The Permutation Group of Affine-Invariant Extended Cyclic Codes

Thierry P. Berger and Pascale Charpin

Abstract— **The extended cyclic codes of length p^m, p a prime, which are invariant under the affine-group acting on $\mathbb{F}_{p^m}$, are called affine-invariant codes. Following recent results of Berger, we present the formal expression of the permutation group of these codes. Afterwards we give several tools in order to determine effectively the group of a given code or of some infinite class of codes. We next prove, by studying some examples, that our tools are efficient. In the end, we give our main application, the permutation group of primitive BCH codes defined on any prime field.**

Index Terms—**Automorphism group, permutation group, cyclic code, affine-invariant code, BCH code, poset, antichain.**

NOMENCLATURE

- $\boldsymbol{k}$ is the alphabet field $\mathbb{F}_q$, $q = p^r$, p a prime.
- $n = q^{m'} - 1$, $N = q^{m'}$, $m = rm'$, $S = [0, p^m - 1]$.
- $\omega_q(s)$ is the q-weight of $s \in [0, n]$ (see Definition 3).
- G is the field $\mathbb{F}_{q^{m'}}$, generally identified with $\mathbb{F}_{p^m}$.
- $G^* = G\backslash\{0\}$; it is the multiplicative group of the field G.
- α is a primitive element of the field G.
- $\boldsymbol{R}$ is the quotient algebra $\boldsymbol{k}[X]/(X^n - 1)$.
- $\boldsymbol{M}$ is the group algebra $\boldsymbol{k}[\{G^*, \times\}]$.
- $\boldsymbol{A}$ is the group algebra $\boldsymbol{k}[\{G, +\}]$..
- If C is a cyclic code, its extension is denoted by $\widehat{C}$.
- $\mathrm{Sym}\,(p^m)$ is the symmetric group acting on G.
- $\mathrm{Alt}\,(p^m)$ is the alternating group acting on G.
- $\mathrm{Per}\,(D)$ is the permutation group of the code D.
- $\mathrm{Aut}\,(D)$ is the automorphism group of the code D.
- K is a subfield of G of order p^e.
- $\mathrm{GL}\,(m/e, p^e)$ is the linear group of G on K.
- $\mathrm{AGL}\,(m/e, p^e)$ is the affine group.
- $\Gamma\mathrm{L}\,(m/e, p^e)$ is the semi-linear group.
- $\mathrm{A}\Gamma\mathrm{L}(m/e, p^e)$ is the semi-affine group.
- θ_k is the kth power of the Frobenius mapping on G.
- $(S, \prec)$ is a poset (see Definition 7).
- $(S, \ll_e)$, e dividing m, is a poset (see Theorem 4).
- $\mathrm{cl}\,(j)$, $j \in S$, is the orbit of j under the multiplication by p modulo n.

Manuscript received July 10, 1995; revised April 16, 1996. The material in this paper was presented at the Meeting of the American Mathematical Society, Chicago, IL, March 1995.

T. P. Berger is with UFR des Sciences de Limoges, 87060 Limoges Cedex, France.

P. Charpin is with INRIA, Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le Chesnay Cedex, France.

Publisher Item Identifier S 0018-9448(96)06886-1.

I. INTRODUCTION

IN this paper we consider only primitive cyclic codes—i.e., cyclic codes of length $p^m - 1$ over a field of order p^r, where p is a prime and r a divisor of m. We will say that such a code C is a p^k-ary code, whenever k is the smallest integer such that C is invariant under θ_k, the kth power of the Frobenius mapping. The Bose–Chaudhuri–Hocquenghem (BCH) codes will always be narrow-sense BCH codes. The extended code is usually defined by adding an overall parity check. Henceforth the field of order p^m, denoted by G, will be the support of the extended codes, while G^*, its multiplicative group, will be the support of the cyclic codes. The permutations of coordinate places which send a code C into itself form the *permutation group* of C. Since a permutation acts on the support of C, it will be seen as a permutation on G. When the code is binary, this permutation group is actually the *automorphism group* of C (see [28, ch. 8]). References on coding theory can be found in [28].

Denote by $\mathrm{AGL}\,(m, p)$ the affine group of G viewed as a vector space over its prime field $\mathbb{F}_p$, and by $\mathrm{AGL}\,(1, p^m)$ the affine group of G—which we view as a subgroup of $\mathrm{AGL}\,(m, p)$. Primitive cyclic codes whose extension is invariant under $\mathrm{AGL}\,(1, p^m)$ were characterized about thirty years ago by Kasami *et al.* ([22], 1967). They form a class including codes of great interest such as BCH codes, generalized Reed–Muller (GRM) codes or Reed–Solomon (RS) codes. Delsarte later proved more general results, giving a condition for a code to be invariant under a subgroup of $\mathrm{AGL}\,(m, p)$. He proved that only p-ary Reed–Muller codes can be invariant under $\mathrm{AGL}\,(m, p)$ ([17], 1970), but the problem of the complete determination of the automorphism group of affine-invariant codes has remained unsolved.

The study of the automorphism groups of RS codes and of their extensions is due to Dür ([19], 1987). We gave the full automorphism groups of GRM codes in [5] (1993). More recently, Berger has proved that the permutation group of any affine-invariant code is contained in $\mathrm{AGL}\,(m, p)$ [7], [8]. We show here that one can construct a formal expression for the permutation group of any affine-invariant code. This result provides the complete determination of the permutation groups for a large class of codes. In the general case, it provides only an algorithm that is not always immediately practical.

The main part of the paper consists of the description of several tools designed for the determination of permutation groups. On one hand, we want to give algorithms such that, up to reasonable lengths, computation of the group becomes

easy. On the other hand, our aim is to obtain the permutation groups of infinite classes of codes.

The paper is organized as follows. In Section II, we present and explain all definitions and properties we need for the study of the permutation groups of affine-invariant codes. The cyclic codes are viewed in the group algebra of the multiplicative group G^*, while the extended codes are viewed in the field algebra of G. Then the structure of the support of codes is clearly defined and the permutations on it appear as elements of the symmetric group of G. There is a general definition of permutations of cyclic codes: the polynomial approach (see Theorem 1). We introduce Example 1 to show that it seems difficult to apply this approach directly.

We then present the affine-invariant codes. These codes are those invariant under $\mathrm{AGL}(1, p^m)$, but they can be invariant under a larger subgroup of $\mathrm{AGL}(m, p)$. This result is due to Delsarte [17]. The next part is based on his work which remains crucial to our paper. We present the work of Kasami and its generalization by Delsarte in term of partial orders, studying extensively their combinatorial properties. We briefly present background material describing affine-invariant codes by antichains. At the end of Section II, we explain the recent results of Berger, giving precisely their consequences. We also present the formal description of the permutation group of an affine-invariant code (Theorem 5).

It is important to notice that our formal expression sheds new light on the result of Delsarte. Actually, his result is completed as follows: *the permutation group of a given affine-invariant code can be fully characterized from combinatorial properties of its defining set.* Section III consists of the description of several tools devoted to the effective determination of permutation groups. We mainly give two methods and both are based on the combinatorial structure of the defining set.

The first one is derived from the work of Delsarte, by using the classification of affine-invariant codes by antichains. We show in fact that the permutation group of a given code can be described through relations between only two antichains. The second method comes from the polynomial representation of permutations given by Theorem 1. It is a new condition equivalent to those of Delsarte, although we obtain it independently. This condition is very powerful in proving a property related to the BCH bound (see Corollary 5). We give many examples in order to explain these methods in detail and to establish their efficiency. Many affine-invariant codes have as permutation group the smallest group $\mathrm{AGL}(1, p^m)$ (or $A\Gamma L(1, p^m)$ for the p-ary codes); this is generally the case for BCH codes. However, there are a number of exceptions and we want to show that also by well-chosen examples. We exhibit infinite classes of such codes in Section III-C. In the last section, we determine the permutation group of any BCH code defined over a prime field.

II. Preliminaries

In this paper codes are linear and primitive. Cyclic codes are of length $n = q^{m'} - 1$ and have symbols from the finite field of order q, $q = p^r$, denoted by $\boldsymbol{k}$. The finite field of order $q^{m'}$, denoted by G, will generally be identified with $\mathbb{F}_{p^m}$. We will denote a primitive root of G by α. Using standard terminology of coding theory, a cyclic code is an ideal C in the ring $\boldsymbol{R} = \boldsymbol{k}[X]/(X^n - 1)$, generated by a polynomial $g(X)$ which is the product of minimal polynomials of some α^i. The roots of $g(X)$ are said to be the *zeros* of the cyclic code C [28, ch. 7]. Let T be the subset of the interval $[0, n-1]$ composed of those s such that α^s is a zero of C. Then we have

$$C = \{a(X) \in \boldsymbol{R} | a(\alpha^s) = 0, \forall s \in T\}. \tag{1}$$

We will say that T is the *defining set* of C. The code C is said to be *trivial* when either T is $\{0\}$ or T is the set $\{0, \cdots, n-1\}$. In this paper we will use another representation of cyclic codes and of their extension. We explain that now.

A. Primitive Cyclic Codes and their Extension

We denote by $\boldsymbol{M}$ the group algebra $\boldsymbol{k}[\{G^*, \times\}]$. That is the group algebra of the multiplicative group G^* of the field G, over the field $\boldsymbol{k}$. An element of $\boldsymbol{M}$ is a formal sum

$$\mathrm{x} = \sum_{g \in G^*} x_g(g), \quad x_g \in \boldsymbol{k}.$$

Addition and scalar multiplication are component-wise and the multiplication is given by the multiplication in G^*

$$\sum_{g \in G^*} x_g(g) + \sum_{g \in G^*} y_g(g) = \sum_{g \in G^*} (x_g + y_g)(g)$$

and

$$\sum_{g \in G^*} x_g(g) \times \sum_{g \in G^*} y_g(g) = \sum_{g \in G^*} \left(\sum_{hk = g} x_h y_k \right)(g).$$

It is obvious that the following map is an automorphism between the algebras $\boldsymbol{R}$ and $\boldsymbol{M}$

$$\psi : \sum_{i=0}^{n-1} \lambda_i X^i \in \boldsymbol{R} \longmapsto \sum_{i=0}^{n-1} \lambda_i (\alpha^i) = \sum_{g \in G^*} x_g(g).$$

Consider the following $\boldsymbol{k}$-linear map of $\boldsymbol{M}$ into G:

$$\rho_s \left(\sum_{g \in G^*} x_g(g) \right) = \sum_{g \in G^*} x_g g^s \tag{2}$$

where $0 \leq s < n$. Note that $\rho_s(\mathrm{x}) = a(\alpha^s)$, for any x in $\boldsymbol{M}$ corresponding to $\psi(a(X))$ (see (1)).

Definition 1: Let $\boldsymbol{M} = \boldsymbol{k}[\{G^*, \times\}]$, $\boldsymbol{k} = \mathbb{F}_q$ and $G = \mathbb{F}_{q^{m'}}$. Let T be a subset of $[0, n-1]$, invariant under the multiplication by q (mod n). The cyclic code of length n over $\boldsymbol{k}$, with defining set T, is as follows:

$$C = \{\mathrm{x} \in \boldsymbol{M} \mid \rho_s(\mathrm{x}) = 0, \forall s \in T\}.$$

The code C is said to be a cyclic code in $\boldsymbol{M}$. We will say that C is a p^ℓ-ary code, $\ell \leq r$, where ℓ is the least integer such that T is invariant under multiplication by p^ℓ.[1] Generally C will be a q-ary code.

[1] There is another definition that appears in the literature: a code is p^ℓ-ary provided its definition set is invariant under multiplication by p^ℓ.

Whenever T does not contain 0, we *extend the code C by an overall parity check.* We denote by $\widehat{C}$ the *extended code* of C and define it in the group algebra $\boldsymbol{A} = \boldsymbol{k}[\{G, +\}]$. This algebra is the group algebra of the additive group of G over $\boldsymbol{k}$. An element of $\boldsymbol{A}$ is a formal sum

$$\mathrm{x} = \sum_{g \in G} x_g X^g, x_g \in \boldsymbol{k}.$$

The operations are

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

and

$$\sum_{g \in G} x_g X^g \times \sum_{g \in G} y_g X^g = \sum_{g \in G} \left(\sum_{h+k=g} x_h y_k \right) X^g.$$

As previously (for the algebra $\boldsymbol{M}$), we consider the $\boldsymbol{k}$-linear map of $\boldsymbol{A}$ into G

$$\phi_s \left(\sum_{g \in G} x_g X^g \right) = \sum_{g \in G} x_g g^s \tag{3}$$

where $0 \leq s \leq n$ and $0^0 = 1$. Note that

$$\phi_s \left(\sum_{g \in G} x_g X^g \right) = \rho_s \left(\sum_{g \in G^*} x_g (g) \right)$$

unless $s = 0$ or $s = n$.

Definition 2: Let $\boldsymbol{A} = \boldsymbol{k}[\{G, +\}]$, $\boldsymbol{k} = \mathbb{F}_q$, and $G = \mathbb{F}_{q^{m'}}$. Let T be a subset of $[0, n]$, containing 0 and invariant under multiplication by q (mod n)—by convention $q.n \bmod n \equiv n$. The extended cyclic code $\widehat{C}$ with defining set T is defined as follows:

$$\widehat{C} = \{\mathrm{x} \in \boldsymbol{A} \mid \phi_s(\mathrm{x}) = 0, \ \forall s \in T\}.$$

The code $\widehat{C}$ is said to be an extended cyclic code in $\boldsymbol{A}$. We say that $\widehat{C}$ is a p^ℓ-ary extended cyclic code when C is a p^ℓ-ary cyclic code.

We now recall the definition of two classes of codes of $\boldsymbol{A}$ which will often appear in our study—that is, the Generalized Reed–Muller (GRM) codes and the extended Bose–Chaudhury–Hocquenghem (BCH) codes.

Definition 3: Let $s \in [0, n]$. The q-weight of s is

$$\omega_q(s) = \sum_{i=0}^{m'-1} s_i$$

where

$$\sum_{i=0}^{m'-1} s_i q^i$$

is the q-ary expansion of s. Let $\nu \in [1, m'(q-1)[$ and $\mu = m'(q-1) - \nu$.

The GRM code of length $q^{m'}$ over $\boldsymbol{k}$ and of order ν is the extended cyclic code in $\boldsymbol{A}$ with defining set

$$T_\nu = \{s \in [0, n] | \omega_q(s) < \mu\}.$$

Note that binary GRM codes are usually called RM codes. More generally, a GRM code defined on a prime field of order p is called a p-ary RM code.

The extended BCH code of length $q^{m'}$ over $\boldsymbol{k}$ and of designed distance d is the extended cyclic code in $\boldsymbol{A}$ with defining set

$$\bigcup_{s \in [0, d-1]} \{s, qs, ..., q^{m'-1} s\}$$

where d is the smallest element of its cyclotomic coset (of q modulo n) and the multiplication is calculated modulo n. When $m' = 1$, the definitions of GRM and BCH codes are equivalent, defining the extended Reed–Solomon (RS) codes of length q over $\boldsymbol{k}$.

B. Permutation Groups

Let us denote by θ_k the kth power of the Frobenius mapping on G—i.e., the map $g \longmapsto g^{p^k}$. Recall that codes have symbols from $\boldsymbol{k}$, a finite field of order $q = p^r$, r dividing m. Therefore, they are invariant under θ_r. From now on the field G of order $q^{m'}$ will be always identified with the field $\mathbb{F}_{p^m}$, where $m = rm'$. Let K be the subfield of G of order p^e. In this subsection, we give the definitions of the permutation groups which will appear in the paper. We also recall and explain general results mainly due to Kasami *et al.* and Delsarte. At the end we present the recent results of Berger [7], [8].

1) Definitions: We denote by $\mathrm{Sym}\,(p^m)$ the symmetric group acting on G; it is the set of permutations of the field G. Let $\sigma \in \mathrm{Sym}\,(p^m)$. Then σ acts as follows on the elements of $\boldsymbol{A}$

$$\sigma : \sum_{g \in G} x_g X^g \longmapsto \sum_{g \in G} x_g X^{\sigma(g)}. \tag{4}$$

Whenever $\sigma(0) = 0$, the permutation acts on G^* and then on codewords of $\boldsymbol{M}$.

$$\sigma : \sum_{g \in G^*} x_g (g) \longmapsto \sum_{g \in G^*} x_g (\sigma(g)). \tag{5}$$

Definition 4: Let C be a code of $\boldsymbol{M}$ and let $\widehat{C}$ its extension in $\boldsymbol{A}$. A permutation of C is an element of $\mathrm{Sym}\,(p^m)$ which leave 0 invariant and sends C into itself. A permutation of $\widehat{C}$ is an element of $\mathrm{Sym}\,(p^m)$ which send $\widehat{C}$ into itself.

The permutations group of a given code is the set of its permutations. For binary codes this group equals the automorphism group of the code (see the classical definition in [28, p. 238]).

We denote by $\mathrm{Per}\,(C)$ (resp., by $\mathrm{Per}\,(\widehat{C})$) the permutation group of C (resp., of $\widehat{C}$).

Remark 1: Clearly *the permutation group of C is the subgroup of the permutation group of $\widehat{C}$ which leaves zero invariant.* Indeed, the coefficient x_0 is the parity-check symbol

$$x_0 + \sum_{g \in G^*} x_g = 0.$$

Any permutation of G^* leaves the position "0" invariant.

It is well known that each element σ of $\mathrm{Sym}(p^m)$ admits a unique polynomial representation; that is,

$$f_\sigma(X) = \sum_{g \in G} \sigma(g)\left(1 - (X-g)^{p^m-1}\right), \quad f_\sigma(X) \in G[X] \tag{6}$$

which is computed modulo $X^{p^m} - X$ (see [25, ch. 7]). We say that f_σ is the *associated polynomial* of σ; f_σ is an invertible element of $G[X]/(X^{p^m} - X)$, considered as a ring for composition of polynomials. From Hermite's criterion, we know that, for any $s \in [1, p^m - 2]$, the reduction of $(f_\sigma(X))^s$ modulo $X^{p^m} - X$ has degree less than or equal to $p^m - 2$ [25, Theorem 7.4]. That means

$$(f_\sigma(X))^s \mod X^{p^m} - X = (f_\sigma(X))^s \mod X^{p^m-1} - 1.$$

Then we have a general theorem a proof of which can be found in [6].

Theorem 1: Let C be a cyclic code with defining set T. Let $\sigma \in \mathrm{Sym}(p^m)$ such that $\sigma(0) = 0$ and let $f_\sigma(X)$ be its associated polynomial.

Then $\sigma \in \mathrm{Per}(C)$ if and only if for all s in T the polynomial $f_\sigma(X)^s$ has all its exponents in T—where $f_\sigma(X)^s$ is computed modulo $X^{p^m-1} - 1$.

This theorem is a special case of [26, Theorem 3.1.3] which applies to any cyclic code, primitive or not. It provides a general method for the study of permutation groups of cyclic codes. However it is difficult to apply this method except for very special codes [6], [26], [27]. We wish to show that by the following example, continued in Example 3.

Example 1: Let C be the BCH code of length 26 on $\mathbb{F}_3$, with designed distance $d = 4$. Its defining set is $T = \{1, 3, 9, 2, 6, 18\}$. Let $\sigma \in \mathrm{Per}(C)$ and $s \in T$. According to Theorem 1, getting $s = 1$, we obtain

$$f_\sigma(X) = a_1X + a_2X^2 + a_3X^3 + a_6X^6 + a_9X^9 + a_{18}X^{18}.$$

If we get $s = 2$, we obtain for $f_\sigma(X)^2$ the polynomial

$$\begin{aligned} &- a_9a_{18}X + a_1^2X^2 - a_1a_2X^3 + (a_2^2 - a_1a_3)X^4 - a_2a_3X^5 \\ &+ a_3^2X^6 - a_1a_6X^7 - a_2a_6X^8 - a_3a_6X^9 + (a_{18}^2 - a_1a_9)X^{10} \\ &- a_2a_9X^{11} + (a_6^2 - a_3a_9)X^{12} - a_6a_9X^{15} + a_9^2X^{18} \\ &- a_1a_{18}X^{19} - a_2a_{18}X^{20} - a_3a_{18}X^{21} - a_6a_{18}X^{24}. \end{aligned}$$

In this polynomial the coefficients of X^i, $i \notin T$, must be zero. We then have to solve a system of equations and we can do that in reality because there are few variables. We can prove that $\mathrm{Per}(C)$ is $\Gamma\mathrm{L}(1, 3^3)$, but it is clear to us that our method has no application in general use.

Definition 5: We denote by K the subfield of G of order p^e. Then G can be considered as a vector-space of dimension m_e over K (where $m_e e = m$). For any K we can define the following subgroups of $Sym(p^m)$:

i) The linear group of G on K:

$$\mathrm{GL}(m_e, p^e) = \{\sigma | f_\sigma(X) = \sum_{i=0}^{m_e-1} f_i X^{p^{ei}}\}.$$

ii) The affine group $\mathrm{AGL}(m_e, p^e)$ is

$$\{\sigma | f_\sigma(X) = \sum_{i=0}^{m_e-1} f_i X^{p^{ei}} + b, b \in G\}.$$

iii) The semi-linear group $\Gamma\mathrm{L}(m_e, p^e)$ is

$$\{\sigma \mid f_\sigma = (f_{\sigma'})^{p^j},\ \sigma' \in \mathrm{GL}(m_e, p^e),\ 0 \le j < e\}.$$

iv) The semi-affine group $\mathrm{A}\Gamma\mathrm{L}(m_e, p^e)$ is

$$\{\sigma \mid f_\sigma = (f_{\sigma'})^{p^j},\ \sigma' \in \mathrm{AGL}(m_e, p^e),\ 0 \le j < e\}.$$

Note that $\Gamma\mathrm{L}(m_e, p^e)$ (resp., $\mathrm{A}\Gamma\mathrm{L}(m_e, p^e)$) is the group generated by $\mathrm{GL}(m_e, p^e)$ (resp., by $\mathrm{AGL}(m_e, p^e)$) and by the Frobenius mapping θ_1.

Remark 2: Let K and K' be two subfields of G, respectively, of order p^e and $p^{e'}$. Assume that K' is a subfield of K—i.e., $e = te'$. Then we have obviously

$$\mathrm{GL}(m_e, p^e) \subset \mathrm{GL}(m_e t, p^{e'})$$

and

$$\Gamma\mathrm{L}(m_e, p^e) \subset \Gamma\mathrm{L}(m_e t, p^{e'}) \tag{7}$$

where $m = m_e e = m_e t e'$. This result holds for the affine groups as well.

Now we are able to define cyclic codes, extended cyclic codes, and affine-invariant codes by means of a property of their automorphism group:

Definition 6: A code C of length $p^m - 1$ over $\mathbb{F}_q$, where q divides p^m is cyclic if and only if its permutation group contains

$$\mathrm{GL}(1, p^m) = \{\sigma | f_\sigma(X) = aX,\ a \in G^*\}.$$

Let $\widehat{C}$ be the extension of C. Then $\widehat{C}$ is an extended cyclic code if and only if its permutation group contains $\mathrm{GL}(1, p^m)$. It is an affine-invariant code if and only if its permutation group contains

$$\mathrm{AGL}(1, p^m) = \{\sigma \mid f_\sigma(X) = aX + b,\ a \in G^*, b \in G\}.$$

In this paper, we study the permutation groups of primitive cyclic codes whose extension is affine-invariant. We will see in Section II-B3 that for these codes to determine $\mathrm{Per}(C)$ is equivalent to determining $\mathrm{Per}(\widehat{C})$. Among these codes the most famous are GRM codes and BCH codes. We proved in [5] that the permutation group of a q-ary RM code of length $q^{m'}$ is $\mathrm{AGL}(m', q)$. We will treat later the p-ary BCH codes.

2) Codes Invariant under the GL and AGL Groups: Let C be a cyclic code in $\boldsymbol{M}$ such that its extended code is affine-invariant. In accordance with the operations in the algebra $\boldsymbol{A}$ and with Definition 6, the code $\widehat{C}$ is an ideal of $\boldsymbol{A}$. These special ideals were mainly studied by Charpin [11]–[13], [15] (see also [2] and [10]). Affine-invariant codes were characterized by Kasami *et al.* in [22]. The authors showed that an extended cyclic code is affine-invariant if and only if its defining set satisfies certain combinatorial property. This property was explained by Charpin in terms of a partial order [14]. We recall briefly her presentation.

Definition 7: Let $S = [0, p^m - 1]$. The p-ary expansion of $s \in S$ is

$$\sum_{i=0}^{m-1} s_i p^i, \ s_i \in [0, p-1].$$

We denote by $\prec$ the partial order relation on S defined as follows:

$$\forall s, t \in S : s \prec t \Longleftrightarrow s_i \leq t_i, \ i \in [0, m-1].$$

Then we can define the poset $(S, \prec)$.

When $s \prec t$, s is said to be a *descendant* of t and t to be an *ascendant* of s. We can define a maximal (resp., minimal) element of a subset of S, with respect to $\prec$. Two elements, s and t, are not related when $s \not\prec t$ and $t \not\prec s$. An *antichain* of $(S, \prec)$ is a set of nonrelated elements of S.

Let us define the map

$$\Delta : I \subset S \longmapsto \Delta(I) = \bigcup_{t \in I} \{s \in S, \ s \prec t\} = \bigcup_{t \in I} \Delta(\{t\}). \tag{8}$$

In the following, $\Delta(\{t\})$ will be simply denoted by $\Delta(t)$.

Theorem 2: Let $\widehat{C}$ be an extended cyclic code, with defining set T. Then, $\widehat{C}$ is affine-invariant if and only if $\Delta(T) = T$.

Let $T \subset S$. The *border* of T is the antichain F of $(S, \prec)$ consisting of the minimal elements of the set $S \setminus T$. That is equivalent to

$$F = \{s \in S \setminus T \mid \Delta(s) \setminus \{s\} \subset T\}. \tag{9}$$

Let $\widehat{C}$ be an extended cyclic code with defining set T. For simplification, we will often say *the border of the code* $\widehat{C}$ instead of the border of T. Many extended cyclic codes have the same border. However, one and only one affine-invariant code corresponds to a given antichain. We give a sketch of the proofs of the following theorem and proposition in order to clarify the use of antichains later.

Theorem 3: There is a one-to-one correspondance between antichains of $(S, \prec)$ and affine-invariant codes of length p^m. Each antichain is the border of one and only one affine-invariant code.

Proof: Let F be an antichain of $(S, \prec)$ and define the following subset of S:

$$T = S \setminus \bigcup_{f \in F} \{s \in S | f \prec s\}.$$

Then the extended cyclic code with defining set T is the only affine-invariant code whose border is F. □

Proposition 1: Let $\widehat{C}$ be an affine-invariant code with defining set T and border F. Then we have the following properties:

i) Let M be the set of maximal elements of T (with respect to $\prec$). Then the set $n - M$, $n = p^m - 1$, is the border of the dual of $\widehat{C}$.

ii) The BCH bound of $\widehat{C}$ is the smallest element of F.

In the following we will say that M is the maximal set of $\widehat{C}$.

Proof: The defining set of the dual of $\widehat{C}$ is the set of the elements $n - s$, where s is not in T; i) is immediately deduced.

The BCH bound of $\widehat{C}$ is the cardinality of the largest interval contained in T. Let δ be the smallest element of F. By definition the interval $[0, \delta[$ is contained in T. Suppose now that there is an interval $[s, t]$ in T containing more than δ elements; clearly $\delta < s$. Considering the p-ary expansions of δ and s, we cannot have $\delta \prec s$. So there is a $j > 0$ such that

$$s_j < \delta_j \quad \text{and} \quad \delta_i \leq s_i \text{ for } i > j.$$

Set

$$s' = \sum_{i=0}^{j} \delta_i p^i + \sum_{i=j+1}^{m} s_i p^i.$$

By construction, s' is an ascendant of δ. Moreover, s' is in $[s, t]$, because

$$s' - s \leq \sum_{i=0}^{j} \delta_i p^i$$

which is less than or equal to δ. Since $\delta \notin T$ and $\Delta(T) = T$ we cannot have $\delta \prec u$ for u in T; so we have here a contradiction, completing the proof of ii). □

We have seen that a code $\widehat{C}$ is affine-invariant if and only if its permutation group contains AGL $(1, p^m)$. The following theorem, due to Delsarte, gives a necessary and sufficient condition for extended cyclic codes to be invariant under the group AGL $(m/e, p^e)$. Since AGL $(1, p^m)$ is contained in AGL $(m/e, p^e)$, for all e dividing m, this result is, in fact, a generalization of the result of Kasami *et al.*, as we remark later. We begin by noticing a link between the permutation group and the alphabet field, which clarifies the hypothesis of the next theorem.

Lemma 1: Let $\widehat{C}$ be an extended q-ary cyclic code with defining set T, where $q = p^r$. Assume that $\widehat{C}$ is invariant under AGL $(m/e, p^e)$, e dividing m. Then r divides e.

Proof: The Frobenius map θ_e is contained in AGL $(m/e, p^e)$. In other words, the code $\widehat{C}$ is invariant under the permutation

$$\sum_{g \in G} x_g X^g \longmapsto \sum_{g \in G} x_g X^{g^{p^e}}$$

(see Definition 5). So we have, for any x in $\widehat{C}$ and for any s in T, $\phi_{sp^e}(\mathrm{x}) = 0$. Then T is invariant under multiplication by p^e modulo n. Since $\widehat{C}$ is a q-ary cyclic code, q divides p^e, completing the proof. □

The following theorem is due to Delsarte [17, Theorems 5 and 6]. We give it with our notation and in terms of partial order. For any divisor e of m we obtain a poset $(S, \ll_e)$, which becomes the poset $(S, \prec)$ when $e = m$.

Theorem 4: Let $\widehat{C}$ be an extended q-ary cyclic code in $\boldsymbol{A}$, which is affine-invariant. Let e be a divisor of m such that q divides p^e. Then Per $(\widehat{C})$ contains AGL $(m/e, p^e)$ if and only if the defining set T of $\widehat{C}$ satisfies (D_e).

$$(D_e) : s \in T \quad \text{and} \quad t \ll_e s \Longrightarrow t \in T$$

where $\ll_e$ is the partial order

$$\omega_{p^e}(p^k t) \leq \omega_{p^e}(p^k s), \quad k \in [0, e-1] \tag{10}$$

—the multiplication in S is calculated modulo n.

Remark 3: For $e = m$, we have $\omega_{p^m}(s) = s$, for any s in S. Then the condition (10) becomes: $p^k t \leq p^k s$, for all k in $[0, m-1]$. Obviously, it is equivalent to $t \prec s$. We then obtain the condition of Kasami *et al.* for extended cyclic codes to be invariant under $\mathrm{AGL}(1, p^m)$ (see Theorem 2).

Remark 4 [17]: A corollary of Theorem 4 is the characterization the codes of $\boldsymbol{A}$ invariant under $\mathrm{AGL}(m, p)$. In this case, T is invariant under multiplication by p and the condition (10) becomes: $\omega_p(t) \leq \omega_p(s)$. Thus there is an element μ of $[1, m(p-1)]$ such that the defining set T is the set $\{s | \omega_p(s) < \mu\}$, which is the defining set of the p-ary RM code of order $m(p-1) - \mu$. Then *a nontrivial extended cyclic code of $\boldsymbol{A}$ which is invariant under $\mathrm{AGL}(m, p)$ is a p-ary RM code.*

Example 2: Notation is that of Theorem 4. It is not difficult to construct an extended cyclic code invariant under $\mathrm{AGL}(m/e, p^e)$. The most evident construction is the following:

- Choose $\lambda \in [1, m(p^e - 1)/e]$.
- Consider the code whose defining set is

$$T = \left\{ s \mid \sup \{\omega_{p^e}(p^k s) \mid k \in [0, e-1]\} \leq \lambda \right\}.$$

Obviously, T satisfies (D_c). Note that such a defining set is invariant under the multiplication by p modulo $p^m - 1$ (see Proposition 3). It defines a p-ary code.

3) Recent Results of Berger: Recall that the alternating group, denoted by $\mathrm{Alt}(p^m)$, is the subgroup of $\mathrm{Sym}(p^m)$, composed of even permutations. By definition, a permutation group $\mathcal{G}$ of an affine-invariant code is a subgroup of the full symmetric group $\mathrm{Sym}(p^m)$ which contains the affine group $\mathrm{AGL}(1, p^m)$. These groups were recently classified by Berger [7], [8]. Using his results we can be more precise about the form of these groups, as we show with the following theorem.

Theorem 5: Let $\mathcal{G}$ be a permutation group of G. Suppose that $m \geq 2$. If $\mathcal{G}$ contains the affine group $\mathrm{AGL}(1, p^m)$ as a subgroup, then one of the following assertions holds.

i) $\mathcal{G} = \mathrm{Sym}(p^m)$.
ii) $p = 2$ and $\mathcal{G} = \mathrm{Alt}(2^m)$.
iii) There exists a divisor e of m such that

$$\mathrm{AGL}(m/e, p^e) \subseteq \mathcal{G} \subseteq \mathrm{A\Gamma L}(m/e, p^e).$$

Proof: This theorem is the direct consequence of two results. The first one is due to Berger. He proved in [7] that, with the hypothesis of the theorem, either $\mathcal{G}$ is a subgroup of $\mathrm{AGL}(m, p)$, or there are two possibilities:

- if p is odd then $\mathcal{G} = \mathrm{Sym}(p^m)$;
- if $p = 2$ then either $\mathcal{G} = \mathrm{Sym}(2^m)$ or $\mathcal{G} = \mathrm{Alt}(2^m)$.

Suppose that $\mathcal{G}$ is a subgroup of $\mathrm{AGL}(m, p)$, and let $\mathcal{G}_0$ be the stabilizer of 0 in $\mathcal{G}$. Then $\mathcal{G}_0$ is a subgroup of the linear group $\mathrm{GL}(m, p)$ and contains the Singer cycle $\mathrm{GL}(1, p^m)$ (i.e., a cycle of length $p^m - 1$). But Kantor proved in [21] the following result: if $\mathcal{G}_0$ is a subgroup of $\mathrm{GL}(m, p)$ containing a Singer cycle, then there exists a divisor e of m such that $\mathrm{GL}(m/e, p^e)$ is a normal subgroup of $\mathcal{G}_0$.

We remark that the normalizer of the linear group $\mathrm{GL}(m/e, p^e)$ in $\mathrm{Sym}(p^m)$ is the semi-linear group $\Gamma\mathrm{L}(m/e, p^e)$, i.e., $\Gamma\mathrm{L}(m/e, p^e)$ is the maximal subgroup of $\mathrm{Sym}(p^m)$ containing $\mathrm{GL}(m/e, p^e)$ as a normal subgroup. This implies

$$\mathrm{GL}(m/e, p^e) \subseteq \mathcal{G}_0 \subseteq \Gamma\mathrm{L}(m/e, p^e)$$

and completes the proof. □

It is clear that Theorem 5 involves strong results on the permutation group of affine-invariant codes. We have mainly the following corollary:

Corollary 1: Let C be a nontrivial primitive cyclic code such that its extended code $\widehat{C}$ is affine-invariant. Then there exists a divisor e of m such that

i) $\mathrm{GL}(m/e, p^e) \subseteq \mathrm{Per}(C) \subseteq \Gamma\mathrm{L}(m/e, p^e)$
ii) $\mathrm{AGL}(m/e, p^e) \subseteq \mathrm{Per}(\widehat{C}) \subseteq \mathrm{A\Gamma L}(m/e, p^e)$.

Proof: From Remark 1, the permutation group $\mathrm{Per}(C)$ is the subgroup of $\mathrm{Per}(\widehat{C})$ which leaves 0 invariant. Then ii) implies i).

In [23, sec. 4], Knapp and Schmidt proved that the only codes whose permutation group contains the alternating group are the repetition codes and their duals. So if $\mathrm{Per}(\widehat{C})$ is the symmetric group or the alternating group then $\widehat{C}$ is trivial. □

Suppose that $\widehat{C}$ is affine-invariant and let e be the divisor of m defined by the theorem above. The quotient of $\mathrm{A\Gamma L}(m/e, p^e)$ by $\mathrm{AGL}(m/e, p^e)$ is isomorphic to the automorphism group of the field of order p^e; that is, a cyclic group of order e generated by the Frobenius mapping. Therefore, the quotient of $\mathrm{Per}(\widehat{C})$ by $\mathrm{AGL}(m/e, p^e)$ is a subgroup of this group; note that this quotient is clearly isomorphic to the quotient of $\mathrm{Per}(C)$ by $\mathrm{GL}(m/e, p^e)$. For the determination of this subgroup, it is sufficient to find the least integer ℓ such that θ_ℓ leaves $\widehat{C}$ invariant. This integer ℓ must be a divisor of e. So we have proved that $\mathrm{Per}(\widehat{C})$ (and then $\mathrm{Per}(C)$) is characterized as soon as e and ℓ are determined. Note that when the alphabet field is $\mathbb{F}_p$, then $\ell = 1$ and we only need to determine e. This can be summarized as follows:

Corollary 2: Let $\widehat{C}$ be a nontrivial affine-invariant code of $\boldsymbol{A}$ and let e be the divisor of m such that

$$\mathrm{AGL}(m/e, p^e) \subseteq \mathrm{Per}(\widehat{C}) \subseteq \mathrm{A\Gamma L}(m/e, p^e).$$

Let ℓ be the least divisor of m such that the defining set of $\widehat{C}$ is invariant under multiplication by p^ℓ modulo n. The permutation group $\mathrm{Per}(\widehat{C})$ is then generated by $\mathrm{AGL}(m/e, p^e)$ and by θ_ℓ.

Example 3: Following Example 1, we consider again the BCH code of length $3^3 - 1$ and designed distance 4 over $\mathbb{F}_3$. This code is denoted by C; let T be its defining set. We want to determine $\mathrm{Per}(C)$. In accordance with the corollary above it is sufficient to know the value of ℓ and e.

As C is a ternary code, $\ell = 1$. Moreover, m is here a prime, implying $e \in \{1, 3\}$. If $e = 1$ then $\widehat{C}$ is a ternary RM code. We know it is not true because, for instance, $4 \notin T$ and $2 \in T$ have both the same 3-weight. So $e = 3$, proving that $\mathrm{Per}(C) = \Gamma\mathrm{L}(1, 27)$ and $\mathrm{Per}(\widehat{C}) = \mathrm{A\Gamma L}(1, 27)$.

At the end of this section, we have formally characterized the permutation group of any affine-invariant code. In the next section we want to develop some tools which allow us to determine effectively the group for a given code or for some infinite classes of codes. It is important to notice that the group of the cyclic code and the group of its extension are immediately deduced one from the other. According to the context we will determine one or the other group.

III. Permutation Groups of Affine-Invariant Codes

Notation is that of Section II. A cyclic code is a code in $\boldsymbol{M}$ and its extension a code in $\boldsymbol{A}$. The parameters will be specified only when it needs to be done. For a large number of affine-invariant p-ary codes (and for some q-ary codes), the permutation group is completely determined by applying Theorem 5 and its corollaries; it is actually either the smallest group $\mathrm{AGL}(1,p^m)$, which is $\mathrm{A\Gamma L}(1,p^m)$ for the p-ary codes, or the largest group $\mathrm{AGL}(m,p)$ (see Definition 6). This result is explained in the following theorem.

Theorem 6: Recall that $q=p^r$, r dividing m, and $n=p^m-1$. Let C be a q-ary cyclic code, whose extension $\widehat{C}$ is an affine-invariant code. Assuming that C (resp., $\widehat{C}$) is not trivial, we have:

i) If $r=1$ and m is a prime, $m>1$, then either $\widehat{C}$ is a p-ary RM code or $\mathrm{Per}(\widehat{C})$ is $\mathrm{A\Gamma L}(1,p^m)$ (resp., $\mathrm{Per}(C)$ is $\mathrm{\Gamma L}(1,p^m)$). In the first case, $\mathrm{Per}(\widehat{C})$ is $\mathrm{AGL}(m,p)$ (resp., $\mathrm{Per}(C)$ is $\mathrm{GL}(m,p)$).

ii) Suppose that $q=p^m$, $m\geq 1$. Then $\mathrm{Per}(\widehat{C})$ is $\mathrm{AGL}(1,p^m)$ (resp., $\mathrm{Per}(C)$ is $\mathrm{GL}(1,p^m)$), which is the permutation group of the extended Reed–Solomon code.

Proof: Notation is that of Corollary 1. In both cases, the value of e is obviously deduced from the hypothesis. As $\widehat{C}$ is affine-invariant, its permutation group contains $\mathrm{AGL}(1,p^m)$. Note that $\mathrm{A\Gamma L}(m/e,p^e)$ equals $\mathrm{AGL}(m/e,p^e)$ when $e=1$.

i) Since m is a prime, a divisor e of m is either 1 or m. When $e=1$, the group of $\widehat{C}$ is $\mathrm{AGL}(m,p)$; the only p-ary codes which have this group as a permutation group are the nontrivial p-ary RM codes (cf. Remark 4). If $e=m$ then the group of $\widehat{C}$ is exactly $\mathrm{A\Gamma L}(1,p^m)$, because $\widehat{C}$ is a p-ary code.

ii) Since $\widehat{C}$ is a p^m-ary code, it cannot be a p^ℓ-ary code, $\ell<m$. So m divides e. That means $e=m$ and $\mathrm{Per}(\widehat{C})=\mathrm{AGL}(1,p^m)$. Then any such code has the same group as the extended RS code [19]. □

We deduce immediately the automorphism group of a large class of binary affine-invariant codes.

Corollary 3: Let m be a prime. Let $\widehat{C}$ be a binary affine-invariant code of length 2^m. Suppose that $\widehat{C}$ is neither trivial nor an RM code. Then the automorphism group of $\widehat{C}$ (resp., of C) is $\mathrm{A\Gamma L}(1,2^m)$ (resp., $\mathrm{\Gamma L}(1,2^m)$).

Remark 5: Part i) of Theorem 6 can be generalized as follows: if $m=rm'$, where m' is a prime, and if $\widehat{C}$ is a p^r-ary code then the permutation group of $\widehat{C}$ is either $\mathrm{AGL}(m',p^r)$ or the group generated by $\mathrm{AGL}(1,p^m)$ and θ_r. Indeed, suppose that $\widehat{C}$ is invariant under $\mathrm{AGL}(m/e,p^e)$. One must have $r\mid e\mid m$. As m' is a prime, e is either r or m. However, this more general result does not give precisely the permutation group. We need to verify whether e can be r or not.

Example 4 : Let $\widehat{C}$ be the code of length 2^6 over $\mathbb{F}_{2^6}$ with defining set $T=\{0,1,4,5\}$. Clearly, $\widehat{C}$ is a 2^6-ary affine-invariant code. From Theorem 6, $\mathrm{Per}(\widehat{C})$ is $\mathrm{AGL}(1,2^6)$. Difficulties appear for codes invariant under θ_2 or θ_3. For instance, we now let $T=\{0,1,8,9\}$. So $\widehat{C}$ is affine-invariant and it is a 2^3-ary code—i.e., T is invariant under the multiplication by 8 or $\widehat{C}$ is invariant under θ_3. The permutation group of $\widehat{C}$ could contain $\mathrm{AGL}(2,2^3)$. But we have

$$\omega_8(2)=2,\ \omega_8(4)=4,\ \omega_8(8)=1$$
$$\text{and } \omega_8(2^k9)=2^{k+1},\quad 0\leq k\leq 2$$

proving that $2\ll_3 9$ with $9\in T$ and $2\notin T$. Hence T does not satisfy the condition (D_3) (see Theorem 4). So the group $\mathrm{Per}(\widehat{C})$ is generated by $\mathrm{AGL}(1,2^6)$ and θ_3.

From now on we will restrict our study to the codes which are not covered by the theorem above. There are a variety of situations, depending of the number of divisors of m and of the alphabet field. Considering together Theorem 4 and Corollary 2, it appears that the condition of Delsarte could be the best way for the compution of the groups. So we begin by an extensive study of this condition.

A. An Extensive Study of Delsarte's Condition

Let C be a cyclic code and $\widehat{C}$ the extended code. Recall that code symbols are from the field of order q, $q=p^r$. However, such a code can be a p^ℓ-ary code, with $\ell<r$. In other words, $\widehat{C}$ can be invariant under θ_ℓ, $\ell<r$. We generally suppose that $\widehat{C}$ is affine-invariant and we want to characterize its permutation group. As we claimed in Section II, $\mathrm{Per}(C)$ is obviously deduced from $\mathrm{Per}(\widehat{C})$. So we want to determine ℓ and a divisor e of m such that $\widehat{C}$ satisfies ii) of Corollary 1. Note that we have implicitly: $\ell|r|m$ and $\ell|e|m$.

In Section II-B2, we defined the border of any affine-invariant code $\widehat{C}$. It is an antichain of the poset $(S,\prec)$. We will represent $\widehat{C}$ by its border and deduce a simplification of the condition of Delsarte—i.e., a corollary of Theorem 4. Moreover, the parameter ℓ is a parameter of the border of $\widehat{C}$, as we prove now.

Proposition 2: Let $\widehat{C}$ be an affine-invariant code, with border F. Then $\widehat{C}$ is invariant under θ_u if and only if $p^uF=F$. Therefore, $\widehat{C}$ is a p^ℓ-ary code if and only if ℓ is the smallest integer such that $p^\ell F=F$.

Proof: Let T be the defining set of $\widehat{C}$ and set $T'=S\backslash T$. Recall that F is the set of minimal elements of T', with respect to $\prec$. Let $u\in[1,m-1]$; by definition, $s\prec t$ if and only if $p^us\prec p^ut$. We want to prove that T is invariant under multiplication by p^u if and only if F is.

Suppose that T is invariant under multiplication by p^u, then T' satisfies this property too. Hence for any minimal element s of T', p^us is also a minimal element of T'. That means that F is a union of cyclotomic cosets of p^u.

Conversely, assume that F is such a union. Then the set of ascendants of p^us, $s\in F$, is the set of elements p^ut where t is an ascendant of s. So T' is a union of cyclotomic cosets of p^u, proving that T is such a union. □

Corollary 4: Let $\widehat{C}$ be an affine-invariant code, with defining set T and border F. Let M be the set of maximal elements of T, with respect to $\prec$—i.e., the maximal set of T.Then $\widehat{C}$ is invariant under $\mathrm{AGL}(m/e, p^e)$ if and only if it satisfies (F_e).

(F_e) : for all $f \in F$ there is no $\bar{s}$ in M such that $f \ll_e \bar{s}$

where the relation $\ll_e$ is the partial order defined by (10) in Theorem 4.

Proof: We must prove that the condition (F_e) is equivalent to the condition (D_e) of Theorem 4. Note that M is a subset of T.

Assume that $\widehat{C}$ satisfies (D_e). Let $f \in F$ and suppose that there exists $\bar{s} \in M$ such that $f \ll_e \bar{s}$. From (D_e), that means $f \in T$, a contradiction.

Conversely, assume that $\widehat{C}$ satisfies (F_e). Let $s \in T$ and let t such that $t \ll_e s$. In order to prove that (D_e) is satisfied, we must prove that $t \in T$. Suppose that $t \notin T$. By definition of the border, there is f in F such that $f \prec t$. Clearly, $f \prec t$ implies $\omega_{p^e}(p^k f) \leq \omega_{p^e}(p^k t)$, for any k. So $f \ll_e t$. On the other hand, there exists $s \in M$ such that $s \prec \bar{s}$, which yields $s \ll_e \bar{s}$. Finally, we have

$$f \ll_e t \ll_e s \ll_e \bar{s}$$

which contradicts (F_e). Therefore, $t \in T$. □

Remark 6: The condition (F_e) is of most interest for the computation of the group of a given code. Indeed, it needs less operations than the condition (D_e), especially when the code satisfies (D_e). When the code does not satisfy (D_e), the negative answer is quickly obtained (as our tests proved). The border and the maximal set are first computed and they are used for testing any divisor e of m. Morcover, in some situations, it is possible to prove a general result by means of Corollary 4, as the following examples show.

The use of Corollary 4 necessitates handling p^e-weights in diverse situations. The following property, given by Delsarte in [17], yields many simplifications.

Proposition 3: Let $v = p^e$, e dividing m. For $\lambda \in [0, v-1]$ and $i \in [0, e-1]$, let us define

$$[\lambda p^i] = \begin{cases} \lambda p^i \mod v - 1, & \text{if } \lambda < v-1 \\ v-1, & \text{if } \lambda = v-1 \,. \end{cases}$$

If

$$\sum_{j=0}^{m/e-1} s_j v^j$$

is the v-ary expansion of s, we have

$$\omega_v(p^i s) = \sum_{j=0}^{m/e-1} [s_j p^i].$$

Note that $\omega_v(vs) = \omega_v(s)$, so that

$$\{\omega_v(p^i s) | i \in [0, e-1]\} = \{\omega_v(p^i(ps)) | i \in [0, e-1]\}.$$

Example 5 : Let C be the binary BCH code of length 63 and designed distance 7. Denote by T the defining set of the extended code $\widehat{C}$. We have

$$T = \{0\} \cup \mathrm{cl}(1) \cup \mathrm{cl}(3) \cup \mathrm{cl}(5)$$

where $\mathrm{cl}(i)$ is the cyclotomic coset of 2 modulo 63 containing i. As T does not contain $\mathrm{cl}(9)$, $\widehat{C}$ is not an RM code. So its permutation group is strictly contained in $\mathrm{AGL}(6,2)$. The border of $\widehat{C}$ is

$$F = \mathrm{cl}(7) \cup \mathrm{cl}(9) \cup \mathrm{cl}(21).$$

The maximal set of T is the union of $\mathrm{cl}(3)$ and $\mathrm{cl}(5)$. It is easy to prove that T satisfies (F_3). Indeed, for $\bar{s} = 3$ or 5

$$\{\omega_{2^3}(2^k \bar{s}) | k \in [0,2]\} = \{3,5,6\}$$

while $\omega_{2^3}(7) = 7$, $\omega_{2^3}(2^2.9) = 8$, and $\omega_{2^3}(21) = 7$. So it is impossible to have $f \ll_3 \bar{s}$, for some $f \in F$. Hence, *the automorphism group of $\widehat{C}$ is $A\Gamma L(2, 2^3)$; the automorphism group of C is $\Gamma L(2, 2^3)$.*

Example 6 : In this example, m is even and $m \geq 6$. We denote by C_m the binary BCH code of length $2^m - 1$ and designed distance $d = 2^{m-2} - 1$. Let T_m be the defining set of the extended code $\widehat{C}_m$. Set

$$\lambda = \sum_{i=0}^{(m-2)/2} 2^{2i}.$$

By definition, the border of T_m contains $\mathrm{cl}(d)$; moreover, it is easy to check that it contains $\mathrm{cl}(\lambda)$. The maximal set of T_m is

$$M_m = \bigcup_{i=0}^{m-3} \mathrm{cl}(d - 2^i).$$

By using (F_2), we want to determine if such a code is invariant under $A\Gamma L(m/2, 2^2)$. Denote by $W(s)$ the set $\{\omega_4(s), \omega_4(2s)\}$. We have

$$W(d) = \left\{ \frac{3(m-2)}{2} \right\} \quad W(\lambda) = \{m/2, m\}$$

and for any $s \in \mathrm{cl}(d - 2^i)$, $i \in [0, m-3]$

$$W(s) = \left\{ \frac{3(m-4)}{2} + 1, \frac{3(m-4)}{2} + 2 \right\}.$$

Note that $W(s) = W(2s)$ (see Proposition 3). Suppose that T_m satisfies (F_2). Then it is impossible to have $\lambda \ll_2 s$, for some $s \in M_m$. Since $m/2 \leq 3(m-4)/2 + 1$, for all $m > 5$, that yields $3(m-4)/2 + 2 < m$ (i.e., $m < 8$). *Therefore, $\widehat{C}_m$ is not invariant under $A\Gamma L(m/2, 2^2)$, for any $m \geq 8$.*

Consider now the code C_6: $d = 15$, $\lambda = 21$, $W(d) = \{6\}$, $W(\lambda) = \{3,6\}$, and, for any $s \in M_m$, $W(s) = \{4,5\}$. The border of T_6 is the union of $\mathrm{cl}(15)$, $\mathrm{cl}(21)$, and $\mathrm{cl}(27)$, where $W(27) = \{6\}$. It is easy to see that any element f of the border satisfies : $\sup W(f) \geq 6$. On the other hand, any element s of M_6 satisfies: $\sup W(s) \leq 5$. Hence T_6 satisfies (F_2), proving that $\widehat{C}_6$ is invariant under $A\Gamma L(3, 2^2)$. As $\widehat{C}_6$ is not an RM code, *the automorphism group of $\widehat{C}_6$ is exactly $A\Gamma L(3, 2^2)$.* Indeed, $\mathrm{Aut}(\widehat{C}_6)$ is smaller than $\mathrm{AGL}(6,2)$ and then cannot contain $A\Gamma L(2, 2^3)$. *The automorphism group of C_6 is $\Gamma L(3, 2^2)$.*

Example 7: In this example, codes are self-dual, affine-invariant, and of length 64 over $\mathbb{F}_4$. Note that self-duality is here defined by using the standard inner product:

$$< x, y >= \sum_{g \in G} x_g y_g.$$

The border is denoted by F and the maximal set by M. We denote by $\mathrm{c}(s)$ the cyclotomic coset of 4 modulo 63 containing s. Set $u(s) = (\omega_4(s), \omega_4(2s))$; note that $u(s) = u(t)$ for any $t \in \mathrm{c}(s)$. *There are at most nine nonequivalent self-dual affine-invariant codes of length* 64 *over* GF (4). This result was obtained by determining any antichain, which can be a border of such a code [16]. Among the nine codes there is a GRM code, whose permutation group is known to be $\mathrm{AGL}(3, 2^2)$. All codes are 2^2-ary codes, implying that the only divisors of 6 we must take in account are 2 and 6. So there are two possibilities: either the permutation group is those of the GRM code or it is generated by $\mathrm{AGL}(1, 2^6)$ and θ_2, the 2th power of the Frobenius mapping. *We claim that there is only one code, different from the GRM code, which has the same permutation group as the GRM code.* Moreover, we strongly conjecture that this code is not equivalent to the GRM code.

The nine borders are given in [16]; they contain few elements and these elements appear in several borders. So it is easy to write the binary expansion of all elements of the nine borders. Since codes are self-dual, the maximal set is obviously deduced from the border. That is, M is the coset of $63 - f$, $f \in F$. For instance, there is the border $\mathrm{c}(10)$, providing $M = \mathrm{c}(53)$. The binary expansions we need are

$$10 = (010100) \quad \text{and} \quad 53 = (101011).$$

We then compute $u(10) = (4, 2)$ and $u(53) = (5, 7)$, proving $10 \ll_2 53$. Hence, from Corollary 4, the code whose border is $\mathrm{c}(10)$ cannot be invariant under $\mathrm{AGL}(3, 2^2)$. We obtain this result for six other codes. Only the GRM code and the code with border

$$F = \mathrm{c}(11) \cup \mathrm{c}(14) \cup \mathrm{c}(21) \cup \mathrm{c}(26)$$

remain. We write below the $u(s)$ appearing in F and in M.

$$\begin{array}{llll} F: & u(11) = (5,4) & u(14) = (5,4) & \\ & & u(21) = (3,6) & u(26) = (5,4) \\ M: & u(52) = (4,5) & u(49) = (4,5) & \\ & & u(42) = (6,3) & u(37) = (4,5). \end{array}$$

We can check immediately that for all $f \in F$ there is no $s \in M$ such that $f \ll_2 s$. From Corollary 4, this code is invariant under $\mathrm{AGL}(3, 2^2)$.

Another extension of the result of Delsarte is the construction of codes invariant under $\mathrm{AGL}(m/r, p^r)$, for a given r dividing m. We have given in Example 2 an obvious construction of such p-ary codes (see also Section III-C2). In fact, there is a more general way which is immediate when the relation of Delsarte is viewed as a partial order.

Proposition 4: Assume that m has a nontrivial divisor r and consider the poset $(S, \ll_r)$. Let $M(r)$ be an antichain of this poset and set

$$T = \bigcup_{t \in M(r)} \{s \in S | s \ll_r t\}.$$

Then $qT = T$, $q = p^r$,, and the extended cyclic code on $\mathbb{F}_q$ whose defining set is T is invariant under $\mathrm{AGL}(m/r, q)$.

Proof: As $\omega_q(s) = \omega_q(qs)$, $s \ll_r t$ implies $qs \ll_r t$, proving $qT = T$. Moreover, T satisfies (D_r) by definition; so its permutation group contains $\mathrm{AGL}(m/r, q)$. □

Example 8: Consider codes of length 2^{2k} over $\mathbb{F}_4$. The notation $\mathrm{c}(s)$ and $u(s)$ is that of Example 7. We get

$$T = \{s \in S | s \ll_2 10\}.$$

Since $u(10) = (4, 2)$, the value of $u(s)$, $s \in T$, can only be one of the following: $(0, 0)$, $(1, 2)$, $(2, 1)$, $(4, 2)$. We have $u(5) = (2, 4)$, proving that $5 \notin T$ (while $10 \in T$). Hence the code $\widehat{C}$ with defining set T is a 2^2-ary code. This property implies that its permutation group cannot contain $\mathrm{AGL}(m/e, 2^e)$ for e odd. From the proposition above, $\widehat{C}$ is invariant under $\mathrm{AGL}(k, 2^2)$ and this group contains $\mathrm{AGL}(m/e, 2^e)$ for any e even. We can conclude that the permutation group of $\widehat{C}$ is exactly $\mathrm{AGL}(k, 2^2)$. Note that $\widehat{C}$ is not a 2^2-ary RM code. Indeed, $\omega_4(10) = 4$ and $\omega_4(5) = 2$, with $10 \in T$ and $5 \notin T$.

B. An Equivalent Condition

In this section, we propose a new condition for a code of $\boldsymbol{M}$, whose extended code is affine-invariant, to be invariant under $\mathrm{GL}(m/e, p^e)$. It is a necessary and sufficient condition and then it is equivalent to that of Delsarte. However, our proof does not use Theorem 4. Theorem 7 can be viewed as a corollary of Theorem 5. As it will be shown through examples, this condition is a very efficient tool for the determination of the permutation group. For instance, it will allow us to determine the group of the p-ary BCH codes (in Section IV).

Let e be a divisor of m and let σ be a permutation which is in $\mathrm{AGL}(m/e, p^e)$ and not in $\mathrm{A\Gamma L}(m/\ell, p^\ell)$, for any ℓ strictly greater than e and $e \mid \ell \mid m$. Denote by $\mathcal{G}$ the permutation group generated by the affine group $\mathrm{AGL}(1, p^m)$ and by σ. In accordance with Theorem 5, $\mathcal{G}$ is exactly $\mathrm{AGL}(m/e, p^e)$. From now on σ will be the permutation σ_β with associated polynomial

$$f_\beta(X) = X - \beta X^{p^e}, \beta \in G^*$$

(for simplification we denote it f_β instead of f_{σ_β}). Note that f_β cannot be in $\mathrm{A\Gamma L}(m/\ell, p^\ell)$, for any ℓ strictly greater than e (see Definition 5).

Lemma 2: Denote by $N(\beta)$ the norm of β over $\mathbb{F}_{p^e}$. The polynomial $f_\beta(X)$ is a permutation polynomial if and only if $N(\beta) \neq 1$.

Proof: Let $v = p^e$, $m_e = m/e$, and

$$Q = (p^m - 1)/(p^e - 1) = (v^{m_e} - 1)/(v - 1) = \sum_{i=0}^{m_e - 1} p^{ei}.$$

By definition, the norm of β is β^Q [25, p. 57]. Since f_β is a linearized polynomial, it is a permutation polynomial if and

only if its kernel is $\{0\}$. That is equivalent to saying that there is no g, different from zero, such that $\beta g^{v-1} = 1$.

Recall that α denotes a primitive root of G. It is clear that the $\alpha^{j(v-1)}$, $j \in [1, Q]$, are the roots of the equation $X^Q - 1$. Moreover, the inverse of $\alpha^{j(v-1)}$ is $\alpha^{k(v-1)}$, $k = Q - j$. So β^Q equals 1 if and only if the inverse of β is g^{v-1}, for some g, providing $\beta g^{v-1} = 1$. □

Throughout the section, the notation is as we defined above: e, v, Q, β, f_β.

Lemma 3: Let $\widehat{C}$ be an affine-invariant code with defining set T. For any $s \in T$ and for any $j \in T$, there exists at least one λ, $0 \leq \lambda < v - 1$, such that $j + \lambda Q$ is not a descendant of s, with respect to $\prec$ ($j + \lambda Q$ is calculated modulo $p^m - 1$).

Proof: Recall that $n = p^m - 1$. We get s and j in T. We want to study the set

$$T(j) = \{j + \lambda Q \bmod n \mid 0 \leq \lambda < v - 1\}.$$

Suppose that $j = j' + cQ$, with $j' < Q$. Obviously, $T(j) = T(j')$. So without loss of generality, we can choose $j < Q$. With this hypothesis, the elements $j + \lambda Q$ are less than n. As the multiplication is calculated modulo n, to choose $j < Q$ makes easier the manipulation of elements $j + \lambda Q$. From now on, in this proof, t_k denotes the kth symbol of the p-ary expansion of any t in $[0, n]$.

$$t = \sum_{k=0}^{m-1} t_k p^k, \quad t_k \in [0, p-1].$$

We will say that $T(j)$ *satisfies* $H(s)$ *if and only if*

$$j + \lambda Q \prec s, \text{ for every } \lambda, \quad 0 \leq \lambda < v - 1.$$

Suppose that $T(j)$ satisfies $H(s)$. Consider $\lambda = (p - 1 - j_\ell)p^\ell$, for any $\ell \in [0, e-1]$. Since $j + \lambda Q < n$, we are sure that $(j + \lambda Q)_\ell = p - 1$. As $T(j)$ satisfies $H(s)$, $s_\ell = p - 1$ and this equality holds for any $\ell \in [0, e-1]$. Now, by definition of $\prec$, $j + \lambda Q \prec s$ implies $v^i(j + \lambda Q) \prec v^i s$, for any i and for any λ. Note that $v\lambda Q = \lambda Q \pmod{p^m - 1}$, since for any $\lambda \in [0, v-1]$ we have

$$\lambda Q = \sum_{i=0}^{m_e - 1} \lambda v^i.$$

Hence $T(v^i j)$ satisfies $H(v^i s)$, for any i. Using the method above, we can prove that $(v^i s)_\ell = p - 1$, for any $\ell \in [0, e-1]$ and any $i \in [1, m_e - 1]$. But $(v^i s)_\ell = s_k$, with $k = (m_e - i)e + \ell$. Finally, we obtain that all coefficients of the p-ary expansion of s are equal to $p-1$, proving that $s = n$. An affine-invariant code whose defining set contains n is the null-vector, a contradiction completing the proof. □

Theorem 7: Let C be a nontrivial cyclic code whose extended code $\widehat{C}$ is affine-invariant. We denote by T the defining set of C and by e a divisor of m. Then C (resp., $\widehat{C}$) is invariant under the action of GL $(m/e, p^e)$ (resp., AGL $(m/e, p^e)$) if and only if the following condition is satisfied:

$$\forall s \in T, j \prec s \Rightarrow s + j(p^e - 1) \in T \qquad (11)$$

where $s + j(p^e - 1)$ is calculated modulo n ($n = p^m - 1$).

Proof: The code C is a code of $\boldsymbol{M}$ (Definition 1), and then q divides p^e (see Lemma 1). In order to prove the theorem we will simply apply Theorem 1 to the permutation polynomial f_β. As we said at the beginning of this section, the code $\widehat{C}$ is invariant under AGL $(m/e, p^e)$ if and only if it is invariant under the permutation σ_β, for some β whose norm is 1; in other words, if and only if for all s in T, the polynomial $(f_\beta(X))^s$, evaluated modulo $X^n - 1$, has all its exponents in T.

Suppose first that (11) is satisfied. By writing $(f_\beta(X))^s$, for any s in T,

$$(X - \beta X^v)^s = \sum_{j \prec s} \binom{s}{j} (-1)^j \beta^j X^{s-j+vj} \pmod{X^n - 1}$$
$$= \sum_{j \prec s} \binom{s}{j} (-1)^j \beta^j X^{s+j(v-1)} \pmod{n}$$

we check immediately that f_β is associated with a permutation of $\widehat{C}$. Recall that the binomial coefficient of s and j is not zero (modulo p) if and only if $j \prec s$.

We suppose now that $\widehat{C}$ is invariant under AGL (m_e, p^e); i.e., f_β is associated with a permutation of $\widehat{C}$, for any β whose norm is not 1. Let $s \in T$ and $j \prec s$. We want to prove that $s + j(v-1)$ is in T and then we consider the exponents of $(f_\beta(X))^s$ above. Suppose there is a j' such that

$$s + j'(v-1) \equiv s + j(v-1) \bmod n.$$

Obviously, that means $j' \equiv j \bmod Q$. Hence the coefficient of $X^{s+j(v-1)}$, where the exponent is calculated modulo n, in $(f_\beta(X))^s$ is

$$A_{\beta,j} = \sum_{i=0}^{v-2} \binom{s}{j + iQ} (-1)^{j+iQ} \beta^{j+iQ}.$$

If this coefficient is not 0 we are sure that $s + j(v-1)$ is in T, and that is independent of the choice of β. It is sufficient to exhibit at least one β such that $A_{\beta,j}$ is not 0. Suppose that for every β, $A_{\beta,j}$ is 0. Consider the following polynomial:

$$P(X) = \sum_{i=0}^{v-2} \binom{s}{j + iQ} (-1)^{iQ} X^i.$$

Clearly, $A_{\beta,j} = (-\beta)^j P(\beta^Q)$. But the set of the β^Q (the norms of the element β) consists of elements of the field $\mathbb{F}_v^*$, except 0 and 1. With our hypothesis, all these elements must be roots of $P(X)$. Since the degree of $P(X)$ is $v-2$, we have here all the roots of $P(X)$. The polynomial

$$P'(X) = (X^{v-1} - 1)/(X - 1) = \sum_{i=0}^{v-2} X^i$$

has the same roots and the same degree as $P(X)$. Then $P(X)$ is equal to $P'(X)$, up to a scalar multiple. In particular, all coefficients of $P(X)$ are different from 0, implying

$$j + iQ \prec s, i \in [0, v-2].$$

This result contradicts Lemma 3, completing the proof. □

As a corollary of Theorem 7, we can give the form of the BCH bound of any affine-invariant code whose permutation group contains AGL $(m/e, p^e)$. This result is very powerful, as we will show in Example 9 following the corollary.

Corollary 5: Let $\widehat{C}$ be an affine-invariant code with defining set T and BCH bound δ. Let e be a divisor of m and

$$\delta = \sum_{i=0}^{\kappa} \delta_i p^{ei}, \quad \delta_i \in [0, p^e - 1].$$

If $\widehat{C}$ is invariant under $\mathrm{AGL}(m/e, p^e)$, then $\delta_{i+1} \prec \delta_i$, for any i.

Proof: Recall that the BCH bound of $\widehat{C}$ is the smallest element of its border (see Proposition 1). For any i let the p-ary expansion of δ_i be

$$\delta_i = \sum_{j=0}^{e-1} \delta_{i,j} p^j, \quad \delta_{i,j} \in [0, p-1].$$

Note that $\delta_{i+1} \prec \delta_i$ means $\delta_{i+1,j} \leq \delta_{i,j}$, for all j. Suppose that there is an i such that $\delta_{i+1} \not\prec \delta_i$. Then there is a j such that $\delta_{i,j} < \delta_{i+1,j}$. Set

$$s = \delta + p^{ei+j} - p^{e(i+1)+j}, \; t = p^{ei+j}, \quad \text{and} \quad s' = s + t(p^e - 1).$$

As $s < \delta$, $s \in T$. Moreover, we have clearly $t \prec s$ and $s' = \delta$ (so $s' \notin T$). Hence, T cannot satisfy (11); $\widehat{C}$ cannot be invariant under $\mathrm{AGL}(m/e, p^e)$. □

Example 9: Consider an affine-invariant code $\widehat{C}$ of length 2^{30} over $\mathbb{F}_4$, with BCH bound $\delta = 2937$. The 2-ary expansion of δ is

$$(1001111011010\ldots0).$$

Suppose that $\widehat{C}$ is a 4-ary code. So $\widehat{C}$ could be invariant under $\mathrm{AGL}(m/e, p^e)$, for $e \in \{2, 6, 10\}$ because e must be an even divisor of m. With the notation of Corollary 5, it is clear that $\delta_1 \not\prec \delta_0$, in all cases. Indeed, by identifying δ_i to its 2-ary expansion, we have:

- For $e = 2$, $\delta_0 = 10$ and $\delta_1 = 01$.
- For $e = 6$, $\delta_0 = 100111$ and $\delta_1 = 101101$.
- For $e = 10$, $\delta_0 = 1001111011$ and $\delta_1 = 010\ldots0$.

So *the automorphism group of $\widehat{C}$ is generated by $AGL(1, 2^{30})$ and θ_4.*

C. Some Examples

1) Codes with Defining Det $\{cl(1), cl(1+p^\lambda)\}$: As an example of application of Theorem 7, we will study the codes C_λ, of length $p^m - 1$, whose defining set is

$$T_\lambda = \mathrm{cl}(1) \cup \mathrm{cl}(1 + p^\lambda)$$

($\mathrm{cl}(j)$ is the orbit of j under multiplication by p). Clearly, the extension of such a code is an affine-invariant code. Since $T_{m-\lambda} = T_\lambda$, we assume λ is in $[1, m/2]$. By definition, C_λ is a p-ary code. So the integer ℓ of Corollary 2 is here equals to 1.

Lemma 4: Let i and j be nonnegative integers such that $0 \leq i < j < m$. Then

$$p^i + p^j \in T_\lambda \iff \{j - i = \lambda \quad \text{or} \quad j - i = m - \lambda\}.$$

Proof: Obviously, $p^i + p^j$ is in T_λ if and only if $p^i + p^j$ is in $cl(1 + p^\lambda)$. In other words, $p^i + p^j$ is in T_λ if and only if there is λ' in $[0, m-1]$ such that

$$p^i + p^j = p^{\lambda'} + p^{\lambda+\lambda'} \pmod m.$$

So either $i = \lambda'$, providing $j = \lambda + i$, or $j = \lambda'$, providing $i = \lambda + j - m$. □

Proposition 5: Assume $\lambda \leq m/2$. The permutation group of C_λ is the semi-linear group $\Gamma\mathrm{L}(1, p^m)$, except for the following cases:

1) $p = 2$, m even and $\lambda = m/2$. The permutation group is $\Gamma\mathrm{L}(2, 2^{m/2})$.
2) $p = 2$, $m \equiv 0 \bmod 3$, and $\lambda = m/3$. The permutation group is $\Gamma\mathrm{L}(3, 2^{m/3})$.
3) $m \equiv 0 \bmod 4$ and $\lambda = m/4$. The permutation group is $\Gamma\mathrm{L}(2, p^{m/2})$.

These properties hold for the extended codes $\widehat{C}_\lambda$, by replacing $\Gamma\mathrm{L}$ by $A\Gamma\mathrm{L}$. When parameters are those of 1), the dual of $\widehat{C}_\lambda$ is the extension of the BCH code of designed distance $2^{m-1} - 2^{(m-2)/2} - 1$. When $p = 2$ the permutation group is actually the automorphism group.

Proof: Let e be any divisor of m. We get $e \leq m/2$, because we know that C_λ is invariant under $\mathrm{GL}(1, p^m)$. We want to verify if a code C_λ may be invariant under $\mathrm{GL}(m/e, p^e)$—i.e., if T_λ satisfies (11).

For s in $\mathrm{cl}(1)$, $j \prec s$ yields $j = 0$ or s; in both cases $s + j(p^e - 1)$ is in T_λ. Consider now $s = 1 + p^\lambda$. Let j be such that $j \prec 1 + p^\lambda$ and $j \notin \{0, s\}$. So $j = 1$ or p^λ. Suppose that (11) is satisfied. One must have

$$1 + p^\lambda + (p^e - 1) \in T_\lambda \quad \text{and} \quad 1 + p^\lambda + p^\lambda(p^e - 1) \in T_\lambda.$$

That means

$$\text{i) } p^\lambda + p^e \in T_\lambda \quad \text{and} \quad \text{ii) } 1 + p^{\lambda+e} \in T_\lambda.$$

As $\lambda \leq m/2$ and $e \leq m/2$, $\lambda + e \leq m$; moreover, $\lambda + e < m$ when $\lambda \neq e$. We are going to examine if i) and ii) may be satisfied together. There are three cases:

1) Suppose $\lambda > e$. By applying Lemma 4, i) implies $\lambda - e = \lambda$ or $\lambda - e = m - \lambda$, which means $e = 0$ or $\lambda = (m + e)/2$, a contradiction.
2) If $\lambda = e$, i) means $2p^\lambda \in T_\lambda$. That is possible only for $p = 2$. If $p = 2$, ii) implies $1 + 2^{2\lambda} \in T_\lambda$ and we have:
   - If $\lambda = e = m/2$, then $1 + 2^{2\lambda} = 2 \bmod 2^m - 1$ and 2 is in $\mathrm{cl}(1)$. So in this case, (11) is satisfied and that is the first exception.
   - If $2\lambda < m$, Lemma 4 yields $2\lambda = \lambda$ or $2\lambda = m - \lambda$, providing the second exception: $p = 2$ and $e = \lambda = m/3$.
3) Now suppose $\lambda < e$. By applying Lemma 4, i) implies $e = 2\lambda$ or $e = m$. Only $e = 2\lambda$ is of interest. Then ii) becomes $1 + p^{3\lambda} \in T_\lambda$. Applying Lemma 4, ii) is satisfied only for $\lambda = m/4$. We then obtain the third exception: $\lambda = m/4$ and $e = m/2$.

Consider the first exception. The dual of $\widehat{C}_\lambda$ is such that the elements which are not in its defining set are

$$2^m - 1,\ \mathrm{cl}\,(2^{m-1} - 1),\ \text{and}\ \mathrm{cl}\,(2^{m-1} - 2^{(m-2)/2} - 1).$$

So it is easy to see that, in this case, the defining set of $\widehat{C}_\lambda$ is

$$\bigcup_{i=0}^{d-1} cl(i), d = 2^{m-1} - 2^{(m-2)/2} - 1$$

which is the defining set of the extended BCH code of designed distance d. □

.2) Special Infinite Classes: We have shown, in Example 2, that one can easily construct a p-ary affine-invariant code whose permutation group is bigger than $A\Gamma L\,(1, p^m)$. We want to define precisely these codes by means of their border.

Proposition 6: Let $\widehat{C}$ be an affine-invariant code with defining set T and border F. Denote by M the maximal set of T (see Proposition 1). Let e be a divisor of m and set for any $s \in S$

$$W(s) = \{\omega_{p^e}(p^k s) | k \in [0, e-1]\}.$$

Then there exists λ such that

$$T = \{s \in S \mid \sup W(s) \leq \lambda\}$$

if and only if i) and ii) are satisfied:

i) for any f in F, $\sup W(f) > \lambda$;
ii) for any s in M, $\sup W(s) \leq \lambda$.

In this case, $\widehat{C}$ is a p-ary code, invariant under $A\Gamma L\,(m/e, p^e)$.

Proof: This result is immediately deduced from the definition of M and of F : any element t of T satisfies $t \prec s$, for some $s \in M$; any element $u \notin T$ satisfies $f \prec u$, for some $f \in F$. □

We now come back to Example 6, in which an infinite class C_m of binary BCH codes was studied. We proved that the automorphism group of $\widehat{C}_6$ is $A\Gamma L\,(3, 2^2)$. Clearly, i) and ii) are satisfied, with $\lambda = 5$.

For any m, the maximal set M_m satisfies ii), with $\lambda = 3(m-4)/2 + 2$. *We claim that $\widehat{C}_6$ is the first element of an infinite class of binary codes, whose automorphism group is $A\Gamma L\,(m/2, 2^2)$.* That is, the codes D_m, m even and $m \geq 6$, with defining set

$$\{s \in [0, 2^m] \mid \sup W(s) \leq \lambda_m\}$$

where λ_m is $3(m-4)/2+2$. Note that $\lambda_6 = 5$. By definition, D_m is invariant under $A\Gamma L\,(m/2, 2^2)$, so that we need only prove that D_m is not a binary RM code. It is clear that $d = 2^{m-2} - 1$ is the first element of the border of D_m. Since $\omega_2(d) = m - 2$, if D_m is an RM code it is the RM code of order 2. But we have, for instance, $\mu = 2^{m-1} - 2^{m-3} - 3$ which satisfies

$$W(\mu) = \{3(m-4)/2, 3(m-4)/2 + 3\} \text{ and } \omega_2(\mu) = m - 3$$

proving that the element μ is not in the defining set of D_m while it is in the defining set of the RM code of order 2.

In Example 5, we studied another special binary BCH code. In this case also i) and ii) are satisfied, with $\lambda = 6$. Using the method above, we can construct an infinite class of binary codes whose automorphism group contains $A\Gamma L\,(2, 2^3)$. It is important to notice that *there exist affine-invariant p-ary codes whose permutation group is bigger than $A\Gamma L\,(1, p^m)$ and which cannot be defined through Proposition 6.* Some examples of such codes appear in Proposition 5.

3) Affine-Invariant Codes which are Principal Ideals of $\mathcal{A}$: Any ideal I of the algebra $\mathcal{A}$ can be represented as a sum of principal ideals. These principal ideals form a *system of generators of I*. Moreover, any such system can be reduced to a minimal system, whose cardinality is a constant only depending on I [24]. Affine-invariant codes are ideals of $\mathcal{A}$. Such a code is a principal ideal if and only if its border contains one and only one element. It is because *the cardinality of the border is equal to the cardinality of minimal systems of generators of the code* [14]. Consider an affine-invariant code on $\boldsymbol{k}$, $\boldsymbol{k} = \mathbb{F}_q$ and $q = p^r$, whose border is $\{f\}$. As $qf = f$ the form of f is as follows:

$$f = \lambda \sum_{i=0}^{m/r-1} q^i, \quad \lambda \in [1, q-1]. \tag{12}$$

It appears that such an affine-invariant code satisfies the necessary condition of Corollary 5 (Section III-B) to be invariant under $\mathrm{AGL}\,(m/e, p^e)$, for any multiple e of r. However, we will prove that, for any nontrivial case, this property is only possible for $e = m$. From Proposition 2 (Section III-A), a binary affine-invariant code, which is principal, is trivial; it is because $2f = f$ means $f = 0$ or $2^m - 1$. When $\boldsymbol{k}$ is a prime field, only extended BCH codes can be principal [15]. Since we will treat later such BCH codes, we will assume here that $\boldsymbol{k}$ is an extension field; the basis field is $\boldsymbol{k} = \mathbb{F}_q$, $q = p^r$ with $r > 1$.

Proposition 7: Let $\widehat{C}$ be an affine-invariant code on $\boldsymbol{k}$, which is a principal ideal of $\mathcal{A}$. We assume that $\widehat{C}$ is not trivial. Let ℓ be the smallest integer such that θ_ℓ leaves $\widehat{C}$ invariant. Then the permutation group of $\widehat{C}$ is generated by the group $\mathrm{AGL}\,(1, p^m)$ and θ_ℓ.

Proof: We suppose that $\boldsymbol{k} = \mathbb{F}_q$, $q = p^r$ with $r > 1$. When $r = 1$, the result is given later by Theorem 8; hence this result holds for $\ell = 1$ and any r. When $\ell = m$ the result comes immediately from Theorem 6. From now on, we assume that $1 < \ell < m$. In this proof, an element $s \in S$ will be often identified with its p-ary expansion $(s_0, \cdots, s_{m-1})$. Let $\{f\}$ be the border of $\widehat{C}$ and T its defining set. By definition, s is not in T if and only if $f \prec s$. So it is clear that the maximal set M of T is composed of the following elements:

$$t(j) = \sum_{\substack{i \in [0, m-1] \\ i \neq j}} (p-1)p^i + (f_j - 1)p^j, \quad \text{where } f_j > 0.$$

Let e be a multiple of ℓ (i.e., $p^e f = f$), different from m, and $v = p^e$. In order to prove the theorem we only need to prove that $\widehat{C}$ is not invariant under $\mathrm{AGL}\,(m/e, p^e)$, for any such e.

We first suppose that $p > 2$ and that there is a j such that $0 < f_j < p - 1$. Because of the form of f we can choose j in $[0, e-1]$ and we know that $f_j = f_{j+e}$ (see (12)). Now we let $t = t(j+e) + p^j(p^e - 1)$. Then $t_i = p - 1$ for any i different from $j + e$ and j; moreover, by using the formula above, we

easily obtain $t_{j+e} = f_{j+e}$ and $t_j = p-2$. Hence $f \prec t$ which means $t \notin T$. We have $t(j+e) \in T$, $p^j \prec t(j+e)$, and $t(j+e)+p^j(p^e-1) \notin T$. In accordance with Theorem 7, we can conclude that $\widehat{C}$ is not invariant under AGL$(m/e, p^e)$.

Suppose now that f_i is either 0 or $p-1$, for any i. From (12) and since the code is not trivial, we can choose $j \in [e, 2e-1]$ such that $f_j = p-1$ and $f_{j-1} = 0$. By using the formula of Proposition 3, we have for any k in $[0, e-1]$

$$\omega_v(p^k t(j)) = (m/e-1)(v-1) + [p^k(v-p^{j-e}-1)],$$

while $\omega_v(p^k f) = [p^k\lambda]\cdot m/e$. Now it is easy to check that the difference $\omega_v(p^k t(j)) - \omega_v(p^k f)$ is greater than or equal to 0, for all k. Indeed, we have always this kind of situation

$$[p^k(v-p^{j-e}-1)] = (p-1\cdots, p-1, \overset{i}{p-2}, p-1\cdots, p-1)$$

and

$$[p^k\lambda] = (\lambda_0, \cdots, \lambda_{i-2}, 0, p-1, \lambda_{i+1}\cdots\lambda_{m-1})$$

where λ_i is in $\{0, p-1\}$. Since $2 \le m/e$ we are sure that our differences are greater than or equal to γ, with

$$\gamma = 2(p-1)p^{i-1} - p^i = p^i - 2p^{i-1}$$

when $i > 0$, and $\gamma = 2(p-1)p^{m-1} - 1$ when $i = 0$ (the place of i is determined by the value of k). So we have proved that $f \ll_e t(j)$. In accordance with Corollary 4, it yields that $\widehat{C}$ cannot be invariant under AGL$(m/e, p^e)$, completing the proof. □

IV. The Permutation Group of p-ary Primitive BCH Codes

The automorphism groups of binary BCH codes, of length 2^m-1, were previously studied by Lu in his thesis by means of a slightly different version of Theorem 1 [26]. The author characterized some BCH codes which have an automorphism group larger than GL$(1, 2^m)$. Moreover, he conjectured that there are no others *exceptional* BCH codes (see also [27]). In this section, we prove that this conjecture is true. Moreover, we determine the permutation groups of BCH codes, extended or not, when the alphabet field is any prime field.

We will denote by $\widehat{B}(d)$, the extended BCH code of designed distance d and of length p^m over $\mathbb{F}_p$. We are only considering values of d which are the smallest values (coset leaders) in their p cyclotomic cosets modulo p^m-1. The GRM codes of same length over $\mathbb{F}_p$, say the p-ary RM codes, are denoted by $\mathcal{R}(\nu, m)$, where ν is the order. We suppose that $m > 1$, which means that we do not treat here the RS codes (see Definition 3). Some, but few, BCH codes are p-ary RM codes; we enumerate these exceptions in the following lemma.

Lemma 5: Assume that $\widehat{B}(d)$ is not trivial (i.e., $d \notin \{1, p^m-1\}$). The codes $\widehat{B}(d)$ which are p-ary Reed–Muller codes are the following:

1) For any p and any m, $\widehat{B}(p^{m-1}(p-1)-1) = \mathcal{R}(1, m)$.
2) When $p = 2$
   a) $\widehat{B}(3) = \mathcal{R}(m-2, m)$, for any m;
   b) $\widehat{B}(7) = \mathcal{R}(2, 5)$, for the length 32.
3) When $p > 2$
   a) $\widehat{B}(2) = \mathcal{R}(m(p-1)-2, m)$, for any m and any p;
   b) $\widehat{B}(5) = \mathcal{R}(3, 3)$, for the length 3^3 (i.e., $p = 3$ and $m = 3$);
   c) $\widehat{B}(p(p-2)-1) = \mathcal{R}(2, m)$, for the length p^2, $p > 3$.

Proof: For any fixed length, an extended BCH code could be an RM code if and only if it belongs to the class of BCH codes whose designed distance has the following form:

$$d = \sum_{i=0}^{\tau-1}(p-1)p^i + kp^\tau,\ k \in [1, p-1],\ \tau \in [0, m-1].$$

Indeed, a code $\widehat{B}(d)$, d given above, has the same minimum distance as the largest RM code it contains; moreover, it is the smallest BCH code containing this RM code, which is of order $m(p-1)-\mu$, $\mu = \tau(p-1)+k$, and of minimum distance $d+1$. Let T_d be the defining set of $\widehat{B}(d)$. Note that the cases $\{\tau = m-1$ and $k = p-1\}$ and $\{\tau = 0$ as well as $k = 1\}$ correspond to trivial BCH codes. Clearly, d is the smallest element of p-weight $\tau(p-1)+k$. So the code $\widehat{B}(d)$ equals $\mathcal{R}(m(p-1)-\mu, m)$ if and only if all elements s, satisfying $\omega_p(s) = \omega_p(d)-1$, are in T_d—i.e., the leader of the cyclotomic coset of such an s is less than d. It is easy to check that this property is satisfied by each exception indicated in the Lemma. Otherwise, one can always exhibit an s which contradicts the property. When $p = 2$, we can suppose $m > 5$ and $7 \le d \le 2^{m-2}-1$. Then we get

$$s = d - 2^\tau - 2^{\tau-2} + 2^{\tau+1}, \quad \text{for } d > 7$$

and $s = 9$ for $d = 7$. Assume now that $p > 2$ and $2 < d \le p^{m-1}(p-2)-1$. Then we choose s as follows:

- for $\tau \ge 2$ and $m \ge 3$: $s = d + p^j - p^{j-1} - p^{j-2}$, where $j = \tau$ if $k < p-1$ and $j = \tau+1$, otherwise (note that k is at most $p-3$ when $\tau = m-1$);
- for $\tau = 1$, $m \ge 3$, and $p > 3$: $s = (p-3)+(k+1)p$ if $k < p-1$ and $s = (p-2)+(p-2)p+p^2$, otherwise;
- for $\tau = 1$, $m \ge 3$, and $p = 3$: when $k = 2$, $s = 13$; when $k = 1$, either $m > 3$ and $s = 10$ or $m = 3$ and we obtain case 3b).
- for $\tau = 1$, $m = 2$: when $p = 3$ we obtain case 1); if $p > 3$ and $k \le p-4$, $s = (p-3)+(k+1)p$ ($k = p-3$ is case 3c));
- for $\tau = 0$ (i.e., $k > 2$ which implies $p > 3$) and $m \ge 2$: $s = (k-2)+p$. □

We are going to determine precisely the permutation group of any p-ary BCH code. From now on we will use the same notation.

Notation: Let e be a divisor of m and

$$2 \le e < m,\ m_e e = m,\ v = p^e. \tag{13}$$

For any d in $[1, p^m-2]$, d being the designed distance of any p-ary BCH code:

$$d = \sum_{i=0}^{\tau} d_i p^i = \sum_{j=0}^{\kappa} \delta_j v^j \tag{14}$$

where $d_i \in [0, p-1]$, $\delta_j \in [0, v-1]$, $d_\tau > 0$, $\delta_\kappa > 0$ (p-ary and v-ary expansions); we will denote by T_d the defining set

of $\widehat{B}(d)$. Generally, we treat BCH codes which are not trivial and not equal to some p-ary RM code.

The proof of Theorem 8 is very technical because there are many different situations. Actually, there are few exceptions and we mainly want to prove that a given BCH code is not invariant under $\mathrm{AGL}(m_e, p^e)$, e dividing m. In order to be easily understood, we begin by proving two lemmas; moreover, we choose to use the same method, for each case. This method, implied by Theorem 7, is as follows: we want to exhibit $s(d)$ and t such that $s(d)$ is in T_d, $t \prec s(d)$ and $s(d) + t(v-1)$ is not in T_d. In almost every case, t will be p^j, for some j. In order to do so, we often need to determine the leader of $\mathrm{cl}(s)$—i.e., the smallest element of the the cyclotomic coset of s. Recall that $\mathrm{cl}(s)$ is the orbit of s under the multiplication by p modulo $p^m - 1$. The p-ary expansion of s can be viewed as a sequence of m p-ary symbols ; the p-ary expansion of any element of $\mathrm{cl}(s)$ is a shift of those of s.

Lemma 6: Notation is that of (13) and (14). Assume that $\kappa \in [0, m_e - 3]$ with $m_e \geq 3$, and set

$$s(d) = \begin{cases} \sum_{i=0}^{\tau-1} (p-1)p^i, & \text{if } \tau > 0 \\ d_0 - 1, & \text{otherwise .} \end{cases} \tag{15}$$

Set

$$s_1 = \begin{cases} s(d) + p^{\tau-1}(p^e - 1), & \text{if } \tau > 0 \\ s(d) + (p^e - 1), & \text{if } \tau = 0 . \end{cases}$$

Then $s(d) \in T_d$ and $s_1 \notin T_d$.

Proof: By definition $s(d) < d$, showing $s(d) \in T_d$. When $\tau \neq 0$, the p-ary expansion of s_1 has this form

$$(p-1, \cdots, p-1, \overset{\tau-1}{p-2}, \underbrace{0, \cdots, 0}_{e-1}, \overset{\tau-1+e}{1}, \underbrace{0, \cdots, 0}_{m-\tau-e}).$$

It is clear that $s_1 > d$, because $e > 1$ implies $\tau - 1 + e > \tau$. Moreover, $\kappa \leq m_e - 3$ yields $(m-1) - \tau \geq 2e$, implying $m - \tau - e > e$. Hence the longest sequence of "0" in the p-ary expansion of s_1 is at the end of the word above. Note that we are assuming $d > 3$ when $p = 2$; so we cannot have $\tau = 1$ with $p = 2$, implying that the first symbol cannot be zero. Thereby s_1 is the leader of its cyclotomic coset.

Suppose now that $\tau = 0$. As $\widehat{B}(d)$ is not a p-ary RM code, $d_0 > 2$ implying $p > 3$. The p-ary expansion of s_1 is

$$(\overset{0}{d_0 - 2}, \underbrace{0, \cdots, 0}_{e-1}, \overset{e}{1}, \underbrace{0, \cdots, 0}_{m-e-1})$$

with $m - e \geq 2e$; clearly, $s_1 > d$ and s_1 is the leader of $\mathrm{cl}(s_1)$. So in any case, s_1 is not in T_d, completing the proof. □

Lemma 7: Notation is that of (13) and (14); $s(d)$ is given by (15). Assume that $\kappa \in \{m_e - 2, m_e - 1\}$, $m_e \geq 3$, and d such that $\tau < m - 2$. Moreover, we do not treat this situation

$$\tau = m - 3,\ e = 2,\ p = 2,\ d = 2^{m-2} - 1. \tag{16}$$

Set

$$s_2 = s(d) + p^{\tau-(e-1)}(p^e - 1).$$

Then $s(d) \in T_d$ and $s_2 \notin T_d$.

Proof: It remains to prove that $s_2 \notin T_d$. The p-ary expansion of s_2 is the word

$$(p-1, \cdots, p-1, \overset{\tau+1-e}{p-2}, \underbrace{p-1 \cdots, p-1, 0}_{e-1}, \overset{\tau+1}{1}, \underbrace{0, \cdots, 0}_{m-\tau-2}) \tag{17}$$

Obviously, $s_2 > d$. We want to determine the leader of the cyclotomic coset of s_2. Note that, by hypothesis, $e \leq \tau < m-2$. Then $m - \tau - 2 > 0$, which means that there is at least one "0" at the end of the word above.

When $\tau < m - 3$, there is at least two consecutive zeros at the end of the word. On the left of the label $\tau + 1$, there is only one sequence of at most two consecutive zeros; it is "00" if and only if $e = 2$ and $p = 2$. So it is clear that s_2 is the leader of $\mathrm{cl}(s_2)$ unless $\tau = m - 4$, $e = 2$, and $p = 2$. But in this case the 2-ary expansion of s_2 is $(1, \cdots, 1, 0, 0, 1, 0, 0)$, proving that s_2 is the leader.

Suppose now that $\tau = m - 3$—i.e., the word above ends in the sequence "010." When $\{e > 2\}$ or $\{e = 2, p > 2\}$, either there is no other zero in the word $(p > 2)$ or we have this configuration

$$(1, \cdots, 1, \overset{\tau+1-e}{0}, \underbrace{1 \cdots, 1, 0}_{e-1}, \overset{\tau+1}{1}, 0)$$

where $e - 1 \geq 2$ and $\tau + 1 - e \geq 1$ yield that s_2 is the leader of $\mathrm{cl}(s_2)$. So it remains to examine the case $\tau = m - 3$, $e = 2$, $p = 2$, for $d < 2^{m-2} - 1$ (since we do not treat (16)). The 2-ary expansion of s_2 is here

$$(1, \cdots, 1, 1, 0, 0, 1, 0).$$

Clearly, the leader of $\mathrm{cl}(s_2)$ has 2-ary expansion

$$(1, 0, 1, \cdots, 1, 0, 0)$$

proving it is greater than or equal to d, completing the proof. □

Theorem 8 The permutation group of $\widehat{B}(d)$, the extended BCH code of designed distance d and length p^m, is the semi-affine group $A\Gamma L(1, p^m)$, except for the few cases we describe below.

1) When $p = 2$, the permutation group is actually the automorphism group denoted by Aut( ); we have
   a) The trivial BCH codes $\widehat{B}(1)$ and $\widehat{B}(2^m - 1)$, whose automorphism group is $\mathrm{Sym}(2^m)$.
   b) BCH codes which are RM codes. That is, $\widehat{B}(3)$, $\widehat{B}(2^{m-1} - 1)$, and $\widehat{B}(7)$ when $m = 5$. The automorphism group is $\mathrm{AGL}(m, 2)$.
   c) For m even and $d = 2^{m-1} - 2^{(m-2)/2} - 1$, $\mathrm{Aut}(\widehat{B}(d)) = A\Gamma L(2, 2^{m/2})$.
   d) When $m = 6$, then $\mathrm{Aut}(\widehat{B}(7)) = A\Gamma L(2, 2^3)$ and $\mathrm{Aut}(\widehat{B}(15)) = A\Gamma L(3, 2^2)$.
2) When p is odd, the only exceptions are trivial BCH codes and BCH codes which are p-ary RM codes:
   a) $\mathrm{Per}(\widehat{B}(1))$ and $\mathrm{Per}(\widehat{B}(p^m - 1))$ are $\mathrm{Sym}(p^m)$.
   b) $\mathrm{Per}(\widehat{B}(2))$ and $\mathrm{Per}(\widehat{B}(p^{m-1}(p-1) - 1))$ are $\mathrm{AGL}(m, p)$.

c) For $m = 2, p > 3$, and $d = p^2 - 2p - 1$, $\mathrm{Per}(\widehat{B}(d)) = \mathrm{AGL}(2,p)$.

d) For $m = 3$ and $p = 3$ then $\mathrm{Per}(\widehat{B}(5)) = \mathrm{AGL}(3,p)$.

In any case, when the group of the extended BCH code is AGL (resp., AΓL) then the group of the BCH code is the corresponding group GL (resp., ΓL).

Proof: All exceptions were treated before. BCH codes which are RM codes are given by Lemma 5. Exception 1.c) is given by Proposition 5. Exceptions 1d) appeared in Examples 5 and 6, in Section III-A. Note that the binary exceptions were already found by Lu [26]; partial results on binary BCH codes were given in [6], [26], [27]. In all these works, results were obtained by means of Theorem 1.

Notation is now that of (13) and (14). In any situation we want to apply Theorem 7, proving that $\widehat{B}(d)$ is not invariant under $\mathrm{AGL}(m_e, p^e)$. We have found $s(d)$ and t such that $s(d) \in T_d$, $t \prec s(d)$ and $s = s(d) + t(p^e - 1)$ not in T_d in the following cases:

- $\kappa \in [0, m_e - 3]$, $m_e \geq 3$ (Lemma 6, s is s_1 and $t = p^{\tau-1}$ or 1).
- $\kappa \in \{m_e - 2, m_e - 1\}$, $m_e \geq 3$ and d such that $\tau < m-2$, unless when parameters satisfy (16) (Lemma 7, s is s_2, $t = p^{\tau-(e-1)}$).

In Example 6 we solved the case where parameters satisfy (16). So it remains to examine the cases: $m_e = 2$, for $\tau < m - 2$, and $m_e \geq 2$, for $\tau \in \{m-2, m-1\}$. In all these cases we will exhibit $s(d)$, t, and s which contradict (11).

1) Assume that $m_e = 2$, $\tau < m - 2$, and $\kappa = 1$. Note that $e = 2$ and $\tau < m - 2$ imply $\kappa = 0$. So we have $e > 2$. Then we get for s the element s_2 given by Lemma 7. In this case, its p-ary expansion (17) is such that it cannot be a sequence "00" before the label $\tau + 1$, because $e > 2$. Moreover, the word cannot begin with a zero, because $\tau \geq e$.

2) Assume that $m_e = 2$ and $\kappa = 0$; $s(d)$ is given by (15). When $p > 2$ we get $t = 1$, $s = s(d) + p^e - 1$. The p-ary expansion of s has this form

$$(\underbrace{p-2, p-1 \cdots}_{e}, \underbrace{1, 0, \cdots}_{e})$$

proving that $s > d$ and s is the leader of $\mathrm{cl}(s)$. So $s \notin T_d$. Suppose now that $p = 2$. We can suppose that $d > 3$, implying $e > 2$; moreover, $\{e = 3$ and $d = 7\}$ is also an exception. When $e = 3$ and $d = 5$, then $s(d) = 3$ and $s = 10$ (i.e., $3 + (2^3 - 1)$) which is not in T_5. So we assume $e \geq 4$ and $\tau \geq 2$. We get $s = s(d) + 2(2^e - 1)$. When $d \in \{5, 7\}$, then $s(d) = 3$ and $s = 1 + 2^{e+1}$. The leader of $\mathrm{cl}(s)$ is $1 + 2^{e-1}$, which is greater than 7; hence $s \notin T_d$. Assuming $d > 7$, the 2-ary expansion of s is now

$$(1, 0, 1, \cdots, \overbrace{1}^{\tau-1}, \underbrace{0, \cdots, 0}_{e-\tau+1}, 1, \underbrace{0, \cdots, 0}_{e-2}).$$

As $\tau \geq 3$, $e - \tau + 1 \leq e - 2$; moreover, $e - 2 > 2$. So $s \geq d$ and s is the leader of $\mathrm{cl}(s)$, proving $s \notin T_d$.

3) Assume that $\tau \in \{m-2, m-1\}$, $m_e \geq 2$ (here we have: $\kappa \geq 1$). We first suppose that there is a j such that $j < \tau$ and $d_j < p - 1$. Let θ be the biggest such j. If $\theta + e < \tau$ then $d_{\theta+e} = p - 1$ and $d_\theta < p - 1$. From Corollary 5, $\widehat{B}(d)$ cannot be invariant under $\mathrm{AGL}(m_e, p^e)$. So we can suppose $\tau - e \leq \theta$. We get

$$s(d) = \sum_{i=0}^{\tau-1} (p-1)p^i + (d_\tau - 1)p^\tau$$

and

$$s = s(d) + p^{\tau-e}(p^e - 1).$$

Clearly, $s(d) \in T_d$ and $p^{\tau-e} \prec s(d)$; as $\tau - e \leq \theta$, $s \geq d$. If $\tau = m - 1$, then $p > 2$ and $d_\tau \leq p - 2$. The p-ary expansion of s is

$$(\cdots, \underbrace{p-1 \cdots p-1, p-2}_{e}, \underbrace{p-1 \cdots p-1, d_\tau}_{e})$$

proving that s is the leader of $\mathrm{cl}(s)$. Now suppose that $\tau = m - 2$. When $p > 2$, s is the leader of $\mathrm{cl}(s)$, because there is only one zero in its p-ary expansion—the last symbol. When $p = 2$, the 2-ary expansion of s is

$$(\cdots, \underbrace{1 \cdots 1}_{e-2}, 0, \underbrace{1 \cdots 1}_{e}, 0).$$

Clearly, s is the leader of $\mathrm{cl}(s)$, when $m_e \geq 3$. If $m_e = 2$ the leader s' of $\mathrm{cl}(s)$ has 2-ary expansion

$$(\underbrace{1 \cdots 1}_{e}, 0, \underbrace{1 \cdots 1}_{e-2}, 0).$$

So $s \notin T_d$ if and only if $d \leq s'$. But $d > s'$ means $d = 2^{m-1} - 2^{(m-2)/2} - 1$ which is Exception 1c), completing the proof when θ exists.

We suppose now that θ does not exist. So

$$d = \sum_{i=0}^{\tau-1} (p-1)p^i + d_\tau p^\tau.$$

If $p = 2$ then $\tau = m - 2$ and $\widehat{B}(d)$ is an RM code (see 1b)). From now on $p > 2$. When $\tau = m - 2$ we get $s(d) = d - p^\tau$, $t = p^{m-1-e} + p^{\tau-e}$, and

$$s = s(d) + t(p^e - 1) = d + p^{m-1} - p^{m-1-e} - p^{\tau-e}.$$

s cannot be in T_d because there is no zero in its p-ary expansion. When $\tau = m - 1$ we get $s(d) = d - p^{\tau-1}$, $t = p^{\tau-e}$, and

$$s = s(d) + t(p^e - 1) = d + p^\tau - p^{\tau-1} - p^{\tau-e}.$$

As $\widehat{B}(d)$ is not an RM code, $d_\tau < p - 2$ (so $p > 3$). In the p-ary expansion of s, the only symbols which are not $p-1$ are $s_\tau = d_\tau + 1$, $s_{\tau-1} = p - 2$, and $s_{\tau-e} = p - 2$; so all symbols are greater than d_τ, proving $s \notin T_d$. In both cases ($\tau = m - 2$ or $m-1$), we have clearly $s(d) \in T_d$ and $t \prec s(d)$, completing the proof of the theorem. □

V. Conclusion

The aim of our work is the effective determination of permutation groups of affine-invariant codes. At the end of this paper, we think that we have presented the main tools and that for any given code the characterization of its permutation group can be achieved. However, we are convinced that many other simplifications, analogous to those given by Corollary 5 can be obtained.

We did not study infinite classes of codes defined on an extension field, except in Section III-C3. Of course, the immediate open problem is the group of the q-ary BCH codes, $q = p^r$ and $r > 1$. We think that the complication comes from the obligation to study separately the different values of r. We strongly conjecture that the results will be close to the results we obtained for p-ary BCH codes. Indeed, we think that a large part of our proof, when $r = 1$, can be generalized. Moreover, we are convinced that there are special 2^r-ary BCH codes, generalizing results of Theorem 8 in the binary case. We are confirmed in our idea by many numerical results: only BCH codes of very small (or very large) dimension could have a permutation group larger than $\mathrm{GL}(1, p^m)$ (when the Frobenius mappings are not taken in account). When $p = 2$ we found exceptions analogous to those given in Theorem 8c) for binary BCH codes.

In fact there is a possibility to describe by antichains of $(S, \ll_e)$ the codes invariant under $\mathrm{AGL}(m/e, p^e)$ and maybe it is a good way for classification of q-ary codes whose permutation group is greater than the affine group. We have only indicated this way by Proposition 4.

During this work we did not pay much attention to the problem of the permutation group of any cyclic code. It is possible that some material can be used for specific classes. We have noticed some possibilities of extensions of our Theorem 7 which is obtained from the general definition of permutations of cyclic codes. Finally, we must specify the basic difference between our work and the recent work of Huffman dealing with the extended generalized quadratic residue codes. These codes are nontrivial linear codes of length $p^m + 1$ over an alphabet field which is not of characteristic p. Their automorphism groups, which contain $\mathrm{PSL}(2, p^m)$, were completely determined in [20].

Recently, Berger proved that the automorphism group of an affine-invariant code is exactly the group generated by its permutation group and the scalar multiplications [9].

Acknowledgment

The authors wish to express their gratitude to E. F. Assmus, Jr., C. Huffman, J. D. Key, and F. Laubie for many discussions that were really stimulating for this research. They would like to thank anonymous referees for careful reading of the manuscript and for many useful suggestions that greatly improved the manuscript.

References

[1] E. F. Assmus, Jr., and J. D. Key, "Designs and their codes," in *Cambridge Tracts in Mathematics*. Cambridge, UK: Cambridge Univ. Press, 1992.
[2] ——, "Codes and finite geometries," INRIA Rep. 2027, Sept. 1993.
[3] T. P. Berger, "A direct proof for the automorphism group of the extended Reed–Solomon codes," in *EUROCODE'90, LNCS*. Berlin, Germany: Springer-Verlag pp. 21–29.
[4] ——, "Sur le groupe d'automorphismes des codes cycliques étendus primitifs affine-invariants," Thèse, Université de Limoges, Limoges, France, 1991.
[5] T. P. Berger and P. Charpin, "The automorphism group of Generalized Reed-Muller codes," *Discr. Math.*, vol. 117, pp. 1–17, 1993.
[6] T. P. Berger, "The automorphism group of double-error-correcting BCH codes," *IEEE Trans. Inform. Theory*, vol. 40, no. 2, pp. 538–542, Mar. 1994.
[7] ——, "On the automorphism groups of affine-invariant codes," *Des., Codes Cryptogr.*, vol. 7, pp.. 215–221, 1996.
[8] ——, "Classification des permutations d'un corps fini contenant le groupe affine," *C. R. Acad. des Sciences de Paris*, ser. I, pp. 117–119, 1994.
[9] ——, "Automorphism groups and the permutation groups of affine-invariant codes," to be published in *Proc. 3rd Int. Conf. on Finite Fields and their Applications* (Lecture Note Series of the London Math. Soc.), (Glasgow, Scotland, July 11–14, 1995). Cambridge, UK: Cambridge Univ. Press.
[10] S. D. Berman, "On the theory of group codes," *Kibernetica*, vol. 1, no. 1, pp. 31–39, 1967.
[11] P. Charpin, "Codes cycliques étendus invariants sous le groupe affine," Thèse d'Etat, Université Paris 7, LITP 87-6, Paris, France.
[12] ——, "Codes cycliques étendus et idéaux principaux d'une algèbre modulaire," *C. R. Acad. des Sciences de Paris*, vol. .295, ser. I, pp 313–315, 1982.
[13] ——, "The extended Reed–Solomon codes considered as ideals of a modular algebra," *Ann. Discr. Math.*, vol. 17, pp. 171–176, 1983.
[14] ——, "Codes cycliques étendus affines-invariants et antichaines d'un ensemble partiellement ordonné," *Discr. Math.* vol. 80, pp. 229–247, 1990.
[15] ——, "On a class of primitive BCH-codes," *IEEE Trans. Inform. Theory*, vol. 36, no. 1, pp. 222–228, January 1990.
[16] P. Charpin and F. Levy-dit-Vehel, "On self-dual affine-invariant codes," *J. Comb. Theory*, ser. A, vol. 67, no. 2, pp. 223–244, Aug. 1994.
[17] P. Delsarte, "On cyclic codes that are invariant under the general linear group," *IEEE Trans. Inform. Theory*, vol. IT-16, no. 6, Nov. 1970.
[18] P. Delsarte, J. M. Goethals, and F. J. MacWilliams "On generalized Reed–Muller codes and their relatives," *Inform. Contr.*, vol. 16, pp. 403–442, 1974.
[19] A. Dür, "The automorphism groups of Reed–Solomon codes," *J. Comb. Theory*, ser. A, vol. 44, no. 1, 1987.
[20] W. C. Huffman, "The automorphism group of the generalized quadratic residue codes," *IEEE Trans. Inform. Theory*, vol. 41, no. 2, pp. 378–386, Mar. 1995.
[21] W. M. Kantor, "Linear groups containing a Singer cycle," *J. Algebra*, vol. 62, pp. 232–234, 1980.
[22] T. Kasami, S. Lin, and W. W. Peterson, "Some results on cyclic codes which are invariant under the affine group and their applications," *Inform. Contr.*, vol. 11, pp. 475–496, 1967.
[23] W. Knapp and P. Schmidt, "Codes with prescribed permutation group," *J. Algebra*, vol. 67, pp. 415–435, 1980.
[24] F. Laubie, "Codes idéaux de certaines algèbres modulaires et ramification," *Commun. in Algebra*, vol. 15, no. 5, pp. 1001–1006, 1987.
[25] R. Lidl and H. Niederreiter, *Finite Fields*. Cambridge, UK: Cambridge Univ. Press.
[26] C. C. Lu, "The automorphism groups of binary primitive BCH codes," Ph.D. dissertation, Dept. Elec. Engi., Univ. Southern Carolina, Los Angeles, CA, Aug. 1987.
[27] C. C. Lu and L. R. Welch, "On automorphism groups of binary primitive BCH codes," in *Proc. 1994 IEEE Int. Symp. on Information Theory* (Trondheim, Norway), p. 51.
[28] F. J. Macwilliams and N. J. A. Sloane *The Theory of Error Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1986.