DRDO–IISc Programme on
Advanced Research in Mathematical Engineering

Affine Invariant Extended Cyclic Codes over Galois Rings

(TR-PME-2003-06)

by
Bikash Kumar Dey and B Sundar Rajan

ECE, IISc., Bangalore
E-mail: bsrajan@ece..iisc.ernet.in

May 19, 2003

Indian Institute of Science
Bangalore 560 012

Affine Invariant Extended Cyclic Codes over Galois Rings

Bikash Kumar Dey and B. Sundar Rajan

June 14, 2003

ABSTRACT

Recently, Blackford and Ray-Chaudhury used transform domain techniques to permutation groups of cyclic codes over Galois rings. They used the same technique to find a set of necessary and sufficient conditions for extended cyclic codes of length 2^m over any subring of $GR(4, m)$ to be affine invariant. Here we use the same technique to find a set of necessary and sufficient conditions for extended cyclic codes of length p^m over any subring of $GR(p^e, m)$ to be affine invariant, for $e = 2$ with arbitrary p and for $p = 2$ with arbitrary e. These are used to find two new classes of affine invariant BCH and GRM codes over $\mathbb{Z}_{2^e}$ for arbitrary e and a class of affine invariant BCH codes over $\mathbb{Z}_{p^2}$ for arbitrary prime p.

1 Introduction

The rank-distance properties are useful to construct space-time codes and also for coding for storage devices (See the reports [1, 2] and the references therein). In [1] rank-distance properties of the general class of linear codes over finite fields have been studied and toward obtaining closed form expressions, in [2], the study was restricted to the class of cyclic codes and modest progress have been reported. This study made use of the well known Discrete Fourier Transform (DFT) approach [3] for cyclic codes. In the report [4] to facilitate the study the rank-distance properties of nonlinear cyclic codes DFT domain approach has been extended to certain non-linear codes. It is well known that more the structure of the code it may be easier to decode it. A similar conclusion is indicated by the study that lead to [1, 2] for the study of rank-distance properties of codes. That is, more the structure in the code easier it is to obtain rank-distance properties of the code. Towards this end we studied codes with the additional structure of being affine-invariant. This report presents the results obtained regarding the affine-invariant cyclic codes.

The automorphism/permutation groups of codes over finite fields are known to be useful for decoding (see [5–11] for examples). Permutations of F_{p^m} (where p is a prime) of the form $x \mapsto ax+b$, where $a, b \in F_{p^m}$, $a \neq 0$, are called the affine permutations. These permutations form a subgroup of the symmetric group of order p^m

[0]This work was supported partly by the DRDO-IISc Program on Mathematical Engineering through a grant to B.S.Rajan and partly by CSIR India, through Research Grant (22(0298)/99/EMR-II).
A part of the content of this report has been accepted for publication in IEEE Transactions on Information Theory subject to minor revisions.

and is denoted as $AGL(1,p^m)$. A code of length p^m with components indexed by elements of F_{p^m} is said to be affine invariant if it is invariant under the affine permutations.

Clearly, affine invariant codes, after the 0'th component deleted, are cyclic codes. Kasami, Lin and Peterson [12] found a necessary and sufficient condition on the defining set of any cyclic code over a finite field, under which the extended cyclic code is affine invariant. As corollaries, they showed that the famous extended BCH and generalized Reed-Muller codes are affine invariant. Often it is comparatively easier to determine the full permutation groups of affine invariant codes [13–17].

Though coding theorists have for a long time had theoretical interest on codes over integer residue rings [18, 19], codes over integer residue rings and more generally over Galois rings have received serious attention [20–26] after it was shown [27] that some important families of nonlinear binary codes can be obtained via the Gray map from linear codes over $\mathbb{Z}_4$.

The conditions for extended cyclic codes over integer residue rings to be affine-invariant were derived by Abdukhalikov [28]. Blackford and Ray-Chaudhuri [29] used a transform domain approach to characterize affine invariant extended cyclic codes of length 2^m over subrings of $GR(4,m)$ and using this characterization, they found new classes of affine invariant BCH and GRM codes over Galois rings. In this paper, we extend their approach to extended cyclic codes of length 2^m over any subring of $GR(2^e,m)$ and also to extended cyclic codes of length p^m over $GR(p^2,m)$ for arbitrary prime p.

In the next section, we discuss some basic facts about Galois rings and cyclic codes over Galois rings as a preparation to the subsequent section, where the results of this paper are presented. We conclude with some finishing remarks in Section 4.

2 Preliminaries

Let us start with some basic important properties of Galois rings. For details on these properties and their proofs, the reader is referred to [30].

Let $\phi(x) \in \mathbb{Z}_{p^e}[x]$ be a basic irreducible polynomial of degree m (such a polynomial exists by Hensel's lemma). The Galois ring $GR(p^e,m)$ is defined as the quotient $\frac{\mathbb{Z}_{p^e}[x]}{(\phi(x))}$. If m_1 is a positive integer such that $m_1|m$, then $GR(p^e,m_1)$ is a subring of $GR(p^e,m)$. Moreover, any subring of $GR(p^e,m)$ is of the form $GR(p^e,m_1)$ for some $m_1|m$. The ring $GR(p^e,m)$ is a finite chain ring i.e., it is a finite ring whose ideals can be linearly ordered by inclusion. Its only maximal ideal is given by $(p) = pGR(p^e,m)$ and the quotient field is $\frac{GR(p^e,m)}{pGR(p^e,m)} \simeq F_{p^m}$. For any element $u \in GR(p^e,m)$, we shall denote by $\bar{u}$, the image of u under the canonical homomorphism of $GR(p^e,m)$ onto F_{p^m}. All the ideals of $GR(p^e,m)$ are ordered as

$$\{0\} = p^eGR(p^e,m) \subset p^{e-1}GR(p^e,m) \subset \cdots \subset p^2GR(p^e,m) \subset pGR(p^e,m) \subset GR(p^e,m). \quad (1)$$

Any element $u \in GR(p^e, m)$ can be expressed as

$$u = p^i u'$$

where $u' \in GR^*(p^e, m)$ and i is unique in this expression. u' is unique up to modulo p^{e-i}. The abelian group $GR^*(p^e, m)$ is a direct product of two groups H_1 and H_2, where H_1 is cyclic of order $p^m - 1$ and H_2 is of order $p^{(e-1)m}$. Suppose $H_1 = \{1, \xi, \xi^2, \cdots, \xi^{p^m-2}\}$. Then the set $\mathcal{T}_m = H_1 \cup \{0\} = \{0, 1, \xi, \xi^2, \cdots, \xi^{p^m-2}\}$ forms a set of coset representatives of $GR(p^e, m)$ modulo $pGR(p^e, m)$. Every element $u \in GR(p^e, r)$ can be uniquely expressed as

$$u = u_0 + pu_1 + \cdots + p^{e-1}u_{e-1} \tag{2}$$

where $u_0, u_1, \cdots, u_{e-1} \in \mathcal{T}_m$. Let n be a positive integer relatively prime to p. If any $\mathbf{c} = (c_0, \cdots, c_{n-1}) \in (GR(p^e, m))^n$ is associated with a polynomial $c_0 + c_1X + \cdots + c_{n-1}X^{n-1}$, then a cyclic code of length n over $GR(p^e, m)$ is an ideal of the modular algebra $\frac{GR(p^e,m)[X]}{(X^n-1)}$. Any cyclic code of length n over $GR(p^e, m)$ is [21] of the form $(f_0, pf_1, \cdots, p^{e-1}f_{e-1})$, where f_j are monic irreducible divisors of $X^n - 1$ and $f_{e-1}|f_{e-2}|\cdots|f_1|f_0$. If r is the smallest positive integer such that n divides $p^{mr} - 1$, then $GR(p^e, mr)$ is the smallest extension ring of $GR(p^e, m)$ where there is a primitive n-th root ζ of 1 and over which $X^n - 1$ factors into distinct linear factors. The defining sets $T_1, \cdots, T_e$ of the code are defined as

$$T_j = \{s \in [0, n-1] | f_{j-1}(\zeta^s) = 0\}.$$

By definition, $T_e \subseteq \cdots \subseteq T_2 \subseteq T_1$. It is also easy to see that each defining set is the union of p^m-cyclotomic cosets modulo n.

For any $\mathbf{c} = (c_0, \cdots, c_{n-1}) \in (GR(p^e, m))^n$, the Mattson-Solomon (MS) polynomial of $\mathbf{c}$ is defined [29] as

$$C(Z) = \sum_{i=0}^{n-1} \hat{c}(n-i)Z^i$$

where

$$\hat{c}(i) = c(\zeta^i) = \sum_{j=0}^{n-1} c_j \zeta^{ij}$$

for $0 \leq i \leq n$.

Let us consider $n = p^m - 1$. If $\hat{T}_e \subseteq \cdots \subseteq \hat{T}_1 \subseteq [0, p^m - 2]$ are unions of q-cyclotomic cosets (where $q = p^m$) modulo n, then the extended cyclic code $\hat{\mathcal{C}}$ over $GR(p^e, m)$ of length p^m with defining sets $(\hat{T}_1, \cdots, \hat{T}_e)$ is the set of vectors $\mathbf{a} \in (GR(p^e, m))^{p^m}$, such that

$$\sum_{x \in \mathcal{T}_m} a_x x^s \equiv 0 \bmod p^j \ ; \ \forall s \in \hat{T}_j.$$

Clearly if $0 \in \hat{T}_e$, then $\hat{\mathcal{C}}$ is the extension of the cyclic code $\mathcal{C}$ via a parity check, where $\mathcal{C}$ has defining sets

$$T_j = \{s \bmod n | s \in \hat{T}_j \setminus \{0\}\}.$$

Let us assume $n \notin \hat{T}_1$, since otherwise the code $\hat{\mathcal{C}}$, if affine invariant, is over $pGR(p^e, m)$. The MS polynomial of a codeword is defined to be that of the corresponding codeword of the cyclic code.

In the following, two important classes of cyclic (and extended cyclic) codes are discussed.

BCH Codes: BCH codes over $\mathbb{Z}_{p^e}$ were first defined by Shankar [18]. Generalization to BCH codes over Galois rings is very straight forward and natural. But Blackford and Ray-Chaudhuri [29] gave a more general definition of BCH codes over Galois rings. For $(n, p) = 1$, suppose $1 \le \delta_e \le \delta_{e-1} \le \cdots \le \delta_1 \le n-1$. Then the BCH code $B(n, \delta_1, \cdots, \delta_e)$ of length n over $GR(p^e, m)$ with designed distances $\delta_1, \cdots, \delta_e$ is defined to be the cyclic code with defining sets

$$T_j = \cup_{i \in [1, \delta_j - 1]} [i]^q$$

where $[i]^q$ denotes the q-cyclotomic coset modulo n of i. Similarly, the extended BCH code $\hat{B}(n, \delta_1, \cdots, \delta_e)$ of length $n+1$ is defined as the extended cyclic code with defining sets

$$\hat{T}_j = \{0\} \cup T_j.$$

Shankar's definition of BCH codes is obtained by assuming $\delta_1 = \delta_2 = \cdots = \delta_e$. Note that, if $p = 2$, we can always take each designed distance to be odd, since if $\delta_i - 1 \in \hat{T}_i$ is odd, then δ_i is also in $\hat{T}_i$ and so we can take $\delta_i + 1$ to be the i'th designed distance as well.

Generalized Reed-Muller Codes over $\mathbb{Z}_{p^e}$: Suppose $0 \le r_1 \le r_2 \le \cdots \le r_e \le (p-1)m$. The Generalized Reed-Muller code of length p^m and orders $(r_1, \cdots, r_e)$ over $\mathbb{Z}_{p^e}$ is defined [29] as the extended cyclic code with defining sets

$$\hat{T}_j = \{s \in [0, p^m - 1] : wt_p(s) < m(p-1) - r_j\}$$

where $wt_p(s)$ denotes the p-adic weight of s: $wt_p(s) = \sum_{i=0}^{m-1} s_i$. GRM codes of length p^m and orders $(r, \cdots, r)$ are well known as the Hensel lifts of GRM codes of order r over $\mathbb{Z}_p$ [27, 28].

Let $Sym(n)$ denote the group of permutations of n elements. For $n = p^m$, we can consider $Sym(p^m)$ as the group of permutations of F_{p^m}. Let us consider a code $\mathcal{C}$ of length n with components indexed by $\{0, 1, \cdots, n-1\}$. For a codeword $\mathbf{a}$, any permutation $\sigma \in Sym(n)$ acts on $\mathbf{a}$ as $\sigma(\mathbf{a}) \stackrel{\triangle}{=} \left(a_{\sigma^{-1}(0)}, a_{\sigma^{-1}(1)}, \cdots, a_{\sigma^{-1}(n-1)}\right)$. The subgroup of $Sym(n)$ defined as

$$Per(\mathcal{C}) \stackrel{\triangle}{=} \{\sigma \in Sym(n) | \sigma(\mathbf{a}) \in \mathcal{C} \ \forall \mathbf{a} \in \mathcal{C}\}$$

is called the permutation group of $\mathcal{C}$.

Associated with any permutation $\sigma \in Sym(p^m)$ is a unique permutation polynomial $f_\sigma(X)$ over F_q of degree at most $q-1$. Clearly, there is a 1-1 correspondence between F_q and $\mathcal{T}_m$ via the canonical homomorphism of

$GR(p^e,m)$ onto F_q. For each polynomial $f(X) \in F_q[X]$, the lifted polynomial $f^{(L)}(X) \in \mathcal{T}_m(X)$ is obtained by lifting each coefficient of $f(X)$ to its representative in $\mathcal{T}_m$.

Suppose $\tau = \lceil \frac{e-1}{m} \rceil$. In [29], Blackford et. al. assumed $m \geq e-1$, i.e., $\tau = 1$. That restriction can be avoided by noting that, for any $u \in GR(p^e,m)$, $u^{p^{\tau m}} \in \mathcal{T}_m$. So, any permutation σ of F_q has a corresponding permutation σ' induced by the polynomial $f_\sigma^{(L)}(X)$ as

$$\sigma'(u) = \left(f_\sigma^{(L)}(u)\right)^{q\tau} \quad , \ \forall u \in \mathcal{T}_m.$$

Clearly, the lifted permutation polynomial corresponding to any affine permutation of $\mathcal{T}_m$ is of the form $aX+b$ where $a,b \in \mathcal{T}_m$ and $a \neq 0$.

The following theorem is a modified version of [29, Theorem 4.2] for arbitrary τ.

Theorem 2.1. *Suppose $n = p^m - 1$, and $\hat{\mathcal{C}}$ is an extended cyclic code over any subring of $GR(p^e,m)$ of length $n+1$ with defining sets $(\hat{T}_1, \cdots, \hat{T}_e)$, with $0 \in \hat{T}_e$. If $\sigma \in Sym(p^m)$, and $f_\sigma(X) \in F_q[X]$ is the corresponding permutation polynomial, then $\sigma \in Per(\hat{\mathcal{C}})$ if and only if for all j, $1 \leq j \leq e$, $s \in \hat{T}_j$,*

$$p^{e-j}\left(f_\sigma^{(L)}(X)\right)^{sp^{m\tau}} \equiv \sum_{l=1}^{j} p^{e-l} \sum_{i \in \hat{T}_l} a_{s,l,i} X^i \qquad (mod\ X^n - 1)$$

where $a_{s,l,i} \in \mathcal{T}_m$.

3 Affine Invariant Codes over Galois Rings

In [13], a partial order $\preceq_p$ for the set $[0, p^m-1]$ was defined. For any two elements $s,t \in [0,p^m-1]$, they can be uniquely decomposed as $s = \sum_{i=0}^{m-1} s_i p^i$ and $t = \sum_{i=0}^{m-1} t_i p^i$, with $0 \leq s_i, t_i \leq p-1$. Then $s \preceq_p t$ if $s_i \leq t_i$ for $0 \leq i \leq m-1$. The m-tuples $(s_{m-1}, \cdots, s_0)$ and $(t_{m-1}, \cdots, t_0)$ are called the p-ary representations of the integers s and t respectively. It should be noted that for any $s \in [0, p^m-2]$, $ps \mod (p^m-1)$ has the p-ary representation $(s_{m-2}, \cdots, s_0, s_{m-1})$. Any subset $T \subseteq S$ is called a lower ideal of S if $t \in T$, $s \preceq_p t \Rightarrow s \in T$.

Lemma 3.1 (Lucas). *For $s,t \in [0,p^m-2]$, $\binom{s}{t} \equiv \binom{s_0}{t_0} \cdots \binom{s_{m-1}}{t_{m-1}}$ mod p.*

So, $\binom{s}{t} \not\equiv 0 \bmod p$ if and only if $t \preceq_p s$.

3.1 $p = 2$ and Arbitrary e

Let us consider $p=2$ and define $M_{m,2}^{(i)}(s,k);\ i \geq 0,\ s,k \in [0, 2^m-2]$ recursively as

$$M_{m,2}^{(0)}(s,k) = \begin{cases} 1 & \text{if } k \preceq_2 s \\ 0 & \text{otherwise} \end{cases}$$

$$M_{m,2}^{(i)}(s,k) * M_{m,2}^{(j)}(s,k) = \sum_{\substack{0 \leq k_1, k_2 \leq n-1 \\ 2^j k_1 + 2^i k_2 \equiv k \ mod\ n \\ k_1 < k_2\ if\ i=j}} M_{m,2}^{(i)}(s,k_1) M_{m,2}^{(j)}(s,k_2)$$

$$\text{and} \quad M_{m,2}^{(i)}(s,k) = \begin{cases} \sum_{\substack{(i_1,i_2) \\ 0 \le i_1 \le i_2 \le i-1 \\ i_1+i_2=i-1}} M_{m,2}^{(i_1)}(s,k) * M_{m,2}^{(i_2)}(s,k) & \text{if } i \text{ is odd} \\ \sum_{\substack{(i_1,i_2) \\ 0 \le i_1 \le i_2 \le i-1 \\ i_1+i_2=i-1}} M_{m,2}^{(i_1)}(s,k) * M_{m,2}^{(i_2)}(s,k) + \left(M_{m,2}^{(\frac{i}{2})}(s, 2^{m-\frac{i}{2}}k)\right)^2 & \text{if } i \text{ is even.} \end{cases}$$

By this definition, $M_{m,2}^{(1)}(s,k)$ is the same as $M_m(s,k)$ in [29], i.e.,

$$M_{m,2}^{(1)}(s,k) = |\{(i,j) | i < j; i,j \preceq_2 s; i+j \equiv k \bmod n\}|.$$

Let us also define the following numbers for $i \ge 0,\ s,k \in [0, 2^m - 2]$.

$$\begin{aligned} & K_{m,2}^{(0)}(s,k) = M_{m,2}^{(0)}(s,k) \\ \text{and} \quad & K_{m,2}^{(i)}(s,k) = M_{m,2}^{(i)}(s,k) + \lfloor \frac{1}{2} K_{m,2}^{(i-1)}(s, k.2^{m-1}) \rfloor \text{ for } i \ge 1. \end{aligned}$$

Here $\lfloor . \rfloor$ denotes the largest integer less than or equal to the number inside.

Parity of any integer i is defined as

$$P(i) = \begin{cases} 0 & \text{if } i \text{ is even} \\ 1 & \text{if } i \text{ is odd.} \end{cases}$$

Lemma 3.2. *If $s,k \in [0, 2^m - 2]$, then*

1. *For $i \ge 0,\ 0 \le j < m,\ M_{m,2}^{(i)}(s,k) = M_{m,2}^{(i)}(2^j s, 2^j k)$.*

2. *For $i \ge 0,\ 0 \le j < m,\ K_{m,2}^{(i)}(s,k) = K_{m,2}^{(i)}(2^j s, 2^j k)$.*

3. *$M_{m,2}^{(i)}(s,k) \ne 0 \Rightarrow k \le 2^i s - 1$ for $i > 0$.*

4. *$K_{m,2}^{(i)}(s,k) \ne 0 \Rightarrow k \le 2^i s - 1$ for $i > 0$.*

Proof: 1) For $i = 0$, the result is obvious. For $i > 0$ also, the proof is trivial by induction.

2) Trivial using the definition of $K_{m,2}^{(i)}(s,k)$ and the first part of this lemma.

3) First, note that for $i = 0$, $M_{m,2}^{(i)}(s,k) \ne 0 \Rightarrow k \le 2^i s = s$. For $i = 1$, the result is the same as [29, Lemma 5.1(3)]. Suppose it is true for $(i-1)$ and smaller integers (where $i \ge 2$) and $M_{m,2}^{(i)}(s,k) \ne 0$. Then either of the following cases hold.

Case I: $\exists i_1, i_2;\ i_1 \le i_2;\ \ i_1 + i_2 + 1 = i$, such that $\exists k_1, k_2$, satisfying $2^{i_2} k_1 + 2^{i_1} k_2 = k \bmod n$, $M_{m,2}^{(i_1)}(s,k_1) \ne 0$ and $M_{m,2}^{(i_2)}(s,k_2) \ne 0$. Clearly, $i_2 \ne 0$. By the induction hypothesis,

$$\begin{aligned} k_1 &\le 2^{i_1} s \\ k_2 &\le 2^{i_2} s - 1. \end{aligned}$$

So,

$$k \quad = \quad 2^{i_2} k_1 + 2^{i_1} k_2$$

$$\begin{aligned}
&\leq 2^{i-1}s + 2^{i-1}s - 2^{i_1}\\
&= 2^i s - 2^{i_1}\\
&\leq 2^i s - 1.
\end{aligned}$$

Case II: i is even and

$$\begin{aligned}
& M_{m,2}^{(\frac{i}{2})}(s, 2^{m-\frac{i}{2}}k) \neq 0\\
\Rightarrow\ & M_{m,2}^{(\frac{i}{2})}(2^{\frac{i}{2}}s, k) \neq 0\\
\Rightarrow\ & k \leq 2^{\frac{i}{2}}.2^{\frac{i}{2}}s - 1 = 2^i s - 1.
\end{aligned}$$

4) For $i = 1$, $K_{m,2}^{(1)}(s,k) = M_{m,2}^{(1)}(s,k)$. So, the claim is true for $i = 1$. Suppose it is true for $i-1$ and $K_{m,2}^{(i)}(s,k) \neq 0$. Then either $M_{m,2}^{(i)}(s,k) \neq 0$ or $K_{m,2}^{(i-1)}(s, 2^{m-1}k) \neq 0$. In the first case, the claim follows from third part of this lemma. In the second case, $K_{m,2}^{(i-1)}(2s,k) \neq 0 \Rightarrow k \leq 2^{i-1}.2s - 1 = 2^i s - 1$. ■

Lemma 3.3. *Suppose $x, y \in GR(2^e, m)$. Then $(x+2y)^{2^{m\tau}} = x^{2^{m\tau}}$.*

Proof:

$$\begin{aligned}
(x+2y)^{2^{m\tau}} &= (x^2 + 2^2 f_1(x,y))^{2^{m\tau-1}} \text{ where } f_1(x,y) = xy + y^2\\
&= (x^{2^2} + 2^3 f_2(x,y))^{2^{m\tau-2}} \text{ where } f_2(x,y) = x^2 f_1(x,y) + 2f_1^2(x,y)\\
&\quad \ldots\\
&= x^{2^{m\tau}} + 2^{m\tau+1} f_{m\tau}(x,y) \text{ where } f_{m\tau}(x,y) = x^{2^{m\tau-1}} f_{m\tau-1}(x,y) + 2^{m\tau-1} f_{m\tau-1}^2(x,y)\\
&= x^{2^{m\tau}} \text{ in } GR(p^e, m).
\end{aligned}$$

Lemma 3.4. *If $x, b \in \mathcal{T}_m \subset GR(2^e, m)$, then*

$$(x+b)^{s.2^{m\tau}} = \left(\sum_{\substack{0 \leq i \leq s\\ i \preceq_2 s}} x^i b^{s-i} \right)^{2^{m\tau}}.$$

Proof: Taking the binomial expansion, we have

$$(x+b)^{s.2^{m\tau}} = \left(\sum_{0 \leq i \leq s} \binom{s}{i} x^i b^{s-i} \right)^{2^{m\tau}}.$$

If $i \preceq_2 s$, then $\binom{s}{i} \equiv 1 \bmod 2$. Otherwise $\binom{s}{i} \equiv 0 \bmod 2$. So the result follows by Lemma 3.3. ■

Lemma 3.5. *Suppose $x, b \in GR(2^e, m)$. Then*

$$\left(\sum_{\substack{0 \leq i \leq s\\ i \preceq_2 s}} x^i b^{s-i} \right)^{2^{m_1}} \equiv \sum_{i=0}^{m_2} 2^i \sum_{k=0}^{n-1} M_{m,2}^{(i)}(s,k) x^{k.2^{m_1-i}} b^{2^{m_1}s - k.2^{m_1-i}} \ mod\ 2^{m_2+1}$$

for any $m_1 \geq 0$, $m_2 \leq m_1$.

Proof: The proof is by induction on m_1. Clearly, the result is true for $m_1 = 0$. Suppose it is true for $m_1 - 1$ for some $m_1 \geq 1$. Then we need to prove it for m_1.

Obviously, the result is true for $m_2 = 0$. Suppose $m_1 \geq m_2 > 0$. By the induction hypothesis,

$$\left(\sum_{\substack{0 \leq i \leq s \\ i \preceq_2 s}} x^i b^{s-i} \right)^{2^{m_1-1}} \equiv \sum_{i=0}^{m_2-1} 2^i \sum_{k=0}^{n-1} M_{m,2}^{(i)}(s,k) x^{k.2^{m_1-1-i}} b^{2^{m_1-1}s - k.2^{m_1-1-i}} \mod 2^{m_2}$$

since $m_2 - 1 \leq m_1 - 1$. So, $\left(\sum_{\substack{0 \leq i \leq s \\ i \preceq_2 s}} x^i b^{s-i} \right)^{2^{m_1-1}}$ can be expanded in the form

$$\left(\sum_{\substack{0 \leq i \leq s \\ i \preceq_2 s}} x^i b^{s-i} \right)^{2^{m_1-1}} = \sum_{i=0}^{m_2-1} 2^i \sum_{k=0}^{n-1} M_{m,2}^{(i)}(s,k) x^{k.2^{m_1-1-i}} b^{2^{m_1-1}s - k.2^{m_1-1-i}} + 2^{m_2} u$$

for some $u \in GR(2^e, m)$. By squaring both sides, we get

$$\begin{aligned}
&\left(\sum_{\substack{0 \leq i \leq s \\ i \preceq_2 s}} x^i b^{s-i} \right)^{2^{m_1}} \equiv \left(\sum_{i=0}^{m_2-1} 2^i \sum_{k=0}^{n-1} M_{m,2}^{(i)}(s,k) x^{k.2^{m_1-1-i}} b^{2^{m_1-1}s - k.2^{m_1-1-i}} \right)^2 \mod 2^{m_2+1} \\
&\equiv \sum_{i=0}^{m_2} 2^i \sum_{\substack{0 \leq i_1 \leq i_2 \leq i-1 \\ i_1+i_2+1=i}} \sum_{\substack{0 \leq k_1, k_2 \leq n-1 \\ k_1 < k_2 \ if \ i_1=i_2}} M_{m,2}^{(i_1)}(s,k_1) M_{m,2}^{(i_2)}(s,k_2) x^{k_1.2^{m_1-1-i_1}+k_2.2^{m_1-1-i_2}} b^{2^{m_1}s - \left(k_1.2^{m_1-1-i_1}+k_2.2^{m_1-1-i_2}\right)} \\
&\quad + \sum_{i=0}^{m_2-1} 2^{2i} \sum_{k=0}^{n-1} \left(M_{m,2}^{(i)}(s,k) \right)^2 x^{k.2^{m_1-i}} b^{2^{m_1}s - k.2^{m_1-i}} \mod 2^{m_2+1} \\
&\equiv \sum_{i=0}^{m_2} 2^i \sum_{\substack{0 \leq i_1 \leq i_2 \leq i-1 \\ i_1+i_2+1=i}} \sum_{\substack{0 \leq k_1, k_2 \leq n-1 \\ k_1 < k_2 \ if \ i_1=i_2}} M_{m,2}^{(i_1)}(s,k_1) M_{m,2}^{(i_2)}(s,k_2) x^{2^{m_1-i}(k_1.2^{i_2}+k_2.2^{i_1})} b^{2^{m_1}s - 2^{m_1-i}(k_1.2^{i_2}+k_2.2^{i_1})} \\
&\quad + \sum_{i=0}^{m_2-1} 2^{2i} \sum_{k=0}^{n-1} \left(M_{m,2}^{(i)}(s,k) \right)^2 x^{k.2^{m_1-i}} b^{2^{m_1}s - k.2^{m_1-i}} \mod 2^{m_2+1} \\
&\equiv \sum_{i=0}^{m_2} 2^i \sum_{\substack{0 \leq i_1 \leq i_2 \leq i-1 \\ i_1+i_2+1=i}} \sum_{k=0}^{n-1} \left(M_{m,2}^{(i_1)}(s,k) * M_{m,2}^{(i_2)}(s,k) \right) x^{2^{m_1-i}k} b^{2^{m_1}s - 2^{m_1-i}k} \\
&\quad + \sum_{\substack{0 \leq i \leq m_2-1 \\ i \text{ even}}} 2^i \sum_{k=0}^{n-1} \left(M_{m,2}^{(\frac{i}{2})}(s,k) \right)^2 x^{k.2^{m_1-\frac{i}{2}}} b^{2^{m_1}s - k.2^{m_1-\frac{i}{2}}} \mod 2^{m_2+1} \\
&\equiv \sum_{i=0}^{m_2} 2^i \sum_{k=0}^{n-1} \left(\sum_{\substack{0 \leq i_1 \leq i_2 \leq i-1 \\ i_1+i_2+1=i}} \left(M_{m,2}^{(i_1)}(s,k) * M_{m,2}^{(i_2)}(s,k) \right) \right) x^{2^{m_1-i}k} b^{2^{m_1}s - 2^{m_1-i}k} \\
&\quad + \sum_{\substack{0 \leq i \leq m_2-1 \\ i \text{ even}}} 2^i \sum_{k'=0}^{n-1} \left(M_{m,2}^{(\frac{i}{2})}(s, 2^{m-\frac{i}{2}}k') \right)^2 x^{k'.2^{m_1-i}} b^{2^{m_1}s - k'.2^{m_1-i}} \mod 2^{m_2+1} \\
&\qquad\qquad\qquad\qquad \text{where } k' = k.2^{\frac{i}{2}} \mod n \\
&\equiv \sum_{i=0}^{m_2} 2^i \sum_{k=0}^{n-1} M_{m,2}^{(i)}(s,k) x^{2^{m_1-i}k} b^{2^{m_1}s - 2^{m_1-i}k} \mod 2^{m_2+1}.
\end{aligned}$$

■

Theorem 3.6. *If $x, b \in \mathcal{T}_m \subset GR(2^e, m)$, $n = 2^m - 1$ and $s \in [0, n-1]$, then*

$$(x+b)^{s.2^{m\tau}} = \sum_{i=0}^{e-1} 2^i \sum_{k=0}^{n-1} M_{m,2}^{(i)}(s,k) x^{2^{m\tau-i}k} b^{2^{m\tau}s - 2^{m\tau-i}k}.$$

Proof: Trivial using Lemma 3.4 and Lemma 3.5. ∎

Lemma 3.7. *Suppose $x, b \in \mathcal{T}_m \subset GR(2^e, m)$, $n = 2^m - 1$ and $s \in [0, n-1]$. Then for any j; $0 \leq j \leq e-1$,*

$$\begin{aligned}(x+b)^{s.2^{m\tau}} &= \sum_{i=0}^{j-1} 2^i \sum_{k=0}^{n-1} P(K_{m,2}^{(i)}(s,k)) x^{2^{m\tau-i}k} b^{2^{m\tau}s - 2^{m\tau-i}k} \\ &\quad + 2^j \sum_{k=0}^{n-1} K_{m,2}^{(j)}(s,k) x^{2^{m\tau-j}k} b^{2^{m\tau}s - 2^{m\tau-j}k} \\ &\quad + \sum_{i=j+1}^{e-1} 2^i \sum_{k=0}^{n-1} M_{m,2}^{(i)}(s,k) x^{2^{m\tau-i}k} b^{2^{m\tau}s - 2^{m\tau-i}k}.\end{aligned}$$

Proof: The proof is by induction on j.

Clearly the statement is true for $j = 0$. Suppose it is true for $j (< e-1)$. Then it needs to be proved for $j+1$. It is trivial by using the fact:

$$K_{m,2}^{(j)}(s,k) = P\left(K_{m,2}^{(j)}(s,k)\right) + 2\lfloor \frac{1}{2} K_{m,2}^{(j)}(s,k) \rfloor.$$

∎

Taking $j = e-1$, we get the following corollary.

Corollary 3.8. *Suppose $x, b \in \mathcal{T}_m \subset GR(2^e, m)$, $n = 2^m - 1$ and $s \in [0, n-1]$. Then*

$$(x+b)^{s.2^{m\tau}} = \sum_{i=0}^{e-1} 2^i \sum_{k=0}^{n-1} P(K_{m,2}^{(i)}(s,k)) x^{2^{m\tau-i}k} b^{2^{m\tau}s - 2^{m\tau-i}k}.$$

Theorem 3.9. *An extended cyclic code over any subring of $GR(2^e, m)$ of length $n+1 = 2^m$ with defining sets $\hat{T}_1, \cdots, \hat{T}_e$ is affine invariant if and only if for all $i = 1, 2, \cdots, e$; $j = 1, 2, \cdots, i$,*

$$s \in \hat{T}_i, P\left(K_{m,2}^{(i-j)}(s,k)\right) = 1 \Rightarrow 2^{m\tau-(i-j)}.k \in \hat{T}_j. \tag{3}$$

Proof: By Theorem 2.1, the code is affine invariant if and only if for $i = 1, \cdots, e$ and $\sigma \in AGL(1, 2^m)$, each polynomial in the set

$$\left\{ 2^{e-i} \left(f_\sigma^{(L)}(Z) \right)^{s.2^{m\tau}} | s \in \hat{T}_i \right\}$$

is of the form

$$\sum_{j=1}^{i} 2^{e-j} \sum_{k \in \hat{T}_j} a_{s,j,k} Z^k \qquad \mod Z^n - 1$$

where $a_{s,j,k} \in \mathcal{T}_m$. Since the code is extended cyclic, it is sufficient to consider the polynomials $f_\sigma^{(L)}(Z) = Z + b$; $b \in \mathcal{T}_m$. Now, by Corollary 3.8, for any $i = 1, \cdots, e$, $b \in \mathcal{T}_m$, $s \in \hat{T}_i$,

$$2^{e-i}(Z+b)^{s,2^{m\tau}} = \sum_{j=1}^{i} 2^{e-j} \sum_{k=0}^{n-1} P\left(K_{m,2}^{(i-j)}(s,k)\right) b^{(2^{(i-j)}s-k)2^{m\tau-(i-j)}} Z^{k.2^{m\tau-(i-j)}} \qquad \mod Z^n - 1.$$

So, the code is affine invariant if and only if for all $i = 1, 2, \cdots, e;\ j = 1, 2, \cdots, i$,

$$s \in \hat{T}_i, P\left(K_{m,2}^{(i-j)}(s,k)\right) = 1 \Rightarrow 2^{m\tau-(i-j)}.k \in \hat{T}_j.$$

■

For $i < e$, the necessary and sufficient conditions can also be put as

$$s \in \hat{T}_i \setminus \hat{T}_{i+1}, P\left(K_{m,2}^{(i-j)}(s,k)\right) = 1 \Rightarrow 2^{m\tau-(i-j)}.k \in \hat{T}_j$$

since for $s \in \hat{T}_{i+1} \subseteq \hat{T}_i$, $P\left(K_{m,2}^{(i-j)}(s,k)\right) = 1 \Rightarrow P\left(K_{m,2}^{((i+1)-(j+1))}(s,k)\right) = 1 \Rightarrow 2^{m\tau-(i-j)}.k = 2^{m\tau-((i+1)-(j+1))}.k \in \hat{T}_{(j+1)} \subseteq \hat{T}_j$.

For $j = i$, the necessary and sufficient condition in Theorem 3.9 states that, $\hat{T}_1, \cdots, \hat{T}_e$ are lower ideals in $[0, n]$. In particular, for $i = 2, j = 1$, the condition is equivalent to

$$s \in \hat{T}_2,\ \ M_{m,2}^{(1)}(s,k) \not\equiv 0 \mod 2 \Rightarrow 2^{m-1}.k \in \hat{T}_1.$$

So, for $e = 2$, the theorem gives [29, Theorem 5.1] as a special case.

Note that if the code is over a subring $GR(2^e, m_1)$ of $GR(2^e, m)$, then $\hat{T}_j$ is a union of 2^{m_1}-cyclotomic cosets modulo $p^m - 1$. So $2^{m\tau-l}.k \in \hat{T}_j \Leftrightarrow 2^{(m\tau-l)\ mod\ m_1}k \in \hat{T}_j$. Hence if $m_1 = 1$, then $2^{m\tau-l}.k \in \hat{T}_j \Leftrightarrow k \in \hat{T}_j$. So, we have

Corollary 3.10. *An extended cyclic code over $\mathbb{Z}_{2^e}$ of length $n+1 = 2^m$ with defining sets $\hat{T}_1, \cdots, \hat{T}_e$ is affine invariant if and only if for all $i = 1, 2, \cdots, e;\ j = 1, 2, \cdots, i$,*

$$s \in \hat{T}_i, P\left(K_{m,2}^{(i-j)}(s,k)\right) = 1 \Rightarrow k \in \hat{T}_j.$$

Though the condition for extended cyclic codes to be affine invariant as derived here as well as in [29] do not seem to have any similarity with that derived in [28], as seen in the following example, they impose the same conditions on the defining sets.

Example 3.1. Consider an extended cyclic code of length $n = 16 = 2^4$ over $\mathbb{Z}_8$. So, we have $m = 4, e = 3$. Let us take $\hat{T}_3 = \{0, 1, 2, 4, 8\}$. Clearly, $\hat{T}_2 = \{0, 1, 2, 4, 8\}$ satisfies the conditions of Theorem 3.9 as well as [28, Theorem 11]. The conditions imposed by the case $i = 2,\ j = 1$ (in Theorem 3.9) is $\hat{T}_1 \supseteq \{0, 1, 2, 4, 8\}$. To check the conditions imposed by the case $i = 3,\ j = 1$, one needs to compute $M_{4,2}^{(2)}(0,k), M_{4,2}^{(2)}(1,k), M_{4,2}^{(2)}(2,k)$, $M_{4,2}^{(2)}(4,k), M_{4,2}^{(2)}(8,k)$. It can be checked that

$$M_{4,2}^{(2)}(0,k) = 0\ \ \forall k$$
$$M_{4,2}^{(2)}(1,k) = \begin{cases} 1 & \text{when } k = 1,2,3 \\ 0 & \text{otherwise} \end{cases}$$

$$M_{4,2}^{(2)}(2,k) = \begin{cases} 1 & \text{when } k = 2,4,6 \\ 0 & \text{otherwise} \end{cases}$$
$$M_{4,2}^{(2)}(4,k) = \begin{cases} 1 & \text{when } k = 4,8,12 \\ 0 & \text{otherwise} \end{cases}$$
$$M_{4,2}^{(2)}(8,k) = \begin{cases} 1 & \text{when } k = 8,1,9 \\ 0 & \text{otherwise} \end{cases}$$

where $M_{4,2}^{(2)}(2,k)$, $M_{4,2}^{(2)}(4,k)$ and $M_{4,2}^{(2)}(8,k)$ are computed from $M_{4,2}^{(2)}(1,k)$ using Lemma 3.2.

So, according to Theorem 3.9, the code is affine invariant if and only if $\hat{T}_1$ is a lower ideal containing $\{0,1,2,4,8,3,6,12,9\}$. Abdukhalikov's result also imposes the same condition on $\hat{T}_1$ for the code to be affine invariant. However, one has to be careful in comparing his result with that presented here, since his definition of defining sets differs from the way they are defined here and in [29].

The following theorem identifies a class of affine invariant BCH codes using Theorem 3.9.

Theorem 3.11. *Let $\hat{B}(n,\delta_1,\cdots,\delta_e)$ be the extended BCH codes of length $n+1=2^m$ over $\mathbb{Z}_{2^e}$ with designed distances $\delta_1,\cdots,\delta_e$. If $\delta_{i-l} \geq 2^l(\delta_i-2)$ for $i=1,\cdots,e$, $l=0,\cdots,i-1$, then $\hat{B}(n,\delta_1,\cdots,\delta_e)$ is affine-invariant.*

Proof: As mentioned in Section 2, without loss of generality, we can assume each designed distance to be odd. By Theorem 3.9, it is sufficient to prove that for $i=1,\cdots,e$, $l=0,\cdots,i-1$,

$$s \leq \delta_i - 1 \text{ and } K_{m,2}^{(l)}(s,k) \neq 0 \Rightarrow k \leq \delta_{i-l} - 1.$$

By Lemma 3.2(2), it suffices to check only for the odd values of s. Since $\delta_i - 1$ is even, it is sufficient to consider $s \leq \delta_i - 2$. For $l=0$, it is trivial. For $l \neq 0$, $s \leq \delta_i - 2$ and $K_{m,2}^{(l)}(s,k) \neq 0 \Rightarrow k \leq 2^l s - 1 \leq 2^l(\delta_i-2)-1 \leq \delta_{i-l}-1$.
■

The following corollary gives stronger conditions for pairs of consecutive designed distances, under which a BCH code is affine invariant. If these stronger conditions are satisfied by the designed distances, one need not check for the other conditions required by Theorem 3.11, since, then they are automatically satisfied.

Corollary 3.12. *Let $\hat{B}(n,\delta_1,\cdots,\delta_e)$ be the extended BCH code of length $n+1=2^m$ over $\mathbb{Z}_{2^e}$ with designed distances $\delta_1,\cdots,\delta_e$. If $\delta_{i-1} \geq 2\delta_i - 2$ for $1 < i \leq e$, then the code $\hat{B}(n,\delta_1,\cdots,\delta_e)$ is affine invariant.*

Proof: We shall show that if $\hat{B}(n,\delta_1,\cdots,\delta_e)$ satisfies these conditions, then it also satisfies the conditions of Theorem 3.11. For $i=1,\cdots,e$, $l=0,\cdots,i-1$,

$$\begin{aligned} \delta_{i-l} &\geq 2\delta_{i-l+1} - 2 \\ &\geq 2(2\delta_{i-l+2} - 2) - 2 \\ &\cdots \\ &\geq 2(2(\cdots 2(2\delta_i - 2) - 2)\cdots 2) - 2 \end{aligned}$$

$$\begin{aligned} &= 2^l\delta_i - 2(1+2+\cdots+2^{l-1}) \\ &= 2^l\delta_i - 2(2^l-1) = 2^l(\delta_i-2)+2 > 2^l(\delta_i-2). \end{aligned}$$

■

The GRM codes over $\mathbb{Z}_4$ of order (r,r) are known to be affine invariant. However, the same is not true for GRM codes over $\mathbb{Z}_{p^e}$ for $e>2$, that is, GRM codes of order $(r,r,\cdots,r)$ over $\mathbb{Z}_{2^e}$ are not necessarily affine invariant. In the following, we proceed towards finding a class of affine invariant GRM codes over $\mathbb{Z}_{2^e}$.

Lemma 3.13.

$$K^{(i)}_{m,2}(s,k)\neq 0 \Rightarrow \begin{cases} wt_2(k)\leq 2^{i-1}wt_2(s) & \textit{for } i>0 \\ wt_2(k)\leq wt_2(s) & \textit{for } i=0. \end{cases}$$

Proof: The proof is by induction on i. For $i=0$, the result is obvious. For $i=1$, $K^{(i)}_{m,2}\neq 0 \Rightarrow$ there exist integers $k_1,k_2 \preceq_2 s$ such that $k_1+k_2\equiv k \bmod n$. So, $wt_2(k)\leq wt_2(s)$.

Suppose the claim is true for i and smaller integers, where $i>0$. Then it needs to be proved for $i+1$.

$$K^{(i+1)}_{m,2}(s,k)\neq 0 \Rightarrow M^{(i+1)}_{m,2}(s,k)\neq 0 \text{ or } K^{(i)}_{m,2}(s,2^{m-1}k)\neq 0. \tag{4}$$

If $K^{(i)}_{m,2}(s,2^{m-1}k)\neq 0$, then by the induction hypothesis, $wt_2(k)\leq 2^{i-1}wt_2(s)\leq 2^i wt_2(s)$. If $M^{(i+1)}_{m,2}(s,k)\neq 0$, then either $\exists i_1,i_2,k_1,k_2$ satisfying $i_1+i_2=i, i_1\leq i_2, 2^{i_2}k_1+2^{i_1}k_2\equiv k \bmod n$ such that $M^{(i_1)}_{m,2}(s,k_1)\neq 0$ and $M^{(i_2)}_{m,2}(s,k)\neq 0$, or, $(i+1)$ is even and $M^{\frac{(i+1)}{2}}_{m,2}(s,2^{m-\frac{(i+1)}{2}}k)\neq 0 \Leftrightarrow M^{\frac{(i+1)}{2}}_{m,2}(2^{\frac{(i+1)}{2}}s,k)\neq 0$. In the second case, by the induction hypothesis,
$wt_2(k)\leq 2^{\frac{(i-1)}{2}}wt_2(2^{\frac{(i+1)}{2}}s \bmod n) = 2^{\frac{(i-1)}{2}}wt_2(s)\leq 2^i wt_2(s)$. For the first case, the following subcases hold.
Case I: $i_1=0$:

$$\begin{aligned} wt_2(k) &= wt_2(2^{i_2}k_1+2^{i_1}k_2) \\ &\leq wt_2(2^{i_2}k_1)+wt_2(2^{i_1}k_2) \\ &= wt_2(k_1)+wt_2(k_2) \\ &\leq (2^{i_2-1}+1)wt_2(s) \\ &\leq (2^{i-1}+1)wt_2(s)\leq 2^i wt_2(s). \end{aligned}$$

Case II: $i_1\neq 0$:

$$\begin{aligned} wt_2(k) &= wt_2(2^{i_2}k_1+2^{i_1}k_2) \\ &\leq wt_2(2^{i_2}k_1)+wt_2(2^{i_1}k_2) \\ &= wt_2(k_1)+wt_2(k_2) \\ &\leq 2^{i_1-1}wt_2(s)+2^{i_2-1}wt_2(s) \end{aligned}$$

$$\begin{aligned} &\leq 2^{i-1}wt_2(s) + 2^{i-1}wt_2(s) \\ &\leq 2^{i}wt_2(s). \end{aligned}$$

■

Theorem 3.14. *A GRM code $GRM(r_1, \cdots, r_e, m)$ over $\mathbb{Z}_{2^e}$ is affine invariant if either $e = 1$ or for $i = 2, \cdots, e;\ l = 1, \cdots, i-1,\ r_{i-l} \leq m - 2^{l-1}(m - r_i)$.*

Proof: Clearly for $i = 1, \cdots, e$, $\hat{T}_i$ is a lower ideal. This completes the proof for $e = 1$. Now, we need to prove (3) for $i = 1, \cdots, e;\ l = i - j = 1, \cdots, i-1$. For these values of i and l,

$$\begin{aligned} & s \in \hat{T}_i \text{ and } K^{(l)}_{m,2}(s,k) \neq 0 \\ \Rightarrow\ & wt_2(s) \leq m - r_i \text{ and } wt_2(k) \leq 2^{l-1}wt_2(s) \\ \Rightarrow\ & wt_2(k) \leq 2^{l-1}(m - r_i) \\ \Rightarrow\ & wt_2(k) \leq m - r_{i-l} \\ \Rightarrow\ & k \in \hat{T}_{i-l}. \end{aligned}$$

By Corollary 3.10, the code is affine invariant. ■

Example 3.2. For any $m + 1 \geq e \geq 1$, let us consider the code $GRM(r_1, \cdots, r_e, m)$ over $\mathbb{Z}_{2^e}$ with $r_e = m - 1$ and $r_i = m - 2^{e-i-1}$ for $i < e$. For $i = 2, \cdots, e$,

$$\begin{aligned} & r_i \geq m - 2^{e-i} \\ \Rightarrow\ & 2^{e-i} \geq m - r_i \\ \Rightarrow\ & m - 2^{l-1}.2^{e-i} \leq m - 2^{l-1}(m - r_i). \end{aligned}$$

So, for $l = 1, \cdots, i-1$,

$$\begin{aligned} r_{i-l} &= m - 2^{e-(i-l)-1} \\ &= m - 2^{l-1}.2^{e-i} \\ &\leq m - 2^{l-1}(m - r_i). \end{aligned}$$

So, the code is affine invariant.

3.2 Arbitrary p and $e = 2$

In this subsection, extended cyclic codes over $GR(p^2, m)$ is considered for arbitrary p and the affine invariant codes among them are investigated. For any $i_1, i_2, \cdots, i_k$ with $i_1 + i_2 + \cdots + i_k \leq s$, let us define the quantity $\begin{pmatrix} & s & \\ i_1\ i_2 & \cdots & i_k \end{pmatrix}$ to be the number of ways the disjoint subsets $S_1, S_2, \cdots, S_k \subset [0, n-1]$ can be chosen with

$|S_j| = i_j$ for $1 \le j \le k$. Its value is given by

$$\binom{s}{i_1\ i_2\ \cdots\ i_k} = \binom{s}{i_1}\binom{s-i_1}{i_2}\cdots\binom{s-i_1-\cdots-i_{k-1}}{i_k}.$$

Lemma 3.15 (Generalized Lucas Lemma). *Suppose $s, i_1, \cdots, i_k \in [0, p^m-2]$ have the p-ary representations $(s_0, \cdots s_{m-1}), (i_{1,0}, \cdots, i_{1,m-1}), \cdots, (i_{k,0}, \cdots, i_{k,m-1})$ respectively. Then*

$$\binom{s}{i_1\ i_2\ \cdots\ i_k} = \prod_{j=0}^{m-1}\binom{s_j}{i_{1,j}\ i_{2,j}\ \cdots\ i_{k,j}} \text{ mod } p.$$

Proof: Trivial. ■

This gives the following corollary.

Corollary 3.16. *Suppose $s, i_1, \cdots, i_k \in [0, p^m-2]$ have the p-ary representations $(s_0, \cdots s_{m-1})$, $(i_{1,0}, \cdots, i_{1,m-1}), \cdots, (i_{k,0}, \cdots$ respectively. Then $\binom{s}{i_1\ i_2\ \cdots\ i_k} \not\equiv 0$ mod p if and only if $i_{1,j} + \cdots + i_{k,j} \le s_j$ for $0 \le j \le m-1$.*

For any $s, k \in [0, p^m-2]$, let us define the set $S_{(s,k)} \triangleq \{(i_0, \cdots, i_s) | \sum_{j=0}^{s} i_j = p; i_j \neq p \forall j; j \preceq_p s$ whenever $i_j \neq 0; \sum_{j=0}^{s} j i_j \equiv k \text{ mod } p^m - 1\}$. Let us also define the quantity

$$M_{m,p}(s,k) = \frac{1}{p}\sum_{(i_0,\cdots,i_s)\in S_{(s,k)}} \binom{p}{i_0\ \cdots\ i_{s-1}}\binom{s}{1}^{i_1}\cdots\binom{s}{s-1}^{i_{s-1}}.$$

For $p = 2$, it reduces to $M_m(s,k)$ as defined in [29]: $M_{m,2}(s,k) = M_m(s,k) = |\{(i,j) | i < j; i, j \preceq_2 s; i + j \equiv k \text{ mod } n\}|$.

Lemma 3.17. *If $n = p^m - 1$, $1 \le i \le m$ and $s, k \in [0, n-1]$, then*

1. *$M_{m,p}(s,k) = M_{m,p}(p^i s, p^i k)$.*
2. *$M_{m,p}(p^i s, k) = M_{m,p}(s, p^{(m-i)} k)$.*
3. *$M_{m,p}(s,k) \neq 0 \Rightarrow k \le ps - 1$.*

Proof: 1) It is sufficient to assume $i = 1$. By definition,

$$M_{m,p}(s,k) = \frac{1}{p}\sum_{(i_0,\cdots,i_s)\in S_{(s,k)}} \binom{p}{i_0\ \cdots\ i_{s-1}}\binom{s}{1}^{i_1}\cdots\binom{s}{s-1}^{i_{s-1}} \tag{5}$$

$$M_{m,p}(ps,pk) = \frac{1}{p}\sum_{(i'_0,\cdots,i'_{ps})\in S_{(ps,pk)}} \binom{p}{i'_0\ \cdots\ i'_{ps-1}}\binom{ps}{1}^{i'_1}\cdots\binom{ps}{ps-1}^{i'_{s-1}} \tag{6}$$

where multiplication by p is modulo n. Note that multiplication modulo n by p cyclically shifts the p-ary representation of any integer. The inverse operation is multiplication modulo n by $p^{(m-1)}$.

For any $(i_0, \cdots, i_s) \in S_{(s,k)}$, whenever $i_j \neq 0$, $j \preceq_p s \Rightarrow pj(\bmod n) \preceq_p ps(\bmod n)$ and so $pj(\bmod n) \leq ps(\bmod n)$. This gives a 1-1 correspondence

$$\begin{array}{rcl} S_{(s,k)} & \rightarrow & S_{(ps,pk)} \\ (i_0, \cdots, i_s) & \mapsto & (i'_0, \cdots, i'_{ps \bmod n}) \end{array}$$

given by

$$\begin{array}{l} i'_{pj \bmod n} = i_j \text{ whenever } i_j \neq 0 \\ i'_{pj \bmod n} = 0 \text{ otherwise .} \end{array}$$

Such a $(i'_0, \cdots, i'_{ps \bmod n})$ satisfies all the conditions to be in $S_{(ps,pk)}$.

Clearly, under this 1-1 correspondence, the corresponding terms in (5) and (6) are the same. So, $M_{m,p}(s,k) = M_{m,p}(ps,pk)$.

2) directly follows from (1).

3)

$$\begin{array}{rl} & M_{m,p}(s,k) \neq 0 \\ \Rightarrow & (i_0, \cdots, i_s) \in M_{m,p}(s,k) \\ \Rightarrow & k = \sum_{j=0}^{s} j i_j \bmod n \\ \Rightarrow & k \leq (s-1).1 + s.(p-1) \;\; \text{since} \sum_{j=0}^{s} j i_j \text{ is maximum when } i_s = p-1, i_{s-1} = 1 \\ \Rightarrow & k \leq ps - 1. \end{array}$$

∎

In [12], the authors proved that an extended cyclic code of length p^m over F_{p^m} is affine invariant if and only if its defining set is a lower ideal of $[0, p^m - 1]$. It was shown in [29] that an extended cyclic code of length 2^m over $GR(4,m)$ is affine invariant if and only if $\hat{T}_1, \hat{T}_2$ are lower ideals in $[0, 2^m - 1]$ and $s \in \hat{T}_2, M_{m,2}(s,k) \not\equiv 0 \bmod 2 \Rightarrow 2^{(m-1)}k \in \hat{T}_1$. In the following, we show that the same conditions are valid for codes over $GR(p^2,m)$ for any prime p.

Lemma 3.18. *If $x, b \in \mathcal{T}_m \subseteq R = GR(p^2,m)$, $m \geq 1$ and $s \in [0,n], n = p^m - 1$, then*

$$(x+b)^{sp^m} = \sum_{j \preceq_p s} \binom{s}{j}^{p^m} x^j b^{s-j} + p \sum_{k=0}^{n-1} M_{m,p}(s,k) x^{kp^{(m-1)}} b^{(ps-k)p^{(m-1)}}.$$

Proof: Let $x, b \in \mathcal{T}_m$. Then

$$(x+b)^{sp^m} = \left(\sum_{i=0}^{s} \binom{s}{i} x^i b^{s-i} \right)^{p^m}$$

$$
\begin{aligned}
&= \sum_{i=0}^{s} \left[\binom{s}{i} x^i b^{s-i} \right]^{p^m} \\
&+ \sum_{\substack{(i_0,\cdots,i_s) \\ \sum_{j=0}^{s} i_j = p;\ i_j \neq p \forall j \\ j \preceq_p s \text{ whenever } i_j \neq 0}} \binom{p}{i_0 \ \cdots \ i_{s-1}} \binom{s}{0}^{i_0} \binom{s}{1}^{i_1} \cdots \binom{s}{s}^{i_{s-1}} \left[x^{\sum_{j=0}^{s} j i_j} b^{\sum_{j=0}^{s} i_j (s-j)} \right]^{p^{(m-1)}} \\
&= \sum_{j \preceq_p s} \binom{s}{j}^{p^m} x^j b^{s-j} \\
&+ \sum_{\substack{(i_0,\cdots,i_s) \\ \sum_{j=0}^{s} i_j = p;\ i_j \neq p \forall j \\ j \preceq_p s \text{ whenever } i_j \neq 0}} \binom{p}{i_0 \ \cdots \ i_{s-1}} \binom{s}{1}^{i_1} \cdots \binom{s}{s-1}^{i_{s-1}} \left[x^{\sum_{j=0}^{s} j i_j} b^{ps - \sum_{j=0}^{s} i_j j} \right]^{p^{(m-1)}} \\
&= \sum_{j \preceq_p s} \binom{s}{j}^{p^m} x^j b^{s-j} + p \sum_{k=0}^{n-1} M_{m,p}(s,k) x^{kp^{(m-1)}} b^{(ps-k)p^{(m-1)}}.
\end{aligned}
$$

■

Theorem 3.19. *Let $\hat{\mathcal{C}}$ be an extended cyclic code over a subring $GR(p^2, m_1)$ of $GR(p^2, m)$ of length p^m with defining sets $(\hat{T}_1, \hat{T}_2)$. $\hat{\mathcal{C}}$ is affine invariant if and only if*

1. *$\hat{T}_1, \hat{T}_2$ are lower ideals in $[0, n]$.*
2. *$s \in \hat{T}_2, M_{m,p}(s,k) \not\equiv 0 \mod p \Rightarrow p^{(m-1)} k \in \hat{T}_1$.*

Proof: By [29, Theorem 4.2], $\hat{\mathcal{C}}$ is affine invariant if and only if the polynomials in the set

$$\{(f_\sigma^{(L)}(Z))^{sp^m} | s \in \hat{T}_2\} \cup \{p(f_\sigma^{(L)}(Z))^{sp^m} | s \in \hat{T}_1\}$$

are MS polynomials of $\hat{\mathcal{C}}$ $\forall \sigma \in AGL(1, p^m)$. Since $\hat{\mathcal{C}}$ is extended cyclic, it is sufficient to check this only for permutations given by $f_\sigma^{(L)}(Z) = Z + b,\ b \in \mathcal{T}_m \setminus \{0\}$.

If $s \in \hat{T}_1$, then

$$p(Z+b)^{sp^m} \equiv p \sum_{i \preceq_p s} \binom{s}{i}^{p^m} b^{s-i} Z^i \mod Z^n - 1.$$

This is an MS polynomial of $\hat{\mathcal{C}}$ if $i \in \hat{T}_1$ $\forall i \preceq_p s$, i.e. $\hat{T}_1$ must be a lower ideal.

If $s \in \hat{T}_2$, then by Lemma 3.18,

$$
\begin{aligned}
(Z+b)^{sp^m} &= \sum_{i \preceq_p s} \binom{s}{i}^{p^m} b^{s-i} Z^i \\
&+ p \sum_{k=0}^{n-1} M_{m,p}(s,k) b^{(ps-k)p^{(m-1)}} Z^{kp^{(m-1)}} \mod (Z^n - 1).
\end{aligned}
$$

This will be an MS polynomial of $\hat{\mathcal{C}}$ if $i \in \hat{T}_2$ whenever $i \preceq_p s$ (i.e. $\hat{T}_2$ is a lower ideal) and if $M_{m,p}(s,k) \not\equiv 0 \bmod p \Rightarrow kp^{(m-1)} \in \hat{T}_1$. Thus conditions (1) and (2) must hold for $\hat{\mathcal{C}}$ to be affine invariant and vice versa. ∎

The following theorem gives some sufficient conditions under which extended BCH codes of length p^m over $\mathbb{Z}_{p^2}$ are affine invariant.

Theorem 3.20. *Let $\hat{B}(n,\delta_1,\delta_2)$ be an extended BCH code of length p^m over $\mathbb{Z}_{p^2}$. If either (i) $p|(\delta_2-1)$ and $\delta_1 \geq p(\delta_2-2)$ or (ii) $\delta_1 \geq p(\delta_2-1)$, then $\hat{B}(n,\delta_1,\delta_2)$ is affine invariant.*

Proof: The defining sets of the code are

$$\hat{T}_1 = \cup_{i\in[0,\delta_1)}[i]^p$$
$$\hat{T}_2 = \cup_{i\in[0,\delta_2)}[i]^p.$$

Clearly, both these sets are lower ideals. We need to check that $k \in T_1$ whenever $M_{m,p}(s,k) \not\equiv 0 \bmod p$ and $s \in T_2$. By Lemma 3.17(2), it is sufficient to consider $s \leq \delta_2 - 1$ which are not divisible by p.

Suppose condition (ii) holds and $s \in T_2$, $M_{m,p}(s,k) \not\equiv 0 \bmod p$. Then

$$\begin{aligned} & s \leq \delta_2 - 1 \\ \Rightarrow\quad & ps - 1 \leq p(\delta_2-1) - 1 = p\delta_2 - p - 1 \\ \Rightarrow\quad & k \leq p\delta_2 - p - 1 \text{ whenever } M_{m,p}(s,k) \not\equiv 0 \bmod n \text{ (by Lemma 3.17(3))} \\ \Rightarrow\quad & k \leq \delta_1 - 1 \text{ whenever } M_{m,p}(s,k) \not\equiv 0 \bmod n \\ \Rightarrow\quad & k \in \hat{T}_1 \text{ whenever } M_{m,p}(s,k) \not\equiv 0 \bmod n. \end{aligned}$$

If condition (i) holds, then it is sufficient to consider $s \leq \delta_2 - 2$ since by Lemma 3.17(2), we need not consider s, which are divisible by p. Then

$$\begin{aligned} & s \leq \delta_2 - 2 \\ \Rightarrow\quad & ps - 1 \leq p(\delta_2-2) - 1 = p\delta_2 - 2p - 1 \\ \Rightarrow\quad & k \leq p\delta_2 - 2p - 1 \text{ whenever } M_{m,p}(s,k) \not\equiv 0 \bmod n \text{ (by Lemma 3.17(3))} \\ \Rightarrow\quad & k \leq \delta_1 - 1 \text{ whenever } M_{m,p}(s,k) \not\equiv 0 \bmod n \\ \Rightarrow\quad & k \in \hat{T}_1 \text{ whenever } M_{m,p}(s,k) \not\equiv 0 \bmod n. \end{aligned}$$

∎

4 Conclusion

A set of necessary and sufficient conditions were derived for extended cyclic codes of length p^m over any subring of $GR(p^e,m)$ to be affine invariant for $p=2$ with arbitrary e and for $e=2$ with arbitrary p. Classes of affine invariant BCH codes and GRM codes over $\mathbb{Z}_{2^e}$ and over $\mathbb{Z}_{p^2}$ are found using these conditions. However, it is still not known exactly which BCH and GRM codes are affine invariant.

References

[1] K.N.Manoj and B.Sundar Rajan, "Full Rank Distance Codes," Technical Report No:TR-PME-2002-16, Electrical Communication Engineering Department, IISc, Bangalore, India, October 4, 2002.

[2] B.Sundar Rajan and U.Sripati, "On the Rank-Distance Codes," Technical Report No:TR-PME-2003-04, Electrical Communication Engineering Department, IISc, Bangalore, India, October 4, 2002.

[3] R. E. Blahut, *Theory and Practice of Error Control Codes*, Addison Wesley (1983).

[4] Bikash Kumar Dey, "F_q-linear Cyclic Codes over F_{q^m}: DFT Approach," Technical Report No:TR-PME-2003-05, Electrical Communication Engineering Department, IISc, Bangalore, India, October 4, 2003.

[5] F. J. MacWilliams, "Permutation decoding of systematic codes," *Bell Sys. Tech. Jl.*, pp. 485–505, 1964.

[6] L. M. G. M. Tolhuizen and W. J. V. Gils, "A large automorphism group decreases the computations in the construction of an optimal encoder/decoder pair for a linear block code," *IEEE Trans. Inform. Theory*, vol. 34, no. 2, pp. 333–337, 1988.

[7] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes.* North-Holland, 1988.

[8] H. Chabanne, "Permutation decoding of abelian codes," *IEEE Trans. Inform Theory*, vol. 38, no. 6, pp. 1826–1829, 1992.

[9] W. C. Huffman, "Codes and groups," in *Handbook of Coding Theory* (V. S. Pless and W. C. Huffman, eds.), vol. 2, ch. 17, pp. 1345–1440, New York, NY, USA: Elsevier Science, 1998.

[10] D. M. Gordon, "Minimal permutation sets for decoding the binary golay codes," *IEEE Trans. Inform. Theory*, vol. 28, pp. 541–543, 1982.

[11] J. Wolfman, "A permutation decoding of the (24,12,8) golay code," *IEEE Trans. Inform. Theory*, vol. 29, pp. 748–750, 1983.

[12] T. Kasami, S. Lin, and W. W. Perterson, "Some result on cyclic codes which are invariant under the affine group and their applications," *Information and Control*, vol. 11, pp. 475–496, 1968.

[13] T. P. Berger and P. Charpin, "The permutation group of affine-invariant extended cyclic codes," *IEEE Trans. Inform. Theory*, vol. 42, no. 6, pp. 2194–2209, 1996.

[14] T. P. Berger, “On the automorphism groups of affine-invariant codes,” *Design, Codes and Cryptography*, vol. 7, pp. 215–221, 1996.

[15] T. P. Berger and P. Charpin, “The automorphism group of generalized Reed-Muller codes,” *Discrete Math.*, vol. 117, no. 6, pp. 1–17, 1993.

[16] T. P. Berger and P. Charpin, “The automorphism groups of BCH codes and of the affine-invariant codes over extension fields,” *Design, Codes and Cryptography*, vol. 18, pp. 29–53, 1999.

[17] A. Dur, “The automorphism groups of Reed-Solomon codes,” *Jl. Comb. Theory, Series A*, vol. 44, pp. 69–82, 1987.

[18] P. Shankar, “On BCH codes over arbitrary integer rings,” *IEEE Trans. Inform. Theory*, vol. 25, no. 4, pp. 480–483, 1979.

[19] S. K. Wasan, “On codes over $\mathbb{Z}_m$,” *IEEE Trans. Inform. Theory*, vol. 28, pp. 117–120, 1982.

[20] J. C. Interlando, R. Palazzo, and M. Elia, “On the decoding of Reed-Solomon and BCH codes over integer residue rings,” *IEEE Trans. Inform. Theory*, vol. 43, pp. 1013–1021, 1997.

[21] A. R. Calderbank and N. J. A. Sloane, “Modular and p-adic codes,” *Design, Codes and Cryptography*, vol. 6, pp. 21–35, 1995.

[22] G. H. Norton and A. Sălăgean, “On the Hamming distance of linear codes over a finite chain ring,” *IEEE Trans. Inform. Theory*, vol. 46, no. 3, pp. 1060–1067, 2000.

[23] G. H. Norton and A. Sălăgean, “On the structure of linear and cyclic codes over a finite chain ring,” *Applicable algebra in engineering, communication and computing*, vol. 10, pp. 489–506, 2000.

[24] A. Bonnecaze, P. Solé, C. Bachoc, and B. Mourrain, “Type II codes over $\mathbb{Z}_4$,” *IEEE Trans. Inform. Theory*, vol. 43, pp. 969–976, 1997.

[25] A. R. Calderbank, G. McGuire, P. V. Kumar, and T. Helleseth, “Cyclic codes over $\mathbb{Z}_4$, locator polynomials and Newton’s identities,” *IEEE Trans. Inform. Theory*, vol. 42, pp. 217–226, 1996.

[26] V. S. Pless and Z. Qian, “Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$,” *IEEE Trans. Inform. Theory*, vol. 42, pp. 1594–1600, 1996.

[27] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, “The $\mathbb{Z}_4$ linearity of Kerdock, Preparata, Goethals and related codes,” *IEEE Trans. Inform. Theory*, vol. 40, no. 2, pp. 301–319, 1994.

[28] K. S. Abdukhalikov, "Affine invariant and cyclic codes over p-adic numbers and finite rings," *Design, Codes and Cryptography*, vol. 23, no. 3, pp. 343–370, 2001.

[29] J. T. Blackford and D. K. Ray-Chaudhuri, "A transform approach to permutation groups of cyclic codes over galois rings," *IEEE Trans. Inform. Theory*, vol. 46, pp. 2350–2358, 2000.

[30] B. R. McDonald, *Finite Rings with Identity.* New York: Marcel Dekker, 1974.