The automorphism group of the generalized Reed-Muller codes

Thierry Pierre Berger, Pascale Charpin

UNITÉ DE RECHERCHE
INRIA-ROCQUENCOURT

Institut National
de Recherche
en Informatique
et en Automatique

Domaine de Voluceau
Rocquencourt
B.P.105
78153 Le Chesnay Cedex
France
Tél.:(1) 39 63 55 11

Rapports de Recherche

N° 1363

Programme 2
Calcul symbolique, Programmation et Génie logiciel

THE AUTOMORPHISM GROUP OF THE GENERALIZED REED-MULLER CODES

Thierry BERGER
Pascale CHARPIN

Janvier 1991

RR-1363

Groupe d'automorphismes des codes de Reed et Muller généralisés

The automorphism group of the Generalized Reed-Muller codes

Thierry Berger* Pascale Charpin**

Résumé

Nous démontrons que le groupe d'automorphismes des codes de Reed et Muller généralisés est le groupe général affine. Les codes de Reed et Muller généralisés ont été définis par KASAMI, LIN et PETERSON. Ils ont ensuite été étudiés en détail par DELSARTE, GOETHALS et MAC-WILLIAMS ; notre résultat a pour point de départ leur description de l'ensemble des mots de poids minimum de ces codes. Un automorphisme d'un code cyclique q-aire est ici une permutation des éléments du corps fini $GF(q^m)$.

Abstract

We prove that the automorphism group of the Generalized Reed-Muller codes is the general linear nonhomogeneous group. The Generalized Reed-Muller codes are introduced by KASAMI, LIN and PETERSON. An extensive study was made by DELSARTE, GOETHALS and MAC-WILLIAMS ; our result follows their description of the minimum weight codewords. An automorphism of a cyclic q-ary code is here a substitution over the field $GF(q^m)$.

* UFR des Sciences de Limoges, 123 av. A. Thomas, 87060 Limoges Cedex, France.

** INRIA, Projet CODES, Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le Chesnay Cedex, France.

1 Introduction

In this paper we consider linear codes of length q^m, $q = p^r$ and p is a prime, over a finite field K of characteristic p. Usually these codes are called *extended primitive codes*. Let G be the finite field of order q^m; an *automorphism* of such a code C is a permutation on G which preserves C. We denote by $G(m,q)$ the general linear nonhomogeneous group GLNH(m,q) whose elements are the permutations on G of the form:

$$\pi_{M,h} \; : \; g \longmapsto Mg + h \quad , \tag{1}$$

where M is a non singular matrix of order m over $GF(q)$ and h is any point of G represented as a column vector. The whole class of extended primitive codes being invariant under $G(m,q)$ was characterized by DELSARTE. We denote by $\mathcal{D}(m,q)$ this class of codes. The result of DELSARTE[10] derived from a significant work on the *polynomial codes* due essentially to KASAMI et al.[13,14,15] and DELSARTE et al.[11]. In particular, DELSARTE generalized the condition, obtained by KASAMI et al., for extended cyclic codes which are invariant under the affine group $G(1,q)$. These conditions are of great interest, because a code of $\mathcal{D}(m,q)$ is then recognizable by the form of its zero's-set; so it is clear that the class $\mathcal{D}(m,q)$ contains interesting subclasses as the extended Bose-Chaudhury-Hocquenghem (BCH) codes, for $m = 1$, or the Generalized Reed-Muller (GRM) codes. However there are few results about the whole automorphism group of the codes belonging to $\mathcal{D}(m,q)$. For instance, the automorphism groups of BCH-codes are not known; on the other hand, the automorphism group of the extended Reed-Solomon (RS) codes of length q is exactly $G(1,q)$ [12] and it is well-known that the automorphism group of the binary Reed-Muller (RM) codes is $G(m,2)$ [16].

We say that a GRM-code of length q^m over $K = GF(q^e)$ is a q-ary RM-code. Our main result in the present paper is that the automorphism group of the q-ary Reed-Muller codes, for any q and any m, is exactly $G(m,q)$ (Theorem 5). The generalisation of the RM-codes to the nonbinary case was originally introduced by KASAMI et al.[15]; DELSARTE et al. later studied, in great detail, the properties of these codes and their relatives; in particular, they obtain in the general case an enumeration of the minimum weight codewords of the GRM-codes [11]. Starting from this last result we can characterize, in some cases, the permutations on G which preserve the set of the

minimum weight codewords of a given GRM-code. The whole result follows from the fact that the dual of a GRM-code is a GRM-code.

A linear code of length q^m over K can be considered as a subspace of the modular algebra $K[G]$, that we denote by $\mathbf{A}$. This property is more interesting for the codes of $\mathcal{D}(m,q)$, because a code belonging to $\mathcal{D}(m,q)$ is an extended cyclic code which is an ideal of $\mathbf{A}$. In Section 2 we present in this context the extended cyclic q-ary codes and the automorphisms of codes. We point out that the product of the algebra $\mathbf{A}$ is an interesting tool for the description of the codes of $\mathcal{D}(m,q)$. In particular, the product of two codes of $\mathcal{D}(m,q)$ is a code of $\mathcal{D}(m,q)$. In Section 3 we explain in $\mathbf{A}$ the set of the minimum weight codewords of the GRM-codes, using the product of the algebra and the minimum codewords of the extended RS-codes of length q. Henceforth we can identify a permutation which preserves a given GRM-code with an affine bijection (in Section 4). The proof follows our description of the minimum weight codewords and uses the *fundamental Theorem of the affine geometry*, applied to finite fields - this Theorem is recalled and explained in the Appendix.

2 GRM-codes in a modular algebra

Recall that $G = GF(q^m)$, $q = p^r$, may be identified to the field $GF(p^{rm})$. In general $K = GF(q^e)$. The algebra $\mathbf{A} = K[G]$ is the set of formal polynomials,

$$x = \sum_{g \in G} x_g \, X^g \quad , \quad x_g \in K \quad ,$$

with the usual operations:

$$a \sum_{g \in G} x_g X^g + b \sum_{g \in G} y_g X^g = \sum_{g \in G} (a x_g + b y_g) X^g \quad ,$$

$$a X^g b X^h = ab X^{g+h} \quad , \quad 0 = \sum_{g \in G} 0 \; X^g \quad , \quad 1 = X^0 \quad ,$$

where $a \in K$, $b \in K$, $x \in \mathbf{A}$, $y \in \mathbf{A}$, $g \in G$, $h \in G$.

By convention, a K-subspace of $\mathbf{A}$ is a *code of* $\mathbf{A}$. An automorphism of a code is a permutation of the q^m coordinate places which transforms

codewords into codewords. Then we define a permutation σ on G as a transformation on $\mathbf{A}$:

$$\sigma \ : \ \sum_{g\in G} x_g \ X^g \ \longmapsto \ \sum_{g\in G} x_g \ X^{\sigma(g)} = \sum_{g\in G} x_{\sigma^{-1}(g)} \ X^g \ . \tag{2}$$

We denote by $Aut(C)$ the automorphism group of a code C. A permutation σ is an element of $Aut(C)$ if and only if $\sigma(x) \in C$ for all $x \in C$.

A code C is an extended cyclic code if and only if $Aut(C)$ contains the permutations:

$$\pi_{u,0} \ : \ x \in \mathbf{A} \ \longmapsto \ \sum_{g\in G} x_g \ X^{ug} \quad , \ u \in G^*$$

- The extension is here the usual one: each codeword is extended by adding an overall parity check [16] -.

In this case, C can be defined by its zeros-set. Let $S = [0, n]$, $n = q^m - 1$; for each $s \in S$ let us define:

$$\phi_s \ : \ x \in \mathbf{A} \ \longmapsto \ \phi_s(x) = \sum_{g\in G} x_g \ g^s \ , \tag{3}$$

where $\phi_s(x)$ is calculated in an overfield of K and G and, by convention, $\phi_0(x) = \sum_{g\in G} x_g$.
Let α be a primitive element of G. The codeword x is an extension of a polynomial which has the root α^s if and only if $\phi_s(x) = 0$. Thus an extended cyclic code can be uniquely defined by the set $\{s \in S \mid \phi_s(C) = 0\}$.

Definition 1 *Let T be a subset of S containing 0, and assume that T is invariant under the multiplication by q mod n. Then the code,*

$$C = \{ \ x \in \mathbf{A} \mid \phi_s(x) = 0 \ , \ s \in T \ \} \ , \tag{4}$$

is an extended cyclic q-ary code. We say that T is the defining-set of C.

Let the q-ary expansion of $s \in S$:

$$s = \sum_{i=0}^{m-1} s_i \ q^i \quad , \ s_i \in [0, q-1] \ ,$$

and define the *q-weight of* s as $\omega_q(s) = \sum_{i=0}^{m-1} s_i$. Let $\nu \in [1, m(q-1)[$. Then the set:

$$I_\nu(m,q) = \{\ s \in S \mid \omega_q(s) < \nu\ \} \tag{5}$$

is the defining-set of the *q-ary RM-code of order* $m(q-1)-\nu$, denoted by $C_\nu(m,q)$ [9,11,15].

REMARKS 1: 1) The code $C_\nu(1,q)$ is the extended Reed-Solomon code of minimum distance $\nu+1$.
2) Recall that the dual of $C_\nu(m,q)$ is the code $C_\mu(m,q)$, with $\mu = m(q-1)-\nu+1$ [15].
3) For each q' dividing q, we can define a class of q'-ary extended cyclic codes as codes of **A**. Then we can always define the p-ary RM-codes as codes of **A**: that is the codes $C_\nu(rm,p)$, with defining-set $I_\nu(rm,p)$.

The following Theorem, due to DELSARTE, gives a necessary and sufficient condition for cyclic q-ary codes to be invariant under the group $G(m,q)$.

Theorem 1 [10] *Let C be a code of* **A**. *Then $Aut(C)$ contains $G(m,q)$ if and only if C is an extended cyclic q-ary code, the defining-set T of which satisfies:*

$$s \in T \ \ and \ \ t \ satisfies \ (I) \implies t \in T\ , \tag{6}$$

where (I) is :

$$(I)\ :\ \omega_q(p^k t) \le \omega_q(p^k s)\ \ ,\ \ k \in [0, r-1]$$

- $q = p^r$ and the multiplication in S is calculated modulo n -

REMARK 2: It is clear that the codes $C_\nu(m,q)$ are invariant under $G(m,q)$. If $m = 1$ - i.e. if we consider codes of length q over K -, we have $\omega_q(s) = s$ for $s \in [0, q-1]$. Then the condition (I) is equivalent to

$$t_i \le s_i\ \ ,\ \ i \in [0, r-1]\ ,$$

where $(s_0, \ldots, s_{r-1})$ and $(t_0, \ldots, t_{r-1})$ are respectively the coefficients of the p-ary expansion of s and t. We then obtain the condition of KASAMI et al. for extended cyclic codes being invariant under the affine group $G(1,q)$ [13]. DÜR proved in [12] that the automorphism group of the codes $C_\nu(1,q)$, $\nu \in [2, q-1[$, is exactly $G(1,q)$ (see also a direct proof in [2]).

REMARK 3: [10] The Theorem 1 characterizes the codes of $\mathbf{A}$ which are invariant under $G(rm,p)$. In this case T is invariant under the multiplication by p and the condition (I) becomes: $\omega_p(t) \leq \omega_p(s)$. Thus there is an element ν of $[1, rm(p-1)]$ such that the defining-set T is the set $\{\ s \mid \omega_p(s) < \nu\ \}$, which is the defining-set $I_\nu(rm,p)$ of the p-ary RM-code $C_\nu(rm,p)$. Then *a code of* $\mathbf{A}$ *which is invariant under* $G(rm,p)$ *is a* p*-ary RM-code.*

A code C is an ideal of $\mathbf{A}$ if and only if $Aut(C)$ contains the permutations:

$$\pi_{0,h} \ : \ x \in \mathbf{A} \ \longmapsto \ \sum_{g \in G} x_g \ X^{g+h} \quad , \ h \in G$$

So a code of $\mathcal{D}(m,q)$ is an ideal of $\mathbf{A}$. The algebra $\mathbf{A}$ has only one maximal ideal namely its *radical*. The radical P of $\mathbf{A}$ is composed with the elements $x \in \mathbf{A}$ satisfying $x^p = 0$. Since $(\sum_{g \in G} x_g X^g)^p = \sum_{g \in G} x_g^p X^0$, we have:

$$P \ = \ \{\ x \in \mathbf{A} \mid \sum_{g \in G} x_g = 0\ \} \ .$$

Hence, by definition, an extended cyclic code is contained in P. We denote by P^j the ideal which is the j-power of the ideal P - i.e. which is generated by the products $\prod_{k=1}^{j} x_k$, $x_k \in P$ -. Suppose that G is identified to $GF(p^{rm})$ and let $(e_1, \ldots, e_{m'})$ be any basis of G, $m' = rm$. Then for each $j \in [1, m'(p-1)]$, the set

$$B(j) = \left\{ \ \prod_{i=1}^{m'} (X^{e_i} - 1)^{k_i} \ \mid \ k_i \in [0, p-1] \ , \ \sum_{i=1}^{m'} k_i \ \geq \ j \ \right\} \qquad (7)$$

is a basis of P^j [7]. This description yields that P^j is invariant under $G(m',p)$. Then it becomes from Remark 3 that *the* j*-powers of the radical of* $\mathbf{A}$ *are the* p*-ary Reed-Muller codes.*

This result was presented by BERMAN in [4]; the reader can see other proofs in [6,9]; it was proved independantly by POLI, which showed that the codes P^j are the only ideals of $\mathbf{A}$ being invariant under $G(m',p)$ [17].

One can remark also that $C_1(m,q) = P$ and

$$C_{m(q-1)}(m,q) = P^{m(q-1)} = (\sum_{g \in G} X^g)K \ .$$

Let U and V be two codes of $\mathbf{A}$; we denote by UV the code generated by the products xy, $x \in U$ and $y \in V$ and we say that UV is *the product* of U and V. Let $\pi_{M,0} \in G(m,q)$; we have

$$\pi_{M,0}(xy) = \pi_{M,0}(x)\pi_{M,0}(y) \quad , \; since \; \pi_{M,0}(X^g X^h) = X^{M(g+h)} = X^{Mg} X^{Mh} \quad .$$

Hence if U and V are invariant under $\pi_{M,0}$, then the code UV is invariant under $\pi_{M,0}$. Particularly a product of two extended cyclic codes is an extended cyclic code.

We have seen that the product of two p-ary RM-codes is a p-ary RM-code. This result does not remain the same for the q-ary RM-codes. For instance, we have $P = C_1(m,q)$ while P^2 is not the code $C_2(m,q)$. However we can prove an inclusion formula and for that, we need to the

Lemma 1 *Let x and y be any codewords in $\mathbf{A}$. Let $s \in S$. Then,*

$$\phi_s(xy) = \sum_{t \prec s} \binom{s}{t} \phi_t(x)\phi_{s-t}(y) \quad , \tag{8}$$

where, $(s_0, \ldots, s_{m'-1})$ and $(t_0, \ldots, t_{m'-1})$ being the coefficients of the p-ary expansion of s and t, $\prec$ denotes the partial order relation:

$$t \prec s \quad \Longleftrightarrow \quad t_i \leq s_i \; , \quad for \; all \; i \quad . \tag{9}$$

Proof:

$$\begin{aligned} \phi_s(xy) &= \sum_{g \in G} x_g \sum_{h \in G} y_h (g+h)^s = \sum_{g \in G} x_g \sum_{h \in G} y_h \sum_{t=0}^{s} \binom{s}{t} g^t h^{s-t} \\ &= \sum_{t=0}^{s} \binom{s}{t} \sum_{g \in G} x_g g^t \sum_{h \in G} y_h h^{s-t} = \sum_{t \prec s} \binom{s}{t} \phi_t(x)\phi_{s-t}(y) \end{aligned}$$

- applying LUCAS'S Theorem, we obtain the summation over $t \prec s$ -. □

Theorem 2 *Let ν and ν' such that $\nu + \nu' \leq m(q-1)$. Then the product of $C_\nu(m,q)$ and $C_{\nu'}(m,q)$ satisfies:*

$$C_\nu(m,q)\, C_{\nu'}(m,q) \subset C_{\nu+\nu'}(m,q) \quad .$$

Proof: Let $U = C_\nu(m,q)$, $V = C_{\nu'}(m,q)$, $x \in U$ and $y \in V$. Let T be the defining-set of UV. Let $s \in I_{\nu+\nu'}(m,q)$ and calculate $\phi_s(xy)$ with (8). Let $t \prec s$; if $t \in I_\nu(m,q)$ then $\phi_t(x) = 0$; if $t \notin I_\nu(m,q)$, we have:

$$\nu \leq \omega_q(t) < \nu + \nu' \ \ and \ \ t \prec s \quad \Rightarrow \quad \omega_q(s-t) < \nu' \quad \Rightarrow \quad \phi_{s-t}(y) = 0 \ .$$

Thus $\phi_s(xy) = 0$; we have proved that $I_{\nu+\nu'}(m,q) \subset T$; that means that UV is contained in $C_{\nu+\nu'}(m,q)$. □

3 The minimum weight codewords of the GRM-codes

Recall that $\mathbf{A} = K[G]$, $G = GF(q^m)$ and $K = GF(q^e)$. For any element x of $\mathbf{A}$, let us define the *support* of x as the set:

$$supp(x) = \{\ g \in G \mid x_g \neq 0\ \} \ , \ where\ x = \sum_{g \in G} x_g X^g \ . \tag{10}$$

The *weight* of x is: $\omega(x) = |supp(x)|$. Let g be a non zero element of G and let $\nu \in [1, q-1[$. We denote by $C_\nu(\{g\},q)$ the extended RS-code of length q and minimum distance $\nu+1$, considered as a code of $\mathbf{A}$ in the sense that each codeword has its support in the subspace $gGF(q)$ of G:

$$C_\nu(\{g\},q) = \{\ x \in \mathbf{A} \mid x = \sum_{\lambda \in GF(q)} x_{\lambda g} X^{\lambda g} \ \ and \ \ \phi_s(x) = 0 \ , \ s \in [0, \nu[\ \} \ . \tag{11}$$

Let $x \in C_\nu(\{g\},q)$ and let $t \in S$ such that $\omega_q(t) < \nu$. Since $\lambda^q = \lambda$, we have:

$$\phi_t(x) = \sum_{\lambda \in GF(q)} x_{\lambda g} (\lambda g)^t = g^t \sum_{\lambda \in GF(q)} x_{\lambda g} \lambda^{\omega_q(t)} = 0 \ .$$

Then $\phi_t(x) = 0$, for each $t \in I_\nu(m,q)$. We have proved:

Lemma 2 *Let $\nu \in [1, q-1[$. Then the code $C_\nu(\{g\},q)$ is contained in $C_\nu(q,m)$, for all $g \in G^*$.*

Let $k \in [1,m]$ and let V be a k-dimensional subspace of G. Let $x = \sum_{g \in V} X^g$; the following property is proved by KASAMI et al. in [15]:

$$s \in S \ \ and \ \ \omega_q(s) < k(q-1) \quad \Longrightarrow \quad \phi_s(x) = 0 \ . \tag{12}$$

In accordance with the definition of $C_{k(q-1)}(m,q)$, this property implies:

Lemma 3 *Let $k \in [1,m]$ and define the subset of* **A**:

$$A_k = \{ \sum_{g \in V} X^g \mid V \text{ is a } k-\text{dimensional subspace of } G \} \qquad (13)$$

Then $A_k \subset C_{k(q-1)}(m,q)$.

Now we are able to present a description of the set of the minimum weight codewords (*mwc*'s) of any GRM-code. We shall show that a *mwc* can be identified to an element y of an A_k or to a *mwc* z of a code $C_\nu(\{g\},m)$ or to a product of type yz.
In [11], DELSARTE et al. gave another description and the enumeration of the *mwc*'s of the GRM-codes of length q^m over $GF(q)$. The following Lemma shows that their results are available for $K = GF(q^e)$, $e > 1$. So we can present the enumeration of the *mwc*'s in this context (Theorem 3).

Lemma 4 *$K = GF(q^e)$. Let C be an extended cyclic q-ary code. Let x be a mwc of C. Then $x = \lambda x'$ where $\lambda \in K$ and x' is a mwc of C whose coefficients are in $GF(q)$.*

Proof: Let T be the defining-set of C and let $x = \sum_{g \in G} x_g X^g$, $x_g \in K$. Assume that at least one x_g, denoted x_h, is not in $GF(q)$. And define:

$$x^{(k)} = \sum_{g \in G} x_g^{q^k} X^g \quad , \; k \in [0, e[\; .$$

Since T is invariant under the multiplication by q, we have for all $s \in T$:

$$\phi_s(x^{(k)}) = \sum_{g \in G} x_g^{q^k} g^s = \left(\sum_{g \in G} x_g g^{sq^{-k}} \right)^{q^k} = 0 \quad .$$

Then $x^{(k)}$ is an element of C. Now we get:

$$x' = \sum_{k=0}^{e-1} x^{(k)} = \sum_{g \in G} \sum_{k=0}^{e-1} x_g^{q^k} X^g = \sum_{g \in G} Tr(x_g) X^g \quad ,$$

where $Tr(x_g)$ is the *trace* of x_g over $GF(q)$. Without lost in generality, we can choose x such that $Tr(x_h) \neq 0$. Since x is a *mwc* of C, we have $\omega(x') = \omega(x)$. Thus we obtain an $x' \in C$ such that the coefficients of x' are in $GF(q)$ and the support of x' equals the support of x - i.e. $x' = \lambda x$, $\lambda \in K$ -. □

Theorem 3 [11] *Let* $\nu \in [1, m(q-1)[$, $m(q-1) - \nu = u(q-1) + v$ *with* $v \in [0, q-1[$. *Then the number of the minimum weight codewords of the code* $C_\nu(m,q)$ *is*

$$L_\nu = |K^*| q^u \prod_{i=0}^{m-u-1} \frac{q^{m-i}-1}{q^{m-u-i}-1} N_v \ , \tag{14}$$

where $N_0 = 1$ *and, for* $v > 0$, $N_v = \begin{pmatrix} q \\ v \end{pmatrix}_{\frac{q^{m-u}-1}{q-1}}$.

Theorem 4 *Let* $\nu = b(q-1) + a$, $a \in [0, q-1[$, $b \in [0, m[$. *A minimum weight codeword (mwc) of the code* $C_\nu(m,q)$ *is an element of* $\mathbf{A}$ *of the form:*

$$x = \lambda X^h yz \quad , \quad \lambda \in K^* \ , \ h \in G \ , \ y \in \mathbf{A} \ , \ z \in \mathbf{A} \tag{15}$$

where

- *If* $b = 0$ *then* $y = X^0$ *else* $y \in A_b$.
- *If* $a = 0$ *then* $z = X^0$ *else there is* $g \in G$, $g \notin supp(y)$, *such that* z *is a mwc of the code* $C_a(\{g\}, q)$.

- The set A_b *and the code* $C_a(\{g\}, q)$ *are respectively defined by (13) and (11)-.*

Proof: It is well-known that the minimum distance of the GRM-code $C_\nu(m,q)$ equals $(a+1)q^b$. When $a > 0$ the codeword z can be considered as a *mwc* of an extended RS-code of length q and minimum distance $a+1$; thus $\omega(z) = a+1$. From Lemma 2, z is a *mwc* of $C_a(m,q)$. The weight of an element of A_b, $b > 0$, is clearly q^b; from Lemma 3, y is a *mwc* of $C_{b(q-1)}(m,q)$. If $a > 0$ and $b > 0$, the Theorem 2 implies that the product yz is an element of $C_{b(q-1)+a}(m,q)$. Moreover:

$$q^b(a+1) \ \leq \ \omega(yz) \ \leq \ \omega(y)\omega(z) \ \leq \ q^b(a+1),$$

which means that $\omega(x) = (a+1)q^b$. Then a codeword x which has the form (15) is a *mwc* of $C_\nu(m,q)$. Note that $yz \neq 0$, because the support of yz contains at least two cosets of a b-dimensional subspace of G.

Let R_ν be the number of the x's defined by (15) and let $m(q-1) - \nu = u(q-1) + v$, $v \in [0, q-1[$. We want to prove that $R_\nu = L_\nu$ (L_ν is given by

(14)).
In all cases the support of x is contained in an $(m-u)$-dimensional affine subspace of G. There is

$$\lambda_u = q^u \prod_{i=0}^{m-u-1} \frac{q^{m-i}-1}{q^{m-u-i}-1}$$

such affine subspaces. If $v = 0$, we have $a = 0$ and $R_\nu = \lambda_u |K^*| = L_\nu$. Suppose now that $v \neq 0$ and fixe $g \in G^*$. It is clear that the code $C_a(\{g\}, q)$, as any extended RS-code, satisfies the following property.

Property 1 *For each subset Λ of $GF(q)$ such that $|\Lambda| = a+1$, there is a mwc of $C_a(\{g\}, q)$ the support of which is the set $\{\lambda g | \lambda \in \Lambda\}$.*

There is $\frac{q^{m-u}}{q-1}$ possibilities for the choice of g in an $(m-u)$-dimensional affine subspace of G. Then we have

$$R_\nu = |K^*| \begin{pmatrix} q \\ a+1 \end{pmatrix} \frac{q^{m-u}}{q-1} \lambda_u = L_\nu$$

- since $\lambda_0 = 1$ and $\begin{pmatrix} q \\ a+1 \end{pmatrix} = \begin{pmatrix} q \\ v \end{pmatrix}$-. □

REMARK 4: Suppose that G is considered as a $GF(p)$-space (i.e. $q = p$ or G is identified with $GF(p^{rm})$). In accordance with (7), the form of the elements of A_b is:

$$\prod_{i=1}^{b} (X^{e_i} - 1)^{p-1} \quad , \{e_1, \ldots, e_b\} \text{ are linearly independent in } G \; . \qquad (16)$$

Indeed

$$(X^{e_i} - 1)^{p-1} = \sum_{k=0}^{p-1} \begin{pmatrix} p-1 \\ k \end{pmatrix} (-1)^k X^{(p-1-k)e_i} \quad and \quad \begin{pmatrix} p-1 \\ k \end{pmatrix} = (-1)^k \; .$$

In the algebra $F[F]$, $F = GF(p)$, the only ideals are the principal ideals generated by $(X^\lambda - 1)^k$, $k \in [1, p-1]$, λ being any element in F. Then a basis of a code $C_a(\{g\}, p)$ is

$$\{ \; (X^g - 1)^k \mid k \in [a, p-1] \; \} \quad , \qquad (17)$$

and the codewords can be represented as follows

$$z = \sum_{i=a}^{p-1} z_i (X^g - 1)^i \quad , \quad z_i \in F$$

- for more details the reader can refer to [6] -.

4 The automorphism group of the GRM-codes

We denote by $\Theta = \{\theta_i | i \in [0, r-1]\}$, the Galois group of the field $GF(q)$, $q = p^r$. Since the field $GF(q^m)$, here denoted G, is an F_p-vector-space, each element of Θ can be considered as a linear permutation on G, $\theta_i : g \in G \rightarrow g^{p^i}$, involving a transformation on $\mathbf{A}$ (cf. (2)). We denote by $\overline{G}(m,q)$the set of the permutations on G:

$$\theta(M,h,i) \ : \ g \in G \ \longmapsto \ (Mg)^{p^i} + h \ , \ h \in G \ , \ i \in [0, r-1] \ , \qquad (18)$$

where M is a non singular matrix of order m over $GF(q)$. The group $\overline{G}(m,q)$ is usually called *the group of the semi-affine bijections on* G (denoted $GSA_F(E)$, $F = GF(q)$ and $E = G$, in the Appendix). The group $\overline{G}(m,q)$ contains $G(m,q)$ (cf. (1)); if $q = p$, Θ contains only the identity and we have clearly $\overline{G}(m,q) = G(m,q)$.

Let C be an extended cyclic q-ary code in $\mathbf{A}$, with defining-set T. Then θ_i is contained in $Aut(C)$ *if and only if* T *is invariant under the multiplication by* p^i *modulo* $q^m - 1$. Indeed we have, for any $x \in C$ and any $s \in T$:

$$\phi_s(\theta_i(x)) = \phi_s(\sum_{g \in G} x_g X^{g^{p^i}}) = \sum_{g \in G} x_g (g^{p^i})^s = \phi_{sp^i}(x) \ ,$$

where ϕ_s is defined by (3) and C by (4). In particular, we shall show that, in general, a q-ary RM-code cannot be invariant under θ_i, $i \neq 0$.

Lemma 5 $q = p^r$, $r > 1$, $\nu \in [2, m(q-1)-1]$. *Then, for all* $i \in [1, r-1]$, *the set* $I_\nu(m,q)$ *is not invariant under the multiplication by* p^i *modulo* $q^m - 1$. *In other words, the set* $\Theta \cap Aut(C_\nu(m,q))$ *is reduced to the identity.*

Proof: The dual of the code $C_\nu(m,q)$ is $C_\mu(m,q)$, $\mu = m(q-1)-\nu+1$. Two dual codes have the same automorphism group. So we can prove the Lemma only for $\nu < \frac{m(q-1)+1}{2}$. We state the property:

H_ν : For each i, $i \in [1, \lfloor r/2 \rfloor]$, there is $s \in I_\nu(m,q)$ such that $p^i s \notin I_\nu(m,q)$ - where $\lfloor r/2 \rfloor$ denotes the integer part of $r/2$ -.

Assume that H_ν is true. Suppose that there is a j, $j \in]\lfloor r/2 \rfloor, r-1]$, such that $I_\nu(m,q)$ is invariant under the multiplication by p^j. Let $i = r-j$; thus $p^r = q = p^i p^j$, with $i \in [1, \lfloor r/2 \rfloor]$. Since $I_\nu(m,q)$ is invariant under the multiplication by q, the hypothesis on j contradicts H_ν. That means: if H_ν is true then the Lemma is proved for ν. So we shall prove the Lemma in proving H_ν, by induction on ν, $\nu < \frac{m(q-1)+1}{2}$. Recall that $I_\nu(m,q)$ is the set of the $s \in S$ such that $\omega_q(s) < \nu$. If $\nu = 2$, we have clearly $1 \in I_2(m,q)$ while $p^i \notin I_2(m,q)$; indeed the q-weight of p^i equals p^i. Then H_2 is true. We suppose now that $H_{\nu'}$ is true for all $\nu' \in [2, \nu[$ and we want to prove H_ν.
Let $i \in [1, \lfloor r/2 \rfloor]$. Since $H_{\nu-1}$ is true, we know that there is $s \in I_{\nu-1}(m,q)$ such that $p^i s \notin I_{\nu-1}(m,q)$. If $\omega_q(p^i s) > \nu - 1$ then $p^i s \notin I_\nu(m,q)$ and H_ν is true. So it remains the case $\omega_q(p^i s) = \nu - 1$. For $\lambda \in [0, q-1]$, let us define:

$$[\lambda p^i] = \begin{cases} \lambda p^i \quad \text{modulo } q-1 & \text{if } \lambda < q-1 \\ q-1 & \text{if } \lambda = q-1 \ . \end{cases}$$

If $\sum_{l=0}^{m-1} s_l q^l$ is the q-ary expansion of s, we have [10]:

$$\omega_q(p^i s) = \sum_{l=0}^{m-1} [s_l p^i] \ . \tag{19}$$

Now we get:

$$t = s + q^k \ \ with \ \ k \in [0, m-1] \ \ such \ that \ \ [p^i s_k] + p^i < q \ .$$

Note that this property implies: $[p^i(s_k+1)] = [p^i s_k] + p^i$.
This choice of k is always possible. Indeed

$$[p^i s_k] \geq q - p^i \ , \ \forall k \ \longrightarrow \ \omega_q(p^i s) \geq m(q-p^i) \ \ , \ from \ (19) \ ;$$

but $\omega_q(p^i s) = \nu - 1$ and $\nu - 1 < \frac{m(q-1)}{2}$. Thus

$$m(q-p^i) < \frac{m(q-1)}{2} \ \longrightarrow \ 2p^i - q - 1 > 0 \ ,$$

which contradicts $i < \lfloor r/2 \rfloor$.
Then we have:

$$\omega_q(t) = \sum_{l \neq k} s_l + (s_k + 1) = \omega_q(s) + 1 < \nu \ ,$$

Thus $t \in I_\nu(m,q)$. Moreover:

$$\omega_q(p^i t) = \sum_{l \neq k} [p^i s_l] + ([p^i s_k] + p^i) = \omega_q(p^i s) + p^i \ \ ,$$

which proves that $p^i t \notin I_\nu(m,q)$. Therefore H_ν is true. □

The automorphism group of the GRM-codes is known in the following cases:

- for $q = 2$, $Aut(C_\nu(m,2)) = G(m,2)$;
- if $m = 1$, $C_\nu(1,q)$ is an extended RS-code and its automorphism group is $G(1,q)$;
- if $\nu = 1$ or $\nu = m(q-1)$, each permutation on G is an automorphism of $C_\nu(m,q)$.

So we suppose now that: $q > 2$, $m > 1$ and $\nu \in [2, m(q-1)-1]$. Recall that Theorem 1 implies that in all cases the automorphism group of $C_\nu(m,q)$ contains $G(m,q)$.

Theorem 5 $\nu \in [2, m(q-1)-1]$. *The automorphism group of the q-ary RM-code of order $m(q-1)-\nu$ is $G(m,q)$ - i.e. $Aut(C_\nu(m,q)) = G(m,q)$.*

Proof: Let $\sigma \in Aut(C_\nu(m,q))$. We denote by Mw_ν the set of the *mwc*'s of $C_\nu(m,q)$. According to (2), σ can be considered as a permutation on G; so, for simplification, we shall apply σ on $\mathbf{A}$ or on G. It is clear that, by definition, $\sigma(Mw_\nu) = Mw_\nu$. We shall prove the Theorem in explaining the action of σ on the elements of Mw_ν. We distinguish four cases:

1. $\nu = b(q-1)$, $b \in [1, m-1]$. From Theorem 4, we have:

$$Mw_\nu = \left\{ \lambda X^h \sum_{g \in L} X^g | \lambda \in K^*,\ h \in G,\ L \textit{ is a } b-\textit{dim. subspace of } G \right\}.$$

That means that σ transforms any b-dimensional affine subspace of G in another. From Corollary 4 and (24) (see in the Appendix), that yields $\sigma \in \overline{G}(m,q)$. Applying Lemma 5, we obtain $\sigma \in G(m,q)$.

2. $\nu = b(q-1)+a$, $b \in [0, m-1[$, $a \in [2, q-1[$. Let $V = h + L$ be any $(b+1)$-dimensional affine subspace of G, where h is any element of G and L is any $(b+1)$-dimensional subspace of G. Let $\{e_1, \ldots, e_{b+1}\}$ be a basis of L; let L' be the b-dimensional subspace of G generated by $\{e_2, \ldots, e_{b+1}\}$. From Theorem 4 the following codewords are elements of Mw_ν:

$$x = yz \ , \ y = X^h \sum_{g \in L'} X^g \ , \ z \in C_a(\{e_1\}, q) \ and \ \omega(z) = a+1 \ , \qquad (20)$$

where $C_a(\{e_1\}, q)$ is defined by (11) - by convention, if $b = 0$ then $y = X^h$ and $L' = \emptyset$-.
It is clear that the support of x is contained in V. Now the code $C_a(\{e_1\}, q)$, which is in fact an extended RS-code of minimum distance $a+1$, satisfies the Property 1 (see in the proof of Theorem 4). Since $a > 1$, the minimum distance of $C_a(\{e_1\}, q)$ is at least 3. So we can define two distinct mwc's of $C_a(\{e_1\}, q)$, let z and z', satisfying:

$$| \ supp(z) \cap supp(z') \ | \ \geq \ 2 \qquad (21)$$

Let y defined by (20) and:

$$x = yz \ \ and \ \ x' = yz' \quad , \quad U = supp(x) \ \ and \ \ U' = supp(x') \ .$$

By definition, a mwc of $C_\nu(m,q)$ has its support contained in only one $(b+1)$-dimensional affine subspace of G. Since $\sigma(x) \in Mw_\nu$ and $\sigma(x') \in Mw_\nu$, we have two $(b+1)$-dimensional affine subspaces of G, let W and W', containing respectively $supp(\sigma(x))$ and $supp(\sigma(x'))$. But $\sigma(U \cap U') = \sigma(U) \cap \sigma(U')$; moreover (20) and (21) yield

$$| \ \sigma(U \cap U') \ | \ \geq \ 2q^b \ .$$

We then obtain:

$$2q^b \leq | \ \sigma(U) \cap \sigma(U') \ | \leq | \ W \cap W' \ | \leq q^{b+1}$$

Since $W \cap W'$ is an affine subspace of G, we can conclude that $W = W'$.

Applying the Property 1, we can construct a sequence,

$$x_0, \ldots, x_k, \ldots, x_\zeta \quad , \quad x_k = yz_k \ ,$$

such that

- z_k is a *mwc* of $C_a(\{e_1\}, q)$
- for each $k > 0$, z_{k-1} and z_k satisfy (21)
- $\bigcup_{k=0}^{\zeta} supp(x_k) = V$.

Let $U_k = supp(x_k)$ and let W_k be the $(b+1)$-dimensional affine subspace of G containing $\sigma(U_k)$. Applying the preceding result to x_{k-1} and x_k, for each $k > 0$, we obtain:

$$W_0 = W_1 = \ldots = W_\zeta.$$

Moreover any element of V is containing in an U_k. Then $\sigma(V)$ equals W_0. We have proved that σ transforms any $(b+1)$-dimensional affine subspace of G in a $(b+1)$-dimensional affine subspace of G. From Corollary 4, $\sigma \in \overline{G}(m,q)$; Therefore from Lemma 5, $\sigma \in G(m,q)$.

3. $\nu = b(q-1)+1$, $b \in [1, m-1]$. The dual of $C_\nu(m,q)$ is $C_\mu(m,q)$, with

$$\mu = m(q-1) - \nu + 1 = (m-b)(q-1) \ .$$

Then, from **1.**, $Aut(C_\nu(m,q)) = Aut(C_\mu(m,q)) = G(m,q)$.

4. $\nu = (m-1)(q-1)+a$, $a \in [2, q-1[$. The dual of $C_\nu(m,q)$ is $C_\mu(m,q)$, with

$$\mu = m(q-1) - \nu + 1 = q - a \ \ where \ \ q - a \in [2, q-2] \ .$$

Then, from **2.**, $Aut(C_\nu(m,q)) = Aut(C_\mu(m,q)) = G(m,q)$. □

In the parts **1.** and **2.** of the proof of Theorem 5, we prove in fact that a permutation σ on G, which preserves Mw_ν, is an element of the group $\overline{G}(m,q)$. Then we have immediatly:

Corollary 1 *$m > 1$ and $q > p$. Let $\nu \in [2, (m-1)(q-1)]$, $\nu = b(q-1)+a$ with $a = 0$ or $a \in [2, q-1[$. Let C be an extended cyclic q-ary code such that the set of the mwc's of C equals Mw_ν. Then $Aut(C) \subset \overline{G}(m,q)$.*

If $q = p$ it is well-known that a GRM-code is generated by the set of its *mwc*'s; recall that the p-ary RM-codes are the powers P^ν of the radical P of the algebra **A** (see Remarks 3 and 4). Then, in this case, Theorem 5 involves a property which is available for all ν:

Corollary 2 *$q = p$. Let $\nu \in [2, m(p-1)-1]$. Let C be an extended cyclic p-ary code such that the set of the mwc's of C equals the set of the mwc's of P^ν. Then $Aut(C) \subset G(m,p)$.*

We suppose now that $q = p^r$, $r > 1$, and we denote by M_ν the *minimum weight subcode* of $C_\nu(m,q)$; the defining-set of M_ν is given by DELSARTE in [10]; that is, for $\nu = b(q-1)+a$, $a \in [0, q-1[$:

$$J_\nu = \bigcap_{c \in [a, q-1[} \{\, s \in S \mid \exists i,\ i \in [0, r[\ such\ that\ \omega_q(p^i s) < b(q-1) + [p^i c] \,\} \quad (22)$$

- where $S = [0, q^m - 1]$ -. Clearly M_ν is invariant under $G(m,q)$; moreover if ν satisfies the hypotheses of Corollary 1, *the automorphism group of M_ν is contained in $\overline{G}(m,q)$.*
Suppose that $a = 0$. Then it becomes from (22) that

$$J_{b(q-1)} = \{\, s \in S \mid \exists i,\ i \in [0, r[\ such\ that\ \omega_q(p^i s) < b(q-1) \,\} = \bigcup_{i \in [0,r[} p^i I_\nu(m,q)\,.$$

Hence $J_{b(q-1)}$ is invariant under the multiplication by p^j modulo $q^m - 1$, for all $j \in [1, r[$. Then, from Corollary 1 and (18):

Corollary 3 *The automorphism group of the minimum weight subcode of $C_{b(q-1)}(m,q)$, $b \in [1, m[$, is $\overline{G}(m,q)$.*

REMARK 5: Let $\nu = b(q-1)+a$, $a \in [1, q-1[$ and $b \in [1, m[$. The Corollary 1 can be applied to the code $U = C_a(m,q)C_{b(q-1)}(m,q)$. Indeed this code is generated by the products xy, $x \in C_a(m,q)$ and $y \in C_{b(q-1)}(m,q)$. From Theorem 2 and Theorem 4, the set of the *mwc*'s of U is exactly the set of the *mwc*'s of $C_\nu(m,q)$. Thus if ν satisfies the hypotheses of Corollary 1, the automorphism group of U is contained in $\overline{G}(m,q)$.

APPENDIX

The reader can find in [1] a proof of the Theorem 6, namely *the fundamental Theorem of the affine geometry.* We only shall explain this theorem for finite fields. The permutations on the field $GF(q^m)$, which conserve the affine subspaces of same dimension, are characterized by Corollary 4. The formula (24) means that the group composed with these permutations is exactly the group $\overline{G}(m,q)$ defined by (18).

We denote by E a vector-space over a field F.

Definition 2 *An application* $f : E \longrightarrow E$ *is semi-linear if there is an automorphism* τ *of the field* F *such that:*

1. $f(x+y) = f(x) + f(y)$, $x \in E$ *and* $y \in E$.
2. $f(\lambda x) = \tau(\lambda) f(x)$, $x \in E$ *and* $\lambda \in F$.

Definition 3 *An application* $f' : E \longrightarrow E$ *is semi-affine if there is* $a \in E$ *and* $f : E \longrightarrow E$ *semi-linear such that:*

$$f'(x) = f(x) + a \quad , \quad x \in E \quad .$$

The *group of the semi-linear bijections* is denoted by $GSL_F(E)$; The *group of the semi-affine bijections* is denoted by $GSA_F(E)$.

Theorem 6 [1] *Suppose that the dimension of* E *is strictly greater than* 1 *and that* F *is not the finite field of order* 2. *Let* $f : E \longrightarrow E$ *be a bijection satisfying: if* a, b *and* c *are collinear in* E, *then* $f(a)$, $f(b)$ *and* $f(c)$ *are collinear in* E.
Then f *is an element of* $GSA_F(E)$.

From now on , assume that F is the finite field $GF(q)$, $q > 2$, and that E is the finite field $GF(q^m)$, $m > 1$, considered as an F-vector-space.

Corollary 4 *Let* $s \in [1, m-1]$ *and* $f : E \longrightarrow E$ *be a bijection which transforms any* s*-dimensional affine subspace in an* s*-dimensional affine subspace. Then* f *is an element of* $GSA_F(E)$.

Proof: If $s = 1$, the Theorem 6 implies $f \in GSA_K(E)$. Suppose that $s > 1$. Each 1-dimensional affine subspace L has q elements and can be considered as an intersection of some s-dimensional affine subspaces. By hypothesis $f(L)$

has q elements and is an intersection of some s-dimensional affine subspaces. Then we can apply the Theorem 6. □

When F is the finite field $GF(q)$, with $q = p^r$ (p is a prime and $r \geq 0$), the group of the automorphisms of the field F is

$$\Theta = \{ \theta_i : F \longrightarrow F \mid \theta_i(g) = g^{p^i},\ i \in [0, r-1] \} .$$

Since E is a field of characteristic p, each θ_i is an automorphism of the field E; thus for any $h : E \longrightarrow E$, h being a linear bijection, the application $\theta_i \circ h$ is an element of $GSL_F(E)$.
Conversely let $f \in GSL_F(E)$, associated with the automorphism θ_i. By definition, it is clear that the application $\theta_{-i} \circ f$ is linear; hence $f = \theta_i \circ h$, h linear and bijective. Then we can state:

$$GSL_F(E) = \{ \theta_i \circ h \mid \theta_i \in \Theta,\ h \textit{ linear and bijective} \} , \qquad (23)$$

and deduce

$$GSA_F(E) = \{ \theta_i \circ h + b \mid \theta_i \in \Theta,\ h \textit{ linear bijective},\ b \in E \} . \qquad (24)$$

Then $GSA_F(E)$ is the group $\overline{G}(m, q)$ defined by (18) in Section 4.

References

[1] M. BERGER *Géométrie*, Tome 1, CEDIC, F. NATHAN,1977.

[2] T. BERGER *A direct proof for the automorphism group of the extended Reed-Solomon codes*, preprint.

[3] T. BERGER *Sur le groupe d'automorphismes des codes cycliques étendus primitifs affine-invariants*, Thèse de l'Université de Limoges, in preparation.

[4] S.D. BERMAN *On the theory of group codes*, KIBERNETICA, Vol. 1, n. 1, p. 31-39, 1967.

[5] P. CHARPIN *Puissances du radical d'une algèbre modulaire et codes cycliques*, Revue du CETHEDEC, 18ième année, NS81-2, pp. 35-43.

[6] P. CHARPIN *Codes idéaux de certaines algèbres modulaires*, Thèse de 3ième cycle, Université Paris 7, 1982.

[7] P. CHARPIN *The extended Reed-Solomon codes considered as ideals of a modular algebra*, Annals of Discrete Mathematics, 17 (1983) 171-176.

[8] P. CHARPIN *Codes cycliques étendus invariants sous le groupe affine*, Thèse d'Etat, Université Paris 7, LITP 87-6.

[9] P. CHARPIN *Une généralisation de la construction de* BERMAN *des codes de Reed et Muller p-aires*, Communications in Algebra, 16(11), 2231-2246 (1988).

[10] P. DELSARTE *On cyclic codes that are invariant under the general linear group*, IEEE Trans. on Info. Theory, vol. IT-16, n.6, 1970.

[11] P. DELSARTE, J.M. GOETHALS & F.J. MACWILLIAMS *On generalized Reed-Muller codes and their relatives*, Info. and Control, 16 (1974) 403-442.

[12] A. DÜR *The automorphism groups of Reed-Solomon codes*, J. of Combinatorial Theory, Series A, Vol. 44, n.1 (1987).

[13] T. KASAMI, S. LIN & W.W. PETERSON *Some results on cyclic codes which are invariant under the affine group and their applications*, Info. and Control, vol. 11, p. 475-496 (1967).

[14] T. KASAMI, S. LIN & W.W. PETERSON *Polynomial codes*, IEEE Trans. on Info. Theory, IT-14, 1968, pp. 807-814.

[15] T. KASAMI, S. LIN & W.W. PETERSON *New generalisations of the Reed-Muller codes*, IEEE Trans. on Info. Theory, vol. IT-14, pp. 189-199 (1968) .

[16] F.J. MACWILLIAMS & N.J.A. SLOANE *The theory of Error Correcting Codes*, North-Holland 1986.

[17] A. POLI *Codes stables sous le groupe des automorphismes isométriques de* $A = F_p[X_1, \ldots, X_n]/(X_1^p - 1, \ldots, X_n^{p-1})$, C. R. Acad. Sci. Paris, t. 290 (1980) .

Imprimé en France
par
.l'Institut National de Recherche en Informatique et en Automatique.

ISSN 0249-6399