Affine Invariant Extended Cyclic Codes over Galois Rings

Bikash Kumar Dey
Department of E.C.E.
Indian Institute of Science,
Bangalore 560012 , India
email: bikash@ieee.org

B. Sundar Rajan
Department of E.C.E.
Indian Institute of Science,
Bangalore 560012 , India
e-mail: bsrajan@ece.iisc.ernet.in

Abstract — **Affine invariant extended cyclic codes of length p^m over any subring of $GR(p^e, m)$ for $e = 2$ with arbitrary p and for $p = 2$ with arbitrary e are characterized using transform technique. New classes of affine invariant BCH and GRM codes over such rings are found.**

I. Summary

Blackford and Ray-Chaudhuri introduced a transform technique to permutation groups of cyclic codes in [1]. They characterized affine invariant extended cyclic codes of length 2^m over any subring of $GR(4, m)$. They defined generalized BCH and GRM codes over Galois rings which are not necessarily free submodules and found new classes of affine invariant BCH and GRM codes over Galois rings. In this paper, we extend their approach to codes over Galois rings with more general parameters and find new classes of affine invariant BCH and GRM codes. All the terms and notations which are not defined here are from [1].

To state the results, we first introduce some definitions and notations below.

Any element $s \in S = [0, p^m - 1]$ can be uniquely decomposed as $s = \sum_{i=0}^{m-1} s_i p^i$ where $0 \le s_i \le p-1$. A partial order $\preceq_p$ for the set $[0, p^m - 1]$ is defined as: $s \preceq_p t$ if $s_i \le t_i$ for $0 \le i \le m-1$. Any subset $T \subseteq S$ is called a lower ideal of S if $t \in T$, $s \preceq_p t \Rightarrow s \in T$.

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

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

$$M^{(i)}_{m,2}(s,k) * M^{(j)}_{m,2}(s,k) = \sum_{\substack{0 \le k_1, k_2 \le n-1 \\ 2^j k_1 + 2^i k_2 \equiv k \bmod n \\ k_1 < k_2 \text{ if } i=j}} M^{(i)}_{m,2}(s,k_1) M^{(j)}_{m,2}(s,k_2)$$

and

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

By this definition, $M^{(1)}_{m,2}(s,k)$ is same as $M_m(s,k)$ in [1]. Let us also define the following numbers for $i \ge 0$, $s, k \in [0, 2^m - 2]$.

$$K^{(0)}_{m,2}(s,k) = M^{(0)}_{m,2}(s,k)$$

and $K^{(i)}_{m,2}(s,k) = M^{(i)}_{m,2}(s,k) + \lfloor \frac{1}{2} K^{(i-1)}_{m,2}(s, k.2^{m-1}) \rfloor$ for $i \ge 1$

Here $\lfloor . \rfloor$ denotes the largest integer less than or equal to the number inside. Parity of any integer i is defined as: $P(i) = 0$ if i is even and $P(i) = 1$ if i is odd.

Theorem I.1. *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 $i = 1, 2, \cdots, e$; $j = 1, 2, \cdots, i$,*

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

Theorem I.2. *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 for $i = 1, \cdots, e$, $l = 0, \cdots, i-1$, $\delta_{i-l} \ge 2^l(\delta_i - 2)$, then $\hat{B}(n, \delta_1, \cdots, \delta_e)$ is affine-invariant.*

Corollary I.3. *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 $\delta_{i-1} \ge 2\delta_i - 2$ for $1 < i \le e$, then the code $\hat{B}(n, \delta_1, \cdots, \delta_e)$ is affine invariant.*

Theorem I.4. *A GRM code $GRM(r_1, \cdots, r_e, m)$ over $\mathbb{Z}_{2^e}$ is affine invariant if either $e = 1$ or for $i = 2, \cdots, e$; $l = 1, \cdots, i-1$, $r_{i-l} \le m - 2^{l-1}(m - r_i)$.*

Example I.1. For any $m+1 \ge e \ge 1$, 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 $i < e$ satisfies the conditions of Theorem I.4. So, the code is affine invariant.

Now, let us consider arbitrary p and $e = 2$. For any $i_1, i_2, \cdots, i_k$ with $i_1 + i_2 + \cdots + i_k \le s$, 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 $1 \le j \le k$. For any $s, k \in [0, p^m - 2]$, let us define the quantity

$$M_{m,p}(s,k) = \frac{1}{p} \sum_{\substack{(i_0, \cdots, i_s) \\ \sum_{j=0}^{s} i_j = p;\, i_j \ne p \,\forall j \\ j \preceq_p s \text{ whenever } i_j \ne 0 \\ \sum_{j=0}^{s} j i_j \equiv k \bmod p^m - 1}} \begin{pmatrix} & p & \\ i_0 & \cdots & i_{s-1} \end{pmatrix} \binom{s}{1}^{i_1} \cdots \binom{s}{s-1}^{i_{s-1}}.$$

Theorem I.5. *Let $\hat{C}$ 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 $(\hat{T}_1, \hat{T}_2)$. $\hat{C}$ is affine invariant if and only if 1. $\hat{T}_1, \hat{T}_2$ are lower ideals in $[0, n]$ and 2. $s \in \hat{T}_2, M_{m,p}(s,k) \not\equiv 0 \bmod p \Rightarrow p^{(m-1)}k \in \hat{T}_1$.*

Theorem I.6. *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 $\delta_1 \ge p(\delta_2 - 2)$ or (ii) $\delta_1 \ge p(\delta_2 - 1)$, then $\hat{B}(n, \delta_1, \delta_2)$ is affine invariant.*

References

[1] 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.

[1]This work was partly supported by CSIR India, through Research Grant (22(0298)/99/EMR-II) to B.S.Rajan.

0-7803-7728-1/03/$17.00 ©2003 IEEE.