Interesting Examples on Maximal Irreducible Goppa Codes

Marta Giorgetti

Dipartimento di Fisica e Matematica, Universita' dell'Insubria

Abstract. In this paper a full categorization of irreducible classical Goppa codes of degree 4 and length 9 is given. It is an interesting example in the context of find the number of permutation non-equivalent classical irreducible maximal Goppa codes having fixed parameters q, n and r using group theory techniques.

Key words: Classical Goppa codes, Equivalent codes, Permutation groups.

1 Introduction

In this paper an interesting example is given in the context of finding an upper bound for the number of permutation non-equivalent irreducible maximal Goppa codes. This question was considered by several authors (see for example [1], [2], [4], [5], [6], [8]). The study of classical Goppa codes is important: they are a very large class of codes, near to random codes [3]; they are easy to generate; they possess an interesting algebraic structure. For all these reasons they are used in McEliece's public key cryptosystem [11].

The article is structured as follows: Section 1 gives some notation and preliminaries; Section 2 describes the approach to the problem of find the number of non-equivalent maximal irreducible Goppa codes; in Section 3 the full classification of maximal irreducible classical Goppa codes of degree 4 and length 9 is given, with several notes on polynomials.

2 Preliminaries

In this section we fix some notation and we recall some basic concept about linear codes and in particular about Goppa codes.

We denote by $\mathbb{F}_q$ the finite field with q elements, where $q = p^m$ is a power of a prime p; let N, k, n and r be natural numbers, $k \leq N$. We consider two extensions of $\mathbb{F}_q$, of degree n and nr, $\mathbb{F}_{q^n}$ and $\mathbb{F}_{q^{nr}}$ respectively; $\mathbb{F}_{q^n}[x]$ denotes the polynomial ring over $\mathbb{F}_{q^n}$ and ε is a primitive element of $\mathbb{F}_{q^n}$, $\mathbb{F}^*_{q^n} = \langle \varepsilon \rangle$. We refer to the vector space of dimension N over $\mathbb{F}_q$ as to $(\mathbb{F}_q)^N$.

In the following if H is an $(N-k) \times N$ matrix with entries in $\mathbb{F}_q$ and rank equal to $N-k$, the set C of all vectors $c \in (\mathbb{F}_q)^N$ such that $Hc^T = 0$ is an (N,k)

linear code over $\mathbb{F}_q$, of *length* N and *dimension* k, i.e. a subspace of $(\mathbb{F}_q)^N$ of dimension k. The elements of C are called *codewords* and matrix H is a *parity check matrix* of C. Any $k \times N$ matrix G whose rows form a vector basis of C is called a *generator matrix* of C. We use the notation $[N,k]_q$ to denote a linear code of length N and dimension k over $\mathbb{F}_q$.

Definition 1. *Let $\mathcal{C}$ an $[N,k']_{q^t}$ code. The subfield subcode $C = \mathcal{C}|_{\mathbb{F}_q}$ of $\mathcal{C}$ with respect to $\mathbb{F}_q$ is the set of codewords in $\mathcal{C}$ each of whole components is in $\mathbb{F}_q$; C is a $[N,k]_q$ code.*

By abuse of notation we call parity check matrix also a matrix H with entries in an extention field of $\mathbb{F}_q$ such that $Hc^T = 0$ for all $c \in C$. According to this assumption, H_1 and H_2 may be parity check matrices for the same code even if their entries are in different extension fields or they have different ranks.

Definition 2 ([9]). *Let C_1 and C_2 be two linear codes over $\mathbb{F}_q$ of length N, let G_1 be a generator matrix of C_1. Codes C_1 and C_2 are **permutation equivalent** provided there is a permutation $\sigma \in S_N$ of coordinates which sends C_1 in C_2. Thus C_1 and C_2 are permutation equivalent provided there is a permutation matrix P such that $G_1 P$ is a generator matrix for C_2. They are **monomially equivalent** provided there is a monomial matrix M so that $G_1 M$ is a generator matrix for C_2 and **equivalent** provided there is a monomial matrix M and an automorphism γ of the field $\mathbb{F}_q$ so that $C_2 = C_1 M \gamma$.*

If code C_2 is permutation equivalent to C_1 with parity check matrix H_1, we can obtain a parity check matrix H_2 for C_2 by permuting columns of H_1 (and viceversa).

Definition 3. *Let $g(x) = \sum g_i x^i \in \mathbb{F}_{q^n}[x]$ and let $L = \{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_N\}$ denote a subset of elements of $\mathbb{F}_{q^n}$ which are not roots of $g(x)$. Then the **Goppa code** $\mathcal{G}(L,g)$ is defined as the set of all vectors $c = (c_1, c_2, \ldots, c_N)$ with components in $\mathbb{F}_q$ which satisfy the condition:*

$$\sum_{i=0}^{N} \frac{c_i}{x - \varepsilon_i} \equiv 0 \mod g(x). \tag{1}$$

Usually, but now always, the set $L = \{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_N\}$ is taken to be the set of all elements in $\mathbb{F}_{q^n}$ which are not roots of the Goppa polynomial $g(x)$. In this case the Goppa code is said *maximal.* If the degree of $g(x)$ is r, then the Goppa code is called a Goppa code of degree r. It is easy to see ([12]) that a parity check matrix for $\mathcal{G}(L,g)$ is given by

$$H = \begin{pmatrix} \frac{1}{g(\varepsilon_1)} & \frac{1}{g(\varepsilon_2)} & \cdots & \frac{1}{g(\varepsilon_N)} \\ \frac{\varepsilon_1}{g(\varepsilon_1)} & \frac{\varepsilon_2}{g(\varepsilon_2)} & \cdots & \frac{\varepsilon_N}{g(\varepsilon_N)} \\ \vdots & \vdots & \vdots & \vdots \\ \frac{\varepsilon_1^{r-1}}{g(\varepsilon_1)} & \frac{\varepsilon_2^{r-1}}{g(\varepsilon_2)} & \cdots & \frac{\varepsilon_N^{r-1}}{g(\varepsilon_N)} \end{pmatrix}.$$

Note that the code $C = \ker H$ is a subspace of $(\mathbb{F}_{q^n})^N$ and the Goppa code $\mathcal{G}(L,g)$ is its subfield subcode on $\mathbb{F}_q$.

A Goppa code $\mathcal{G}(L,g)$ is called **irreducible** if $g(x)$ is irreducible over $\mathbb{F}_{q^n}$.

In the following by Goppa code we mean maximal irreducible classical Goppa code of degree r, so that $N = q^n$. By Definition 3, a vector $c = (c_1, c_2, \ldots, c_{q^n}) \in (\mathbb{F}_q)^{q^n}$ is a codeword of $\mathcal{G}(L,g)$ if and only if it satisfies (1). If α is any root of $g(x)$, $\alpha \in \mathbb{F}_{q^{nr}}$, then $g(x) = \prod_{i=0}^{r-1}(x - \alpha^{q^{ni}})$ and (1) is equivalent to the r equations

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

Hence $\mathcal{G}(L,g)$ is completely described by any root α of $g(x)$ and we may denote this code by $\mathcal{C}(\alpha)$. From (2) we easily get a parity check matrix $H_\alpha \in Mat_{1\times q^n}(\mathbb{F}_{q^{nr}})$ for $\mathcal{C}(\alpha)$ (see [4]):

$$H_\alpha = \left(\tfrac{1}{\alpha-\varepsilon_1}, \tfrac{1}{\alpha-\varepsilon_2}, \ldots, \tfrac{1}{\alpha-\varepsilon_{q^n}} \right). \tag{3}$$

It is important to stress that by using parity check matrix H_α to define $\mathcal{C}(\alpha)$ we implicitly fix an order in L. So, we set $L = \{\varepsilon, \varepsilon^2, \ldots, \varepsilon^{q^n-1}, \varepsilon^{-\infty}\}$, where $\varepsilon^{-\infty} = 0$, $\varepsilon_i = \varepsilon^i$ and the matrix H_α is

$$H_\alpha = \left(\tfrac{1}{\alpha-\varepsilon}, \tfrac{1}{\alpha-\varepsilon^2}, \ldots, \tfrac{1}{\alpha-1}, \tfrac{1}{\alpha} \right).$$

We observe that the Goppa code $C(\alpha)$ is the subfield subcode of codes having as parity check matrices both H and H_α. Moreover, there exist matrices having structure different from H and H_α, which are parity check matrices for C.

We denote by

- $\Omega = \Omega(q,n,r)$ the set of Goppa codes, with fixed parameters q, n, r;
- $\mathbb{S} = \mathbb{S}(q,n,r)$ the set of all elements in $\mathbb{F}_{q^{nr}}$ of degree r over $\mathbb{F}_{q^n}$;
- $\mathbb{P} = \mathbb{P}(q,n,r)$ the set of irreducible polynomials of degree r in $\mathbb{F}_{q^n}[x]$.

3 The number of non-equivalent Goppa codes

This section briefly summarize actions on Ω already introduced in literature.

In [14] the action on Ω is obtained by considering an action on $\mathbb{S}$ of an "semi-affine" group $T = AGL(1,q^n)\langle\sigma\rangle$ in the following way: for $\alpha \in \mathbb{S}$ and $t \in T$, $\alpha^t = a\alpha^{q^i} + b$ for some $a, b \in \mathbb{F}_{q^n}$, $a \neq 0$ and $i = 1 \ldots nr$. The action gives a number of orbits over $\mathbb{S}$ which is an upper bound for the number of non equivalent Goppa codes. The main result is the following:

Theorem 1. *[14] If α, $\beta \in \mathbb{S}$ are related as it follows*

$$\beta = \zeta\alpha^{q^i} + \xi \tag{4}$$

for some $\zeta, \xi \in \mathbb{F}_{q^n}$, $\zeta \neq 0, i = 1\ldots nr$, then $C(\alpha)$ is equivalent to $C(\beta)$.

In [8] the action of a group FG isomorphic to $A\Gamma L(1,q^n)$ on the q^n columns of the parity check matrix H_α is considered. We point out that columns of H_α are in bijective correspondence with the elements of $\mathbb{F}_{q^n}$. The group FG induces on Ω the same orbits which arise from the action introduced in [14]. This action does not describe exactly the orbits of permutation non equivalent Goppa codes, since in some cases the number of permutation non-equivalent Goppa codes is less than the number of orbits of T on $\mathbb{S}$.

The group FG acts faithfully on the columns of H_α: it can be seen as a subgroup of the symmetric group S_{q^n}. In [5] it has been proved that it exists exactly one maximal subgroup M (isomorphic to $AGL(nm,p)$) of S_{q^n} (A_{q^n}) containing FG $(q=p^m)$. This suggests that one could consider the action of M on codes to reach the right bound. From this result one could hope that, when it is not possible to reach the exact number s of permutation non-equivalent Goppa codes by the action of FG, s is obtained by considering the group $AGL(nm,p)$. Unfortunately, this is not always true as it is shown in the next section. The following examples were introduced by Ryan in this PhD thesis [14]. In the next section we thoroughly analyze them, pointing out the group action of $AGL(nm,p)$.

4 Interesting examples

In this section we present a complete classification of the maximal irreducible Goppa codes $\Omega(3,2,4)$. We show another example when the bound proposed in [14] is not reached and the action of the maximal subgroup, isomorphic to AGL, is not sufficient to unify disjoint orbits of permutation equivalent codes.

Classification of $\boldsymbol{\Omega(3,2,4)}$ Let $q=3$, $\mathsf{n}=2$, $r=4$; let ε be a primitive element of $\mathbb{F}_{3^2}$ with minimal polynomial x^2+2x+2; let $L=[\varepsilon,\varepsilon^2,\ldots,\varepsilon^{3^2-2},1,0]$; let $\mathbb{P}=\mathbb{P}(3,2,4)$ be the set of all irreducible polynomials of degree 4 in $\mathbb{F}_9$, $|\mathbb{P}|=1620$ and let $\mathbb{S}=\mathbb{S}(3,2,4)$ be the set of all elements of degree 4 over $\mathbb{F}_9$, $|\mathbb{S}|=6480$. Let $\Gamma(g,L)$ be a maximal irreducible Goppa code of length 9 over $\mathbb{F}_3$, $g\in\mathbb{P}$. We denote by $S_{\mathbb{S}}$ the symmetric group on $\mathbb{S}$. We consider the action of T, $T\leq S_{\mathbb{S}}$, on $\mathbb{S}$: there are 13 orbits on $\mathbb{S}$. It means that there are at most 13 classes of maximal irreducible Goppa codes. We choose a representative for each class. We note that these codes have dimension $k=1$, so that they have two not trivial codewords.

Table 1 shows the thirteen classes: for each representative code Γ_i, we give the corresponding Goppa polynomial $g_i(x)$, the code parameters $[n,k,d]$ and the generator matrix M. The analysis of parameters $[n,k,d]$ and generator matrices shows that these 13 code representantives can not be equivalent, since they have different minimum distances. By analyzing thoroughly the code representatives we can observe that:

- Γ_1 is permutation equivalent to Γ_3;
- Γ_2 and Γ_{10} are permutation equivalent to Γ_7;
- Γ_{11} is permutation equivalent to Γ_6;

Γ_i	$g_i(x)$	$[n,k,d]$	M
Γ_1	$x^4+f^3x^3+fx+f^5$	$[9,1,9]$	[112212212]
Γ_2	$x^4+f^7x^3+x^2+f^5x+f^3$	$[9,1,5]$	[010222010]
Γ_3	x^4+f^5x+f	$[9,1,9]$	[122221112]
Γ_4	$x^4+f^5x^2+f^6x+f^2$	$[9,1,6]$	[120101202]
Γ_5	$x^4+f^7x^2+f^2x+f^5$	$[9,1,6]$	[112001011]
Γ_6	$x^4+fx^3+f^5x^2+f^3x+f^6$	$[9,1,7]$	[001111122]
Γ_7	$x^4+f^6x^3+f^2x^2+2x+f^5$	$[9,1,5]$	[001220110]
Γ_8	$x^4+2x^3+2x^2+2x+f^7$	$[9,1,6]$	[121120200]
Γ_9	$x^4+f^5x^3+f^2x^2+f^3$	$[9,1,6]$	[010021112]
Γ_{10}	$x^4+2x^3+f^3x^2+f^6,$	$[9,1,5]$	[120201200]
Γ_{11}	$x^4+fx^3+fx^2+fx+f^2,$	$[9,1,7]$	[120220221]
Γ_{12}	$x^4+f^3x^3+f^2x^2+2x+f^3,$	$[9,1,6]$	[101012012]
Γ_{13}	$x^4+f^3x^3+f^5x^2+x+f^6$	$[9,1,6]$	[011101202]

Table 1. Representatives of the 13 classes obtaining in the action of T over $\mathbb{S}$.

- Γ_4 is permutation equivalent to Γ_8;
- Γ_9 and Γ_{12} are permutation equivalent to Γ_{13}.

We can conclude that the number of different classes of permutation non equivalent codes is 6 and not 13 (Γ_5 composes a permutation equivalence class).

Moreover $\Gamma_5, \Gamma_4, \Gamma_8, \Gamma_9, \Gamma_{12}$ and Γ_{13} are monomially equivalent, so there are only 4 equivalence classes of non equivalent Goppa codes.

In Table 2 we summarize the results of the group actions as follows. The action of T on $\mathbb{S}$, $T \leq S_{\mathbb{S}}$, creates 13 orbits: we report the number of elements in each orbit $|\mathbb{S}^T|$ and we count the number of Goppa codes corresponding to these elements (by abuse of notation we write $|\Gamma_i^T|$). For each representative Γ_i, we consider its permutation group $\mathcal{P}(\Gamma_i)$: we obtain the number of codes permutation equivalent to it by computing $\frac{|S_9|}{|\mathcal{P}(\Gamma_i)|}$; the number of codes which are permutation equivalent to Γ_i under the actions of FG (and $AGL = AGL(2,3)$) is obtained as $\frac{|FG|}{|FG \cap \mathcal{P}(\Gamma_i)|}$ (and $\frac{|AGL|}{|ALG \cap \mathcal{P}(\Gamma_i)|}$, respectively). We use symbols $\clubsuit$, $\diamondsuit$, $\heartsuit$ and $\spadesuit$ to denote the four monomial equivalence classes and symbols $\oplus$, $\odot$, $\otimes$ to denote the permutation classes when they are different from the monomial classes. We write P.E. to say Permutation Equivalent.

In this example, the action of the only maximal permutation group $AGL \leq S_{q^n}$, which contains FG, is not sufficient to unify disjoint orbits of non equivalent codes. Only the whole symmetric group S_{q^n} gives the right number of non equivalent Goppa codes.

Remark 1. It is interesting to analyzing polynomials in $\mathbb{P}$. We denote by $\mathbb{P}_\clubsuit$ the set of polynomials corresponding to Goppa codes in the $\clubsuit$ equivalence class, and so on for the others, hence $\mathbb{P} = \mathbb{P}_\clubsuit \cup \mathbb{P}_\diamondsuit \cup \mathbb{P}_\spadesuit \cup \mathbb{P}_\heartsuit$. We denote by $\mathbb{P}_{*,\Gamma_i}$, the set of polynomials in $\mathbb{P}_*$, $* \in \{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$, corresponding to the codes in Γ_i^T. It is easy to check that if $g \in \mathbb{P}_\clubsuit$, g has the following shape $x^4 + \varepsilon^i x^3 + \varepsilon^j x + \varepsilon^k$

Γ_i			$\lvert\mathbb{S}^T\rvert$	$\lvert\Gamma_i^T\rvert$	$\lvert\mathcal{P}(\Gamma_i)\rvert$	$\frac{\lvert S_9\rvert}{\lvert\mathcal{P}(\Gamma_i)\rvert}$	$\frac{\lvert FG\rvert}{\lvert\mathcal{P}(\Gamma_i)\cap FG\rvert}$	$\frac{\lvert AGL\rvert}{\lvert\mathcal{P}(\Gamma_i)\cap ALG\rvert}$
Γ_1	♣		144	18	2880	126	18	54
Γ_3	♣		576	72	2880	$P.E.\Gamma_1$	72	72
Γ_2	♢		576	144	288	1260	144	432
Γ_{10}	♢		576	144	288	$P.E.\Gamma_2$	144	216
Γ_7	♢		576	144	288	$P.E.\Gamma_2$	144	432
Γ_6	♠		576	144	480	756	144	216
Γ_{11}	♠		288	72	480	$P.E.\Gamma_6$	72	108
Γ_5	♡	⊗	576	144	720	504	144	216
Γ_4	♡	⊕	576	144	432	840	144	432
Γ_8	♡	⊕	576	144	432	$P.E.\Gamma_4$	144	216
Γ_9	♡	⊙	288	72	288	1260	72	108
Γ_{12}	♡	⊙	576	144	288	$P.E.\Gamma_9$	144	216
Γ_{13}	♡	⊙	576	144	288	$P.E.\Gamma_9$	144	216
			6480	1530		4746	1530	2934

Table 2. Different group actions

for some $i, j, k \in [1, \ldots, q^n, -\infty]$, so that the x^2 coefficient is equal to zero. We know that $|\mathbb{P}_{\clubsuit,\Gamma_1}| = 36$ and $|\Gamma_1^T| = 18$: more than one polynomial generates the same code. We can show that couples of polynomials in $\mathbb{P}_{\clubsuit,\Gamma_1}$ generate the same code. Moreover if $g_1, g_2 \in \Gamma_1^T$ generate the same Goppa code then they have the same coefficients except for the constant term: we can obtain one constant term from the other by arising to the q-th power. For example polynomials $x^4 + \varepsilon^6 x^3 + \varepsilon^2 x + \varepsilon^2$ and $x^4 + \varepsilon^6 x^3 + \varepsilon^2 x + \varepsilon^6$ generate the same Goppa code. A similar argument can conduce us to say that polynomials in $\mathbb{P}_{\clubsuit,\Gamma_3}$ are 576, but they generate 72 different Goppa codes. We have that 4 polynomials create the same Goppa code and we find the following relation: given a polynomial $g \in \mathbb{P}_{\clubsuit,\Gamma_3}$, $g = x^4 + \varepsilon^i x^3 + \varepsilon^j x + \varepsilon^k$, then the following tree polynomials generate the same Goppa code: $g' = x^4 + \varepsilon^{iq} x^3 + \varepsilon^{jq} x + \varepsilon^{kq}$, $g'' = x^4 + \varepsilon^j x^3 + \varepsilon^i x + \varepsilon^k$ and $g''' = x^4 + \varepsilon^{jq} x^3 + \varepsilon^{jq} x + \varepsilon^{kq}$. Analogous arguments can be used to describe set of polynomials in $\mathbb{P}_{\diamondsuit}$, $\mathbb{P}_{\heartsuit}$ and $\mathbb{P}_{\spadesuit}$.

Codes in $\boldsymbol{\Omega(2,5,6)}$ Let us consider the codes studied in [13]. Let $q = 2$, $n = 5$ $r = 6$ and let f be a primitive element of $\mathbb{F}_{q^n}$ with minimal polynomial x^5+x^2+1; let $L = [f, f^2, \ldots, f^{32-2}, 1, 0]$. We consider the following two polynomials $p_1 := x^6+f^{22}x^5+f^2x^4+f^{25}x^3+f^{10}x+f^3$ and $p_2 := x^6+f^{20}x^5+f^{19}x^4+f^{19}x^3+f^{12}x^2+f^4x+f^28$. They generate equivalent Goppa codes $\Gamma_1(L, p_1)$ and $\Gamma_2(L, p_2)$, but their roots are in different orbits under the action of T over $\mathbb{S} = \mathbb{S}(2, 5, 6)$. To know how many codes are in each orbits we take a representative code and we construct its orbit under the permutation group $FG \leq S_{32}$. We verify that the action of the maximal subgroup $AGL(2, 5)$ containing FG does not unify the two orbits. Also in this case, the only permutation group which gives the right number of non equivalent Goppa code is the whole symmetric group S_{q^n}.

References

1. Berger, Thierry P., *Cyclic alternant codes induced by an automorphism of a GRS code*, Finite fields: theory, applications, and algorithms (Waterloo, ON, 1997).
2. Berger, Thierry P. and Charpin, P., *The permutation group of affine-invariant extended cyclic codes*, IEEE Trans. Inform. Theory, 42, 1996.
3. Charpin, Pascale, *Open problems on cyclic codes*, Handbook of coding theory, Vol. I, II, 963–1063, North-Holland, Amsterdam, 1998,
4. Chen, Chin-Long, *Equivalent irreducible Goppa codes*, IEEE Trans. Inf. Theory, 24, 766-770, 1978.
5. Dalla Volta, F., Giorgetti, M. and Sala, M., *Permutation equivalent maximal irreducible Goppa codes*, submitted to Designs, Codes and Cryptography and avaible at http://arxiv.org/abs/0806.1763.
6. Fitzpatrick, P. and Ryan, J. A., *Counting irreducible Goppa codes*, Journal of the Australian Mathematical Society, 2001, 71, 299–305.
7. Fitzpatrick, P. and Ryan, J. A., *The number of inequivalent irreducible Goppa codes*, International Workshop on Coding and Cryptography, Paris, 2001.
8. Giorgetti, M., *On some algebraic interpretation of classical codes*, University of Milan, 2006.
9. Huffman, W. Cary and Pless, Vera, *Fundamentals of error-correcting codes*, Cambridge University Press, Cambridge, 2003.
10. Li, Cai Heng, *The finite primitive permutation groups containing an abelian regular subgroup*, Proceedings of the London Mathematical Society. Third Series, 87, 2003.
11. McEliece, R.J., *A public key cryptosystem based on algebraic coding theory*, JPL DSN, 114–116, 1978.
12. MacWilliams, F. J. and Sloane, N. J. A., *The theory of error-correcting codes I*, North-Holland Publishing Co., 1977.
13. Ryan, J.A.; Magamba, K., *Equivalent irreducible Goppa codes and the precise number of quintic Goppa codes of length 32*, AFRICON 2007 , vol., no., pp.1-4, 26-28 Sept. 2007
14. Ryan, J., *Irreducible Goppa codes*, Ph.D. Thesis, University College Cork, Cork, Ireland, 2002.