that these are the only elements in $A(\alpha)$ which satisfy $x^{2^{2^s}}+x+1=0$. Using similar argument to the one in Subsection 3.3.1, all the 2^{2^s} roots of $x^{2^{2^s}}+x+1$ lie in $\mathbb{F}_{2^{2^s-1}}$ not in $\mathbb{S}$. Hence we conclude that there is no affine set fixed under $\langle\sigma^{2^s}\rangle$.

3.4. The number of orbits in $\mathbb{A}$ under the action of G

We use Table 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 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 $\langle\sigma^{n(2^m)}\rangle$ 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.

Subgroup of G	Order of Subgroup	No. of elements not in previous subgroup	No. of fixed affine sets	Product of columns 3 and 4
$\langle\sigma^{2^m n}\rangle$	1	1	$\frac{2^{n(2^m)}-2^{n(2^{m-1})}}{2^n(2^n-1)}$	$\frac{2^{n(2^m)}-2^{n(2^{m-1})}}{2^n(2^n-1)}$
$\langle\sigma^{n(2^{m-1})}\rangle$	2	1	$2^{n(2^{m-1}-1)}$	$2^{n(2^{m-1}-1)}$
$\langle\sigma^{2^m}\rangle$	n	$n-1$	$2^{2^m-1}-2^{2^{m-1}-1}$	$(n-1)(2^{2^m-1}-2^{2^{m-1}-1})$
$\langle\sigma^{2^{m-1}}\rangle$	$2n$	$n-1$	$2^{2^{m-1}-1}$	$(n-1)2^{2^{m-1}-1}$

By the Cauchy Frobenius Theorem, the number of orbits in $\mathbb{A}$ under the action of G is $\frac{(2^{n(2^m)}-2^{n(2^{m-1})})/(2^n(2^n-1))+2^{n(2^{m-1}-1)}+(n-1)\times 2^{2^m-1}}{n(2^m)}$.

Remark 3.3. *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 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 $O(\alpha)$'s 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 $\mathbb{O}_F$. By Remark 3.2, $|\mathbb{S}|=2^{n(2^m)}-2^{n(2^{m-1})}$. Since $|O(\alpha)|=2^n(2^n-1)(2^n+1)$ then $|\mathbb{O}_F|=\frac{|\mathbb{S}|}{2^n(2^n-1)(2^n+1)}$.

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

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

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

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

Suppose $O(\alpha) \in \mathbb{O}_F$ is fixed under $\langle\sigma^{n(2^s)}\rangle$ where $0 \leq s < m$. Then $\langle\sigma^{n(2^s)}\rangle$ acts on $O(\alpha)$. We can consider $O(\alpha)$ as a set of 2^n+1 affine sets. $\langle\sigma^{n(2^s)}\rangle$ partitions this set of 2^n+1 affine sets. The only possible lengths of orbits are all factors of 2^{m-s}. Since $O(\alpha)$ contains an odd number of affine sets then the possibility that all orbits are of even length is precluded. By Subsection 3.3.2, there is no affine set fixed under $\langle\sigma^{n(2^s)}\rangle$. So we also preclude the possibility of length 1. Hence we conclude that no $O(\alpha)$ in $\mathbb{O}_F$ is fixed under $\langle\sigma^{n(2^s)}\rangle$.

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

Suppose $O(\alpha) \in \mathbb{O}_F$ is fixed under $\langle\sigma^{2^m}\rangle$. Then $\langle\sigma^{2^m}\rangle$ acts on $O(\alpha)$ which is seen as a set of 2^n+1 affine sets. $\langle\sigma^{2^m}\rangle$ partitions this set of 2^n+1 affine sets. The only possible lengths of orbits 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 $\langle\sigma^{2^m}\rangle$. We claim that there are only three affine sets in $O(\alpha)$ which are fixed under $\langle\sigma^{2^m}\rangle$. 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 $\langle\sigma^{2^m}\rangle$. So, by Subsection 3.3.3, $A(\alpha)$ contains a fixed point, i.e., some elements of $A(\alpha)$ satisfy the equation $x^{2^{2^m}} = x$. It is clear that α and $\alpha+1$ in $A(\alpha)$ satisfy $x^{2^{2^m}} = x$. Since $(\frac{1}{\alpha})^{2^{2^m}} = \frac{1}{\alpha}$ and $(\frac{1}{\alpha+1})^{2^{2^m}} = \frac{1}{\alpha+1}$ 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 $\langle\sigma^{2^m}\rangle$. First observe that, for $\nu \in \mathbb{F}_{2^n} \setminus \{0, 1\}$, we have $\nu^{2^{2^m}} \neq \nu$ since $(2^m, n) = 1$. So $(\frac{1}{\alpha+\nu})^{2^{2^m}} = \frac{1}{\alpha+\nu^{2^{2^m}}} = \frac{1}{\alpha+\eta}$ implies that $\sigma^{2^m}(A(\frac{1}{\alpha+\nu})) = A(\frac{1}{\alpha+\eta})$ as required. Therefore $A(\alpha)$, $A(\frac{1}{\alpha})$ and $A(\frac{1}{\alpha+1})$ are the only affine sets fixed under $\langle\sigma^{2^m}\rangle$. By Subsection 3.3.3, there are $2^{2^m-1} - 2^{2^{m-1}-1}$ affine sets which are fixed under $\langle\sigma^{2^m}\rangle$. Hence the number of $O(\alpha)$'s in $\mathbb{O}_F$ which are fixed under $\langle\sigma^{2^m}\rangle$ is $(2^{2^m-1} - 2^{2^{m-1}-1})/3$.

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

Suppose $O(\alpha) \in \mathbb{O}_F$ is fixed under $\langle\sigma^{2^{m-1}}\rangle$. Then $\langle\sigma^{2^{m-1}}\rangle$ acts on $O(\alpha)$ which is seen as a set of 2^n+1 affine sets. $\langle\sigma^{2^{m-1}}\rangle$ 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 $\langle\sigma^{2^{m-1}}\rangle$. We claim that any $O(\alpha)$ fixed under $\langle\sigma^{2^{m-1}}\rangle$ contains precisely one affine set fixed under $\langle\sigma^{2^{m-1}}\rangle$. By Subsection 3.3.4, an affine set fixed under $\langle\sigma^{2^{m-1}}\rangle$ contains some elements which satisfy the equation $x^{2^{2^{m-1}}} + x + 1 = 0$. Suppose $A(\alpha)$ is fixed under $\langle\sigma^{2^{m-1}}\rangle$. It is clear that α and $\alpha+1$ satisfy $x^{2^{2^{m-1}}} + x + 1 = 0$. We also observe that $(\frac{1}{\alpha})^{2^{2^{m-1}}} = \frac{1}{\alpha+1}$ and $(\frac{1}{\alpha+1})^{2^{2^{m-1}}} = \frac{1}{\alpha}$ which imply that $\sigma^{2^{m-1}}(A(\frac{1}{\alpha})) = A(\frac{1}{\alpha+1})$ and $\sigma^{2^{m-1}}(A(\frac{1}{\alpha+1})) = A(\frac{1}{\alpha})$. We can conclude that $A(\frac{1}{\alpha})$ and $A(\frac{1}{\alpha+1})$ form an orbit of length 2. Since $\langle\sigma^{2^m}\rangle \subset \langle\sigma^{2^{m-1}}\rangle$ then any $O(\alpha)$ or affine set fixed under $\langle\sigma^{2^{m-1}}\rangle$ is also fixed under $\langle\sigma^{2^m}\rangle$. By Subsection 3.3.3, no affine set after $A(\frac{1}{\alpha+1})$ in the decomposition of $O(\alpha)$ is fixed under $\langle\sigma^{2^m}\rangle$. So we conclude that $\langle\sigma^{2^{m-1}}\rangle$ does not fix any affine set after $A(\frac{1}{\alpha+1})$ in the decomposition of $O(\alpha)$. By Subsection 3.3.4, there are $2^{2^{m-1}-1}$ affine sets fixed under $\langle\sigma^{2^{m-1}}\rangle$. So we conclude that the number of $O(\alpha)$'s in $\mathbb{O}_F$ which are fixed under $\langle\sigma^{2^{m-1}}\rangle$ is $2^{2^{m-1}-1}$.

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

Suppose $O(\alpha) \in \mathbb{O}_F$ is fixed under $\langle\sigma^{2^s}\rangle$ where $0 \le s < m-1$. Then $\langle\sigma^{2^s}\rangle$ acts on $O(\alpha)$ which is seen as a set of 2^n+1 affine sets. $\langle\sigma^{2^s}\rangle$ partitions this set of 2^n+1 affine sets. The possible lengths of orbits are all factors of $n(2^{m-s})$. 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. 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 $2^n+1 \equiv 3 \pmod n$, x has the form $kn+3$ where k is an odd integer. Since $2|x$ then k is non zero. So there are $kn+3 > 3$ affine sets permuted in orbits of length 2 under $\langle\sigma^s\rangle$. Since $\langle\sigma^{s+1}\rangle \subset \langle\sigma^s\rangle$ it is easy to observe that two affine sets that form an orbit under $\langle\sigma^s\rangle$ are fixed under $\langle\sigma^{s+1}\rangle$. If $s = m-2$ then it would mean that there exist a fixed $O(\alpha)$ under $\langle\sigma^{2^{m-1}}\rangle$ which contains more than 3 affine sets fixed under $\langle\sigma^{2^{m-1}}\rangle$, contradicting Subsection 3.5.4. No affine set is fixed under $\langle\sigma^{2^{s+1}}\rangle$ for $s < m-2$ (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 $\langle\sigma^{2^{s+1}}\rangle$. A similar argument can be used to show that length of multiple of 2 and n are also not possible. So there must be at least an affine set in $O(\alpha)$ fixed under $\langle\sigma^{2^s}\rangle$. By Subsection 3.3.5, no affine set is fixed by $\langle\sigma^{2^s}\rangle$. Hence there is no $O(\alpha)$ in $\mathbb{O}_F$ which is fixed under $\langle\sigma^{2^s}\rangle$.

3.6. The number of orbits in $\mathbb{O}_F$ under the action of G

Table 2 shows the number of $O(\alpha)$'s in $\mathbb{O}_F$ which are fixed under the various subgroups of G. The structure of this table is similar to that of Table 1. The subgroups which do not fix any $O(\alpha)$ 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 $\langle\sigma^{n(2^m)}\rangle$ since it contains only 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 $O(\alpha)$'s by the elements in G.

By the Cauchy Frobenius Theorem, the number of orbits in $\mathbb{O}_F$ under the action of G is $\frac{(2^{n(2^m)} - 2^{n(2^{m-1})})/(2^n(2^n-1)(2^n+1)) + 2^{(2^{m-1}-1)n} + (n-1)[(2^{2^m-1}+2^{2^{m-1}})/3]}{n(2^m)}$.

Table 2.

Subgroup of G	Order of Subgroup	No. of elements not in previous subgroup	No. of fixed $O(\alpha)$'s	Product of columns 3 and 4
$\langle\sigma^{n(2^m)}\rangle$	1	1	$\frac{2^{n(2^m)}-2^{n(2^{m-1})}}{2^n(2^n-1)(2^n+1)}$	$\frac{2^{n(2^m)}-2^{n(2^{m-1})}}{2^n(2^n-1)(2^n+1)}$
$\langle\sigma^{n(2^{m-1})}\rangle$	2	1	$2^{(2^{m-1}-1)n}$	$2^{(2^{m-1}-1)n}$
$\langle\sigma^{2^m}\rangle$	n	$n-1$	$2^{2^{m-1}}-2^{2^{m-1}-1}$	$(n-1)(2^{2^{m-1}}-2^{2^{m-1}-1})/3$
$\langle\sigma^{2^{m-1}}\rangle$	$2n$	$n-1$	$2^{2^{m-1}-1}$	$(n-1)2^{2^{m-1}-1}$

We state this result in the following theorem:

Theorem 3.4 (The Main Theorem)**.** *Let n be an odd prime number and $m > 1$. The number of inequivalent extended irreducible binary Goppa codes of degree 2^m and length 2^n+1 is at most*

$$\frac{(2^{n(2^m)}-2^{n(2^{m-1})})/(2^n(2^n-1)(2^n+1))+2^{(2^{m-1}-1)n}+(n-1)[(2^{2^m-1}+2^{2^{m-1}})/3]}{n(2^m)}.$$

Example 3.5. *We find an upper bound on the number of irreducible Goppa codes and extended irreducible Goppa codes of degree 4 for $n = 5, 7, 11,$ 13 and 17 as follows:*

n	*Upper bound on number of irreducible Goppa codes*	*Upper bound on number of extended irreducible Goppa codes*
5	*56*	*4*
7	*596*	*10*
11	*95420*	*94*
13	*1290872*	*316*
17	*252648992*	*3856*

Example 3.6. *We find an upper bound on the number of irreducible Goppa codes of degree 16 and extended irreducible Goppa codes for $n = 7$ and 11.*

n	*Upper bound on number of irreducible Goppa codes*	*Upper bound on number of extended irreducible Goppa codes*
7	*2,851,857,368,342,478,330,960,957,440*	*22,107,421,460,024,199,242,917,600*
11	$1.29813175585637777519535861321\times10^{44}$	$6.335440487342009639887471882 70\times10^{40}$

4. Conclusion

In this paper we have produced an upper bound on the number of extended irreducible binary Goppa codes of degree 2^m and length 2^n+1 where n is a prime number. The result is presented in the Theorem 3.4.

References

[1] T. P. Berger, Goppa and related codes invariant under a prescribed permutation, IEEE Trans. Inform. Theory 46(7) (2000) 2628–2633.

[2] C. L. Chen, Equivalent irreducible Goppa codes, IEEE Trans. Inform. Theory 24(6) (1978) 766–769.

[3] H. Dinh, C. Moore, A. Russell, McEliece and Niederreiter cryptosystems that resist quantum Fourier sampling attacks, In: Rogaway P. (eds) Advances in Cryptology – CRYPTO 2011. CRYPTO 2011. Lecture Notes in Computer Science 6841 (2011) 761–779.

[4] I. M. Isaacs, Algebra: A Graduate Text, Brooks/Cole, Pacific Grove, 1994.

[5] R. Lidl, H. Niederreiter, Introduction to Finite Fields and Their Applications, Cambridge University Press, London, 1994.

[6] S. Ling, C. Xing, Coding Theory; A First Course, Cambridge University Press, United Kingdom, 2004.

[7] 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) 1–4.

[8] J. A. Ryan, Irreducible Goppa Codes, Ph.D. Dissertation, University College Cork, 2004.

[9] J. A. Ryan, A new connection between irreducible and extended irreducible Goppa codes, Proc. SAMSA (2012) 152–154.

[10] J. A. Ryan, Counting extended irreducible binary quartic Goppa codes of length 2^n+1, IEEE Trans. Inform. Theory 61(3) (2015) 1174–1178.