Università di Milano–Bicocca
Quaderni di Matematica

Permutation equivalent maximal irreducible Goppa codes

Francesca Dalla Volta, Marta Giorgetti, Massimiliano Sala

Quaderno n. 9/2008 (arxiv:0806.1763v1)

Stampato nel mese di giugno 2008
presso il Dipartimento di Matematica e Applicazioni,
Università degli Studi di Milano-Bicocca, via R. Cozzi 53, 20125 Milano, ITALIA.

Disponibile in formato elettronico sul sito www.matapp.unimib.it.
Segreteria di redazione: Ada Osmetti - Giuseppina Cogliandro
tel.: +39 02 6448 5755-5758 fax: +39 02 6448 5705

Esemplare fuori commercio per il deposito legale agli effetti della Legge 15 aprile 2004 n.106.

Permutation equivalent maximal irreducible Goppa codes

Francesca Dalla Volta*, Marta Giorgetti†, Massimiliano Sala‡

June 10, 2008

Abstract

We consider the problem of finding the number of permutation non-equivalent classical irreducible maximal Goppa codes having fixed parameters q, n and r from a group theory point of view.
Keywords: Goppa codes, Linear codes, Permutation groups

1 Introduction

The study of classical Goppa codes is important since they are a very large class of codes, near to random codes. They are easy to generate and possess an interesting algebraic structure. For these reasons they are used in McEliece's public key cryptosystem [16]. This cryptosystem is based on the difficulty to find a generator matrix of a Goppa code when a "scrambled" of it is known.

In this paper we consider the problem 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 [6], [2], [3], [7], [9]). In Section 3 we briefly recall these approaches. In particular, we describe the action of a group FG isomorphic to $A\Gamma L(1, q^n)$ on the q^n columns of a suitable parity-check matrix H_α. This induces on maximal irreducible Goppa codes the same action which arises from [18]. This action does not describe exactly the orbits of Goppa codes, since in some cases the

*francesca.dallavolta@unimib.it, Dipartimento di Matematica e applicazioni Università di Milano Bicocca

†marta.giorgetti@uninsubria.it, Dipartimento di Fisica e Matematica Università dell'Insubria, Como

‡msala@bcri.ucc.ie, Dipartimento di Matematica Università di Trento

number of permutation non-equivalent Goppa codes is less than the number of orbits of FG. The group FG acts faithfully on columns of H_α, so that it may be seen as a subgroup of the symmetric group S_{q^n}. It seems interesting to study if there is a proper subgroup of S_{q^n} containing FG, acting on the set Ω of classical irreducible maximal Goppa codes of fixed parameters, and giving on Ω exactly the orbits of permutation equivalent codes. In order to consider this problem, we analyze the subgroups of S_{q^n} containing FG and in Section 4 we find that there 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 this M on codes to reach the right bound.

We are grateful to Andrea Caranti, Andrea Lucchini, John A. Ryan and Patrick Fitzpatrick for helpful discussions on this subject.

2 Preliminaries

In this section we fix some notation and we recall some basic concepts about linear codes and in particular about Goppa codes. Our main references are [11] for coding theory and [5] for group theory.

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.

Definition 2.1. *Let E/K be a field extension. A linear code C is called a* ***subfield subcode*** *if C is obtained as the restriction to K^n of a linear subspace L of E^n.*

By abuse of notation we call parity-check matrix also a matrix H with entries in E 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 2.2 ([11]). *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_1P is a generator matrix for C_2. They are* ***monomially equivalent*** *provided there is a monomial matrix M so that G_1M 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 $C_2 = C_1M\gamma$.*

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 2.3. *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 ([17]) 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 $\mathbb{F}_q$.

Definition 2.4. *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 2.3, 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

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

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 [6]):

$$H_\alpha = \left(\begin{array}{cccc} \frac{1}{\alpha-\varepsilon_1}, & \frac{1}{\alpha-\varepsilon_2}, & \ldots, & \frac{1}{\alpha-\varepsilon_{q^n}} \end{array} \right). \tag{3}$$

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

$$H_\alpha = \left(\begin{array}{cccccc} \frac{1}{\alpha-\varepsilon}, & \frac{1}{\alpha-\varepsilon^2}, & \ldots, & \frac{1}{\alpha-1}, & \frac{1}{\alpha} \end{array} \right).$$

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.

In the following an action on set $\mathbb{S}$ is considered, where $\mathbb{S} = \mathbb{S}(n, r)$ is composed of all elements in $\mathbb{F}_{q^{nr}}$ of degree r over $\mathbb{F}_{q^n}$.

3 Three actions on Ω

In this section we briefly present semiaffine actions introduced in [1] and in [8]. These actions have degrees $\frac{|\mathbb{S}|}{r}$ and $|\mathbb{S}|$ respectively. Moreover we consider an action of the group $A\Gamma L(1, q^n)$ on entries of parity-check matrix of type H_α. This time the degree is q^n.

In [1], the author works directly on polynomials by studying automorphism groups of several classes of codes.

If $\psi \in AGL(1,q^n)$, $\psi(z) = az + b,\ a, b \in \mathbb{F}_{q^n}$, $a \neq 0$, he defines

$$g^{\psi}(x) = \sum_{i=0}^{r} g_i (ax+b)^i.$$

The map ψ acts also on set $L = \mathbb{F}_{q^n}$, $\mathbb{F}_{q^n}^* = \langle \varepsilon \rangle$, by

$$L^{\psi} = \left(\varepsilon^{\psi^{-1}}, \ldots, (\varepsilon^{q^n-1})^{\psi^{-1}}, (\varepsilon^{-\infty})^{\psi^{-1}} \right).$$

The code $\mathcal{G}(L,g)^{\psi} = \mathcal{G}(L^{\psi}, g^{\psi})$ is said the *conjugate* of code $\mathcal{G}(L,g)$ by ψ.

Proposition 3.1. *[1] The Goppa codes are invariant by conjugation under the affine group $AGL(1,q^n)$, i.e. $\mathcal{G}(L,g)^{\psi} = \mathcal{G}(L,g)$ for all ψ such that $\psi(z) = az + b, a, b \in \mathbb{F}_{q^n}, a \neq 0$.*

We get

Corollary 3.2. *Goppa codes $\mathcal{G}(L, g^{\psi})$ is equivalent to Goppa code $\mathcal{G}(L,g)$.*

Proof. We known that $\mathcal{G}(L,g)^{\psi} = \mathcal{G}(L^{\psi}, g^{\psi})$ and from Proposition 3.1 $\mathcal{G}(L,g)^{\psi} = \mathcal{G}(L,g)$. From Definition 2.2 it follows that $\mathcal{G}(L,g^{\psi})$ is equivalent to $\mathcal{G}(L^{\psi}, g^{\psi}) = \mathcal{G}(L,g)$ so $\mathcal{G}(L,g)$ is equivalent to $\mathcal{G}(L,g^{\psi})$. □

More generally, if $\psi \in A\Gamma L(1,q^n)$, $\psi(z) = az^{q^t} + b$, with $a, b \in \mathbb{F}_{q^n}$, $a \neq 0$ ant $t \in \{0, \ldots, n-1\}$, we define

$$g^{\psi}(x) = \sum_{i=0}^{r} g_i (ax^{q^t} + b)^i \tag{4}$$

Equation (4) suggests to consider an action σ on $\mathbb{P} \subseteq \mathbb{F}_{q^n}[x]$, where $\mathbb{P}$ is the set of irreducible polynomials of degree r. For $g \in \mathbb{P}$, $g^{\sigma(\psi)}$ is the unique polynomial f of degree r such that $g(\alpha) = 0$ if and only if $f(\beta) = 0$ for $\beta = \left(\frac{\alpha - b}{a}\right)^{q^{nr-t}}$ (note $g^{\sigma(\psi)} \in \mathbb{P}$).

Indeed, if $g(x) = \sum_{i=0}^{r} g_i x^i$, there exist $\bar{g}_i, \forall i = 1, \ldots, r,\ \bar{a},\ \bar{b}$ such that $\bar{g}_i^{q^t} = g_i, \forall i = 1, \ldots, r,\ \bar{a}^{q^t} = a,\ \bar{b}^{q^t} = b$ so that

$$\sum_{i=0}^{r} \bar{g}_i^{q^t} (\bar{a}^{q^t} x^{q^t} + \bar{b}^{q^t})^i = \left(\sum_{i=0}^{r} \bar{g}_i (\bar{a}x + \bar{b})^i \right)^{q^t} = f(x)^{q^t}.$$

It is immediate to recognize that $g(\alpha) = 0$, for $\alpha \in \mathbb{S}$, if and only if $f(\beta) = 0$, with $\beta = \left(\frac{\alpha - b}{a}\right)^{q^{nr-t}} \in \mathbb{S}$.

With similar arguments used for Proposition 3.1, one gets

Proposition 3.3. *The Goppa codes are invariant by conjugation under the semiaffine group $A\Gamma L(1,q^n)$, i.e. $\mathcal{G}(L,g)=\mathcal{G}(L^\psi,f)$, where $f=g^{\sigma(\psi)}\in\mathbb{P}$.*

Corollary 3.4. *Goppa codes $\mathcal{G}(L,g)$ is equivalent to Goppa code $\mathcal{G}(L,f)$.*

In [18] the same action on Ω is obtained considering an action on $\mathbb{S}$ of an "affine" group $T=AGL(1,q^n)\langle\sigma\rangle$, where σ is defined as $\sigma: x\to x^q$; the group $\langle\sigma\rangle$ has order nr. The main result is the following:

Theorem 3.5. *[18] If $\alpha,\beta\in\mathbb{S}$ are related as it follows*

$$\beta=\zeta\alpha^{q^i}+\xi \tag{5}$$

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

Orbits over $\mathbb{S}$ give orbits on Ω.

Fact 3.6. *The above actions on $\mathbb{S}$ and on $\mathbb{P}$ create the same orbits on Ω.*

Proof. Let $\alpha\in\mathbb{S}$ be a root of $g(x)\in\mathbb{P}$. Let $\beta=\zeta\alpha^q+\xi\in\mathbb{S}$. There exists an irreducible polynomial $g_1\in\mathbb{F}_{q^n}[x]$, such that $g_1(\beta)=0$. From Proposition 3.3 we get that the orbit $\alpha^{FG}=\{t(\beta),\, t\in T\})$ induces on Ω the same orbit than $g^T=\{t(g), t\in T\})$. □

The work in [1] is mainly directed to the study of automorphism group of a given code; [18] is deeply interested in counting the number of non-equivalent Goppa codes.

In [18] the exact number of orbits on $\mathbb{S}$ is given. Unfortunately, several examples are exhibited where the number of orbits T on $\mathbb{S}$ is greater than the number of non-equivalent Goppa codes.

We introduce an action on columns of $H_\alpha=\left(\frac{1}{\alpha-\varepsilon},\frac{1}{\alpha-\varepsilon^2},\ldots,\frac{1}{\alpha-1},\frac{1}{\alpha}\right)$, which induces the same orbits on Ω than T. We state the results and give a sketch of the proofs. For more details see [9].

Let us consider the subgroup $FG\simeq A\Gamma L(1,q^n)\leq S_{q^n}$ in its natural action on points of $\mathbb{F}_{q^n}$. If $\psi\in FG$, then $\psi(x)=ax^{q^i}+b$, where $a,b\in\mathbb{F}_{q^n}$, $a\neq 0$ and $i=1,\ldots,n$. Since each entry (column) of H_α is uniquely determined by an element of $\mathbb{F}_{q^n}$, $A\Gamma L(1,q^n)$ realizes a permutation of H_α entries given by:

$$\left(\frac{1}{\alpha-\varepsilon}\right)^\psi=\frac{1}{\alpha-\varepsilon^\psi}.$$

Writing FG we mean $F=AGL(1,q^n)$ and G the automorphism group of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

The matrices H_β and $\zeta H_\beta^{q^j}$ are parity-check matrices for the same Goppa code $C(\beta)$. We characterize the permutations mapping H_α into $\zeta H_\beta^{q^j}$ in the following proposition.

Proposition 3.7. *Let H_α and H_β be parity-check matrices for Goppa codes $C(\alpha)$ and $C(\beta)$. If there exists a permutation $\rho \in S_{q^n}$, such that $\rho(H_\alpha) = \zeta(H_\beta)^{q^j}$, for some $\zeta, \beta \in \mathbb{F}_{q^n}, \zeta \neq 0$ and $j = 1, \ldots, nr$, then $\rho \in FG$.*

Proof. We consider

$$\rho(H_\alpha) = H'_\alpha = \left(\frac{1}{\alpha - \varepsilon^{i_1}}, \frac{1}{\alpha - \varepsilon^{i_2}}, \cdots, \frac{1}{\alpha - \varepsilon^{i_{q^n-1}}}, \frac{1}{\alpha - \varepsilon^{i_{-\infty}}} \right),$$

where $i_j = \rho(j)$ and matrix $\zeta(H_\beta)^{q^j}$:

$$\zeta(H_\beta)^{q^j} = \left(\frac{\zeta}{\beta^{q^j} - \varepsilon^{q^j}}, \frac{\zeta}{\beta^{q^j} - \varepsilon^{2q^j}}, \ldots, \frac{\zeta}{\beta^{q^j} - 1}, \frac{\zeta}{\beta^{q^j}} \right).$$

Suppose $\zeta = 1$ and $j = 1$ so that $\forall t \in \{1, 2, \ldots, q^n\}$ we have $\frac{1}{\beta^q - \varepsilon^{tq}} = \frac{1}{\alpha - \varepsilon^{i_t}}$ and then $\alpha - \beta^q = \varepsilon^{i_t} - \varepsilon^{tq}$.

If $\alpha - \beta^q = 0$, ρ is the permutation induced by the Frobenius map σ, since $\varepsilon^{i_t} = \varepsilon^{tq}$; it follows that

$$\rho(t) = \begin{cases} tq & \text{if } t = 1, 2, \ldots, q^n - 1 \\ -\infty & \text{if } t = -\infty \end{cases}$$

and $\rho = \sigma$.

If $\alpha - \beta^q \neq 0$, as above $\alpha - \beta^q \in \mathbb{F}_{q^n}$ so that $\alpha - \beta^q = \varepsilon^k$ for some $k \in \{1, \ldots, q^n - 1\}$ and then permutation $\rho \in FG$; explicitly it acts as:

$$\rho(t) = \begin{cases} i_t = tq + f_k(\varepsilon) & \text{if } t = 1, 2, \ldots, q^n - 1 \\ i_t = k & \text{if } t = -\infty \end{cases}$$

where i_t is such that $\varepsilon^{i_t} = \varepsilon^{tq} + \varepsilon^k$, and $f_k(\varepsilon)$ is a function depending on representation of $\mathbb{F}_{q^n}$.

If $\zeta \in \mathbb{F}_{q^n}^*, \zeta \neq 1$ and $j = 1$, then $\zeta = \varepsilon^l$ for some $l \in \{1, \cdots, q^n - 2\}$. With same arguments used in the previous step, we get

$$\zeta\alpha - \zeta\varepsilon^{i_t} = \beta^q - \varepsilon^{tq} \implies \zeta\varepsilon^{i_t} = \zeta\alpha - \beta^q + \varepsilon^{tq} \implies \varepsilon^{i_t} = \alpha - \zeta^{-1}\beta^q + \varepsilon^{tq-l}.$$

Again $\alpha - \zeta^{-1}\beta^q \in \mathbb{F}_{q^n}$; then there is $h \in \{1, \ldots, q^n\}$ so that $\varepsilon^{i_t} = \varepsilon^h + \varepsilon^{tq-l}$, and

$$\rho(t) = \begin{cases} i_t = tq - l + f_h(\varepsilon) & \text{if } t = 1, 2, \ldots, q^n - 1 \\ i_t = h & \text{if } t = -\infty \end{cases}$$

where $\varepsilon^{i_t} = \varepsilon^{tq-l} + \varepsilon^h$ and $f_h(\varepsilon)$ depending on the representation of $\mathbb{F}_{q^n}$. Concluding $\rho = \tau_k \mu_{\zeta^{-1}} \sigma$; here τ_k is the translation defined by $\tau_k : x \to x + \varepsilon^k$, μ_ζ is the map $\mu_\zeta : x \to \zeta x$ and σ is the Frobenius map; this proves $\rho \in FG$.

Finally, if $j \neq 1$ we have: $\frac{\zeta}{\beta^{q^j} - \varepsilon^{tq^j}} = \frac{1}{\alpha - \varepsilon^{i_t}}$ and $\zeta\alpha - \zeta\varepsilon^{i_t} = \beta^{q^j} - \varepsilon^{tq^j}$. As $\zeta = \varepsilon^l$ for some $l \in \{1, \ldots, q^n - 2\}$, we gain:

$$\varepsilon^{i_t} = \alpha - \varepsilon^{-l}\beta^{q^j} + \varepsilon^{tq^j - l}.$$

So there is $v \in \{1, \ldots, q^n\}$ such that $\alpha - \varepsilon^l \beta^{q^j} = \varepsilon^v$ and $\varepsilon^{i_t} = \varepsilon^v + \varepsilon^{tq^j - l}$. Permutation ρ is:

$$\rho(t) = \begin{cases} i_t = tq^j - l + f_v(\varepsilon) & \text{if } t = 1, 2, \ldots, q^n - 1 \\ i_t = v & \text{if } t = -\infty \end{cases}$$

where $\varepsilon^{i_t} = \varepsilon^{tq^j - l} + \varepsilon^v$ and $f_v(\varepsilon)$ depends on the representation of $\mathbb{F}_{q^n}$. Concluding $\rho = \tau_v \mu_{\zeta^{-1}} \sigma^j$. Clearly in all cases $\rho \in FG$. □

Corollary 3.8. *Let H_α and H_β be parity-check matrices for Goppa codes $C(\alpha)$ and $C(\beta)$. If there exists a permutation $\rho \in S_{q^n}$, such that $\rho(H_\alpha) = \zeta H_\beta$, for same $\zeta, \beta \in \mathbb{F}_{q^n}, \zeta \neq 0$, then $\rho \in F$.*

4 Maximal subgroups

The action of $A\Gamma L(1, q^n)$ does not reach the exact number of non-equivalent maximal Goppa codes. So we look for maximal subgroups of S_{q^n} containing a fixed $A\Gamma L(1, q^n) = FG$.

Theorem 4.1 ([5])**.** *A maximal subgroup of S_{q^n} is one of the following:*

1. *intransitive, $S_k \times S_l$, $k + l = q^n$;*
2. *transitive imprimitive: the wreath product $S_k \, Wr \, S_l$ in the standard action, $kl = q^n$;*
3. *primitive non-basic, the wreath product $S_k \, Wr \, S_l$ in the product action, $k^l = q^n, k \neq 2$;*
4. *affine $AGL(d, p), p^d = q^n$;*
5. *diagonal, $T^k.(Out(T) \times S_k)$, T non abelian simple, $|T|^{k-1} = q^n$; here $Out(T)$ denotes, as usual, the factor group $\frac{Aut(T)}{T}$.*

6. *almost simple, that is an automorphism group G of a finite non abelian simple group S, $S \leq G \leq Aut(S)$.*

A maximal subgroup of the alternating group is the intersection of one of these groups with the alternating group.

Remark 4.2. We explicitly observe that for p even, $d \geq 3$, the group $AGL(d,p)$ is actually contained in the alternating group A_{p^d}. It is sufficient to realize that, in this case, the translations are product of 2^{d-1} cycles of length 2, as well as the transvections are product of 2^{d-2} cycles of length 2. As the transvections generate the general linear group $GL(p,2)$, $AGL(p,2)$ is contained in A_{2^d}.

Proposition 4.3. *FG is contained in A_{q^n} if and only if q is even.*

Proof. The thesis follows from the following result.

Claim 4.4. *[14] Let X be a primitive permutation group of degree n. Then X contains an abelian regular subgroup G if and only if either*

i) $X \leq AGL(d,p)$, where p is a prime, $d \geq 1$ and $n = p^d$; or

ii) $X = (\tilde{T_1} \times \ldots \times \tilde{T_l}) \cdot O \cdot P$, $G = G_1 \times \ldots \times G_l$ where $n = m^l$, $l \geq 1$, $G_i < \tilde{T_i}$, with $|G_i| = m$, $\tilde{T_1} \cong \ldots \cong \tilde{T_l}$, $O \leq \mathrm{Out}(\tilde{T_1}) \times \ldots \times \mathrm{Out}(\tilde{T_l})$, P is a transitive permutation group of degree l and one of the following holds:

   (a) $(\tilde{T_i}, G_i) = (PSL(2,11), \mathbb{Z}_{11})$, $(M_{11}, \mathbb{Z}_{11})$, $(M_{12}, \mathbb{Z}_2^2 \times \mathbb{Z}_3)$, $(M_{23}, \mathbb{Z}_{23})$ (M_i are the Mathieu groups);

   (b) $\tilde{T_i} = PGL(d,q)$ e $G_i = \mathbb{Z}_{\frac{q^d-1}{q-1}}$ is a Singer group;

   (c) $\tilde{T_i} = P\Gamma L(2,8)$ and $G_i = \mathbb{Z}_9 \not\leq PSL(2,8)$;

   (d) $\tilde{T_i} = S_m$ or A_m and G_i is an abelian group of order m.

Take $X = FG$. FG contains the subgroup A of translations, $A = \{\tau_\varepsilon : x \to x + \varepsilon\}$, so that FG is contained in $N_{S_{q^n}}(A) = AGL(nm,p)$. By the above remark, if $p = 2$, the group FG is contained in A_{q^n}. If p is odd, then the element $\mu_\varepsilon : x \to \varepsilon x$ belongs to FG and it is odd, as its order is $q^n - 1$ (recall that an element of order $q^n - 1$ is said a Singer cycle); this proves that FG (and $AGL(nm,p)$) is not a subgroup of A_{q^n}. □

Theorem 4.5. *Let $G = A_{q^n}$ if $q = 2^m$, $G = S_{q^n}$ for q odd. If M is a maximal subgroup of G containing FG, then M is isomorphic to the affine group $AGL(nm,p)$. Moreover, there is exactly one maximal subgroup containing FG.*

Proof. As FG is a primitive 2-transitive group of G, a maximal subgroup M of S_{q^n} containing FG, is an almost simple group or it is isomorphic to the affine group $AGL(nm, p)$ ([5]). In the proof of Proposition 4.3 we have seen that FG is contained in $AGL(mn, p)$. We prove that it is not contained in an almost simple group. By contradiction, let M be an automorphism group of a simple non abelian group S, $S \leq M \leq Aut(S)$. If M contains FG, the stabilizer of a point ω in $\mathbb{F}_{q^n}$ has index $q^n = p^{nm}$. As S is normal in M, S is transitive on $\mathbb{F}_{q^n}$, so that we are reduced to consider subgroups of prime power index in S. These were described by Guralnick and for the reader's sake we write the main result of [10].

Claim 4.6 ([10])**.** *Let G be a nonabelian simple group with $H < G$ and $[G : H] = p^d = q^n$, p prime. One of the following holds.*

1. *$G = A_{q^n}$ and $H \cong A_{q^n-1}$;*
2. *$G = PSL(s, t)$ and H is the stabilizer of a line or hyperplane. Then $[G : H] = \frac{t^s-1}{t-1} = q^n$ (Note s must be prime);*
3. *$G = PSL(2, 11)$ and $H \cong A_5$;*
4. *$G = M_{23}$ and $H \cong M_{22}$ or $G = M_{11}$ and $H \cong M_{10}$;*
5. *$G = PSU(4, 2) \cong PSp(4, 3)$, H is the parabolic subgroup of index 27.*

Cases 3, 4, 5, are easily ruled out, as p^{mn} is neither a prime number, nor 27. Similarly, case 1 is ruled out when p is odd, as, in this case, the element μ_ε is odd. If $p = 2$, then FG is actually contained in $M \simeq A_{q^n}$. So, we are left with Case 2. Here, we use Claim 4.4. X satisfies condition ii), with

$$X = S = PSL(s, t), \qquad [S : H] = \frac{s^t - 1}{t - 1} = p^{nm},\ l = 1.$$

and it is easy to see that it is not the case.
Now, we prove that there is exactly one subgroup isomorphic to $AGL(nm, p)$ containing FG.

Let q be odd: in S_{q^n} there is exactly one conjugacy class of maximal subgroups of this type (see for example [15]). So, let $FG \leq M \simeq AGL(nm, p)$, where the normal subgroup of the translation of M is exactly the translation group A of FG ([12]). The element μ_ε generates a Singer subgroup; it is well known that the Singer cycles are conjugated in M; from the knowledge of the overgroups of a Singer cycle [13], [4], one easily proves that also the normalizers of Singer cycles contained in M are conjugate in M. It follows

that if FG^g, $g \in S_{q^n}$ is contained in M, there exists an element $m \in M$, such that $FG^g = FG^m$. So, if s denotes the number of the subgroups of M containing FG, we get:

$$[S_{q^n} : N_{S_{q^n}}(FG)] = \frac{[S_{q^n} : M] \cdot [M : N_M(FG)]}{s};$$

now, from [14] one gets $N_{S_{q^n}}(FG) \leq M$, so that $s = 1$.

Now, suppose q is even. $FG \leq A_{q^n}$ and in A_{q^n} the conjugacy class of S_{q^n} subgroups which are isomorphic to $AGL(nm, p)$. In A_{q^n} $AGL(nm, p)$ splits into two classes so that also the class of Singer cycles splits into two different classes. Same argument used for the odd case leads to the result. □

References

[1] Berger, Thierry P., *On the cyclicity of Goppa codes, parity-check subcodes of Goppa codes, and extended Goppa codes*, Finite Fields and their Applications, 6, 2000.

[2] Berger, Thierry P., *Cyclic alternant codes induced by an automorphism of a GRS code*, Finite fields: theory, applications, and algorithms (Waterloo, ON, 1997).

[3] Berger, Thierry P. and Charpin, P., *The permutation group of affine-invariant extended cyclic codes*, IEEE Trans. Inform. Theory, 42, 1996.

[4] Britnell, John R. and Evseev, Anton and Guralnick, Robert M. and Holmes, Petra E. and Maroti, Attila, *Sets of elements that pairwise generate a linear group*, preprint `www-circa.mcs.st-and.ac.uk`, 2006.

[5] Cameron, P. J., *Permutation groups*, Cambridge University Press, 1999, 45, London Mathematical Society Student Texts, Cambridge.

[6] Chen, Chin-Long, *Equivalent irreducible Goppa codes*, IEEE Trans. Inf. Theory, 24, 766-770, 1978.

[7] Fitzpatrick, P. and Ryan, J. A., *Counting irreducible Goppa codes*, Journal of the Australian Mathematical Society, 2001, 71, 299–305.

[8] Fitzpatrick, P. and Ryan, J. A., *The number of inequivalent irreducible Goppa codes*, International Workshop on Coding and Cryptography, Paris, 2001.

[9] Giorgetti, M., *On some algebraic interpretation of classical codes*, University of Milan, 2006.

[10] Guralnick, Robert M., *Subgroups of prime power index in a simple group*, Journal of Algebra, 81, 2, 304–311 1983.

[11] Huffman, W. Cary and Pless, Vera, *Fundamentals of error-correcting codes*, Cambridge University Press, Cambridge, 2003.

[12] Huppert, B., *Endliche Gruppen 1*, Berlin, Heidelberg, Springer-Verlag, 1967.

[13] Kantor, William M., *Linear groups containing a Singer cycle*, Journal of Algebra, 62, 1980, 1, 232–234.

[14] Li, Cai Heng, *The finite primitive permutation groups containing an abelian regular subgroup*, Proceedings of the London Mathematical Society. Third Series, 87, 2003.

[15] Liebeck, Martin W. and Shalev, Aner, *Maximal subgroups of symmetric groups*, Journal of Combinatorial Theory. Series A, 75, 1996, 2, 341–352.

[16] McEliece, R.J., *A public key cryptosystem based on algebraic coding theory*, JPL DSN, 114–116, 1978.

[17] MacWilliams, F. J. and Sloane, N. J. A., *The theory of error-correcting codes I*, North-Holland Publishing Co., 1977.

[18] Ryan, J., *Irreducible Goppa codes*, Ph.D. Thesis, University College Cork, Cork, Ireland, 2002.