Hindawi Publishing Corporation
Journal of Discrete Mathematics
Volume 2014, Article ID 871871, 4 pages
http://dx.doi.org/10.1155/2014/871871

Research Article

Counting Extended Irreducible Goppa Codes

John A. Ryan

Department of Mathematics, Mzuzu University, Private Bag 201, Luwinga, Mzuzu, Malawi

Correspondence should be addressed to John A. Ryan; jar@mzuzu.org

Received 1 October 2013; Revised 26 December 2013; Accepted 2 January 2014; Published 12 February 2014

Academic Editor: Stavros D. Nikolopoulos

We produce an upper bound on the number of extended irreducible Goppa codes over any finite field.

1. Introduction

The advent of quantum computing has brought Goppa codes to the forefront. Most cryptosystems which are in general use today are asymmetric cryptosystems which are based on the integer factorization problem or the discrete logarithm problem and it is conjectured that these cryptosystems may become insecure when quantum computing is further developed [1]. One cryptosystem which may have potential to withstand attack by quantum computers is the McEliece cryptosystem which is based on the family of Goppa codes [1]. It is conjectured that this family of Goppa codes is near to random codes and a categorization has so far eluded researchers [2]. There have been many attempts to count the number of Goppa codes for fixed parameters and the author of this paper produced in 2004 a computer program which gives the best upper bound available today for the number of such codes [3]. Recent research has clearly shown that many Goppa codes become equivalent when extended by a parity check [4] and so the question of categorizing Goppa codes through their extended versions is now being proposed. As a first step, we investigate the possibility of counting extended Goppa codes using the tools which were developed for counting the nonextended versions. We begin by defining a degree r irreducible Goppa code $\Gamma(\mathbf{L}, g)$ over $\mathbb{F}_q$ of length q^n in terms of a single field element α of degree r over $\mathbb{F}_{q^n}$. We then define the extended code $\overline{\Gamma(\mathbf{L}, g)}$. We give the well-known sufficient conditions on two elements of degree r, α and β, for the corresponding extended irreducible Goppa codes (the extended Goppa codes defined by α and β) to be equivalent. Denoting the set of all elements of degree r as $\mathbb{S}$, counting the cardinality of the set $\mathbb{S}$, and using the well-known conditions for equivalence we produce an upper bound on the number of inequivalent extended irreducible Goppa codes over $\mathbb{F}_q$ of degree r and length $q^n + 1$.

2. Background

Let q be a power of a prime number; let $\mathbb{F}_q$ be the field of order q and $\mathbb{F}_{q^n}$ its extension of order n. In this paper all codes will be over $\mathbb{F}_q$. The family of Goppa codes was first introduced by Goppa in 1971 [5]. For our purposes we focus on irreducible Goppa, codes, and define irreducible Goppa codes as follows.

Definition 1. Let $g(z) \in \mathbb{F}_{q^n}[z]$ be irreducible of degree r and let $L = \mathbb{F}_{q^n} = \{\zeta_i : 0 \le i \le q^n - 1\}$. Then the irreducible Goppa code $\Gamma(L, g)$ is defined as the set of all vectors $\underline{c} = (c_0, c_1, \ldots c_{q^n-1})$ with components in $\mathbb{F}_q$ which satisfy the condition

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

The polynomial $g(z)$ is called the *Goppa Polynomial*. The set L is called the *Defining Set*. Since $g(z)$ is irreducible over $\mathbb{F}_{q^n}$ the code is called an *irreducible Goppa code*. Since $g(z)$ is of degree r the code $\Gamma(L, g)$ is called a *Goppa code of degree* r. In this paper $g(z)$ is always irreducible of degree r over $\mathbb{F}_{q^n}$.

Remark 2. The definition we have given is specific for "irreducible Goppa codes." In the literature, in general, a Goppa code is defined with Defining Set $L \subseteq \mathbb{F}_{q^n}$ such that

no element of L is a root of the Goppa polynomial $g(z)$. Since, in this paper, $g(z)$ is irreducible we take L as large as possible; that is, $L = \mathbb{F}_{q^n}$. Note further that in fixing an order on the elements in L we are implicitly putting an order on the coordinates of the Goppa code as the ordered elements in L label the component positions in the codewords. Thus the length of the Goppa code is q^n.

Next we define extended irreducible Goppa codes.

Definition 3. Let $\Gamma(\mathbf{L}, g)$ be a Goppa code of length q^n over $\mathbb{F}_q$. Then the extended code $\overline{\Gamma(\mathbf{L}, g)}$ is defined by

$$\overline{\Gamma(\mathbf{L}, g)} = \left\{ \left(c_0, c_1, \cdots, c_{q^n}\right) : \left(c_0, c_1, \cdots, c_{q^n-1}\right) \in \Gamma(\mathbf{L}, g), \sum_{i=0}^{q^n} c_i = 0 \right\}. \tag{2}$$

Remark 4. The extended code $\overline{\Gamma(\mathbf{L}, g)}$ is often described as the code obtained from $\Gamma(\mathbf{L}, g)$ by adding a parity check to each codeword of $\Gamma(\mathbf{L}, g)$.

It is shown in [6] that if α is any root of the Goppa polynomial $g(z)$ then $\Gamma(\mathbf{L}, g)$ is completely described by any root α of $g(z)$ and a parity check matrix $\mathbf{H}(\alpha)$ is given by

$$\mathbf{H}(\alpha) = \left(\frac{1}{\alpha - \zeta_0} \quad \frac{1}{\alpha - \zeta_1} \quad \cdots \quad \frac{1}{\alpha - \zeta_{q^n-1}} \right), \tag{3}$$

where $L = \mathbb{F}_{q^n} = \{\zeta_i : 0 \le i \le q^n - 1\}$. We may denote this code by $\mathbf{C}(\alpha)$.

Remark 5. $\overline{\mathbf{C}}(\alpha)$ denotes the same code as $\overline{\Gamma(\mathbf{L}, g)}$, where $g(\alpha) = 0$.

Remark 6. Note that in using this parity check matrix to define $\mathrm{C}(\alpha)$ we are implicitly fixing an order on L and, consequently, an order on the components of the codewords in the code $C(\alpha)$.

Considering that any irreducible Goppa code can be defined by an element of degree r over $\mathbb{F}_{q^n}$ and, conversely, any such element of degree r defines an irreducible Goppa code, we make the following definition.

Definition 7. The set $\mathbb{S} = \mathbb{S}(n, r)$ is the set of all elements in $\mathbb{F}_{q^{nr}}$ of degree r over $\mathbb{F}_{q^n}$.

Finally, as background material, we recall a sufficient condition which is well known for two extended irreducible Goppa codes to be equivalent.

Consider the maps $\pi_{\zeta_1,\zeta_2,\xi_1,\xi_2,i}$ defined on $\mathbb{S}$ by

$$\pi_{\zeta_1,\zeta_2,\xi_1,\xi_2,i} : \alpha \longmapsto \frac{\zeta_1 \alpha^{q^i} + \xi_1}{\zeta_2 \alpha^{q^i} + \xi_2} \tag{4}$$

for fixed i, ζ_j, and ξ_j where $0 \le i < nr$, $\zeta_j, \xi_j \in \mathbb{F}_{q^n}$, $j = 1, 2$, and $\zeta_1\xi_2 \ne \zeta_2\xi_1$.

For simplicity, where there is no confusion, we write π for $\pi_{\zeta_1,\zeta_2,\xi_1,\zeta_2}$.

It is well known that if $\pi(\alpha) = \beta$ then $\overline{\mathbf{C}}(\alpha)$ is equivalent to $\overline{\mathbf{C}}(\beta)$ (see [7]).

Remark 8. Note that in the definition of π the scalars ζ_j and ξ_j are defined up to scalar multiplication. Hence we may assume that $\zeta_1 = 1$ or $\xi_1 = 1$ if $\zeta_1 = 0$.

Remark 9. Note that the map $\pi_{\zeta_1,\zeta_2,\xi_1,\xi_2,i}$ can be broken up into the composition of two maps, namely,

(1) the map $\pi_{\zeta_1,\zeta_2,\xi_1,\xi_2}$ defined on $\mathbb{S}$ by $\pi_{\zeta_1,\zeta_2,\xi_1,\xi_2} : \alpha \mapsto (\zeta_1\alpha + \xi_1)/(\zeta_2\alpha + \xi_2)$ 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.

We immediately justify the statement that $\pi_{\zeta_1,\zeta_2,\xi_1,\xi_2}$ is a map on $\mathbb{S}$.

Lemma 10. *$\pi_{\zeta_1,\zeta_2,\xi_1,\xi_2}$ is a map defined on $\mathbb{S}$.*

Proof. Suppose $\pi_{\zeta_1,\zeta_2,\xi_1,\xi_2}(\alpha) = (\zeta_1\alpha+\xi_1)/(\zeta_2\alpha+\xi_2) = \beta$ where β is an element of degree s strictly less that r over $\mathbb{F}_{q^n}$ (note that $\beta \in \mathbb{F}_{q^{nr}}$ and so β cannot have degree greater than r over $\mathbb{F}_{q^n}$)

$$\begin{aligned} \zeta_1\alpha + \xi_1 &= \zeta_2\alpha\beta + \xi_2\beta, \\ \alpha &= \frac{\xi_2\beta - \xi_1}{\zeta_1 - \zeta_2\beta}. \end{aligned} \tag{5}$$

But this is impossible since $\beta \in \mathbb{F}_{q^{ns}}, \zeta_i, \xi_i \in \mathbb{F}_{q^n}$ and so the right hand side is an element of $\mathbb{F}_{q^{ns}}$ contradicting the fact that α is an element of degree r over $\mathbb{F}_{q^n}$. □

In the light of the foregoing, we make two more definitions

Definition 11. Let F denote the set of all maps $\{\pi_{\zeta_1,\zeta_2,\xi_1,\xi_2} : \zeta_j,\ \xi_j \in \mathbb{F}_{q^n},\ j = 1, 2 \text{ and } \zeta_1\xi_2 \ne \zeta_2\xi_1\}$.

Definition 12. Let G denotes the set of all maps $\{\sigma^i : 1 \le i \le n \times r\}$.

Lemma 13. *F together with the operation of composition of maps $\circ$ is a group.*

Proof. Let $\pi_{\zeta_1,\zeta_2,\xi_1,\xi_2}, \pi_{\zeta_3,\zeta_4,\xi_3,\xi_4} \in F$. First we show that F is closed under the operation of $\circ$:

$$\begin{aligned} &\pi_{\zeta_3,\zeta_4,\xi_3,\xi_4} \circ \pi_{\zeta_1,\zeta_2,\xi_1,\xi_2}(\alpha) \\ &= \frac{\zeta_3\left(\left(\zeta_1\alpha + \xi_1\right)/\left(\zeta_2\alpha + \xi_2\right)\right) + \xi_3}{\zeta_4\left(\left(\zeta_1\alpha + \xi_1\right)/\left(\zeta_2\alpha + \xi_2\right)\right) + \xi_4} \\ &= \frac{\zeta_3\zeta_1\alpha + \zeta_3\xi_1 + \zeta_2\xi_3\alpha + \xi_2\xi_3}{\zeta_4\zeta_1\alpha + \zeta_4\xi_1 + \zeta_2\xi_4\alpha + \xi_2\xi_4} \\ &= \frac{\left(\zeta_3\zeta_1 + \zeta_2\xi_3\right)\alpha + \zeta_3\xi_1 + \xi_2\xi_3}{\left(\zeta_4\zeta_1 + \zeta_2\xi_4\right)\alpha + \zeta_4\xi_1 + \xi_2\xi_4}. \end{aligned} \tag{**}$$

We need to show $(\zeta_3\zeta_1+\zeta_2\xi_3)(\zeta_4\xi_1+\xi_2\xi_4) \neq (\zeta_4\zeta_1+\zeta_2\xi_4)(\zeta_3\xi_1+\xi_2\xi_3)$. The Left Hand Side (LHS) is equal to $\zeta_3\zeta_1\zeta_4\xi_1 + \zeta_2\xi_3\zeta_4\xi_1 + \zeta_3\zeta_1\xi_2\xi_4 + \zeta_2\xi_3\xi_2\xi_4$ and the Right Hand side (RHS) is equal to $\zeta_4\zeta_1\zeta_3\xi_1 + \zeta_2\xi_4\zeta_3\xi_1 + \zeta_4\zeta_1\xi_2\xi_3 + \zeta_2\xi_4\xi_2\xi_3$. Observe that the first and last terms of the LHS are the same as the first and last terms of the RHS and so our task now is to show that $\zeta_2\xi_3\zeta_4\xi_1 + \zeta_3\zeta_1\xi_2\xi_4 \neq \zeta_2\xi_4\zeta_3\xi_1 + \zeta_4\zeta_1\xi_2\xi_3$ or equivalently show that $\zeta_2\xi_1\zeta_4\xi_3 - \zeta_2\xi_1\zeta_3\xi_4 \neq \zeta_1\xi_2\zeta_4\xi_3 - \zeta_1\xi_2\zeta_3\xi_4$; that is $\zeta_2\xi_1(\zeta_4\xi_3 - \zeta_3\xi_4) \neq \zeta_1\xi_2(\zeta_4\xi_3 - \zeta_3\xi_4)$.

But this is immediate from the fact that $\zeta_1\xi_2 \neq \zeta_2\xi_1$ and $\zeta_3\xi_4 \neq \zeta_4\xi_3$.

Secondly, associativity follows from the associativity of mappings. Thirdly, observe that $\pi_{1,0,0,1}$ is the identity. Finally, given $\pi_{\zeta_1,\zeta_2,\xi_1,\xi_2}$ to find $\pi_{\zeta_3,\zeta_4,\xi_3,\xi_4}$ such that $\pi_{\zeta_3,\zeta_4,\xi_3,\xi_4} \circ \pi_{\zeta_1,\zeta_2,\xi_1,\xi_2} = \pi_{1,0,0,1}$ is a matter of solving the equation $((\zeta_3\zeta_1 + \zeta_2\xi_3)a + \zeta_3\xi_1 + \xi_2\xi_3)/((\zeta_4\zeta_1 + \zeta_2\xi_4)a + \zeta_4\xi_1 + \xi_2\xi_4) = a$. See $(**)$ above. This is a matter of solving the four equations:

(a) $\zeta_3\zeta_1 + \zeta_2\xi_3 = 1$

(b) $\zeta_3\xi_1 + \xi_2\xi_3 = 0$

(c) $\zeta_4\zeta_1 + \zeta_2\xi_4 = 0$

(d) $\zeta_4\xi_1 + \xi_2\xi_4 = 1$

in the four unknowns ζ_3, ζ_4, ξ_3 and ξ_4. We know from linear algebra that this is always possible. □

Lemma 14. *G together with the operation of composition of maps is a cyclic group of order $n \times r$.*

Proof. Observe $G =< \sigma >$ where $\sigma : \alpha \mapsto \alpha^q$ is the Frobenius automorphism of $\mathbb{F}_{q^{nr}}$ leaving $\mathbb{F}_q$ fixed. Since σ^{nr} is the identity on $\mathbb{F}_{q^{nr}}$ the result follows. □

3. Strategy to Count All Extended Irreducible Goppa Codes for Fixed q, n, and r

We apply the following method to count the number of extended Goppa codes. Observe that each element $\alpha \in \mathbb{S}$ defines an extended irreducible Goppa code $\overline{\mathbf{C}}(\alpha)$ over $\mathbb{F}_q$ of degree r of length $q^n + 1$ and conversely each such extended Goppa code is defined by an element $\alpha \in \mathbb{S}$. We count the number of orbits in $\mathbb{S}$ under the action of the group F and this gives us an upper bound on the number of irreducible extended Goppa codes.

We first confirm the details that F acts on $\mathbb{S}$.

Lemma 15. *The group F acts on $\mathbb{S}$.*

Proof. We have already seen that $\pi(\alpha) \in \mathbb{S}$, for all $\alpha \in \mathbb{S}$. Clearly $\pi_{1,0,0,1}(\alpha) = \alpha$, for all $\alpha \in \mathbb{S}$. That $\pi_{\zeta_3,\zeta_4,\xi_3,\xi_4} \circ \pi_{\zeta_1,\zeta_2,\xi_1,\xi_2}(\alpha) = \pi_{\zeta_3,\zeta_4,\xi_3,\xi_4}(\pi_{\zeta_1,\zeta_2,\xi_1,\xi_2}(\alpha))$ is merely the definition of $\circ$. □

The orbit containing α is the set

$$\left\{\frac{\zeta_1\alpha+\xi_1}{\zeta_2\alpha+\xi_2} : \zeta_j, \xi_j \in \mathbb{F}_{q^n},\ j = 1, 2,\ \zeta_1\xi_2 - \zeta_2\xi_1 \neq 0\right\} \tag{6}$$

and we denote this set by $O(\alpha)$. We denote the set of all orbits in $\mathbb{S}$ under the action of F by $\mathbb{O}$; that is, $\mathbb{O} = \{O(\alpha) : \alpha \in \mathbb{S}\}$.

It follows from Group Theory and Lemma 15 that the set of all orbits in $\mathbb{S}$ under the group action of F partition the set $\mathbb{S}$ and that $\mathbb{O}$ partitions the set $\mathbb{S}$.

Theorem 16. *For any $\alpha \in \mathbb{S}$, $|O(\alpha)| = q^{3n} - q^n$:*

$$O(\alpha) = \left\{\frac{\zeta_1\alpha+\xi_1}{\zeta_2\alpha+\xi_2} : \zeta_j, \xi_j \in \mathbb{F}_{q^n},\ j = 1, 2,\ \zeta_1\xi_2 - \zeta_2\xi_1 \neq 0\right\}. \tag{7}$$

First remember that the elements ζ_i, ξ_i are defined up to scalar multiplication so we may assume that, if $\zeta_1 \neq 0$, then $\zeta_1 = 1$ (see Remark 8).

(1) If $\zeta_1 = 0$, then w.l.o.g. $\xi_1 = 1$ and there are $q^n(q^n-1) = q^{2n} - q^n$ possibilities.

(2) If $\zeta_1 = 1$, then we need to exclude the cases when $\xi_2 = \zeta_2\xi_1$.

(a) Consider $\xi_2 = 0$, and then exclude

(i) the q^n cases when $\zeta_2 = 0$ and $\xi_1 \in \mathbb{F}_{q^n}$,

(ii) the $q^n - 1$ cases when $\zeta_2 \neq 0 \in \mathbb{F}_{q^n}$ and $\xi_1 = 0$.

(b) Consider $\xi_2 \neq 0$. There are $q^n - 1$ such cases. In each such case, for each $\xi_1 \neq 0$ (and there are $q^n - 1$ of them) there is a unique solution for ζ_2. Hence there are $(q^n - 1)^2$ possibilities when $\xi_2 \neq 0$.

So the total number of possibilities under item (2) is $q^{3n} - (2q^n - 1) - (q^n - 1)^2 = q^{3n} - q^{2n}$.

Adding the possibilities under (1) and (2) we get $q^{3n} - q^{2n} + q^{2n} - q^n = q^{3n} - q^n$.

Theorem 17. *The number of inequivalent extended irreducible Goppa codes over $\mathbb{F}_q$ of degree r and length $q^n + 1$ is less than or equal to $|\mathbb{S}|/(q^{3n} - q^n)$.*

Proof. Any extended irreducible Goppa code is defined by an element of $\mathbb{S}$. The elements of $\mathbb{S}$ contained in the orbit $O(\alpha)$ define codes equivalent to $C(\alpha)$. Since $\mathbb{O}$ partitions $\mathbb{S}$ and by Theorem 16 every set in $\mathbb{O}$ has $q^{3n} - q^n$ elements, we conclude that $|\mathbb{O}| = |\mathbb{S}|/(q^{3n} - q^n)$. This gives an upper bound on the number of inequivalent extended irreducible Goppa codes. □

Remark 18. Note that this bound can be improved upon by further action of the group G of Frobenius automorphisms. It is possible to show that G acts on $\mathbb{O} = \{O(\alpha) : \alpha \in \mathbb{S}\}$ and then the number of orbits in $\mathbb{O}$ under G gives an improved upper bound on the number of inequivalent extended irreducible Goppa codes. This research is in progress.

Conflict of Interests

The author declares that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

The author wishes to acknowledge part funding towards this research provided by MASI (MASAMU Advanced Study Institute) supported by the National Science Foundation (NSF) of the USA.

References

[1] R. Misoczki and P. Barreto, "Compact McEliece keys from Goppa codes," in *Selected Areas in Cryptography*, pp. 376–3392, Springer, Berlin, Germany, 2009.

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

[3] J. A. Ryan and P. Fizpatrick, "Enumeration of inequivalent irreducible Goppa codes," *Discrete Applied Mathematics*, vol. 154, no. 2, pp. 399–412, 2006.

[4] W. Govere and J. A. Ryan, "Binary Goppa codes of degree 4 and their extended versions," in *Proceedings of the International Conference of the Southern African Mathematical Sciences Association (SAMSA '08)*, Maputo, Mozambique, 2008.

[5] V. D. Goppa, "Rational representation of codes and (L,g) codes," *Problemy Peredachi Informatsii*, vol. 7, no. 3, pp. 41–49, 1971.

[6] C. L. Chen, "Equivalent irreducible Goppa codes," *IEEE Transactions on Information Theory*, vol. 24, no. 6, pp. 766–769, 1978.

[7] T. P. Berger, "Goppa and related codes invariant under a prescribed permutation," *IEEE Transactions on Information Theory*, vol. 46, no. 7, pp. 2628–2633, 2000.