Irreducible Goppa codes

John A. Ryan* and Patrick Fitzpatrick†

Abstract

We consider irreducible Goppa codes over $\mathbb{F}_q$ of length q^n defined by polynomials of degree r where q is a prime power and n, r are arbitrary integers. We obtain an upper bound on the number of such codes. We also exhibit categories of quasicyclic Goppa codes which depend only on numerical conditions on the parameters p, n, r. Finally we give a method for generating all cubic Goppa codes.
Key words: Classical Goppa codes, McEliece cryptosystem, enumeration, Cauchy-Frobenius.

1 Introduction

Classical Goppa codes form a large family about which little is known, in general. They are sometimes referred to as being *near to arbitrary* or *near to random* [1]. Their parameters, such as dimension and minimum distance, and their automorphism groups are unknown. However they are easily generated, as any polynomial over a finite field generates such a code. The cryptographic potential of Goppa codes was recognised in the McEliece cryptosystem [4], which is still regarded as secure nearly a quarter of a century after it was first proposed. There is a very large number of Goppa codes with similar parameters. Their number grows exponentially with the length of the code and with the degree of the Goppa polynomial. However, not all irreducible polynomials of a given degree over a finite field generate inequivalent codes and the precise number of such codes, on which the security of the McEliece cryptosystem depends, is not known. In 1978, Chin-Long Chen [5] derived an upper bound on the number of equivalence classes of irreducible Goppa codes. In a previous paper [10, 11] paper we gave an improved bound for certain values of the parameters (field size, length, degree of the Goppa polynomial). In this paper we consider the general case and give an improved bound for the number of Goppa codes of length q^n, defined by irreducible polynomials of degree r, where $q = p^t$ (p a prime), for arbitrary p, n, t, r. In many cases, at least for small values of the parameters, this bound is precise, although we can also generate examples where the bound is not met. In order to make this paper relatively self-contained, we repeat and extend some of the preliminary material from [10, 11].

2 Preliminaries

Let , (L, g) be an irreducible Goppa code over $\mathbb{F}_q$ with defining set $L = \mathbb{F}_{q^n}$, where $g(z) \in \mathbb{F}_{q^n}[z]$ is an irreducible polynomial of degree r. Then a vector $c = (c_0, c_1, \ldots c_{q^n-1})$ with

*Department of Mathematics, Mzuzu University, Mzuzu, Malawi
†Boole Centre for Research in Informatics, National University of Ireland, Cork, Ireland

components in $\mathbb{F}_q$ is a codeword in , (L, g) if and only if

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

where we adopt a fixed ordering on $L = \mathbb{F}_{q^n} = \{\zeta_i : 0 \le i \le q^n - 1\}$. The roots of $g(z)$ lie in $\mathbb{F}_{q^{nr}}$, and if α is any root then $g(z) = \prod_{i=0}^{r-1}(z - \alpha^{q^{ni}})$. Thus condition (1) is equivalent to the r equations

$$\sum_{i=0}^{q^n-1} \frac{c_i}{\alpha^{q^{nj}} - \zeta_i} = 0, \qquad 0 \le j \le r-1. \tag{2}$$

Since all the components c_i of the codeword c lie in $\mathbb{F}_q$ and all the ζ_i lie in $\mathbb{F}_{q^n}$, condition (2) is equivalent to

$$\left(\sum_{i=0}^{q^n-1} \frac{c_i}{\alpha - \zeta_i}\right)^{q^{nj}} = 0, \qquad 0 \le j \le r-1 \tag{3}$$

which is equivalent to the single equation

$$\sum_{i=0}^{q^n-1} \frac{c_i}{\alpha - \zeta_i} = 0. \tag{4}$$

Hence , (L, g) is completely described by any root α of $g(z)$, and we may denote this code $C(\alpha)$. Clearly any element of degree r over $\mathbb{F}_{q^n}$ defines such a code. Using the single equation in (4) we get the following parity check matrix H for $C(\alpha)$

$$H = \begin{pmatrix} \frac{1}{\alpha-\zeta_0} & \frac{1}{\alpha-\zeta_1} & \cdots & \frac{1}{\alpha-\zeta_{q^n-1}} \end{pmatrix}. \tag{5}$$

We make the definition.

DEFINITION 2.1 The set $\mathbb{S} = \mathbb{S}(n, r)$ is the set of all elements in $\mathbb{F}_{q^{nr}}$ of degree r over $\mathbb{F}_{q^n}$.

Next we establish the theorem.

Theorem 2.2 *If $\alpha, \beta \in \mathbb{S}$ are related by an equation $\beta = \zeta\alpha^{q^i} + \xi$ for some $\zeta \neq 0, \xi \in \mathbb{F}_{q^n}$ then $C(\alpha)$ is equivalent to $C(\beta)$.*

We define the following maps on $\mathbb{S}$, where $\zeta, \xi \in \mathbb{F}_{q^n}, \zeta \neq 0$.

1. $\tau_\xi : \alpha \mapsto \alpha + \xi$
2. $\mu_\zeta : \alpha \mapsto \zeta\alpha$.

3 Enumeration of irreducible Goppa codes

Using Theorem 2.2 we construct an upper bound on the number of inequivalent irreducible Goppa codes for fixed q, n and r in the following way. The set of all irreducible Goppa codes over $\mathbb{F}_q$ of length q^n and degree r is $\{C(\alpha) : \alpha \in \mathbb{S}\}$. If $\alpha, \beta \in \mathbb{S}$ are related by an equation

$$\beta = \zeta \alpha^{q^i} + \xi \text{ for some } \zeta \neq 0, \xi \in \mathbb{F}_{q^n} \tag{6}$$

then $C(\alpha)$ and $C(\beta)$ are equivalent (Theorem 2.2). The set $F = \{\tau_\xi \circ \mu_\zeta : \xi, \zeta \neq 0 \in \mathbb{F}_{q^n}\}$ forms the group of affine transformations and acts on $\mathbb{S}$. The set $G = \{\sigma^i : 1 \leq i \leq nr\}$ forms the Frobenius group and again acts on $\mathbb{S}$. It is clear that the orbits in $\mathbb{S}$ under FG (semidirect product) are precisely those elements related by an equation of type (6). Thus any two elements in the same orbit generate equivalent Goppa codes. The number of orbits in $\mathbb{S}$ under FG then gives us the required upper bound on the number of Goppa codes.

4 Orbits of $\mathbb{S}$ under F

We first consider the action of the affine group F. Let α be an arbitrary element of $\mathbb{S}$. If $\zeta_1\alpha + \xi_1 = \zeta_2\alpha + \xi_2$ and $\zeta_1 = \zeta_2$ then $\xi_1 = \xi_2$, while if $\zeta_1 \neq \zeta_2$ then $\alpha = (\xi_2 - \xi_1)/(\zeta_1 - \zeta_2)$, contrary to $\alpha \in \mathbb{S}$. Thus the orbit containing α, denoted $A(\alpha)$ and called *the affine set containing* α, contains $q^n(q^n - 1)$ elements. It is obvious that $A(\beta) = A(\alpha)$ for any $\beta \in A(\alpha)$. We denote the set of all affine sets, that is, $\{A(\alpha) : \alpha \in \mathbb{S}\}$, by $\mathbb{A}$. We conclude that $|\mathbb{A}| = |\mathbb{S}|/q^n(q^n - 1)$.

EXAMPLE 4.1 Let $q = 2, n = 4, r = 3$. Then $\mathbb{S} = \mathbb{F}_{2^{12}} \setminus \mathbb{F}_{2^4}$ and there are $\dfrac{2^{12} - 2^4}{2^4(2^4 - 1)} = 17$ affine sets in $\mathbb{A}$.

EXAMPLE 4.2 Let q and n be arbitrary and let $r = 2$. Then $\mathbb{S} = \mathbb{F}_{q^{2n}} \setminus \mathbb{F}_{q^n}$ and there is only $1 = \dfrac{q^{2n} - q^n}{q^n(q^n - 1)}$ affine set in $\mathbb{A}$.

REMARK 4.3 Since in the case $r = 2$ there is only one orbit, we shall from now on assume $r > 2$.

Next, we observe that σ permutes the affine sets within $\mathbb{A}$ since if $\beta = \zeta\alpha + \xi$ is an arbitrary element of $A(\alpha)$ then $\beta^q = \zeta^q\alpha^q + \xi^q \in A(\alpha^q)$. So $G = \langle\sigma\rangle$ acts on $\mathbb{A}$. Our strategy is first to apply the action of F to $\mathbb{S}$ to obtain $\mathbb{A}$. Then we apply the action of G to $\mathbb{A}$ to obtain the orbits in $\mathbb{S}$ of FG. The action of F on $\mathbb{S}$ is straightforward as shown above. However the action of G on $\mathbb{A}$ is more complicated. This latter action is analyzed in the following section.

5 Orbits of $\mathbb{A}$ under G

The group $G = \langle\sigma\rangle$ is a cyclic group of order nr. In analyzing the action of G on $\mathbb{A}$ we will need to refer to the factorizations of n and r, highlighting the divisors that are products of those primes dividing only one of n or r and those that divide both. In order not to overburden the notation with explicit prime factorizations, we define k to be the largest divisor of n that is relatively prime to r and set $\ell_n = n/k$, and m to be the largest divisor of r

that is relatively prime to n and set $\ell_r = r/m$. Thus $nr = k\ell m = k\ell_n\ell_r m$, where $\ell = \ell_n\ell_r$. We often need to work with a divisor k_1 of k and write $\bar{k}_1 = k/k_1$. The symbols k_2, k_3 etc. will denote divisors of k possibly distinct from k_1, and similar notation will be used for divisors of ℓ, m, n, r, where appropriate, without explicit mention. The letter p will always denote the characteristic of the field and p_1 some other prime distinct from p. We define $K = \langle\sigma^{\ell m}\rangle, L = \langle\sigma^{km}\rangle, M = \langle\sigma^{k\ell}\rangle$. Thus, $|K| = k, |L| = \ell, |M| = m$ and by elementary group theory $G = K \times L \times M$.

EXAMPLE 5.1 Let $q = 2, n = 6, r = 10$. Then $k = 3, \ell = 4, m = 5$ and $K = \langle\sigma^{20}\rangle, L = \langle\sigma^{15}\rangle, M = \langle\sigma^{12}\rangle$. Thus, $|K| = 3, |L| = 4, |M| = 5$ and $G = K \times L \times M$.

In order to count the orbits in $\mathbb{A}$ under the action of G we count the fixed points of this action and then apply the Cauchy-Frobenius Theorem (see [7], for example). In other words we count the affine sets $A(\alpha)$ in $\mathbb{A}$ which are fixed under the various subgroups of G and then calculate the average number of affine sets fixed by an element of G. Observe that if $A(\alpha)$ is fixed by $\langle\sigma^s\rangle$, then $\langle\sigma^s\rangle$ also acts on $A(\alpha)$ and $A(\alpha)$ itself may contain elements of $\mathbb{S}$ fixed by $\langle\sigma^s\rangle$. To make things clear we will refer to these elements as *fixed points* and refer to the elements of $\mathbb{A}$ that are fixed as *fixed affine sets*. We introduce some notation. Let u, v be integers. The greatest common divisor of u, v will be denoted by (u, v). We also write $\pi(u, v) = p_1^{a_1}p_2^{a_2}\cdots p_b^{a_b}$, where $p_1, p_2, \ldots, p_b$ are the primes occurring in the prime factorization of v and a_i is the largest power of p_i dividing u, $1 \le i \le b$, $a_i \ge 0$. Also, since an irreducible polynomial of degree r over $\mathbb{F}_{q^{k_1\ell_n}}$ remains irreducible over $\mathbb{F}_{q^{k\ell_n}}$ [8, Theorem 3.33], we may define $\mathbb{S}(k_1\ell_n, r)$ as the subset of $\mathbb{S}(n, r)$ of elements that are of degree r over $\mathbb{F}_{q^{k_1\ell_n}}$.

We divide the analysis as follows.

1. We first focus on affine sets fixed under subgroups of G having trivial intersection with LM. These are precisely the subgroups of K. We prove that an affine set $A(\alpha)$ is fixed by a subgroup $\langle\sigma^{k_1\ell m}\rangle$ of K if and only if $A(\alpha)$ contains a fixed point. We count the total number of elements of $\mathbb{S}$ which can be fixed by $\langle\sigma^{k_1\ell m}\rangle$ and the number of such elements in each $A(\alpha)$ fixed by $\langle\sigma^{k_1\ell m}\rangle$. Thus we find the number of affine sets fixed by $\langle\sigma^{k_1\ell m}\rangle$.

   Lemma 5.2 *The number of affine sets fixed by $\langle\sigma^{k_1\ell_n r}\rangle$ is*

   $$|\mathbb{S}(k_1\ell_n, r)|/(q^{k_1\ell_n}(q^{k_1\ell_n} - 1)).$$

   EXAMPLE 5.3 Let $q = 2, n = 4, r = 3$. Recall from Example 4.1 that there are 17 affine sets in $\mathbb{A}$. Of these 17 affine sets $\dfrac{2^6 - 2^2}{2^2(2^2 - 1)} = 5$ are fixed by $\langle\sigma^6\rangle$ and $\dfrac{2^3 - 2^1}{2^1(2^1 - 1)} = 3$ are fixed by $\langle\sigma^3\rangle$.

2. Next we consider affine sets fixed under subgroups of G which have non-trivial intersection with LM. Suppose $A(\alpha)$ is fixed by $\langle\sigma^{k_1\ell_1 m_1}\rangle$ such that $\langle\sigma^{k_1\ell_1 m_1}\rangle \cap LM$ is non trivial, that is, $\bar{\ell}_1\bar{m}_1 > 1$. The analysis falls into two cases.

   (a) The case when $p \nmid \bar{\ell}_1\bar{m}_1$. We first show that the fixed points of $\langle\sigma^{k_1\ell m}\rangle$ are permuted in orbits of length precisely $\bar{\ell}_1\bar{m}_1$. We exploit these orbits to gain further information.

i. First, we analyze the case when $\langle \sigma^{k_1\ell_1 m_1}\rangle \subseteq LM$ and $\ell_n|\ell_1$, that is, $k_1 = k$ and $\ell_n|\ell_1$. If $(\bar{\ell}_1\bar{m}_1, p) = 1$ and if $k\ell_n|k_1\ell_1$ then we establish that an affine set $A(\alpha)$ is fixed by $\langle \sigma^{k_1\ell_1 m_1}\rangle$ if and only if the numerical condition $\bar{\ell}_1\bar{m}_1|q^{k_1\ell_n}-1$ is satisfied and then $A(\alpha)$ contains roots of the equation $x^{q^{k_1\ell_1 m_1}-1} = \varepsilon$ where $\varepsilon \in \mathbb{F}_{q^n}$ is of order $\bar{\ell}_1\bar{m}_1$. Counting the roots of this equation which lie in $\mathbb{S}$ and the number of such roots which lie in each $A(\alpha)$ we establish the number of affine sets fixed by $\langle \sigma^{k_1\ell_1 m_1}\rangle$.

ii. Second, we allow $\langle \sigma^{k_1\ell_1 m_1}\rangle \not\subseteq LM$ $(k_1 < k)$ but insist that $\ell_n|\ell_1$. In this case we establish that an affine set $A(\alpha)$ is fixed by $\langle \sigma^{k_1\ell_1 m_1}\rangle$ if and only if the numerical condition $\bar{\ell}_1\bar{m}_1|q^{k_1\ell_n}-1$ is satisfied and then $A(\alpha)$ contains roots of equations of type $x^{q^{k_1\ell_1 m_1}-1} = \varepsilon^i$ where $\varepsilon \in \mathbb{F}_{q^n}$ is of order $\bar{\ell}_1\bar{m}_1$ and $(i, \bar{\ell}_1\bar{m}_1) = 1$. Again we count the roots of these equations which lie in $\mathbb{S}$. To count the number of such roots which lie in $A(\alpha)$ we count the number of elements in the set $U(\bar{\ell}_1\bar{m}_1)$ defined as the set of distinct elements in $\mathbb{F}_{q^n}$ which can be written as ε^{j-i} where $o(\varepsilon) = \bar{\ell}_1\bar{m}_1$, i, j coprime with $\bar{\ell}_1\bar{m}_1$ and such that

$$o(\varepsilon^{j-i}) \text{ divides } \frac{\pi(q^n-1, \bar{\ell}_1\bar{m}_1)}{\left(q^{k_1 d}-1, \pi(q^n-1, \bar{\ell}_1\bar{m}_1)\right)}$$

where $d = (\ell_1, \ell_n)$. In this way we establish the number of affine sets fixed by $\langle \sigma^{k_1\ell_1 m_1}\rangle$ when $\ell_n|\ell_1$.

iii. Third, we examine the case when $\ell_n \nmid \ell_1$. This breaks into two cases.

A. If $q \equiv -1 \bmod 4$ and $k_1\ell_2 m_1$ is odd and $\bar{\ell}_1\bar{m}_1$ is even then $A(\alpha)$ is fixed by $\langle \sigma^{k_1\ell_1 m_1}\rangle$ if and only if $2\bar{\ell}_1\bar{m}_1|q^{k_1\ell_n}-1$ and $A(\alpha)$ contains roots of equations of type $x^{q^{k_1\ell_1 m_1}-1} = \varepsilon^{*i}$ where $\varepsilon^* \in \mathbb{F}_{q^n}$ is of order $2\bar{\ell}_1\bar{m}_1$ and $(i, \bar{\ell}_1\bar{m}_1) = 1$. (Note $2|\bar{\ell}_1\bar{m}_1$.)

B. Otherwise, if any of the three conditions $q \equiv -1 \bmod 4$ and $k_1\ell_2 m_1$ is odd and $\bar{\ell}_1\bar{m}_1$ is even do not hold, we use induction to show that even if $\ell_n \nmid \ell_1$ we still have the result that an affine set $A(\alpha)$ is fixed by $\langle \sigma^{k_1\ell_1 m_1}\rangle$ if and only if $\bar{\ell}_1\bar{m}_1|q^{k_1\ell_n}-1$ and $A(\alpha)$ contains roots of equations of type $x^{q^{k_1\ell_1 m_1}-1} = \varepsilon^i$ where $\varepsilon \in \mathbb{F}_{q^n}$ is of order $\bar{\ell}_1\bar{m}_1$ and $(i, \bar{\ell}_1\bar{m}_1) = 1$.

We use the same technique to count the fixed affine sets when $\ell_n \nmid \ell_1$ as we do for the case when $\ell_n|\ell_1$. Let $T(k_1, \ell_1 m_1)$ $(T^*(k_1, \ell_1 m_1))$ denote the set of roots of the $\phi(\bar{\ell}_1\bar{m}_1)$ $\left(\phi(2\bar{\ell}_1\bar{m}_1)\right)$ equations $x^{q^{k_1\ell_1 m_1}-1} = \varepsilon^i$ $\left(x^{q^{k_1\ell_1 m_1}-1} = \varepsilon^{*i}\right)$, $(i, \bar{\ell}_1\bar{m}_1) = 1$, which lie in $\mathbb{S}$ and let $U^*(\bar{\ell}_1\bar{m}_1)$ be defined in a similar way to $U(\bar{\ell}_1\bar{m}_1)$ but corresponding to ε^*.

Lemma 5.4 *Suppose* $(p, \bar{\ell}_1\bar{m}_1) = 1$. *Then*

i. *If* $q \equiv -1 \bmod 4$ *and* $k_1\ell_2 m_1$ *is odd and* $\bar{\ell}_1\bar{m}_1$ *is even then there are* $\dfrac{|T^*(k_1, \ell_1 m_1)|}{(q^{k_1 d}-1)|U^*(\bar{\ell}_1\bar{m}_1)|}$ *affine sets fixed by* $\langle \sigma^{k_1\ell_1 m_1}\rangle$, *where* $d = (\ell_1, \ell_n)$, *if and only if* $2\bar{\ell}_1\bar{m}_1|q^{k_1\ell_n}-1$.

ii. *In all other cases there are* $\dfrac{|T(k_1, \ell_1 m_1)|}{(q^{k_1 d}-1)|U(\bar{\ell}_1\bar{m}_1)|}$ *affine sets fixed by* $\langle \sigma^{k_1\ell_1 m_1}\rangle$ *if and only if* $\bar{\ell}_1\bar{m}_1|q^{k_1\ell_n}-1$.

EXAMPLE 5.5 Let $q = 3, n = 4, r = 10$. Note that $k = 1, \ell = 8, m = 5$. Then $|T^*(1,5)| = 1920$, $|U^*(8)| = 4$ and there are $\frac{1920}{2 \times 4} = 240$ affine sets fixed by $\langle \sigma^5 \rangle$.

EXAMPLE 5.6 Let $q = 2, n = r = 6$. Note that $9|2^6 - 1$. Then $|T(1,4)| = 72$, $|U(9)| = 3$ and there are $\frac{72}{3 \times 3} = 8$ affine sets fixed by $\langle \sigma^4 \rangle$.

(b) The case when $p|\bar{\ell}_1 \bar{m}_1$.

In this case if $A(\alpha)$ is fixed by $\langle \sigma^{k_1 \ell_1 m_1} \rangle$ then it is also fixed by $\langle \sigma^{k_1 \frac{\ell m}{p}} \rangle$. We show that $A(\alpha)$ is fixed by $\langle \sigma^{k_1 \frac{\ell m}{p}} \rangle$ if and only if it contains a root of $x^{q^{\frac{nr}{p}}} - x - 1$. We then have the following analysis.

i. First we count the affine sets fixed by $\langle \sigma^{k_1 \ell_1 m_1} \rangle$ when $\bar{\ell}_1 \bar{m}_1 = p$, allowing k_1 to be arbitrary. We do this by counting the number of elements in the set $V(k_1)$, which denotes the set of roots of $x^{q^{\frac{nr}{p}}} - x - 1$ which lie in $\mathbb{S}$, and then the number of such roots in each affine set. We get the lemma:

Lemma 5.7 *The number of affine sets fixed by $\langle \sigma^{k_1 \ell_1 m_1} \rangle$ when $\bar{\ell}_1 \bar{m}_1 = p$ is* $\frac{|V(k_1)|}{q^{k_1 \ell_n}}$.

EXAMPLE 5.8 Let $q = 2, n = r = 6$. Then $|V(1)| = 262080$ and there are $\frac{262080}{64} = 4095$ affine sets fixed by $\langle \sigma^{18} \rangle$.

ii. We then show that there are no affine sets fixed by $\langle \sigma^{k_1 \ell_1 m_1} \rangle$ if

A. $\bar{\ell}_1 \bar{m}_1 = p^2$ and $p^2 | r$

B. $\bar{\ell}_1 \bar{m}_1 = p p_1$ where p_1 is some other prime.

iii. Finally, we analyze the case when $\bar{\ell}_1 \bar{m}_1 = p^i$, $i > 1$ and $p^2 \nmid r$. Observe that in this case $m_1 = m$. We show that $A(\alpha)$ is fixed by $\langle \sigma^{k_1 \ell_1 m} \rangle$ if and only if $A(\alpha)$ contains a root of $x^{q^{k_1 \ell_1 m}} - x - \beta_i = 0$, where β_i is a fixed element of $\mathbb{F}_{q^n}$ such that $\mathrm{Tr}_{\mathbb{F}_{q^{\frac{nr}{p}}} / \mathbb{F}_{q^{k_1 \ell_1 m}}}(\beta_i) = 1$. Then again we denote the set of roots of this equation which lie in $\mathbb{S}$ by $W(k_1 \ell_1 m)$, count the elements in this set and the number which lie in any one affine set and then deduce the number of affine sets fixed by $\langle \sigma^{k_1 \ell_1 m} \rangle$ when $\bar{\ell}_1 = p^i$. We get the lemma:

Lemma 5.9 *The number of affine sets fixed by $\langle \sigma^{k_1 \ell_1 m} \rangle$ when $\bar{\ell}_1 = p^i$, $i \geq 2$ is*

A. 1, *if* $r = p$

B. $\frac{|W(k_1 \ell_1 m)|}{q^{k_1 d}}$ *where* $d = (\ell_1, \ell_n)$, *if* $r > p$.

EXAMPLE 5.10 Let $q = 2, n = r = 6$. Then $|W(9)| = 504$ and there are $\frac{504}{2^3} = 63$ affine sets fixed by $\langle \sigma^9 \rangle$.

Finally, we bring all the results of Lemma 5.2, Lemma 5.4, Lemma 5.7 and Lemma 5.9 together to get the theorem.

Theorem 5.11 *Let $d = (\ell_1, \ell_n)$. With the notation we have established:*

1. *There are* $\frac{|\mathbb{S}(k_1 \ell_n, r)|}{q^{k_1 \ell_n}(q^{k_1 \ell_n} - 1)}$ *affine sets fixed by $\langle \sigma^{k_1 \ell_n r} \rangle$.*

2. *If* $(p, \bar{\ell}_1\bar{m}_1) = 1$. *Then*

   (a) *If* $q \equiv -1 \bmod 4$ *and* $k_1\ell_2m_1$ *is odd and* $\bar{\ell}_1\bar{m}_1$ *is even then there are* $\dfrac{|T^*(k_1, \ell_1 m_1)|}{(q^{k_1 d} - 1)|U^*(\bar{\ell}_1\bar{m}_1)|}$ *affine sets fixed by* $\langle \sigma^{k_1\ell_1 m_1} \rangle$, *where* $d = (\ell_1, \ell_n)$, *if and only if* $2\bar{\ell}_1\bar{m}_1 | q^{k_1\ell_n} - 1$.

   (b) *In all other cases there are* $\dfrac{|T(k_1, \ell_1 m_1)|}{(q^{k_1 d} - 1)|U(\bar{\ell}_1\bar{m}_1)|}$ *affine sets fixed by* $\langle \sigma^{k_1\ell_1 m_1} \rangle$ *if and only if* $\bar{\ell}_1\bar{m}_1 | q^{k_1\ell_n} - 1$.

3. *If* $(\bar{\ell}_1\bar{m}_1, r) = p$ *and* $\bar{\ell}_1\bar{m}_1 = p^i$, $i \geq 1$ *then*

   (a) *if* $i = 1$ *there are* $\dfrac{|V(k_1)|}{q^{k_1 d}}$ *affine sets fixed by* $\langle \sigma^{k_1\ell_1 m_1} \rangle$.

   (b) *if* $i > 1$ *and* $r = p$ *then there is precisely* 1 *affine set fixed by* $\langle \sigma^{k_1\ell_1} \rangle$.

   (c) *if* $i > 1$ *and* $r > p$ *there are* $\dfrac{|W(k_1\ell_1 m)|}{q^{k_1 d}}$ *affine sets fixed by* $\langle \sigma^{k_1\ell_1 m} \rangle$.

6 Computation

Using Theorem 5.11 we can develop a program to apply the Cauchy-Frobenius Theorem and calculate the average number of affine sets fixed by an element of G. This gives the number $N(q, n, r)$ of orbits in $\mathbb{S}$ under the action of FG. Among other things, the program calculates the cardinality of the sets $\mathbb{S}, T, T^*, U, U^*, V$ and W. Our main result is as follows.

Theorem 6.1 *The number of inequivalent irreducible Goppa codes over* $\mathbb{F}_q$ *of length* q^n *and degree* r *is at most* $N(q, n, r)$.

The following tables compare $N(2, 7, r)$ and $N(2, n, 7)$ for $6 \leq n, r \leq 16$

q	n	r	$N(2,7,r)$
2	7	6	6442037
2	7	7	706740561
2	7	8	79154980000
2	7	9	9006073495576
2	7	10	1037499670492467
2	7	11	120727233941856231
2	7	12	14165328782916945380
2	7	13	1673688077687467924065
2	7	14	198929782948040712169263
2	7	15	23765478069520611201643781
2	7	16	2851857368342478330960957440

q	n	r	$N(2,n,7)$
2	6	7	25972041
2	7	7	706740561
2	8	7	19711152849
2	9	7	559575017799
2	10	7	16100007541491
2	11	7	468135036352467
2	12	7	13728607731106143
2	13	7	405472442822740719
2	14	7	12047588599432596753
2	15	7	35981033161568841756 3
2	16	7	107941452378686248364 49

Note that $N(2, 7, 6) < N(2, 6, 7)$ but $N(2, 7, 8) > N(2, 8, 7)$ and then $N(2, n, r)$ grows faster with r than with n.
The following table gives some non binary values

q	n	r	$N(q,n,r)$
3	2	3	3
3	3	3	4
3	4	3	9
3	3	4	68
3	3	5	1368
5	2	3	6
5	2	4	86
5	2	5	1644
9	2	3	16
9	2	4	842
9	2	5	53892

7 Quasicyclic Goppa codes

It is already known that there are classes of quasicyclic Goppa codes, see [1,3]. This feature has also arisen in our analysis. Using specific orderings on the defining set L we show that

1. If $p|r$ then there exists a category of quasicyclic irreducible Goppa codes of length q^n and index dividing $\frac{q^n}{p}$. It is not difficult to give an upper bound on the number of codes in this category. We give a method for the generation of such codes and note that they have varying parameters.

2. If $\bar{\ell}_1\bar{m}_1|q^n-1$ there exists a category of quasicyclic Goppa codes of length q^n-1 and index dividing $\frac{q^n-1}{\bar{\ell}_1\bar{m}_1}$. Again it is not difficult to count the Goppa codes in this category and we give a method for generating these codes.

7.1 Cryptosystems based on Goppa codes

The existence of these two categories of quasicyclic Goppa codes has implications for any cryptosystem based on Goppa codes. Some authors have shown that Goppa codes with non trivial automorphism groups are bad keys for the McEliece cryptosystem (See [3]). However it is easy to eliminate the possibility of choosing a Goppa code in either of the above two categories using the numerical condition necessary for their existence.

8 Cubic Goppa codes

The following result can be used to construct an efficient program to generate all all cubic Goppa codes of length q^n. Let q, n and $r \geq 3$ be fixed, let $\alpha \in \mathbb{S}$ and let $D = \{\alpha\} \cup \{\frac{1}{\alpha+\xi} : \xi \in \mathbb{F}_{q^n}\}$. Then $|D| = q^n + 1$ and no two elements of D belong to the same affine set. For suppose β^{-1} and $(\beta+\xi_1)^{-1}$ belong to the same affine set then $(\beta+\xi_1)^{-1} = \zeta\beta^{-1}+\xi$ for some $\zeta, \xi \in \mathbb{F}_{q^n}$ which implies that β is a root of a quadratic over $\mathbb{F}_{q^n}$ which is impossible. Finally note that, when $r = 3$, there are $\dfrac{q^{3n}-q^n}{q^n(q^n-1)} = q^n + 1$ affine sets in $\mathbb{S}$ and so the elements of D in this case characterize all affine sets. If $r > 3$ then the elements of D define $q^n + 1$ affine sets.

Theorem 8.1 *Let q, n and $r = 3$ be fixed, let $\alpha \in \mathbb{S}$ and let $D = \{\alpha\} \cup \{\frac{1}{\alpha+\xi} : \xi \in \mathbb{F}_{q^n}\}$. Then D consists of a full set of representatives of all the affine sets in $\mathbb{S}$. If $r > 3$, D consists of a set of representatives from $q^n + 1$ affine sets.*

Using Theorem 8.1 we outline a method for generating all irreducible cubic Goppa codes of length q^n. A slight modification to this method helps to obtain any required number of irreducible Goppa codes of degree r and length q^n.

References

[1] Charpin P., Open problems on cyclic codes, *in Handbook of Coding Theory,* Pless V.S. and Huffman W.C., Eds. Amsterdam, The Netherlands: Elsevier, 1998, Vol. 1, Ch 11.

[2] Berger T.P., On the cyclic property of Goppa codes, parity check subcodes of Goppa codes and extended Goppa codes, *Finite Fields and their Applications,* Vol 6, pp. 225-281, 2000.

[3] Berger T.P., Goppa and Related Codes Invariant Under a Prescribed Permutation, *IEEE Trans. IT 46*, pp. 2628-2633, 2000.

[4] McEliece, R.J., A public key cryptosystem based on algebraic coding theory, *JPL DSN* Progress Report 42-44 (1978) 114-116.

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

[6] MacWilliams F.J. and Sloane N.J.A., *The Theory of Error Correcting Codes*, North Holland, 1977.

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

[8] Lidl R. and Niederreiter H., *Introduction to Finite Fields and their Applications*, Cambridge University Press, 1994.

[9] Pless, V.S. and Huffman, W.C., eds., *Handbook on Coding Theory*, Elsevier Science, 1998.

[10] Ryan, J.A. and Fitzpatrick, P., The number of inequivalent irreducible Goppa codes, *Proc. Int. Workshop on Coding and Cryptography 2001*, WCC2001, 209-216.

[11] Ryan, J.A. and Fitzpatrick, P., Counting irreducible Goppa codes, *J. Austral. Math. Soc.* 71(3) (2001) 299-306.