
Designs, Codes and Cryptography, 18, 29–53 (1999)

The Automorphism Groups of BCH Codes and of Some Affine-Invariant Codes Over Extension Fields

THIERRY P. BERGER thierry.berger@unilim.fr
UFR des Sciences de Limoges, 123 av. A. Thomas, 87060 Limoges Cedex, France

PASCALE CHARPIN pascale.charpin@inria.fr
INRIA, Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le Chesnay Cedex, France

Dedicated to the memory of E. F. Assmus

Received June 2, 1998; Revised November 10, 1998; Accepted November 24, 1998

Abstract. Affine-invariant codes are extended cyclic codes of length p^m invariant under the affine-group acting on $\mathbb{F}_{p^m}$. This class of codes includes codes of great interest such as extended narrow-sense BCH codes. In recent papers, we classified the automorphism groups of affine-invariant codes [2], [5]. We derive here new results, especially when the alphabet field is an extension field, by expanding our previous tools. In particular we complete our results on BCH codes, giving the automorphism groups of extended narrow-sense BCH codes defined over any extension field.

Keywords: cyclic code, extended cyclic code, affine-invariant codes, BCH codes, GRM codes, permutation group, automorphism group.

1. Introduction

In a recent paper we gave a classification of permutation groups of affine-invariant codes [5]. We developed several tools designed for the effective characterization of these groups and presented some examples, mainly on codes defined on a prime field. In particular we described precisely the permutation groups of extended narrow-sense BCH codes defined over any prime field. Berger proved later that the automorphism group of any affine-invariant code is simply deduced from its permutation group [3]. The aim of this paper is to give more applications of our previous work, especially when the alphabet field is an extension field.

We first recall the terminology and the main results that are presented in [5] and [3]. We recall that two affine-invariant codes are generally not equivalent. We notice that affine-invariant codes with large automorphism group can be easily constructed.

Our main results are presented in Section 4 which is devoted to the effective determination of some automorphism groups. We begin (in Section 4.2) by giving an improvement of our previous result about the link between the BCH bound of a given affine-invariant code and its permutation group. Theorem 8 is a generalization of [5, Corollary 5]. Its main consequence is Corollary 1 which will be of most interest later for the determination of the automorphism groups of BCH codes. In Section 4.3 we describe the automorphism groups of affine-invariant codes which are extensions of cyclic codes with few zeros. Proposition 1 is an immediate generalizations of [5, Proposition 5]. Thus the most important results are

given by Theorem 9: we determine the automorphism groups of some extended cyclic codes whose generator polynomial is the product of three cyclotomic classes.

The last section is devoted to automorphism groups of extended BCH codes whose alphabet field is any extension field. The main result of this paper is the determination of these groups (Theorem 10). Although we here generalize [5, Theorem 8] the proof necessitates new tools especially those presented in Section 4.2.

The proofs of Section 4 are technical and special notation is necessary, which is presented in Section 4.1. Main notation of the paper is listed at the end, in the Annex.

2. Preliminaries

We will use the following terminology throughout. The alphabet field $\mathbb{F}_q$, $q = p^r$ and p is any prime, will be denoted by $\mathbf{k}$. Let G be an extension field of $\mathbf{k}$ of degree m'; the field G will generally be identified with $\mathbb{F}_{p^m}$, $m = rm'$. We consider linear codes of length p^m over $\mathbf{k}$. So G is viewed as the *support-field* and the coordinate positions of the codewords are labelled by the elements of G.

Let $\mathcal{A} = \mathbf{k}[(G, +)]$ be the group algebra of the additive group of G over the field $\mathbf{k}$. An element x of $\mathcal{A}$ is a formal sum:

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

Addition and multiplication are as follows:

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

and

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

In this paper $\mathcal{A}$ is the ambient space. Codes are subspaces of $\mathcal{A}$ and codewords are elements of $\mathcal{A}$. An extensive study of codes of $\mathcal{A}$ is to be found in [1] and [7].

Let $Sym(G)$ be the symmetric group acting on G. Any permutation σ in $Sym(G)$ acts naturally on the elements of $\mathcal{A}$,

$$\sigma \left(\sum_{g \in G} x_g X^g \right) = \sum_{g \in G} x_g X^{\sigma(g)}.$$

DEFINITION 1 *The permutation group $Per(C)$ of any code C is the subgroup of $Sym(G)$ which leaves the code globally invariant. More precisely, in the ambient space $\mathcal{A}$, it is the subgroup of those σ satisfying*

$$\sum_{g \in G} x_g X^{\sigma(g)} \in C \quad \textit{for all } \mathrm{x} = \sum_{g \in G} x_g X^g, \quad \mathrm{x} \in C .$$

DEFINITION 2 *Let $n = p^m - 1$. Let us denote by $\mathbf{a} = (a_g)_{g\in G}$ any element of $(\mathbf{k}^*)^{p^m}$, where $\mathbf{k}^* = \mathbf{k} \setminus \{0\}$. The monomial group $\mathcal{M}_n(\mathbf{k}) = (\mathbf{k}^*)^{p^m} \rtimes Sym(G)$ is the set of transformations $(\mathbf{a}; \sigma)$ which acts on $\mathcal{A}$ as follows:*

$$(\mathbf{a}; \sigma)\left(\sum_{g\in G} x_g X^g\right) = \sum_{g\in G} a_g x_g X^{\sigma(g)},$$

The automorphism group $Aut(C)$ of a code C is then the subgroup of $\mathcal{M}_n(\mathbf{k})$ which leaves the code globally invariant.

2.1. Affine-Invariant Codes

For any divisor e of m, we can consider G as a vector-space of dimension m/e over the subfield $\mathbb{F}_{p^e}$. Then we have the following subgroups of the symmetric group $Sym(G)$:

- The group of the Frobenius mappings

$$\gamma_{p^k} : g \longmapsto g^{p^k}.$$

- The *linear group* $GL(m/e, p^e)$, which is the group of $\mathbb{F}_{p^e}$-linear permutations of G.
- The *affine group* $AGL(m/e, p^e)$, which is the group generated by the linear group $GL(m/e, p^e)$ and by the *translations* of G—i.e. those mappings $g \to g + b, b \in G$. In particular

$$AGL(1, p^m) = \{\sigma_{a,b} : g \longmapsto ag + b,\ a \in G^*,\ b \in G\},$$

  where $G^* = G \setminus \{0\}$.
- The *semi-linear group* $\Gamma L(m/e, p^e)$, which is the group generated by the linear group $GL(m/e, p^e)$ and by the Frobenius mapping γ_p.
- The *semi-affine group* $A\Gamma L(m/e, p^e)$, which is the group generated by the affine group $AGL(m/e, p^e)$ and by the Frobenius mapping γ_p.

DEFINITION 3 *An affine-invariant code is a proper subspace of $\mathcal{A}$ invariant under the affine permutations acting on G. In other words it is a code of $\mathcal{A}$ whose automorphism group contains $AGL(1, p^m)$.*

Let $\sigma_{a,b} \in AGL(1, p^m)$. Then for any x $\in \mathcal{A}$

$$\sigma_{a,b}(\mathrm{x}) = \sum_{g\in G} x_g X^{ag+b} = X^b \sum_{g\in G} x_g X^{ag}.$$

One can say that x is *shifted* by a and *translated* by b. The definition of the *extension* of codes here is the usual one: an overall parity-check symbol is added to each codeword; it

is labelled by "0" and is such that the sum of all symbols of the extended codeword is zero. Translation corresponds to multiplication by X^b in $\mathcal{A}$.

The algebra $\mathcal{A}$ has only one maximal ideal, called its *radical*, which is the set of all codewords x satisfying $\sum_{g\in G} x_g = 0$. So it is clear that a code C, which is a proper subspace invariant under $AGL(1, p^m)$, is an ideal of $\mathcal{A}$ and is an extended cyclic code. On the other hand, Kasami, Lin, and Peterson characterized affine-invariant codes by a combinatorial property of their defining sets [12]. We will define a partial order, on the set $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n, and present their result in this context. This point of view was first developed by Charpin in [6].

We first state the definition of extended cyclic codes in $\mathcal{A}$. A complete description of cyclic codes and of their extension can be found in [7].

DEFINITION 4 *Let $n = p^m - 1$ and let us define, for any $s \in [0, n]$, the* **k***-linear maps of $\mathcal{A}$ into G:*

$$\phi_s\left(\sum_{g\in G} x_g X^g\right) = \sum_{g\in G} x_g g^s, \tag{1}$$

where, by convention, $0^s = 0$ for $s > 0$ and $0^0 = 1$; note that $\phi_0(\mathrm{x}) = \sum_{g\in G} x_g$.

Let T be a subset of $[0, n]$, containing 0 and invariant under multiplication by q (mod n). The extended cyclic code C with defining set T is defined as follows:

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

Denoting by S the set $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n, the defining set of any extended cyclic code is a subset of S. Any $s \in S$ will often be identified with its p-ary expansion

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

We then define a partial order on S as follows:

$$\forall s, t \in S,\ \ s \preceq t \iff s_i \le t_i, i \in [0, m-1] \tag{2}$$

($s \prec t$ means $s \preceq t$ and $s \neq t$).

THEOREM 1 [Kasami, Lin and Peterson [12]] *An extended cyclic code C of $\mathcal{A}$ with defining set T is affine-invariant if and only if T satisfies*

$$t \in T \ \text{ and } \ s \preceq t \ \Rightarrow\ s \in T\ .$$

Note that the only affine-invariant code containing n in its defining set is the trivial code $\{0\}$.

More generally, for each divisor e of m, we can define the v-ary expansion and the v-weight of any $s \in S$:

$$s = \sum_{i=0}^{m''-1} s_i v^i \quad \text{and} \quad wt_v(s) = \sum_{i=0}^{m''-1} s_i, \quad v_i \in [0, v-1], \tag{3}$$

where $v = p^e$ and $m'' = m/e$. In [9], Delsarte gave a necessary and sufficient condition for a code to be invariant under $AGL(m'', p^e)$ which can also be formulated in terms of a partial order. Let us define, for all $s, t \in S$:

$$s \ll_e t \iff wt_v(p^k s) \leq wt_v(p^k t), \ \forall k \in [0, e-1]. \tag{4}$$

THEOREM 2 [Delsarte [9]] *An extended cyclic code C of $\mathcal{A}$ with defining set T is invariant under $AGL(m'', p^e)$ if and only if T satisfies*

$$t \in T \ \text{ and } \ s \ll_e t \ \Rightarrow \ s \in T.$$

The most important classes of affine-invariant codes are the primitive extended narrow-sense BCH codes and the generalized Reed-Muller (GRM) codes. We now give their definitions.

DEFINITION 5 *Recall that $\mathbf{k} = \mathbb{F}_q$, $q = p^r$ and $m = rm'$. The extended primitive BCH code over $\mathbf{k}$ of length p^m and designed distance δ will be denoted by $B_q(\delta)$; it is the code with defining set*

$$T_\delta = \bigcup_{j=0}^{\delta-1} cl_q(j),$$

where $cl_q(j)$, $1 \leq j \leq p^m - 1$, is the orbit of j under multiplication by q—by convention we suppose that δ is the smallest element of $cl_q(\delta)$.

The primitive BCH code of length $p^m - 1$ and designed distance δ over $\mathbf{k}$ (whose extension is $B_q(\delta)$) will be denoted by $B_q^*(\delta)$.

DEFINITION 6 *For any μ, $1 \leq \mu \leq m'(q-1)$, the GRM-code of length p^m over $\mathbf{k}$ and of index μ is the code $GRM_q(\mu)$ of $\mathcal{A}$ with defining set*

$$L(\mu) = \{t \in S \mid 0 \leq wt_q(t) < \mu\}.$$

The integer $v = m'(q-1) - \mu$ is the order of $GRM_q(\mu)$.

Remark. By applying Theorem 1, one deduces immediately that the definitions above give affine invariant codes.

For instance, consider the code $B_q(\delta)$ with defining set T_δ. Let $t \in T_\delta$ and $s \prec t$. By definition of T_δ, there is $t' \in cl_q(t)$ such that $t' < \delta$. Since $s \prec t$ means $qs \prec qt$—by definition, see (2)—, there is $s' \in cl_q(s)$ such that $s' \prec t'$. Moreover it is clear that $s' \prec t'$ implies $s' < t'$; so $s' < \delta$ which yields $s \in T_\delta$. In the same way, it is easy to prove that $GRM_q(\mu)$ is affine invariant by noticing that $s \prec t$ implies $wt_q(s) < wt_q(t)$.

We determined in [4] the automorphism groups of GRM codes. We state our result for the permutation groups in the next theorem; according to Theorem 5 below, the automorphism group is simply deduced from this.

THEOREM 3 (Berger and Charpin [4]) *The permutation group of $GRM_q(\mu)$ is $AGL(m', q)$, when $1 < \mu < m'(q-1)$. If $\mu = 1$ or $\mu = m'(q-1)$ then $GRM_q(\mu)$ is a trivial code whose permutation group is the symmetric group over G.*

2.2. The Automorphism Groups of Affine-Invariant Codes

The aim of this section is to recall the main tools that we introduced for the classification of the permutation groups of affine-invariant codes. The proofs are to be found in [5, Section II-B]. Our notation is as introduced before.

THEOREM 4 (Berger and Charpin [5, Sect. II-B]) *Let C be a nontrivial affine-invariant code of $\mathcal{A}$ of length p^m over $\mathbb{F}_q$, $q = p^r$, $m = rm'$.*

Then there exist a divisor e of m and a divisor ℓ of e such that the permutation group $Per(C)$ of C is generated by $AGL(m/e, p^e)$ together with the Frobenius mapping γ_{p^ℓ}.

Let T be the defining set of C. Then ℓ is the smallest integer such that T is invariant under multiplication by p^ℓ. Moreover r divides e and ℓ divides r.

Berger [2] proved later that the full automorphism group of any affine-invariant code is easily deduced from its permutation group:

THEOREM 5 ([2]) *If C is a non-trivial affine-invariant code, with permutation group $Per(C)$, then*

$$Aut(C) = \mathbf{k}^* \rtimes Per(C) .$$

More precisely, the elements of $Aut(C)$ are of the form

$$\sum_{g\in G} x_g X^g \mapsto a \sum_{g\in G} x_g X^{\sigma(g)}, \quad a \in \mathbf{k}^*, \quad \sigma \in Per(C) .$$

Thus knowledge of the permutation group is sufficient for the complete description of the automorphism group of any affine-invariant code. In accordance with Theorem 4, this is achieved as soon as we know the values of the two parameters, ℓ and e.

Remark. An affine-invariant code C is an extended cyclic code. The permutation group of the corresponding cyclic codes C^* is the stabilizer of 0 in the permutation group of C. It is not so easy to determine the full automorphism group of C^* from the automorphism group of C. For instance, it is easy to prove that the automorphism group of any Reed-Solomon code C^* contains an element which is not in the direct product $\mathbf{k}^* \times Per(C)$ (see [10]).

In a certain sense, Theorem 4 is only an algorithm. For a large class of affine-invariant codes the permutation group is immediately deduced, especially when m is prime. But generally, and always when the alphabet field is an extension field, the following question

remains open: for a given affine-invariant code C with defining set T, how does one compute its permutation group? Some tools were developed in [5] among which is the next theorem.

For some particular values of m or ℓ, the determination of e is easy: if m is a prime, it is sufficient to verify that the code is not a p-ary Reed-Muller code. If $\ell = m$, the only possibility is $e = m$ and the permutation group is $AGL(1, p^m)$. For the general case, the determination of e is more difficult. There are many situations and then we need several different tools. In particular we state a condition which is equivalent to those of Delsarte [9] and is more efficient (or more easy to handle) in some situations.

THEOREM 6 (Berger and Charpin [5]) *Let C be an affine-invariant code with defining set T. Let e be a divisor of m. Then the code C is invariant under $AGL(m/e, p^e)$ if and only if*

$$t \in T \text{ and } j \preceq t \implies t + j(p^e - 1) \in T.$$

2.3. Equivalent Affine-Invariant Codes

To conclude this section, we want to point out that two distinct affine-invariant codes are generally not equivalent. This was shown recently by Berger [2] to be a consequence of Theorem 5. By saying *two codes are equivalent* we mean that there is a monomial transformation from one code to the other.

THEOREM 7 (Berger [2]) *Two distinct affine-invariant codes, say C and C', are equivalent if and only if C is the image of C' by some Frobenius mapping—i.e. $\gamma_{p^k}(C) = C'$ for some k.*

Any affine-invariant code C and any extended cyclic code C' are equivalent if and only if C is the image of C' by a multiplier—i.e. by $g \mapsto g^t$ for some t prime to $p^m - 1$.

Consider two cyclic codes of length n over $\mathbf{k}$, say C and C'. Assume that $\gcd(n, \varphi(n)) = 1$ where φ is the Euler φ-function. It is well-known that C and C' are equivalent if and only if C is the image of C' by a multiplier (see [11]). Note that Theorem 7 provides a necessary and sufficient condition, without the hypothesis on n, when at least one code is affine-invariant.

Actually Theorem 7 provides important applications. For instance *two self-dual affine-invariant codes can be equivalent* under a Frobenius mapping only. These codes were studied in [8], for characteristic 2 only. In particular, an effective method for constructing several classes of such codes was given.

In general, two distinct affine-invariant binary codes are not equivalent. As an example consider the binary extended cyclic codes which contain the Reed-Muller code of order 1 and are contained in the Reed-Muller code of order 2. All these codes are affine-invariant and we know that there are several pairs of such codes which have the same weight polynomial (see [13]). According to Theorem 7 they are not equivalent.

3. Affine-Invariant Codes with Large Automorphism Groups

In this section we point out that affine-invariant codes, whose permutation group is larger than $AGL(1, p^m)$, exist and can be easily constructed.

If we choose randomly an affine-invariant code defined over $\mathbb{F}_q$, its permutation group will probably be the group generated by γ_q and $AGL(1, p^m)$. The exceptional codes to be presented in Section 4.3 are very particular because their defining sets are very small (two or three cyclotomic cosets). The main family of codes with a large permutation group is that of GRM codes. We will show that exceptional BCH codes over an extension field are essentially GRM codes.

However, there exist a lot of affine-invariant codes with larger permutation groups. For instance, by using either Theorem 2 or Theorem 6, we can construct for each $s \in S$ and each divisor e of m the smallest code containing s in its defining set which is invariant under $AGL(m/e, p^e)$. Generally the codes obtained in this way are not GRM codes.

More precisely *many affine-invariant codes have a permutation group which contains* $AGL(m/r, p^r)$ *for some non trivial divisor* r *of* m.

Example 1. Assume that m has a non-trivial divisor r and consider the poset $(S, \ll_r)$, defined by (4). Let $M(r)$ be an antichain of this poset—i.e. a subset of non-related elements. Let us define

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

By definition of $\ll_r$, we have $qT = T$, $q = p^r$. Moreover the extended cyclic code over $\mathbb{F}_q$, whose defining set is T, is invariant under $AGL(m/r, q)$. This is an obvious corollary of Theorem 2.

Our purpose here is to suggest the characterization of special classes of affine-invariant codes with large permutation groups. For instance, we conjecture that such classes can be found in the set of affine-invariant codes whose defining set T is such that $M(r)$ (see the example above) consists of only one cyclotomic coset. Another question is to determine the smallest defining set T such that the corresponding code is invariant under a given subgroup.

The classification induced by Theorem 4 is complete for binary codes of length 2^m where m is a prime, because e is either 1 or m. In the same way the next class which will probably be easy to study is the class of codes over $\mathbb{F}_4$ whose length is 2^m where $m = 2k$ and k is prime.

4. Automorphism Groups of Some Infinite Classes of Codes

In our previous paper [5], we described the automorphism groups of a number of affine-invariant codes. In this section, we generalize our results on codes with few zeros and on primitive BCH codes in the case where the alphabet field is an extension field. Since the proofs are most technical, we need some precise notation and definitions. We use the terminology of Huffman who presented our work in his chapter for the Handbook of Coding Theory [10].

4.1. Notation

Recall that $n = q^{m'} - 1$, $q = p^r$ and $m' = m/r$. Set $S = [0, n]$ and let e be any divisor of m; set $m'' = m/e$. To any element $s \in S$ associate an m''-tuple

$$s \quad \longleftrightarrow \quad (s_0, s_1, \ldots, s_{m''-1})_{p^e}$$

where $s = \sum_{i=0}^{m''-1} s_i\, p^{ei}$ is the p^e-adic expansion of s. When necessary, we will indicate the length of a string within the associated m''-tuple by a brace beneath the string or the position of an entry (counting from the left starting with 0) by a value above the position in the m''-tuple. For example, if $e = r$ and $m'' = m' = m/r$, for $s = q^{m'} - q^2 - 1$, the associated m'-tuple is

$$(q-1, q-1, \overset{2}{q-2}, \underbrace{q-1, \ldots, q-1}_{m'-3})_q$$

A crucial problem in our proofs is to determine if some element $s \in S$ is the smallest element in its p^e-cyclotomic coset. Notice that the elements of the p^e-cyclotomic coset of s are precisely the elements with associated m''-tuple a cyclic shift of the m''-tuple for s. Notice also that the smallest element of its p^e-cyclotomic coset must have its longest string of 0's (counting cyclic shifts) at the right end of the m''-tuple; if the longest string of 0's is unique, by placing it at the right end of the m''-tuple, we will have the smallest element of its p^e-cyclotomic coset. For example, if $q = 2^2$, $r = e = 2$, $m'' = m' = 5$ and $s = 1 + 2q^3 + 3q^4$, the 4-adic expansion of s and of the smallest element of its 4-cyclotomic coset t are:

$$s = (1, 0, 0, 2, 3)_4 \quad \text{and} \quad t = (2, 3, 1, 0, 0)_4\,. \tag{5}$$

Generally in this section, we will identify s and its p^e-adic expansion:

$$s = (s_0, s_1, \ldots, s_{m''-1})_{p^e}.$$

Using the relation $\preceq$, defined by (2), we need not only the p^e-adic expansion of s but also its p-adic expansion. The p-adic expansion will be placed between brackets; for example, if $s = \sum_{i=0}^{m-1} s'_i\, p^i$, then $s = [s'_0, s'_1, \ldots, s'_{m-1}]$. Moreover, we will simultaneously use both notation: if $s = (s_0, s_1, \ldots, s_{m''-1})_{p^e}$ and $s_0 = \sum_{i=0}^{e-1} s_{0,i}\, p^i$, then we write $s_0 = [s_{0,0}, s_{0,1}, \ldots, s_{0,e-1}]$ and

$$s = ([s_{0,0}, s_{0,1}, \ldots, s_{0,e-1}], s_1, \ldots, s_{m''-1})_{p^e}.$$

In (5), we have $s = ([1, 0], 0, 0, [0, 1], [1, 1])_4$.

DEFINITION 7 *Let C be an affine-invariant code with defining set T. Let e be a divisor of m. A disqualifying pair (s, t) for e is a pair such that $s \in T$, $t \preceq s$, but $s' = s + t(p^e - 1) \notin T$.*

According to Theorem 6, a code C is not invariant under $AGL(m/e, p^e)$ if and only if a disqualifying pair for e exists.

4.2. BCH-Bounds and Permutation Groups of Affine-Invariant Codes

DEFINITION 8 *The BCH-bound of an affine-invariant code C with defining set T is the smallest integer $\delta \in [0, n]$ such that δ is not in T.*

Denote by $T^\perp$ the defining set of $C^\perp$—the dual of C. Note that $C^\perp$ is clearly affine-invariant. The next result is easily deduced from the relation

$$T^\perp = \{n - s | s \notin T\}.$$

LEMMA 1 *If δ' is the biggest element of the defining set of an affine-invariant code C, then $n - \delta'$ is the BCH-bound of $C^\perp$.*

THEOREM 8 *Let C be an affine-invariant code with defining set T and BCH-bound δ. Let e be a divisor of m and $m'' = m/e$. If C is invariant under $AGL(m'', p^e)$, then*

$$\delta_{m''-1} \preceq \delta_{m''-2} \preceq \cdots \preceq \delta_1 \preceq \delta_0, \tag{6}$$

where $\delta = (\delta_0, \ldots, \delta_{m''-1})_{p^e}$ is the p^e-adic expansion of δ.
More precisely, if $\delta_i \geq p^j$ for some j, then $p^{j+1} - 1 \preceq \delta_{i-1}$.

Proof. Note, for clarity, that

$$p^{j+1} - 1 = [p - 1, p - 1, \ldots, \overset{j}{p - 1}, 0, \ldots, 0] .$$

Let $0 < i \leq m'' - 1$. To prove our theorem, it is sufficient to prove that $(p - 1)p^j \preceq \delta_{i-1}$ for all j such that $\delta_i \geq p^j$. Indeed, assuming that this property is satisfied, let i be given and denote by j_0 the greatest integer j such that $\delta_i \geq p^j$. Then we clearly have

$$\delta_i = [\delta_{i,0}, \ldots, \delta_{i,j_0}, 0, \ldots, 0] \preceq [p - 1, \ldots, \overset{j_0}{p - 1}, 0, \ldots, 0] = p^{j_0+1} - 1 .$$

But, by hypothesis, $(p - 1)p^j \preceq \delta_{i-1}$, for all $j \leq j_0$. So

$$p^{j_0+1} - 1 = [p - 1, \ldots, \overset{j_0}{p - 1}, 0, \ldots, 0] \preceq \delta_{i-1},$$

implying $\delta_i \preceq \delta_{i-1}$ (for any i).

Let $s = (p^e - 1, \ldots, p^e - 1, \overset{i}{\delta_i - p^j}, \delta_{i+1}, \ldots, \delta_{m''-1})_{p^e}$, for any j such that $\delta_i \geq p^j$. By construction, $s < \delta$, and thus s is in the defining set T. Note that

$$s_{i-1} = [\underbrace{p - 1, \ldots, p - 1}_{e}] \text{ where } s = (s_0, s_1, \ldots, s_{m''-1})_{p^e} .$$

Now set $t = p^{e(i-1)+j}$. Since $p^j \preceq s_{i-1}$, then t satisfies $t \preceq s$. The pair (s, t) cannot be a disqualifying pair for e, since the code C is invariant under $AGL(m'', p^e)$ (see Definition 7). So $s' = s + t(p^e - 1)$ is in T, from Theorem 6. Note that $s' = s + (p^{ei+j} - p^{e(i-1)+j})$;

more precisely s and s' differ only in the $(i-1)$th and the ith symbols. We have

$$s'_{i-1} = [p-1, \ldots, p-1, \overset{j}{p-2}, p-1, \ldots, p-1] = p^e - 1 - p^j$$

and $s'_i = s_i + p^j = \delta_i$.

Since $s' \in T$ and $\delta \notin T$, it is impossible to have $\delta \preceq s'$ (see Theorem 1). But $\delta \not\preceq s'$ if and only if $\delta_{i-1} \not\preceq s'_{i-1}$. Indeed, $\delta_k \preceq s'_k$, for $k < i-1$, because $s'_k = p^e - 1$; moreover $\delta_k = s'_k$ for $k \geq i$. The condition $\delta_{i-1} \not\preceq s'_{i-1}$ implies clearly $\delta_{i-1,j} = p-1$, i.e. $(p-1)p^j \preceq \delta_{i-1}$, completing the proof of (6).

Suppose that $\delta_i \geq p^j$ for some j. We have proved that for any $k \leq j$ we have $(p-1)p^k \preceq \delta_{i-1}$. This means $p^{j+1} - 1 \preceq \delta_{i-1}$ completing the proof. ∎

Example 2. Suppose that m is even, $m \geq 6$. Consider an affine-invariant code C on $\mathbb{F}_q$ with BCH-bound $\delta = p^{m/2+2} + p^{m/2+1} + p^2 + 1$. Then the p-adic expansion of δ is

$$\delta = [1, 0, 1, \underbrace{0, \ldots, 0}_{m/2-2}, 1, 1\underbrace{0, \ldots, 0}_{m/2-3}] .$$

Let e be a divisor of m, $e > 1$. It is clear that if $e \neq m$, then there is an $i > 0$ such that $\delta_i > p$. If C satisfies the hypothesis of Theorem 8, this implies $p^2 - 1 \preceq \delta_{i-1} \preceq \delta_0$ which is impossible. So $e = m$, implying that the permutation group of C is $\langle AGL(1, p^m), \gamma_q \rangle$.

Suppose that the code C is any extended BCH code of designed distance δ over $\mathbb{F}_q$—i.e. the code $B_q(\delta)$. We are going to prove that, according to the hypothesis of Theorem 8, we obtain the precise form of δ for a large set of values of δ. In the sequel T denotes the defining set of $B_q(\delta)$ and $T^\perp$ the defining set of $B_q^\perp(\delta)$. We do not treat binary codes, whose automorphism groups are known (see our previous paper [5]).

COROLLARY 1 *Using notation as before, suppose that the code $B_q(\delta)$ is invariant under $AGL(m'', p^e)$. Moreover we suppose that δ, q and e are such that*

$$q \neq 2, \quad p^e \leq \delta \quad \textit{and} \quad \delta \neq p^m - 1$$

(where δ is the smallest element of its q-cyclotomic coset).

Then the q-adic expansion of δ, say $(d_0, \ldots, d_{m'-1})_q$, is

$$\delta = (\underbrace{q-1, \ldots, q-1}_{\kappa}, \ d_\kappa, \underbrace{0, \ldots, 0}_{\lambda})_q, \tag{7}$$

where κ denotes the biggest i such that $d_i \neq 0$ and $\lambda = m' - (\kappa + 1)$. Moreover, if $\delta \leq p^{m-e} - 1$ then $d_\kappa = 1$.

Proof. Recall that $m'' = m/e$, $m' = m/r$, with $q = p^r$. Since $B_q(\delta)$ is invariant under $AGL(m'', p^e)$, r must divide e (see Theorem 4). Set $e = rv$ (note that $p^e = q^v$ and $m' = vm''$). We take the following pair (s, t):

$$s = (q-1, \ldots, q-1, \overset{\kappa}{d_\kappa - 1}, \underbrace{0, \ldots, 0}_{\lambda})_q \ \text{ and } \ t = q^{\kappa - v} .$$

We have clearly $s < \delta$, implying $s \in T$; moreover $t \prec s$, since $v \leq \kappa$ by hypothesis. If $B_q(\delta)$ is invariant under $AGL(m'', p^e)$ then (s, t) cannot be a disqualifying pair for e (see Definition 7). So $s' = s + t(p^e - 1)$ is in T, where

$$s' = (d_\kappa - 1)q^\kappa + (q^\kappa - 1) + q^{\kappa - v}(q^v - 1) = d_\kappa q^\kappa + (q^\kappa - 1) - q^{\kappa - v},$$

with q-adic expansion

$$s' = (\underbrace{q-1, \ldots, q-1}_{\kappa - v}, \overset{\kappa - v}{q-2}, \underbrace{q-1, \ldots, q-1}_{v-1}, \overset{\kappa}{d_\kappa}, \underbrace{0, \ldots, 0}_{\lambda})_q \ .$$

When $\lambda > 0$, s' is the smallest element of its q-cyclotomic coset, since $q > 2$. Assume that $\lambda = 0$, i.e. $\kappa = m' - 1$. As $\delta < p^m - 1$, it follows that $d_\kappa < q - 1$. Moreover we have $v \leq m'/2 \leq \kappa + 1 - v$, since $\kappa = m' - 1$ and v divides m'. This implies $\kappa - v \geq v - 1$, which means that s' is the smallest element of its q-cyclotomic coset. Note that $\kappa = v$ provides $v = 1$, $m' = 2$ and then $s' = (q - 2, d_k)_q$.

Since s' is thus the smallest member of its q-cyclotomic coset in any case, and $s' \in T$, Definition 5 implies that $s' < \delta$. Therefore $d_j = q - 1$ for v consecutive values of j, $j = \kappa - v, \ldots, \kappa - 1$.

First note that $v = 1$ means $e = r$. In this case δ has the form (7), by applying Theorem 8 with $d_{\kappa-1} = \delta_{\kappa-1} = q - 1$. Suppose now that $v > 1$. We have proved that the p^e-adic expansion of δ satisfies:

$$\delta = (\delta_0, \ \ldots, \ \delta_{\xi-1}, \ \delta_\xi, \ \underbrace{0, \ldots, 0}_{\lambda'})_{p^e}$$

where $q^v - q^j \leq \delta_{\xi-1}$, j being the biggest integer such that $q^j - 1 \leq \delta_\xi$, noticing that λ' might be equal to 0. To prove that δ has the form (7) is to prove that $\delta_i = p^e - 1$ for all $i < \xi$. We apply Theorem 8.

- If $j = 0$ then $\delta_{\xi-1} = p^e - 1$ implying $\delta_i = p^e - 1$ for all $i < \xi - 1$, because $\delta_{\xi-1} \preceq \delta_i$.
- Assuming $j > 0$, then $q^j - 1 \preceq \delta_{\xi-1}$, since $q^j / p \leq \delta_\xi$. We have

  $$\delta_\xi = (q - 1, \ \ldots, \ \overset{j-1}{q - 1}, \ d_\kappa, \ 0, \ \ldots, \ 0)_q$$

  and

  $$\delta_{\xi-1} = (\ldots, \ \overset{j}{q - 1}, \ \ldots, \ q - 1)_q \ .$$

  Then $\delta_\xi \preceq \delta_{\xi-1}$ implies that the first j digits of $\delta_{\xi-1}$ (base q) must also be $q - 1$. So $\delta_{\xi-1} = p^e - 1$. Therefore $\delta_i = p^e - 1$ for all $i < \xi - 1$.

In any case, we obtain $d_i = q - 1$ for $i = 1, \ldots, \kappa - 1$, completing the proof of the first part of the theorem.

Now assume that $\delta \leq p^{m-e}-1$, i.e. $\lambda \geq v$ in (7). Let u be the element of the q-cyclotomic coset of s whose q-adic expansion is

$$u = (d_\kappa - 1, \underbrace{0, \ldots, 0}_{\lambda}, \underbrace{q-1, \ldots, q-1}_{\kappa})_q \ .$$

Then u is the biggest element of T. Indeed, any $u' \in T$ such that $u < u'$ has the form $(u'_0, \ldots, u'_\lambda, q-1, \ldots, q-1)_q$. The smallest element in $cl(u')$ will be $(q-1, \ldots, q-1, u'_0, \ldots, u'_\lambda)_q$, and this will be at least δ, contradicting Definition 5.

We deduce that $\delta^\perp$, the BCH-bound of $B_q^\perp(\delta)$, is equal to $p^m - 1 - u$ and has q-adic expansion

$$(q - d_\kappa, \underbrace{q-1, \ldots, q-1}_{\lambda}, \underbrace{0, \ldots, 0}_{\kappa})_q$$

(see Lemma 1). Consider the p^e-adic expansion of $\delta^\perp$, say $(\delta_0^\perp, \ldots, \delta_{m''-1}^\perp)_{p^e}$. As $\lambda \geq v$, the q-adic expansion of $\delta_1^\perp$ has the form $(q-1, \ldots)_q$. But $\delta_1^\perp \preceq \delta_0^\perp$ yields $q - d_\kappa = q-1$. Hence $d_\kappa = 1$, completing the proof. ∎

4.3. Codes with Few Zeros

In this section we apply Theorem 4 to the study of automorphism groups of cyclic codes with few zeros—i.e. of large dimension. Actually we give a precise description of the automorphism group of some cyclic codes with two or three zeros.

DEFINITION 9 *Recall that $q = p^r$ and $m = rm'$; $cl_q(j)$, $1 \leq j \leq n$, is the q-cyclotomic coset of j modulo n. Let a and b be two integers such that $0 < a < b \leq m'/2$. We denote by C_a the extended cyclic code of length p^m, over $\mathbf{k} = \mathbb{F}_q$ whose defining set is*

$$T_a = \{0\} \cup cl_q(1) \cup cl_q(1+q^a) \ .$$

We denote by $C_{a,b}$ the extended cyclic code of length p^m, over $\mathbf{k} = \mathbb{F}_q$ whose defining set is

$$T_{a,b} = \{0\} \cup cl_q(1) \cup cl_q(1+q^a) \cup cl_q(1+q^b) \ .$$

For the definition of the codes C_a, we suppose that $m' \geq 2$; for any code $C_{a,b}$, we suppose $m' \geq 4$.

Remark. Clearly, the codes C_a and $C_{a,b}$ are affine-invariant. By definition, $1+q^a$ and $1+q^b$ are in two different q-cyclotomic cosets and each is the smallest element of its p-cyclotomic coset. According to Theorem 4, the integer ℓ of Theorem 4 is here equal to r, where $q = p^r$: *these codes are q-ary codes.* So we have to determine the parameter e only, i.e. the divisor of m such that the permutation group $Per(C)$ of C is generated by $AGL(m/e, p^e)$ together with the Frobenius mapping γ_{p^r} (see § 2.2).

PROPOSITION 1 *Assume $a \leq m'/2$. Then the permutation group of C_a is the group generated by γ_q and $AGL(1, p^m)$, except for the following cases:*

1. *$q = 2$, $m' = m$ even and $a = m/2$. The permutation group is $A\Gamma L(2, 2^{m/2})$.*
2. *$q = 2$, $m' = m$, $m \equiv 0 \bmod 3$ and $a = m/3$. The permutation group is $A\Gamma L(3, 2^{m/3})$.*
3. *$m' \equiv 0 \bmod 4$ and $a = m'/4$. The permutation group is $\langle AGL(2, q^{m'/2}), \gamma_q \rangle$.*

Proof. The proof is exactly the same as that of [5, Proposition 5] (where the alphabet field is a prime field). ∎

THEOREM 9 *Assume $0 < a < b \leq m'/2$. Then the permutation group of $C_{a,b}$ is $\langle AGL(1, q^{m'}), \gamma_q \rangle$, except for the following cases:*

E_1 *: $q = 2$, $m' = 5a$, $b = 2a$. The permutation group is $\langle AGL(5, 2^a), \gamma_q \rangle$;*

E_2 *: $q = 2$, $m' = 4a$, $b = 2a$. The permutation group is $\langle AGL(4, 2^a), \gamma_q \rangle$;*

E_3 *: $m' = 6a$, $b = 3a$. The permutation group is $\langle AGL(3, q^{2a}), \gamma_q \rangle$, for any q.*

E_4 *: m' even, $a + b = m'/2$ and $a < b$ (for any q):*

- *If $m' = 8a$ and $b = 3a$ then the permutation group is $\langle AGL(4, q^{2a}), \gamma_q \rangle$*
- *otherwise the permutation group is $\langle AGL(2, q^{a+b}), \gamma_q \rangle$.*

We begin by proving a simple lemma.

LEMMA 2 *Let i and j be non-negative integers such that $0 \leq i < j < m'$. Then $q^i + q^j \in T_{a,b}$ if and only if*

$$j - i \quad \text{is one of} \quad a,\ m' - a,\ b \ \text{ or } \ m' - b\ .$$

Proof. Obviously, $q^i + q^j$ is in $T_{a,b}$ if and only if $q^i + q^j$ is either in $cl_q(1 + q^a)$ or in $cl_q(1 + q^b)$. Suppose first that $q^i + q^j$ is in $cl_q(1 + q^a)$. In other words, there is a' in $[0, m' - 1]$ such that

$$q^i + q^j = q^{a'} + q^{a+a'} \pmod{m'}\ .$$

So either $i = a'$, providing $j = a + i$, or $j = a'$, providing $i = a + j - m'$. In the same way we can prove that $q^i + q^j \in cl_q(1 + q^b)$ if and only if either $j = b + i$ or $i = b + j - m'$, completing the proof. ∎

Proof of Theorem 9: For any divisor e of m, our aim is to determine if a given code $C_{a,b}$ is invariant (or not) under $AGL(m/e, p^e)$. We know that the code $C_{a,b}$ is invariant under

$AGL(1, p^m)$ since it is affine invariant. Recall that $\ell = r$ and r must be a divisor of e: $e = rv$. So $m/e = m'/v$ and $q^v = p^e$.

In accordance with Theorem 6, $C_{a,b}$ is invariant under $AGL(m/e, p^e)$ if and only if $T_{a,b}$ satisfies

$$s \in T_{a,b} \text{ and } j \preceq s \implies s + j(q^v - 1) \in T_{a,b}. \tag{8}$$

For s in $cl_q(1)$, $j \preceq s$ yields $j = 0$ or s; in both cases $s + j(q^v - 1)$ is in $cl_q(1)$ and then in $T_{a,b}$. Consider now $s = 1 + q^a$ and let j be such that $j \preceq 1 + q^a$. If $j = 0$ or $j = s$ then $s + j(q^v - 1)$ is in the cyclotomic coset of s. So we have to check (8) only when $j = 1$ or q^a. Similarly, if $s = 1 + q^b$, we have to check (8) only when $j = 1$ or q^b. Thus (8) is satisfied if and only if the following conditions are satisfied:

(**i**) $q^a + q^v \in T_{a,b}$; (**ii**) $1 + q^{a+v} \in T_{a,b}$;

(**iii**) $q^b + q^v \in T_{a,b}$; (**iv**) $1 + q^{b+v} \in T_{a,b}$.

We will determine the cases where **(i)**, **(ii)**, **(iii)** and **(iv)** are satisfied. We remark that

$$0 < a < b \leq m'/2 \leq m' - b < m' - a \ . \tag{9}$$

We distinguish five cases:

1. Suppose $v < a$. We have $0 < a - v < a$. From (9) and Lemma 2 we can deduce $q^a + q^v \notin T_{a,b}$ which contradicts **(i)**.

2. Assume that $a = v$. Assuming **(i)** we have $2q^a \in T_{a,b}$ which yields $q = 2$, $m = m'$ and $e = v = a$. Now the conditions **(ii)**, **(iii)** and **(iv)** become

   $$1 + q^{2a} \in T_{a,b},\ q^a + q^b \in T_{a,b},\ 1 + q^{a+b} \in T_{a,b} \ .$$

   From (9) and Lemma 2, we must have $b - a = a$; therefore $b = 2a$, which yields $1 + q^{2a} \in T_{a,b}$. Moreover $b + a = 3a$ must be either $m - a$ or $m - 2a$ and we have:

   - if $m - 2a = 3a$ then we obtain the exception E_1;
   - if $m - a = 3a$ then we obtain the exception E_2.

3. Suppose that $a < v < b$. The relation $0 < v - a < b$ and the condition **(i)** imply $v - a = a$. On the other hand, $0 < b - v < b$ and **(iii)** imply $b - v = a$; so $b = 3a$. We deduce $a + v = b$ and $b + v = 5a$. From Lemma 2 and **(iv)** we have these two possible cases:

   - if $b + v = m' - a$ then $m' = 6a$ and we obtain the exception E_3;
   - if $b + v = m' - b$ then $m' = 8a$ and we obtain the exception E_4.

   Note that $v = 2a$ and then $e = 2ar$; m/e is either 3 or 4.

4. Assume that $v = b$. From **(iii)**, $2q^b \in T_{a,b}$ implies $q = 2$, and then $m = m'$ and $e = v = b$. Now the other conditions become

$$q^a + q^b \in T_{a,b},\ 1 + q^{a+b} \in T_{a,b},\ 1 + q^{2b} \in T_{a,b}\ .$$

Since $0 < b - a < b$, then $b - a = a$, i.e. $b = 2a$; note that we must have $4a \leq m$. Moreover we obtain $a + b = 3a$ and $2b = 4a$. So we must examine two cases.

- If $m = 2b = 4a$ then $1 + q^{2b} = 2$ is in $cl_q(1)$ and $a + b = m - a$. This case corresponds to the exception E_2. Note that $m/e = 2$; thus we have proved that $C_{a,2a}$ is invariant under $\langle AGL(2, 2^{2a}), \gamma_2 \rangle$ which is a subgroup of $\langle AGL(4, 2^a), \gamma_2 \rangle$. We previously have proved (see 1. above) that $C_{a,2a}$ is invariant under $\langle AGL(4, 2^a), \gamma_2 \rangle$.
- If $2b = m - a$ then $m = 5a$. So $e = 2a$ does not divide m, a contradiction.

5. The last case is when $b < v \leq m'/2$. Note that we have:

$$0 < v - b < v - a < v + a < v + b < m'\ .$$

According to Lemma 2, the conditions **(i)** to **(iv)** will be satisfied if and only if:

$$v - b = a,\ v - a = b,\ v + a = m' - b \text{ and } v + b = m' - a\ .$$

This gives $v = a + b$ and then $m' = 2v$. This is the last exception E_4.

□

4.4. The Automorphism Groups of Primitive Narrow-Sense BCH-Codes

In [5], we determined the permutation groups of primitive BCH codes over any prime field. At the end of the paper, we noted the difficulties for generalizing our results when the alphabet field $\mathbf{k}$ is an extension field. Now the problem is easier because of the new tools presented in Section 4.2, especially the result given by Corollary 1. In this section we complete our previous results by giving the automorphism groups of primitive narrow-sense BCH codes defined on any extension field.

From now on $\mathbf{k} = \mathbb{F}_q$, with $q = p^r$ and $r > 1$. We will study the extension of BCH codes, because we want to work in the ambient space of GRM-codes; our ambient space is the algebra $\mathcal{A} = \mathbf{k}[(\mathbb{F}_{q^{m'}}, +)]$. So the length of any of the codes is $p^m = q^{m'}$, $m = m'r$. Recall that $B_q(\delta)$ denotes the extended BCH-code of length $q^{m'}$, over $\mathbf{k}$, with designed distance δ and defining set T_δ (see Definition 5).

In accordance with Theorem 4 we must determine for any code $B_q(\delta)$, a divisor e of m and a divisor ℓ of e such that its permutation group is generated by $AGL(m/e, p^e)$ together with the Frobenius mapping γ_{p^ℓ}. We begin by proving that generally $\ell = r$. We next examine some particular cases, called "exceptional" (see Lemma 4). So the proof of Theorem 10 will consist of the determination of e. Actually we will prove that e is equal to m when $B_q(\delta)$ is not exceptional. Recall that $n = p^m - 1$.

LEMMA 3 *Let $1 \leq \delta \leq n$, where δ is the smallest element of its q-cyclotomic coset. Let ℓ be the smallest integer such that T_δ is invariant under multiplication by p^ℓ. Then $\ell = r$, except when $\delta = 1$ or $p^m - 1$, and when $\delta = 3$ for $q = 4$.*

Proof. According to Theorem 4, ℓ must divide r. Recall that $cl_{p^u}(s)$, for some u dividing m, denotes the orbit of s under the multiplication by p^u modulo n, i.e. the p^u-cyclotomic coset containing s.

First consider some particular values of δ. The cases $\delta = 1$ and $\delta = p^m - 1$ are trivial cases where obviously $\ell = 1$. Suppose that $q = 4$. We have $T_2 = \{0\} \cup cl_4(1)$ where clearly $2 \notin T_2$ implying $\ell = 2 = r$. But

$$T_3 = \{0\} \cup cl_4(1) \cup cl_4(2) = \{0\} \cup cl_2(1) \ .$$

So if $\delta = 3$ and $q = 4$ then $\ell = 1$.

Denote by L the number of q-cyclotomic cosets modulo n. Let $\mathcal{C}$ be the following set of coset representatives

$$\mathcal{C} = \left\{ \delta_i \;\middle|\; \begin{array}{l} i \in [1, L],\ \delta_i < \delta_{i+1} \\ \delta_i = \min cl_q(\delta_i) \end{array} \right\} \tag{10}$$

Note that $T_{\delta_i} = cl_q(\delta_{i-1}) \cup T_{\delta_{i-1}}$, $\delta_1 = 1$ and $\delta_L = n = p^m - 1$. We are going to prove by induction on i, $2 \leq i < L$, the following property:

(H_i) Assume that $3 < i$ when $q = 4$. Then for any ℓ dividing r, $\ell < r$, there is an $s \in T_{\delta_i}$ such that $p^\ell s \notin T_{\delta_i}$.

We first prove that (H_i) is true for the smallest value of i. Suppose that $q > 4$ and $i = 2$, i.e. $\delta_2 = 2$. Then $T_2 = \{0\} \cup cl_q(1)$ and clearly p^ℓ is not in T_2 since $1 \leq \ell < r$; so (H_2) is true. If $q = 4$ and $i = 4$ we have $\delta_4 = 5$ and

$$T_5 = T_3 \cup cl_4(3) = \{0\} \cup cl_2(1) \cup cl_4(3).$$

In this case, the only possible value for ℓ is 1. (H_4) is true because $6 = 2 \times 3$ is not in T_5.

Now suppose that (H_i) is true for $i \in [3,\ j[$ when $q > 4$ and for $i \in [4,\ j[$ otherwise. We are going to prove that (H_j) is true. We have

$$T_{\delta_j} = cl_q(\delta_{j-1}) \cup T_{\delta_{j-1}}$$

and we assume that

$$\forall\ \ell,\ \ell | r,\ \exists s \in T_{\delta_{j-1}} \text{ such that } \ p^\ell s \notin T_{\delta_{j-1}} \ .$$

If $p^\ell s \notin cl_q(\delta_{j-1})$ then $p^\ell s \notin T_{\delta_j}$ and (H_j) is true. Assume that $p^\ell s \in cl_q(\delta_{j-1})$; so $\delta_{j-1} \equiv q^u p^\ell s \pmod{n}$, for some u. Moreover we can suppose that s is the smallest element of its q-cyclotomic coset because the condition "$s \in T_{\delta_{j-1}}$ and $p^\ell s \notin T_{\delta_{j-1}}$" is satisfied for $q^k s$, for any k.

So we have: $\delta_{j-1} \equiv q^u p^\ell s \pmod{n}$ and $s < \delta_{j-1}$. Considering the p-adic expansion of s, $s = [s_0,\ \ldots,\ s_{m-1}]$, set $t = s + p^i$ where i is the smallest index such that $s_i < p - 1$.

We remark that this implies $s \geq p^i - 1$. By construction we have $s \prec t$, implying $q^u p^\ell s \prec q^u p^\ell t$ (where $\prec$ is defined by (2)). Note that t is not in $cl_p(s)$. In particular, this implies $t \neq \delta_{j-1}$.

Since $B_q(\delta_{j-1})$ is affine-invariant then $q^u p^\ell t \in T_{\delta_{j-1}}$ would imply that $q^u p^\ell s$ (and any element of $cl_q(p^\ell s)$) is in $T_{\delta_{j-1}}$. So there is no element of $cl_q(p^\ell t)$ in $T_{\delta_{j-1}}$. If $t < \delta_{j-1}$then $t \in T_{\delta_{j-1}}$ with $p^\ell t \notin T_{\delta_{j-1}}$, implying that (H_j) is true.

Suppose that $t > \delta_{j-1}$. Since

$$\delta_{j-1} - t = q^u p^\ell s - s - p^i = s(q^u p^\ell - 1) - p^i,$$

we must have: $0 < s(q^u p^\ell - 1) < p^i$. When $p > 2$ or $p = 2$ with $q^u p^\ell \neq 2$, this implies $s < p^i - 1$ which is not in accordance with the choice of i. So we must have $p = 2, u = 0$ and $\ell = 1$. According to the choice of i, one obtains

$$s = 2^i - 1 \quad \text{and} \quad \delta_{j-1} = 2s = 2(2^i - 1)\,. \tag{11}$$

We are going to prove that (H_j) is true for $\delta_{j-1} = 2s$, with $s \in T_{\delta_{j-1}}$, and $q = 2^r$. Note that $cl_2(s)$ has cardinality m, because of the form of s. Since δ_{j-1} is the smallest element of its q-cyclotomic coset, it is clear that $i \leq m - 2$. Thus we have $s < 2s$ and $2s$ is smaller than any $t \in cl_2(s)$ unless $t = s$. Moreover $cl_2(s)$ is the union of the r classes $cl_q(2^\ell s)$, $0 \leq \ell \leq r - 1$. Each such class has cardinality m/r.

When $q = 2^r$ with $r > 2$ we deduce that $cl_q(4s)$ is not contained in T_{δ_j}; in particular $4s \notin T_{\delta_j}$ while $2s \in T_{\delta_j}$, i.e (H_j) is true.

Suppose that $q = 4$. By hypothesis $\delta_{j-1} \geq 5$; so, according to (11), $i \geq 2$, $s \geq 3$ and $\delta_{j-1} \geq 6$. If $s = 3$, we have clearly $5 \in T_{\delta_{j-1}}$ and $10 \notin T_{\delta_j}$. More generally, suppose that $s \geq 7$ and take $u = s + 2^i - 2^{i-1}$, i.e. $u = 2^{i+1} - 1 - 2^{i-1}$. The 2-adic expansions of u and $2u$ are respectively

$$[1, \ldots, 1, 0, \overset{i}{1}, 0, \ldots] \quad \text{and} \quad [0, 1, \ldots, 1, 0, \overset{i+1}{1}, 0, \ldots]$$

(recall that $i \leq m - 2$). We have $s < u < 2s$; moreover, even when $i = m - 2$, it appears that the smallest element of $cl_4(2u)$ is strictly greater than $2s$ implying $2u \notin T_{\delta_j}$ while $u \in T_{\delta_j}$, i.e (H_j) is true.

We have proved that (H_i) is true, for $2 \leq i < L$. Obviously (H_i) means that the defining set of the BCH code of designed distance δ_i, over the field of order p^r, is not invariant by multiplication by p^ℓ, ℓ dividing r and $\ell < r$, completing the proof. ∎

LEMMA 4 *For the following values of q and δ, the code $B_q(\delta)$ has a permutation group greater than $\langle AGL(1, p^m), \gamma_{p^r} \rangle$. These cases, listed below, will be called "exceptional".*

Some extended BCH codes are in fact GRM codes:

(E1) *$\delta = 1$ or $\delta = q^{m'} - 1$, for any q. The codes $B_q(\delta)$ are the trivial GRM codes, $GRM_q(1)$ and $GRM_q(m'(q-1))$, respectively. Their permutation group is the full symmetric group $Sym(G)$, $G = \mathbb{F}_{p^m}$.*

(E2) *$\delta = 2$, for any q. The code $B_q(2)$ is equal to $GRM_q(2)$; thus $Per(B_q(2)) = AGL(m', q)$.*

(E3) $\delta = q^{m'} - q^{m'-1} - 1$, *for any* q. *The code* $B_q(q^{m'} - q^{m'-1} - 1)$ *is equal to* $GRM_q(m'(q-1)-1)$; *thus* $Per(B_q(\delta)) = AGL(m', q)$.

(E4) $m' = 2$, *and* $\delta = q^2 - 2q - 1$. *The code* $B_q(q^2 - 2q - 1)$ *is equal to* $GRM_q(2q-4)$; *thus* $Per(B_q(\delta)) = AGL(2, q)$.

(E5) $q = 4$ *and* $\delta = 3$. *The code* $B_4(3)$ *is equal to* $GRM_2(2)$, *with scalars extended to* $\mathbb{F}_4$, *and* $Per(B_4(3)) = AGL(m, 2)$.

There is one exception where $B_q(\delta)$ *is not a GRM code:*

(E6) $q = 2^r$, *with* $r > 2$ *(i.e.* q *even and* $q \geq 8$*), and* $\delta = 3$. *Then* $Per(B_q(3)) = AGL(m', 2^r)$.

Proof. Recall that the defining set of $GRM_q(\mu)$, the GRM code of index μ and length $q^{m'}$ over $\mathbb{F}_q$ is denoted by $L(\mu)$ (see Definition 6). The permutation group of $GRM_q(\mu)$ is known to be $AGL(m', q)$ (see Theorem 3).

(E1) This case is obvious because the defining sets are

$$T_1 = \{0\} \quad \text{and} \quad T_{q^{m'}-1} = \{0, 1, \ldots, q^{m'} - 2\} .$$

They correspond to the code containing any word for whom the sum of the coordinates is zero and the code containing the constant vector only, respectively

(E2) It is easy to check that

$$T_2 = \{0\} \cup cl_q(1) = L(2) .$$

(E3) One checks easily that $T_{q^{m'}-q^{m'-1}-1}$ is the set of those s, $s \in [0, q^{m'} - 1]$ such that $0 \leq wt_q(s) < m'(q-1) - 1$. This is exactly the defining set $L(m'(q-1)-1)$ of $GRM_q(m'(q-1)-1)$. These codes are the duals of those in (E2).

(E4) We remark that $\delta = (q-1, q-3)_q$. Let $s = (s_1, s_2)_q$. Then s is in T_{q^2-2q-1} if and only if

- "$s_1 < q-3$ or $s_2 < q-3$"; or
- "$s_1 = q-3$ and $s_2 < q-1$"; or
- "$s_2 = q-3$ and $s_1 < q-1$".

This occurs if and only if $wt_q(s) < 2q-4$. So T_{q^2-2q-1} is the defining set of $GRM_q(2q-4)$.

(E5) We have seen in the proof of the previous lemma that $T_3 = \{0\} \cup cl_2(1)$, when $q = 4$. Thus T_3 is the defining set of $GRM_2(2)$.

(E6) We have already proved that the value of ℓ is always r (cf. Lemma 3). We apply Theorem 6 when the defining set is

$$T_3 = \{0\} \cup cl_q(1) \cup cl_q(2), \quad q = 2^r, \ r > 2.$$

We consider the pairs (s, t), such that $s \in T_3$ and $t \preceq s$, and compute $s' = s + t(2^r - 1)$:

- If $(s, t) = (0, 0)$ then $s' = 0$.
- If $s \neq 0$ and $t = 0$, then $s' = s$.
- If $s \neq 0$ and $t \neq 0$ the only possibility is $s = t$, implying $s' = s2^r$; hence $s' \in cl_q(s)$.

In any case we have $s' \in T_3$; so we have proved that the corresponding pair (s, t) cannot be a disqualifying pair for r (see Definition 7). Hence $B_q(3)$ is invariant under $AGL(m', q)$. Now for any $e = rv$ the group $AGL(m/e, p^e)$ is contained in $AGL(m', q)$. We can conclude that the permutation group of $B_q(3)$ is $AGL(m', q)$, the permutation group of the non-trivial GRM codes over $\mathbb{F}_q$. Note that T_3 is not the defining set of a GRM code, since $wt_q(1 + q) = 2 = wt_q(2)$ where $2 \in T_3$ and $1 + q \notin T_3$. ■

THEOREM 10 *Let $\mathbf{k} = \mathbb{F}_q$, $q = p^r$, p a prime, $r > 1$. Let $B_q(\delta)$ be the extended BCH-code of length p^m, r dividing m, over $\mathbf{k}$.*

Then the permutation group of $B_q(\delta)$ is

$$\langle\ AGL(1, p^m), \gamma_{p^r}\ \rangle$$

except when q, δ and m satisfy the hypothesis of one of the exceptions (E1) to (E6) listed in Lemma 4.

When the permutation group of any $B_q(\delta)$ is generated by $AGL(m/e, p^e)$ and γ_{p^ℓ}, for some ℓ and some e, then the permutation group of the corresponding BCH code $B_q^*(\delta)$ is generated by $GL(m/e, p^e)$ and γ_{p^ℓ}.

The automorphism group of $B_q(\delta)$ is $\mathbf{k}^* \times Per(B_q(\delta))$.

Proof. According to Theorem 4, it remains to determine the value of e, since the value of ℓ is known to be generally r (see Lemma 3). So T_δ is invariant under multiplication by p^r, and r is the smallest integer such that this property holds. Recall that $e = rv$, for some v.

The difficulty of the proof comes from the number of particular cases for δ. We have chosen to treat separately the *small* values of δ, the *medium* values of δ and the *big* values of δ. However the notion of "small", or "big" is relative and depends on the value of e.

Notation was stated in Section 4.1. In particular $m = m'r = m''vr = m''e$; note that $p^e = q^v$. Recall that $q = p^r$ with $1 < r < m$, i.e. $4 \leq q < p^m$, since the cases $r = 1$ and $r = m$ were already treated (see [5]).

From now on, we fix $e < m$, i.e. $v < m'$. This implies $e \leq m/2$ since e divides m. In order to determine if $B_q(\delta)$ is, or is not, invariant under $AGL(m/e, p^e)$, we will try to produce a disqualifying pair for e, $e = rv$ and $1 < r < m$ (see Definition 7 and the following remark). Generally, the defining pair will be (s, t) and $s' = s + t(p^e - 1)$.

We generally identify δ with its q-adic expansion, which is denoted by $(d_0, \ldots, d_{m'-1})_q$. In the proof, κ will be the biggest suffix j such that $d_j \neq 0$; setting $\lambda = m' - 1 - \kappa$, we have:

$$\delta = (d_0, \ldots, \overset{\kappa}{d_\kappa}, \underbrace{0, \ldots, 0}_{\lambda})_q$$

The p^e-adic expansion of δ will be denoted, as previously, by $(\delta_0, \ldots, \delta_{m''-1})_{p^e}$. Notice that $\delta_i = (d_{vi}, d_{vi+1}, \ldots, d_{v(i+1)-1})_q$.

1) The first case: $\delta \leq p^e - 1$. We have $\kappa < v$ implying

$$\delta_1 = \ldots = \delta_{m''-1} = 0 \quad \text{and} \quad \lambda \geq m' - v \ .$$

Suppose that $p = 2$. We consider $3 < \delta$, because the cases where $\delta \in \{1, 2, 3\}$ were already treated—see the exceptions (E1), (E2), (E5) and (E6) in Lemma 4. The pair $(s, t) = (3, 1)$ is disqualifying for e. Indeed we have clearly $3 \in T_\delta$ and $1 \prec 3$; moreover s' is not in T_δ. Indeed $s' = s + t(2^e - 1) = 2^e + 2$ has the following expansions:

$$s' = (2, 1, \underbrace{0, \ldots, 0}_{m''-2})_{2^e} = (2, \underbrace{0, \ldots, 0}_{v-1}, 1, \underbrace{0, \ldots, 0}_{m'-(v+1)})_{2^r} \ .$$

Since $v \leq m'/2$ then $m' - (v + 1) \geq v - 1$, implying that s' is the smallest element of its q-cyclotomic coset. As $\delta \leq p^e - 1$, $\delta < s'$; so s' is not in T_δ.

When $p > 2$, $\delta = 1$ and $\delta = 2$ are exceptions. We suppose $\delta > 2$. The pair $(s, t) = (2, 1)$ is disqualifying for e, since $2 \in T_\delta$, $1 \prec 2$ and $s' = p^e + 1$ has expansions

$$s' = (1, 1, \underbrace{0, \ldots, 0}_{m''-2})_{p^e} = (1, \underbrace{0, \ldots, 0}_{v-1}, 1, \underbrace{0, \ldots, 0}_{m'-(v+1)})_q \ .$$

As above, we have clearly $s' \notin T_\delta$.

2) The second case: $p^e - 1 < \delta \leq p^{m-e} - 1$. Note that $p^{m-e} - 1 = q^{m'-v} - 1$. We have $v \leq \kappa < m' - v$ and $\delta_{m''-1} = 0$. Moreover, according to Corollary 1, we have to treat those δ whose q-adic expansion has the form

$$\delta = (\underbrace{q-1, \ldots, q-1}_{\kappa}, \overset{\kappa}{1}, \underbrace{0, \ldots, 0}_{\lambda \geq v})_q,$$

i.e. $\delta = 2q^\kappa - 1$. Take $(s, t) = (\delta - 1, q^{\kappa - v})$. Clearly $\delta - 1 \in T_\delta$ and we have obviously $q^{\kappa-v} \prec \delta - 1$ when $\kappa > v$. If $\kappa = v$ then $t = 1$ and we have $t \prec s$ unless $p = 2$. We will treat later the case where $p = 2$ and $\kappa = v$. We have $s' = s + t(q^v - 1) = 2q^\kappa + (q^\kappa - q^{\kappa-v} - 2)$ whose q-adic expansion is

$$s' = (q-2, q-1, \ldots, q-1, \overset{\kappa-v}{q-2}, q-1, \ldots, q-1, \overset{\kappa}{2}, \underbrace{0, \ldots, 0}_{\lambda \geq v})_q,$$

when $\kappa > v$. If $\kappa = v$ then $s' = 2q^v + q^v - 3$, which yields

$$s' = (q-3, q-1, \ldots, q-1, \overset{v}{2}, \underbrace{0, \ldots, 0}_{\lambda \geq v})_q \ . \tag{12}$$

In any case s' is the smallest element of its q-cyclotomic coset and $\delta < s'$, implying $s' \notin T_\delta$. So (s, t) is disqualifying for e.

If $p = 2$ and $\kappa = v$, we choose $(s, t) = (\delta - q^v, 2)$. We have $s = q^v - 1$, $2 \prec s$ and $s' = 2q^v + (q^v - 3)$. Since s' has the q-adic expansion (12), we conclude that (s, t) is disqualifying for e.

3) The third case: $p^{m-e} - 1 < \delta$ We have $\kappa \geq m' - v$; thus $\delta_{m''-1} \neq 0$ and $\lambda < v$ ($\lambda = m' - 1 - \kappa$). Moreover, according to Corollary 1, we have to treat those δ whose q-adic expansion has the form

$$\delta = (\underbrace{q-1, \ldots, q-1}_{\kappa},\ d_\kappa, \underbrace{0, \ldots, 0}_{\lambda<v})_q \ .$$

Recall that $m' = vm''$, $m'' > 1$; so $m' = v + 1$ if and only if $m' = 2$ (and $v = 1$).

3.1) We first suppose that $m' > 2$ (then $m' > v + 1$) and consider the pair $(s, t) = (\delta - 1, q^{m'-v-1})$, where clearly $\delta - 1 \in T_\delta$. Since $\kappa > m' - (v + 1)$, we have obviously $t \prec s$ and

$$\begin{aligned} s' &= s + t(p^e - 1) = d_\kappa q^\kappa + q^\kappa - 2 + q^{m'-v-1}(q^v - 1) \\ &= q^{m'-1} + d_\kappa q^\kappa + (q^\kappa - q^{m'-v-1} - 2) \ . \end{aligned}$$

Whenever $s' \notin T_\delta$, we can conclude that the pair (s, t) is a disqualifying pair for e. We distinguish three cases:

- If $\lambda \geq 2$, we have

$$s' = (q-2, \underbrace{q-1, \ldots, q-1}_{m'-v-2}, \overbrace{q-2}^{m'-v-1}, q-1, \ldots, q-1, \overbrace{d_\kappa}^{\kappa}, \underbrace{0, \ldots, 0}_{\lambda-1}, 1)_q \ .$$

  The smallest element of the q-cyclotomic coset of s' is

$$(1, q-2, \underbrace{q-1, \ldots, q-1}_{m'-v-2}, \overbrace{q-2}^{m'-v}, q-1, \ldots, q-1, \overbrace{d_\kappa}^{\kappa+1}, \underbrace{0, \ldots, 0}_{\lambda-1})_q,$$

  which is greater than δ, implying $s' \notin T_\delta$.

- If $\lambda = 1$, then

$$s' = (q-2, \underbrace{q-1, \ldots, q-1}_{m'-v-2}, \overbrace{q-2}^{m'-v-1}, q-1, \ldots, q-1, \overbrace{d_\kappa}^{\kappa}, 1)_q \ .$$

  Clearly, s' is the smallest element of its the q-cyclotomic coset, since $q = p^r$ with $r > 1$. Then s' is greater than δ which yields $s' \notin T_\delta$.

- If $\lambda = 0$, then

$$s' = (q-2, \underbrace{q-1, \ldots, q-1}_{m'-v-2}, \overbrace{q-2}^{m'-v-1}, \underbrace{q-1, \ldots, q-1}_{v-1}, d_\kappa + 1)_q \ .$$

When $d_\kappa < q-3$, it is clear that $s' \notin T_\delta$, because s' is the smallest member of its q-cyclotomic coset.

If $d_\kappa = q-3$, s' is not in T_δ because the coefficients of its q-adic expansion are $q-1$ or $q-2$, implying that any element of its q-cyclotomic coset is greater than δ.
If $d_\kappa = q-2$ then $\delta = q^{m'} - q^{m'-1} - 1$; we obtain the exception (E3) (see Lemma 4).

3.2) We now treat the particular case where $m' = 2$. Then $e = r$, $v = 1$ and $\delta = (q-1)+d_1 q$, i.e. $\delta = (q-1, d_1)_q$.

We remark that $d_1 = q-2$ corresponds to the exception (E3) ($\delta = q^2 - q - 1$) and $d_1 = q-3$ to the exception (E4) ($\delta = q^2 - 2q - 1$). Thus we assume that $d_1 \leq q-4$; since $d_1 \neq 0$ we then assume $q > 4$. We will distinguish when the characteristic is 2 or odd.

- If $p > 2$, we choose $(s, t) = (\delta - 1, 1)$. We have clearly $\delta - 1 \in T_\delta$ and $1 \prec \delta - 1$. Moreover

$$s' = s + t(q-1) = d_1 q + 2q - 3 \quad \text{—i.e} \quad s' = (q-3, d_1+1)_q \ .$$

Since $d_1 \leq q-4$, it follows that s' is the smallest member of its q-cyclotomic coset. As $s' > \delta$, $s' \notin T_\delta$. Thus (s, t) is a disqualifying pair for r.

- Assume that $p = 2$. When $d_1 \leq q-5$ we choose the pair $(s, t) = (\delta - 2, 1)$. We have $\delta - 2 \in T_\delta$, $1 \prec (\delta - 2)$ and

$$s' = s + t(q-1) = d_1 q + 2q - 4 \quad \text{—i.e.} \quad s' = (q-4, d_1+1)_q \ .$$

Again, s' is the smallest member of its q-cyclotomic coset and $s' > \delta$; i.e. (s, t) is a disqualifying pair for r.

When $d_1 = q-4$, then $\delta = q^2 - 3q - 1$, i.e. $\delta = (q-1, q-4)_q$. We choose the pair $(s, t) = (q^2 - 4q - 1, 2)$. Since $s = (q-1, q-5)_q$, it is clear that $s \in T_\delta$ and $t \prec s$. Moreover

$$s' = s + t(q-1) = q^2 - 2q - 3 \quad \text{—i.e.} \quad s' = (q-3, q-3)_q \ ;$$

s' is the only element of its q-cyclotomic coset and is greater than δ; so (s, t) is a disqualifying pair for r.

We have proved that any $B_q(\delta)$ which is not exceptional cannot be invariant under $AGL(m/e, p^e)$, for any e such that $e = rv$, $1 \leq v < m'$. We conclude that $e = m$ is the only possibility, implying that the permutation group of $B_q(\delta)$ is generated by $AGL(1, p^m)$

and γ_q. Then the permutation group of $B_q^*(\delta)$ is $\langle GL(1, p^m), \gamma_q \rangle$. The automorphism group of $B_q(\delta)$ is immediately deduced, according to Theorem 5. ■

Remark. At the end of our previous paper [5], we noted that the complete description of the automorphism group of BCH codes, defined on any extension field, could be difficult because of the number of different ambient spaces (the value of p, the number of subfields of $\mathbb{F}_{p^m}$ and so on). Corollary 1 was decisive and there are probably other corollaries of Theorem 8 which can be stated for other specific classes.

On the other hand we expected other results, similar to our results concerning BCH codes defined on any prime field. We were surprised to find only one more exceptional class of BCH codes which are not GRM codes. This comes from the form of the designed distance. As we noted in Section 3 it is, however, easy to construct affine-invariant codes with large automorphism group.

Annex: Main notation

- $\mathbf{k}$ is the alphabet field $\mathbb{F}_q$, $q = p^r$, p a prime.
- $n = q^{m'} - 1 = p^m - 1$, $m = rm'$.
- S is the set $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n; $S = [0, p^m - 1]$.
- $wt_v(s)$, $v = p^u$ with u dividing m, is the v-weight of $s \in [0, n]$ (see (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.
- $\mathcal{A}$ is the group algebra $\mathbf{k}[\{G, +\}]$ (Section 2).
- If C is an extended cyclic code, it is the extension of the cyclic code C^*.
- $Sym(G)$ is the symmetric group acting on G.
- $Per(D)$ is the permutation group of the code D (Definition 1).
- $Aut(D)$ is the automorphism group of the code D (Definition 2).
- γ_{p^k} is the kth-power of the Frobenius mapping on G.
- $GL(m/e, p^e)$ is the linear group, the group of $\mathbb{F}_{p^e}$-linear permutations of G.
- $AGL(m/e, p^e)$ is the affine group.
- $\Gamma L(m/e, p^e)$ is the semi-linear group.
- $A\Gamma L(m/e, p^e)$ is the semi-affine group (for all these groups see Section 2.1).
- m'': m/e is often denoted by m''.

- $(S, \preceq)$ is the poset defined by (2).
- $(S, \ll_e)$, e dividing m, is a poset defined by (4).
- $cl_{p^u}(j)$, $j \in S$, is the orbit of j under the multiplication by p^u modulo n.

Acknowledgments

The authors wish to express their gratitude to 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, Polynomial codes and finite geometries, in *Handbook of Coding Theory*, Part 2: Connections, chapter 16 (V. S. Pless, W. C. Huffman, eds., R. A. Brualdi, assistant ed.), Amsterdam, The Netherlands, Elsevier, 1998.
2. T. P. Berger, Automorphism groups and permutation groups of affine-invariant codes, Proceedings of Finite Fields and Applications (third conference), Glasgow, UK, London Mathematical Society, Lecture Series 233, Cambridge University Press, (1996) pp. 31–45.
3. T. P. Berger, On the automorphism group of affine-invariant codes, *Designs, Codes and Cryptography*, Vol. 7 (1996) pp. 215–221.
4. T. P. Berger and P. Charpin, The automorphism group of Generalized Reed-Muller codes, *Discrete Mathematics*, Vol. 117 (1993) pp. 1–17.
5. T. P. Berger and P. Charpin, The permutation group of affine-invariant extended cyclic codes, *IEEE Transactions on Information Theory*, Vol. 42 (1996) pp. 2194–2309.
6. P. Charpin, Codes cycliques étendus affines-invariants et antichaînes d'un ensemble partiellement ordonné, *Discrete Mathematics*, Vol. 80 (1990) pp. 229–247.
7. P. Charpin, Open problems on cyclic codes, in *Handbook of Coding Theory, Part 1: Algebraic Coding*, chapter 11, (V. S. Pless, W. C. Huffman, eds., R. A. Brualdi, assistant ed.), Amsterdam, The Netherlands, Elsevier, 1998.
8. P. Charpin and F. Levy-dit-Vehel, On self-dual affine-invariant codes, *Journal of Combinatorial Theory, Series A*, Vol. 67, No. 2 (1994) pp. 223–244.
9. P. Delsarte, On cyclic codes that are invariant under the general linear group, *IEEE Transactions on Information Theory*, Vol. IT-16, No. 6 (1970).
10. W. C. Huffman, Codes and groups, in *Handbook of Coding Theory, Part 2: Connections*, chapter 17, (V. S. Pless, W. C. Huffman, eds., R. A. Brualdi, assistant ed.), Amsterdam, The Netherlands, Elsevier, 1998.
11. W. C. Huffman, V. Job and V. Pless, Multipliers and generalized multipliers of cyclic objects and cyclic codes, *Journal of Combinatorial Theory, Series A*, Vol. 63 (1993).
12. T. Kasami, S. Lin and W. W. Peterson Some results on cyclic codes which are invariant under the affine group and their applications, *Info. and Control*, Vol. 11 (1967) pp. 475–496.
13. T. Kasami, Weight distributions of Bose-Chaudhuri-Hocquenghem Codes, *Combinatorial Math. and Applications*, (R. C. Bose and T. A. Dowlings, eds.), Univ. of North Carolina Press, Chapel Hill, NC (1969) Ch. 20.
14. F. J. Macwilliams and N. J. A. Sloane *The Theory of Error Correcting Codes*, North-Holland (1986).