AAECC 5, 261–275 (1994)

AAECC
Applicable Algebra in
Engineering, Communication
and Computing

Transform Domain Characterization of Cyclic Codes over Z_m

B. Sundar Rajan[1], **M. U. Siddiqi**[2]

[1] Electrical Engineering Department, Indian Institute of Technology, Delhi, N. Delhi 110016, India
[2] Electrical Engineering Department, Indian Institute of Technology, Kanpur 208016, India

Received July 13, 1992; revised version May 18, 1993

Abstract. Cyclic codes with symbols from a residue class integer ring Z_m are characterized in terms of the discrete Fourier transform (DFT) of codewords defined over an appropriate extension ring of Z_m. It is shown that a cyclic code of length n over Z_m, n relatively prime to m, consists of n-tuples over Z_m having a specified set of DFT coefficients from the elements of an ideal of a subring of the extension ring. When m is equal to a product of distinct primes every cyclic code over Z_m has an idempotent generator and it is shown that the idempotent generators can be easily identified in the transform domain. The dual code pairs over Z_m are characterized in the transform domain for cyclic codes. Necessary and sufficient conditions for the existence of self-dual codes over Z_m are obtained and nonexistence of self-dual codes for certain values of m is proved.

Keywords: Codes over rings, Galois rings, Dual codes, Transforms

1 Introduction

Error correcting codes have been studied extensively under the assumption that the symbols to be transmitted constitute a finite field. In this paper it is assumed that the symbols constitute a residue class integer ring Z_m. Codes constructed over such rings have unique feature that make them appropriate for phase modulated channels [11]. Other applications are in multifrequency phase telegraphy [14], and in multilevel quantized pulse amplitude modulated channels [1]. The discrete memoryless Lee metric channels suitable for such codes have been derived by Chiang and Wolf [6]. A subclass of these codes is useful in certain multiuser communication systems [13]. Specific classes of cyclic codes over Z_m have been obtained from codes over finite fields [3,4] and using p-adic fields [17,18]. Using polynomial theory over integer rings cyclic and BCH codes over Z_m, for arbitrary value of m, have been studied by Prithi Shankar [15].

Our approach is a generalization of Blahut's transform approach for codes over prime fields to codes over integer residue class rings. Through this approach we obtain new results concerning idempotent generators for the case when m is a product of distinct primes and non-existence results concerning dual codes over Z_m.

The content of this paper is arranged as follows. In Sect. 2 spectral characterization of cyclic codes over Z_m when m is a power of a prime is obtained and then generalized to arbitrary m. Section 3 deals with the special case of m being a product of distinct primes. Results concerning dual codes are given in Sect. 4. Section 5 contains some concluding ramarks. A brief introduction to Galois rings is given in Appendix 1 and in Appendix 2 results concerning DFT over rings are described. These two appendices contain the necessary mathematical background for this paper.

Throughout the paper it is assumed that the length of the code is relatively prime to the size of the alphabet.

2. Spectral Characterization of Cyclic Codes over Z_{p^k}

Let Z_m^n be the set of n-tuples over Z_m. Z_m^n is a module over Z_m and a linear code over Z_m is defined as a submodule of Z_m^n [4]. Let $m = \Pi_{i=1}^{s} p_i^{k_i}$ be the prime power factorization of m. By the Chinese remainder theorem we have the isomorphism $Z_m \equiv Z_{p_1^{k_1}} \oplus Z_{p_2^{k_2}} \oplus \cdots \oplus Z_{p_s^{k_s}}$, from which follows the isomorphism $Z_m^n \equiv Z^n_{p_1^{k_1}} \oplus Z^n_{p_2^{k_2}} \oplus \cdots \oplus Z^n_{p_s^{k_s}}$. Hence any linear code over Z_m is isomorphic to a direct sum of linear codes over $Z^{k_i}_{p_i}$, $i = 1, 2, \ldots, s$. Throughout this section, except the last subsection, it is assumed that $m = p^k$.

Z_{p^k} is a local ring with the maximal ideal generated by p and every non-trivial ideal is generated by p^j for some $j = 1, 2, \ldots, k-1$. The order of $Z^n_{p^k}$ is equal to p^{kn} and the order of any submodule of $Z^n_{p^k}$ divides p^{kn}. Hence the number of codewords in a linear code is of the form p^μ where $0 \leqq \mu \leqq kn$.

2.1 Cyclic Codes in the Transform Domain

Definition 1. A cyclic code C *over* Z_{p^k} of length n is an ideal of the residue class polynomial ring $Z_{p^k}[x]/(x^n - 1)$.

The required DFT to describe these cyclic codes in the transform domain is constructed as follows.

Definition 2. Let $\underline{a} = (a_0, a_1, \ldots, a_{n-1})$ be an n-tuple over Z_{p^k}. The DFT of $\underline{a}$ is defined as

$$A_j = \sum_{i=0}^{n-1} \alpha^{ij} a_i, \quad j = 0, 1, \ldots, n-1$$

where α is an element of multiplicative order n in the Galois ring, $GR(p^k, r)$ [Appendix A], where r is the least integer such that n divides $(p^r - 1)$. The vector $\underline{A} = (A_0, A_1, \ldots, A_{n-1})$ is called the transform vector or spectrum of $\underline{a}$. The components A_i, $i = 1, 2, \ldots, n$, are called the DFT coefficients or spectral components of $\underline{a}$.

Let $GR^n(p^k, r)$ denote the set of n-tuples over $GR(p^k, r)$. The DFT maps $Z^n_{p^k}$ to a subset of $GR^n(p^k, r)$. Identifying the structure of this subset, given in the following theorem, is the key idea that leads to transform domain characterization.

Theorem 1. Let R_τ denote the subset of $GR^n(p^k, r)$ which is the set of transform vectors of all n-tuples over Z_{p^k}. Then

$$R_\tau \equiv \bigoplus_{i=1}^{t} GR(p^k, r_i)$$

where t is the number of conjugacy classes for the integer n and the prime p and r_i, $i = 1, 2, \ldots, t$, are the exponents of the conjugacy classes.

Proof. For a fixed $j, 0 \leqq j < n$, let the conjugacy class $C_{p,n}(j)$ have exponent e. For any element $(A_0, A_1, \ldots, A_{n-1})$ of R_τ it is required that $\sigma(A_{p^{e-1}j}) = A_{p^e j}$, (conjugate symmetry property) i.e., $\sigma^e(A_k) = A_k$ for all k in the conjugacy class $C_{p,n}(j)$. In other words A_k is an element of degree e and hence belongs to the subring $GR(p^k, e)$. Let R_{τ_j} denote the subset of R_τ consisting of only those elements of R_τ which have all spectral components zero except the ones that belong to $C_{p,n}(j)$. Since the value of one spectral component of a conjugacy class uniquely specifies the values at other components in the conjugacy class, it follows that

$$R_{\tau_j} \equiv \bigoplus_{i=1}^{t} GR(p^k, e).$$

Moreover, since the conjugacy classes are disjoint and operations in R_τ are pointwise it follows that $R_\tau \equiv R_{\tau_{j_1}} \oplus R_{\tau_{j_2}} \oplus \cdots \oplus R_{\tau_{j_t}}$, where $j_1, j_2, \ldots, j_t$ belong to different conjugacy classes and t is the number of conjugacy classes. □

From the above theorem and the convolution property of the DFT we get

$$Z_{p^k}[x]/(x^n - 1) \equiv \bigoplus_{i=1}^{t} GR(p^k, r_i).$$

Therefore there is a one-to-one correspondence between the ideals (cyclic codes) of $Z_{p^k}[x]/(x^n - 1)$ and ideals of $\oplus_{i=1}^{t} GR(p^k, r_i)$. For all i, $i = 1, 2, \ldots, t$, all the ideals of $GR(p^k, r_i)$, are $p^j GR(p^k, r_i)$, $j = 0, 1, \ldots, k$. Hence cyclic codes over Z_{p^k} can be characterized in terms of spectral components as follows:

For an integer n and a prime p, let there be t conjugacy classes with exponents r_i, $i = 1, 2, \ldots, t$. Let r be the least integer such that n divides $(p^r - 1)$. A cyclic code of length n over Z_{p^k} consists of the inverse DFT coefficients of all vectors of the subring isomorphic to $\oplus_{i=1}^{t} GR(p^k, r_i)$ of $GR(p^k, r)$ whose specified spectral components take values from an ideal $p^j GR(p^k, r_i)$, $0 \leqq j \leqq k$, for $i = 1, 2, \ldots, t$. In other words any cyclic code L over Z_{p^k} is of the form

$$L = \bigoplus_{i=1}^{t} p^{j_i} GR(p^k, r_i) \quad 0 \leqq j_i \leqq k.$$

Example 1. Let $n = 3$ and $m = 2^2$. The extension ring is $GR(4, 2)$, every element of which is of the form $a + bx$ where $a, b \in Z_4$. We have $Z_4[x]/(x^3 - 1) \equiv GR(4, 1) \oplus GR(4, 2) = Z_4 \oplus GR(4, 2)$. Let us denote $a + bx$ by the ordered 2-tuple ab. Ideals of $GR(4, 2)$ are $\{00\}$, $\{00, 02, 20, 22\}$ and $GR(4, 2)$. Ideals of $GR(4, 1)$ are $\{00\}$, $\{00, 20\}$ and $\{00, 10, 20, 30\}$. We can choose $\alpha = 3 + 3x$. The conjugacy classes are $\{0\}$ and $\{1, 2\}$. The conjugacy class $\{0\}$ can take values from ideals of $GR(4, 1)$ and the

Table 1. Codewords and spectrum of all cyclic codes of length 3 over Z_4.

	codeword	spectrum	codeword	spectrum	codeword	spectrum	codeword	spectrum
Code 1	000	00 00 00	222	20 00 00				
Code 2	000	00 00 00	220	00 22 02	022	00 20 20	202	00 02 22
Code 3	000	00 00 00	111	30 00 00	222	20 00 00	333	10 00 00
Code 4	000	00 00 00	200	20 20 20	020	20 02 22	022	00 20 20
	220	00 22 02	002	20 22 02	202	00 02 22	222	20 00 00
Code 5	000	00 00 00	310	00 31 23	220	00 22 02	013	00 12 32
	130	00 13 21	301	00 23 31	211	00 10 10	103	00 21 13
	121	00 01 33	031	00 32 12	202	00 02 22	233	00 30 30
	112	00 33 01	022	00 20 20	332	00 11 03	323	00 03 11
Code 6	000	00 00 00	020	20 02 22	111	30 00 00	220	00 22 02
	200	20 20 20	311	10 20 20	202	00 02 22	313	30 02 22
	131	10 02 22	331	30 22 02	002	20 22 02	133	30 20 20
	022	00 20 20	222	20 00 00	113	10 22 02	333	10 00 00
Code 7	000	00 00 00	200	20 20 20	110	20 11 03	323	00 03 11
	310	00 31 23	020	20 02 22	220	00 22 02	123	20 23 31
	130	00 13 21	330	20 33 01	101	20 03 11	213	20 32 12
	301	00 23 31	011	20 30 30	211	00 10 10	013	00 12 32
	121	00 01 33	321	20 21 13	031	00 32 12	303	20 01 33
	231	20 12 32	233	00 30 30	033	20 10 10	103	00 21 13
	002	20 22 02	202	00 02 22	112	00 33 01	332	00 11 03
	312	20 13 21	022	00 20 20	222	20 00 00	132	20 31 23

conjugacy class $\{1,2\}$ can take values from the ideals of $GR(4,2)$. The codewords of all cyclic codes that their spectrum are listed in Table 1.

In the above example the automorphism is given by $\sigma(x) = 3 + 3x$. This means given $A_1 = a + bx$, A_2 is obtained by a polynomial substitution of the form $x = f(x)$. This can be done for all p^k and n by choosing $\phi(x)$ in $Z_{p^k}[x]/\phi(x)$ to be an irreducible factor of cyclotomic polynomial, an algorithm for which is given in [10].

Now we identify a set of cyclic codes over Z_{p^k} from which all other cyclic codes over Z_{p^k} can be obtained.

Definition 3. Given Z_{p^k} and code length n, the cyclic codes L_i, $i = 1, 2, \ldots, t$, given by $L_i = GR(p^k, r_i)$ are called minimal codes and cyclic codes $L_{i,j} \equiv p^{j_i}GR(p^k, r_i)$, $0 \leqq j_i \leqq k$, are called subminimal codes corresponding to L_i.

Every minimal cyclic code is isomorphic is a Galois ring. (When $k = 1$, this reduces to the well known fact, that every minimal cyclic code over $GF(q)$ is isomorphic to a finite field.) Minimal codes are cyclic codes with one conjugacy class (say ith conjugacy class) taking values from $GR(p^k, r_i)$ and zeros in all other conjugacy classes. Subminimal cyclic codes are cyclic codes with one conjugacy class taking values from an ideal $p^{j_i}GR(p^k, r_i)$, $0 < j_i < k$, of the Galois ring corresponding to the conjugacy class, and zeros in all other conjugacy classes. It follows from the local ring structure of Galois ring that every subminimal cyclic code is a subcode of the corresponding minimal code. Explicitly, there is the following chain structure of subminimal codes corresponding to L_i,

$$p^{k-1}GR(p^k, r_i) \subset p^{k-2}GR(p^k, r_i) \subset \cdots \subset p^2GR(p^k, r_i) \subset pGR(p^k, r_i)$$

i.e.,

$$L_{i,k-1} \subset L_{i,k-2} \subset \cdots \subset L_{i,2} \subset L_{i,1} \subset L_i.$$

Also every cyclic code over Z_{p^k} is a direct sum of some minimal and subminimal codes. (In finite field case, because of the absence of nontrivial ideals, counterpart of subminimal cyclic codes over Z_{p^k} do not exist.) Hence there are $(k+1)^t - 2$ nontrivial cyclic codes of length n over Z_{p^k} since each direct summand $GR(p^k, r_i)$ has $(k+1)$ ideals $p^j GR(p^k, r_i)$, $j = 0, 1, \ldots, k$.

2.2 Metrics and Decoding for Codes over Z_{p^k}

The choice of metric depends on the criterion of decoding and channel [6]. We consider both Hamming and Lee metric. As far as Hamming distance is concerned cyclic codes with elements from nonzero ideals in some conjugacy classes have the same minimum distance as codes with full ring in those conjugacy classes, all other conjugacy classes having zeros in both the codes. This is proved in Theorem 2.

Lemma 1. Let two cyclic codes M_1 and M_2 over Z_{p^k} of same length with minimum Hamming distances d_1 and d_2 respectively be $M_1 \equiv p^{j_1} GR(p^k, r_i)$ and $M_2 \equiv p^{j_2} GR(p^k, r_i)$ for some i, where $0 \leqq j_1 < k$ and $0 \leqq j_2 \leqq k$, i.e., M_1 and M_2 are minimal codes or subminimal codes corresponding to a minimal code. Then $d_1 = d_2$.

Proof. If $j_1 = j_2$, then M_1 and M_2 are same and hence $d_1 = d_2$. If $j_1 \neq j_2$, let $j_1 > j_2$. Then M_1 is a subcode of M_2 and it follows that $d_1 \geqq d_2$. Our aim is to prove that $d_1 = d_2$. It is sufficient if we prove this for the case $j_1 = j_2 + 1$. Suppose $d_1 > d_2$. We have $pM_2 \equiv pp^{j_2} GR(p^k, r_i) \equiv p^{j_1} GR(p^k, r_i) \equiv M_1$. Since $d_1 > d_2$, there is a codeword $\underline{a} = (a_0, a_1, \ldots, a_{n-1})$ in M_2, with Hamming distance d_2, which is not in M_1. Consider the vector $\underline{b} = p(\underline{a}) = (pa_0, pa_1, \ldots, pa_{n-1})$. If b is not a all zero vector, then since $pM_2 = M_1$ and $\underline{a} \in M_2$, we have $\underline{b} \in M_1$. Let the Hamming distance of $\underline{b} = d_3$. We have $d_3 \leqq d_2$. But $d_2 < d_1$. Hence $d_3 < d_1$. This contradicts the minimality of d_1. Hence $d_1 = d_2$. It remains to prove that $\underline{b} = p(\underline{a})$ is not a all zero vector. Let j be the minimum of power of p in the expression of all components of $\underline{a}$ in the form up^t where u is a unit. (Note that for a zero component $t = k$.) Suppose $\underline{b}$ is all zero vector. Then we have $j = k - 1$. This means, since $\underline{a} \in M_2$, $j_2 \geqq k - 1$. Since $j_2 < k$, we have $j_2 = k - 1$. Since $j_1 = j_2 + 1$, we have $j_1 = k$. This is not possible since $j_1 < k$. Hence $\underline{b}$ is not a all zero vector. □

Theorem 2. Let M_1 and M_2 be two cyclic codes over Z_{p^k} of same length with zeros in the identical set of conjugacy classes and nonzeros in other conjugacy classes. Irrespective of the ideals from which nonzero values are assumed, M_1 and M_2 have the same minimum distance.

Proof. Let M_1 and M_2 be cyclic over Z_{p^k}, given by

$$M_1 \equiv \bigoplus_{i=1}^{t'} p^{j_i} GR(p^k, r_i), \quad 0 \leqq j_i < k, \quad i = 1, 2, \ldots, t',$$

$$M_2 \equiv \bigoplus_{i=1}^{t'} p^{j'_i} GR(p^k, r_i), \quad 0 \leqq j'_i < k, \quad i = 1, 2, \ldots, t'.$$

Let d_1 and d_2 be respectively the minimum Hamming distances of M_1 and M_2. We have to show that $d_1 = d_2$. Let M be the cyclic code given by

$$M \equiv \bigoplus_{\substack{i=1 \\ i \neq u}}^{t} p^{j_i} GR(p^k, r_i) \oplus p^{j_u - 1} GR(p^k, r_u)$$

for some $u \in \{1, 2, \ldots, t'\}$. Let the minimum Hamming distance of M be d. It is sufficient if we prove $d = d_1$. Clearly M_1 is contained in M. Hence $d \leqq d_1$. Suppose $d < d_1$. Let $\underline{a} = (a_0, a_1, \ldots, a_{n-1})$ be a codeword in M of Hamming distance d, and $\underline{a}$ is not in M_1. Define $\underline{b} = p\underline{a} = (pa_0, pa_1, \ldots, pa_{n-1})$. Clearly $p(\underline{a})$ is a codeword in M_1. Multiplication by p of $\underline{a}$ cannot increase the Hamming distance of $\underline{a}$. Hence Hamming distance of $\underline{b} \leqq d$. We assume that $\underline{b}$ is not a all zero vector. Since $\underline{b}$ is in M_1, minimality of d_1 is contradicted. Hence $d = d_1$. It remains to prove that $\underline{b}$ is not a all zero vector. Let j be the minimum of powers of p in the expression of all components of $\underline{a}$ in the form up^t where u is a unit. Suppose $\underline{b}$ is a all zero vector. Then we have $j = k - 1$. This means, in the transform vector of $\underline{a}$, say $(A_0, A_1, \ldots, A_{n-1})$, the components corresponding to the u-th conjugacy class belong to $p^{k-1}GR(p^k, r)$. Since $\underline{a} \in M$, we have $j_u - 1 = k - 1$, i.e., $j_u = k$. But by definition of M_1, we have $j_u < k$. Hence $\underline{b}$ is not a all zero vector. □

Regarding the minimum Lee distance it is observed that for the same number of codewords, in certain cases, codes over Z_{p^k}, with DFT coefficients from nontrivial ideals of extension ring have greater Lee distance compared to codes with DFT coefficients from only trivial ideals. No general result regarding this is reported. We list below the codewords and DFT coefficients of two codes from Example 1, both having four codewords of length 3 over Z_4. Code A has Lee distance 4, wereas code B has Lee distance 3. In codes of length 3 over Z_8 also similar case can be seen. The two codes with eight codewords, one with nontrivial ideal in both the conjugacy classes and the other one with trivial ideals in both conjugacy classes, are listed below. It is seen that code C has Lee distance four whereas code D has Lee distance three.

Code A		Code B		Code C		Code D	
codeword	spectrum	codeword	spectrum	codeword	spectrum	codeword	spectrum
000	000000	000	000000	000	000000	000	000000
202	000222	111	300000	400	404040	111	300000
220	002002	222	200000	404	000444	222	600000
022	002020	333	100000	040	400444	333	100000
				044	004040	444	400000
				440	004404	555	700000
				004	404404	666	200000
				444	400000	777	400000

As in the case of codes over finite fields one can define BCH codes over Z_{p^k} as one whose all codewords have a specified set of spectral components taking values from the same specified ideal of the extension ring. With this definition of BCH codes over Z_{p^k} the class of BCH codes studied by Prithi Shankar turns out to be a subclass where the code has a consecutive set of spectral components taking value zero. It can be shown [19] that the BCH codes of this subclass can be decoded by using a minimal shift register synthesis algorithm over appropriate Galois rings. Such an algorithm is obtained by minor adjustments of an algorithm available for minimal shift register synthesis over Z_m [16]. However, the problem of decoding general cyclic codes and decoding for Lee metric remains open.

2.3 *Characterization for Arbitrary m*

In this subsection we consider the general case where $m = p_1^{k_1} p_2^{k_2}, \dots, p_s^{k_s}$. Define m_i such that $m_i = 1 \pmod{p_i^{k_i}}$ and $m_i = 0 \pmod{p_j^{k_j}}$ for $i \neq j$, $j = 1, 2, \dots, s$. Let $\phi_i(x)$ be a monic irreducible polynomial of degree r over Z_{p_i} and hence over $Z_{p_i}^{k_i}$, where r is the least integer such that $n \mid g.c.d.\,((p_1^r - 1), (p_2^r - 1), \dots, (p_s^r - 1))$. Then $\phi(x)$ given by

$$\phi(x) = (m_1 \phi_1(x) + m_2 \phi_2(x) + \cdots + m_s \phi_s(x)) \bmod m$$

is a monic irreducible polynomial over Z_m. We have [15] $Q(m,r) \equiv \oplus_{i=1}^{s} GR(p_i^{k_i}, r)$ and the group of units $Q^*(m,r) \equiv \otimes_{i=1}^{s} GR^*(p_i^{k_i}, r)$. $Q^*(m,r)$ has order N given by $N = \Pi_{i=1}^{s} p_i^{r_i(k_i - 1)}(p_i^r - 1)$. Since we can choose r such that $n \mid g.c.d.$ $((p_1^r - 1)$, $(p_2^r - 1), \dots, (p_s^r - 1))$, we can find an element α in $Q^*(m,r)$ of order n and hence construct DFT over $Q(m,r)$. Next, we identify the subring R_τ of $Q^n(m,r)$ which is the image of all n-tuples over Z_m under DFT, using the group of automorphisms of $Q(m,r)$.

The group of automorphisms of $Q(m,r)$ is an abelian group which is direct product of s cyclic groups each of order r. Let $\sigma_1, \sigma_2, \dots, \sigma_s$ be the generator automorphisms of these cyclic groups. Then σ_i, $i = 1, 2, \dots, s$, is the generator of the group of automorphism of $GR(p_i^{k_i}, r)$ [5]. Clearly any map $\sigma: Q(m,r) -\!\!\rightarrow Q(m,r)$ of the form $(\sigma_1^{j_1}, \sigma_2^{j_2}, \dots, \sigma_s^{j_s})$ is an automorphism and conversely. Each generating automorphism relates different set of spectral components of conjugacy classes corresponding to different p_i. Let $(A_0, A_1, \dots, A_{n-1})$ be a transform vector where $A_i \in Q(m,r)$ and A_{ij} is the component of A_i in $GR(p_j^{k_j}, r)$. Then from conjugacy symmetry property we have $\sigma_j(A_{ij}) = A_{i(pj)}$. Let there be t_i conjugacy classes corresponding to p_i with exponents e_{ij}, $j = 1, 2, \dots, t_i$, for $i = 1, 2, \dots, s$. The following theorem, which can be proved using Chinese Remainder Theorem, identifies the subring R_τ of $Q^n(m,r)$.

Theorem 3. The subring R_τ of $Q^n(m,r)$ which contains all the transform vectors of n-tuples over Z_m, $m = p_1^{k_1} p_2^{k_2}, \dots, p_s^{k_s}$, is isomorphic to $\oplus_{i=1}^{s} \oplus_{j=1}^{t_i} GR(p_i^{k_i}, e_{ij})$ where t_i is the number of conjugacy classes and e_{ij}, $j = 1, 2, \dots, t_i$, are the exponents corresponding to p_i.

By choosing zero ideal from all $GR(p_i^{k_i}, e_{ij})$ except for a particular i, leads to

Theorem 4. Every clyclic code over Z_m, $m = p_1^{k_1} p_2^{k_2}, \dots, p_s^{k_s}$, is a direct sum of cyclic codes over $Z_{p_i}^{k_i}$, $i = 1, 2, \dots, s$.

Theorem 5. The minimum Hamming distance of a code L over Z_m, where

$$L \equiv \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{t_i} p^{h_{ii}} GR(p^{k_i}, e_{ij}), \quad 0 \leqq h_{ij} \leqq k_i,$$

is equal to the minimum of the Hamming distances of the codes, L_i, $i = 1, 2, \dots, s$, over $Z_{p_i}^{k_i}$, given by

$$L_i \equiv \bigoplus_{j=1}^{t_i} p^{h_{ij}} GR(p_i^{k_i}, e_{ij}).$$

Proof. Let d be the minimum Hamming distance of L and d_i, $i = 1, 2, \dots, s$, be the minimum Hamming distances of L_i, $i = 1, 2, \dots, s$. Let $d_v = \min\,\{d_1, d_2, \dots, d_s\}$ for some $v \in \{1, 2, \dots, s\}$. We have $L \equiv \oplus_{i=1}^{s} L_i$. By choosing the zero vector from all L_i, except $i = v$, and a vector of Hamming weight d_v in L_v, we obtain a codeword in L of Hamming weight d_v in L. Hence $d \leqq d_v$. We want to show that $d = d_v$. Suppose $d < d_v$. Let Γ be a codeword in L of Hamming weight d, i.e., there are only d nonzero components in Γ which are elements of Z_m. In the isomorphism $Z_m \equiv \oplus_{i=1}^{s} Z_{p_i^{k_i}}$, the zero of Z_m has only zero components in all $Z_{p_i}^{k_i}$, and any nonzero element of Z_m has nonzero component in at least one $Z_{p_i}^{k_i}$. Hence if Γ_i, $i = 1, 2, \ldots, s$ are components of Γ in L_i, $i = 1, 2, \ldots, s$, then Hamming weight of each L_i is atmost d. This means the minimum Hamming weight of each L_i is equal to $d < d_v$ for at least one i, which contradicts the minimality of d_v. Hence $d = d_v$. □

3 Cyclic Codes Over Z_m; $m = p_1 p_2, \ldots, p_s$

When m is a product of distinct primes, Z_m is a semisimple ring and by Masche's theorem the ring $Z_m[x]/(x^n - 1)$ is also semisimple. Hence every cyclic code over Z_m has an idempotent generator. Proceeding as in the previous section and using the facts $GR(p, r) \equiv GF(p^r)$ and $Q(m, r) \equiv \oplus GF(p_i^r)$, we have $Q^*(m, r) \equiv \otimes_{i=1}^{s} GF^*(p_i^r)$. Putting $k_1 = k_2 = \cdots = k_s = 1$ in Theorem 3, we obtain,

Theorem 6. The subring R_τ of $Q^n(m, r)$ which contains all the transform vectors of n-tuples over Z_m, $m = p_1 p_2, \ldots, p_s$, is isomorphic to $\oplus_{i=1}^{s} \oplus_{j=1}^{t_i} GF(p_i^{e_{ij}})$, where t_i is the number of conjugacy classes corresponding to p_i and e_{ij}, $j = 1, 2, \ldots, t_i$, are their exponents.

From Theorem 6, it follows that

$$Z_m[x]/(x^n - 1) \equiv R_\tau \equiv \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{t_i} GF(p_i^{e_{ij}})$$

i.e., $Z_m[x]/(x^n - 1)$ is a direct of finite fields $GF(p_i^{e_{ij}})$, $i = 1, 2, \ldots, s$ and $j = 1, 2, \ldots, t_i$. Hence every cyclic code over Z_m, has an idempotent generator.

Lemma 2. If $a_0 + a_1 x + \cdots + a_{r-1} x^{r-1} \in Q(m, r)$ is an idempotent generator of some ideal of $Q(m, r)$ then $a_1 = a_2 = \cdots = a_{r-1} = 0$ and a_0 is an idempotent element of Z_m.

Proof. Let I be an ideal of $Q(m, r)$ with idempotent generator e. From $Q(m, r) \equiv \oplus_{i=1}^{s} GF(p_i^r)$, it follows that $I \equiv \oplus_{i=1}^{s} I_i$, where I_i is an ideal in $GF(p_i^r)$ and $e = (m_1 e_1 + m_2 e_2 + \cdots + m_3 e_s)(\mathrm{mod}\, m)$, where e_i is an idempotent generator of I_i. Since I_i is a finite field $e_i = 0$ or 1, which means e is an idemptonent element of Z_m. □

Theorem 7. Every cyclic code over Z_m, $m = p_1 p_2, \ldots, p_s$, is uniquely determined by a subset of idempotent elements of Z_m.

Proof. Every cyclic code over Z_m, $m = p_1 p_2, \ldots, p_s$, has an idempotent generator. Let $(f_0, f_1, \ldots, f_{n-1})$ be an idempotent generator of a cyclic code with spectrum $(F_0, F_1, \ldots, F_{n-1})$. Since the conjugacy constraints corresponding to a prime p_j, $j = 1, 2, \ldots, s$ is of the form $F_i = F_{ip_j}$, $i = 0, 1, 2, \ldots, n - 1$, from Lemma 2, it follows that $F_i \in Z_m$, for $i = 1, 2, \ldots, n - 1$. Moreover, the group of automorphisms of $Q(m, r)$ leave the subring Z_m invariant. This means if j-th component of transform vector in $F_j \in Z_m$ then all the DFT components of the conjugacy class $C_{p,n}(j)$ take the value F_j. Hence idempotent generators can be identified in the transform domain as those which have some idempotent elements of Z_m in all the conjugacy classes. □

Table 2. Listing of idempotent generators of all cyclic codes of length 5 over Z_6

idempotent generator	spectrum	idempotent generator	spectrum
00000	0000 0000 0000 0000 0000	03333	0000 3000 3000 3000 3000
10000	1000 1000 1000 1000 1000	13333	1000 4000 4000 4000 4000
30000	3000 3000 3000 3000 3000	33333	3000 0000 0000 0000 0000
40000	4000 4000 4000 4000 4000	43333	4000 1000 1000 1000 1000
51111	0000 1000 1000 1000 1000	24444	0000 4000 4000 4000 4000
21111	3000 4000 4000 4000 4000	54444	3000 1000 1000 1000 1000
22222	4000 0000 0000 0000 0000	25555	4000 3000 3000 3000 3000
52222	1000 3000 3000 3000 3000	55555	1000 0000 0000 0000 0000

Example 2. Let $m = 6$ and $n = 5$. $Z_6 \equiv GF(2) \oplus GF(3)$, $\phi_1(x) = x^4 + x + 1$ and $\phi_2(x) = x^4 + x + 2$. are irreducible polynomials of degree 4 over $GF(2)$ and $GF(3)$. The corresponding irreducible polynomial of degree 4 over Z_6 is $x^4 + x + 5$. We have $Q(6,4) \equiv Z_6[x]/(x^4 + x + 5)$. In $Q(6,4)$ an element of order 5 is $2x^2 + 3x^3$, which is taken to be the transform factor. The conjugacy classes are $C_{2,5}(0) = 0$, $C_{2,5}(1) = \{1,2,3,4\}$, $C_{3,5}(0) = \{0\}$ and $C_{3,5}(1) = \{1,2,3,4\}$. We have $Z_6/(x^5 - 1) \equiv GF(2) \oplus GF(2^4) \oplus GF(3) \oplus GF(3^4)$. We take zero ideal for the conjugacy classes $C_{2,5}(0)$ and $C_{3,5}(1)$ and full ring for the conjugacy classes $C_{3,5}(0)$ and $C_{2,5}(1)$. The idempotent elements of Z_6 are 0, 1, 3 and 4. The idempotent generators of all cyclic codes and their spectrum are listed in Table 2.

4 Dual Codes over Z_m

Dual codes are useful in the study of weight enumeration of linear codes. When the symbol alphabet has the structure of a finite field, it is well known that the weight enumerators of a linear code and its dual code are related by MacWilliams identities. Delsarte [7] has assumed the Abelian group structure for symbol alphabet, and obtained linear codes called additive codes. For additive codes, he has defined a duality relation which reduces to the classical concept of linear codes over a prime field and has shown that the MacWilliams identities on the weight distribution are still satisfied. Obviously Z_m is a subclass of additive codes and hence MacWilliams identities are satisfied for dual codes of linear codes over Z_m.

4.1 Dual Codes of Linear Codes over Z_m

First we show that for the case of codes over Z_m, the duality relation of Delsarte for additive codes reduces to the familiar relation of dot product being equal to zero. Let G be an Abelian group of exponent q and G^n denote the set of all n-tuples over G. Let Φ denote the group of characters of G. It is well known that $\Phi \equiv G$. Let ϕ_g denote the character corresponding to g in G under this isomorphism. For $a, b \in G^n$, where $\underline{a} = (a_0, a_1, \ldots, a_{n-1})$ and $\underline{b} = (b_0, b_1, \ldots, b_{n-1})$, the inner product of $\underline{a}$ and $\underline{b}$, denoted by $\langle \underline{a}, \underline{b} \rangle$, is defined [16] as

$$\langle \underline{a}, \underline{b} \rangle = \prod_{i=0}^{n-1} \Phi_{b_i}(a_i).$$

Let H be a subgroup of G^n. H is called as additive code over G. The dual of H is defined as the subset H^d of G^n given by $H^d = \{b \in G^n : < \underline{a}, \underline{b} > = 1 \; for \; \forall a \in H\}$. H^d is a subgroup of G^n and $H^d \equiv G^n/H$. When q is prime, an additive code is merely a linear code over $GF(q)$ and the dual is the classical one.

For the case of linear codes over Z_m, we consider the Abelian group $(Z_{m,} +)$. It can be seen that the group of characters of $(Z_{m,} +)$ is $\Phi = \{\Phi_0, \Phi_1, \ldots, \Phi_{m-1}\}$, where Φ_i, $i = 0, 1, \ldots, m-1$, is given by $\Phi_i(x) = \alpha^{ix}$ *for* $x \in Z_m$ where α is an element of multiplicative order m, and the group operation in Φ is given by $\Phi_i \Phi_j = \Phi_{i+j(\mathrm{mod}\, m)}$. Now the inner product of $\underline{a}$ and $\underline{b}$ is given by

$$\langle \underline{a}, \underline{b} \rangle = \prod_{i=0}^{n-1} \Phi_{b_i}(a_i) = \prod_{i=0}^{n-1} (\alpha^{b_i})^{a_i} = \alpha \exp\left(\sum_{i=0}^{n-1} a_i b_i \right).$$

Hence $< \underline{a}, \underline{b} > = 1$ iff $\sum_{i=0}^{n-1} a_i b_i = 0$. This leads to

Definition 4. Let C be a linear code over Z_m. Then its dual code, denoted by $\hat{C}$, is defined as

$$\hat{C} = \left\{ (b_0, b_1, \ldots, b_{n-1}) : \sum_{i=0}^{n-1} a_i b_i = 0 \text{ for all } (a_0, a_1, \ldots, a_{n-1}) \in C \right\}.$$

Note that this definition is same as that for codes over finite fields.

4.2 *Spectral Characterization of Dual Codes of Cyclic Codes*

Let $m = p^k$ and let us call the conjugacy class $C_{p,n}(n-j)$ the dual conjugacy class of $C_{p,n}(j)$ and the ideal $p^{k-j}GR(p^k, r)$ of $GR(p^k, r)$ the orthogonal ideal of $p^j GR(p^k, r)$. Note that product of two elements, one each from $p^j GR(p^k, r)$ and $p^{k-j} GR(p^k, r)$, is zero. If I denotes an ideal of $GR(p^k, r)$ then I_d is used to denote the orthogonal ideal of I. Note that $I.\, I_d = 0$.

Lemma 3. Let $\underline{a} = (a_0, a_1, \ldots, a_{n-1})$ and $\underline{b} = (b_0, b_1, \ldots, b_{n-1})$ be codewords and $\underline{A} = (A_0, A_1, \ldots, A_{n-1})$ and $\underline{B} = (B_0, B_1, \ldots, B_{n-1})$ be their transform vectors. If $b_j = a_{n-j}$ for all $j = 0, 1, \ldots, n-1$, then $B_j = A_{n-j}$ for all $j = 0, 1, 2, \ldots, n-1$. In other words the permutation defined by $i - \to (n-i)$ is preserved under DFT.

Proof. Let α be the transform factor of the DFT. For any $j \in \{0, 1, 2, \ldots, n-1\}$, we have

$$B_j = \sum_{i=0}^{n-1} \alpha^{ij} b_i = \sum_{i=0}^{n-1} \alpha^{ij} a_{n-i} = \sum_{k=0}^{n-1} \alpha^{(n-k)j} a_k = \sum_{k=0}^{n-1} \alpha^{-kj} a_k.$$

Also

$$A_{(n-j)} = \sum_{i=0}^{n-1} \alpha^{i(n-j)} a_i = \sum_{i=0}^{n-1} \alpha^{-ij} a_i = \sum_{k=0}^{n-1} \alpha^{-kj} a_k.$$

Hence $B_j = A_{n-j}$. □

Theorem 8. If C is a cyclic code of length n over Z_{p^k} whose transform vectors take values from the ideals $I_1, I_2, \ldots, I_t$ for the conjugacy classes $C_{p,n}(j_1), C_{p,n}(j_2), \ldots, C_{p,n}(j_t)$ respectively then the transform vectors of the dual code $\hat{C}$ take values from the ideals $(I_1)_d, (I_2)_d, \ldots, (I_t)_d$ respectively for the conjugacy classes $C_{p,n}(n-j_1), \ldots, C_{p,n}(n-j_t)$.

Proof. Let $\underline{a} = (a_0, a_1, \ldots, a_{n-1})$ be represented by $a_0 + a_1x + \cdots + a_{n-1}x^{n-1} = a(x)$ and let $a(x) \in C$. Let C^* denote the code with ideals $(I_1)_d, (I_2)_d, \ldots, (I_t)_d$ in the conjugacy classes $C_{p,n}(j_1), C_{p,n}(j_2), \ldots, C_{p,n}(j_t)$ and let $h(x) = h_0 + h_1x + \cdots + h_{n-1}x^{n-1} \in C^*$. From the convolution property of DFT it is clear that $a(x)h(x) = 0$ for all $a(x) \in C$ and for all $h(x) \in C^*$. In particular, the constant term in the product $a(x)h(x)$ is zero i.e. $\sum_{i=0}^{n-1} a_ih_{n-i} = 0$. For a given $h(x)$ in C^* define $b(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$ by $b_i = h_{n-i}$, $i = 0, 1, \ldots, n-1$. We have $\sum_{i=0}^{n-1} a_ib_i = 0$. Hence $b(x)$ belongs to the dual code $\hat{C}$. From Lemma 3, it follows that the transform vector of $b(x)$ have values from ideals $(I_1)_d, (I_2)_d, \ldots, (I_t)_d$ for the conjugacy classes $C_{p,n}(n - j_1)$, $C_{p,n}(n - j_2), \ldots, C_{p,n}(n - j_t)$. So we have shown that the set of all $b(x)$ corresponding to all the elements of C^*, denoted by C^{**}, is contained in $\hat{C}$. It remains to show that they are, in fact, all the codewords of $\hat{C}$. We know that $\hat{C}$ is contained in $Z^n_{p^k}/C$, which is the factor group, considering both $Z^n_{p^k}$ and C as groups. So, it is sufficient to show that

$$|C||C^{**}| = (p^k)^n = p^{kn}$$

where $|C|$ denotes the number of elements in C. Let I_u be the ideal $p^{i_u}GR(p^k, r)$ for some $I_u, 0 \leqq i_u \leqq k$, for $u = 1, 2, \ldots, t$. Also let $e_1, e_2, \ldots, e_t$ be the exponents of $C_{p,n}(j_1)$, $C_{p,n}(j_2), \ldots, C_{p,n}(j_t)$ respectively. Note that sum of the exponents of all the conjugacy classes, $e_1 + e_2 + \cdots + e_t$, is equal to n. Then $|C| = (p^{i_1})^{e_1}(p^{i_2})^{e_2} \cdots (p^{i_t})^{e_t} = p^{i_1e_1}p^{i_2e_2}, \ldots, p^{i_te_t}$. Similarly, $|C^{**}| = (p^{k-i_1})^{e_1}(p^{k-i_2})^{e_2}, \ldots, (p^{k-i_t})^{e_t}$.

Hence, $|C\|C^{**}| = (p^k)^{(e_1+e_2+\cdots+e_t)} = p^{kn}$. Q.E.D.

4.3 Non-Existence Theorems for Cyclic Self-Dual Codes

The following spectral characterization of self-dual cyclic codes follows immediately from Theorem 8.

Theorem 9. A code C is a self-dual cyclic code iff whenever $C_{p,n}(j)$ has values from the ideal I then $C_{p,n}(n - j)$ has values from the ideal I_d.

Example 3. Let $n = 3$ and $m = 4$. The appropriate extension ring is $GR(4, 2)$. The only ideal in it such that $I = I_d$ is $2GR(4, 2)$. Both the conjugacy classes $\{0\}$ and $\{1, 2\}$ are self-dual. So the only possible self-dual code in this case is the one with all the conjugacy classes taking values from the ideal $2GR(4, 2)$. All the codewords and their transform vectors are shown below.

Codewords:	0 0 0	2 0 0	0 2 0	2 2 0	2 0 2	0 0 2	0 2 2	2 2 2
Spectrum:	00 00 00	20 20 20	20 02 22	00 22 02	00 02 22	20 22 02	00 20 20	20 00 00

Example 4. Consider length 5 cyclic codes over Z_4. The conjugacy classes are $\{0\}$ and $\{1, 2, 3, 4\}$. Both are self-dual conjugacy classes. The extension rings is $GR(4, 4)$. The only self-orthogonal ideal is $2GR(4, 4)$. Hence there is only one self-dual code in this case.

Now we identify a set of values of m and n for which self-dual codes do not exist.

Theorem 10. If $m = p^k$ and $(n, m) = 1$ then self-dual cyclic codes of length n over Z_m do not exist for all odd integer values of k.

Proof. For all values of m and n, $\{0\}$ is the conjugacy class $C_{p,n}(0)$ and $C_{p,n}(n-0)$ is also $\{0\}$. Considering the conjugacy class $\{0\}$, from Theorem 8, it is necessary that for a code C to be self-dual there must be at least one ideal I in $GR(p^k, r)$ such that $I = I_d$, i.e., at least for one value of j, such that $p^j GR(p^k, r) = p^{k-j} GR(p^k, r)$. This can happen only if $j = k - j$ of $k = 2j$. □

The well known result that a binary self-dual cyclic code is always of even length follows from Theorem 10.

For any arbitrary integer $m = p_1^{k_1} p_2^{k_2}, \ldots, p_s^{k_s}$, let $\underline{a} = (a_0, a_1, \ldots, a_{n-1})$ and $\underline{b} = (b_0, b_1, \ldots, b_{n-1})$ be in Z_m^n. Choose m_i's such that $m_i m_j = 1 \ (\mathrm{mod}\, m)$ if $i = j$ and $m_i m_j = 0 (\mathrm{mod}\, m)$ if $i \neq j$. We have

$$a_i = (m_1 a_{i1} + m_2 a_{i2} + \cdots + m_s a_{is}) \bmod m$$

$$b_i = (m_1 b_{i1} + m_2 b_{i2} + \cdots + m_s b_{is}) \bmod m$$

where a_{ij} and $b_{ij} \in Z_{p_j}^{k_j}$ for $i, j = 1, 2, \ldots, s$. It can be verified that $\sum_{i=0}^{n-1} a_i b_i = 0$ iff $\sum_{i=0}^{n-1} a_{ij} b_{ij} = 0$ for $j = 1, 2, \ldots, s$. Combining this result with Theorem 4, Theorem 9 and Theorem 10 leads to

Theorem 11. If $m = p_1^{k_1} p_2^{k_2}, \ldots, p_s^{k_s}$ and $(n, m) = 1$ then self-dual codes of length n over Z_m do not exist if any one of k_i's is an odd number.

5 Conclusion

Transform domain characterization of cyclic codes and dual-codes over residue class integer rings Z_m have been obtained. For the special case of m being a product of distinct primes it is shown that the idempotent generators of the cyclic codes can be easily identified in the transform domain. Nonexistence of self-dual codes have been proved for certain values of m and n. Since the Galois rings $GR(p^k, r)$ include finite fields $GR(p, r)$ and integer residue rings $GR(p^k, 1)$ as special cases a general theory of codes can be developed by studying codes for the alphabet which has the structure of a Galois ring. Decoding algorithm has been obtained only for a specific class of BCH codes, that too only for the Hamming metric. It would be of interest to devise decoding schemes for the general cyclic code both for Hamming and Lee metrics.

Appendix 1: Galois rings

Let p^k be a power of a prime number. Galois rings are residue class polynomial rings $Z_{p^k}[x]/\phi(x)$, denoted by $GR(p^k, r)$ where $Z_{p^k}[x]$ is the ring of polynomials over Z_{p^k} and $\phi(x)$ is a monic irreducible polynomial of degree r over $Z_p[x]$ and hence over $Z_{p^k}[x]$ [12]. It is easy to see that $GR(p^k, 1)$ is isomorphic to Z_{p^k} and $GR(p^k, r)$ is isomorphic to $GF(p^r)$. Results concerning Galois rings that are of interest to us are listed below. Proofs can be seen in [12].

1. If $\phi_1(x)$ and $\phi_2(x)$ are monic irreducible polynomials of degree r in $Z_p[x]$ then $Z_{p^k}[x]/\phi_1(x) = Z_{p^k}[x]/\phi_2(x)$. This justifies the notation $GR(p^k, r)$.
2. Every ideal in $GR(p^k, r)$ is, of the form $\langle p^i \rangle = p^i GR(p^k, r)$ for $0 \leqq i \leqq k$. The

maximal ideal is $pGR(p^k, r)$. i.e., $GR(p^k, r)$ is a principal ideal ring as well as a local ring.

3. If $GR^*(p^k, r)$ denotes the group of units of $GR(p^k, r)$ then $GR^*(p^k, r) = G_1 x G_2$ (direct product of groups) where (a) G_1 is the cyclic group of order $p^r - 1$ and this is the only cyclic subgroup of $GR^*(p^k, r)$ of order relatively prime to p.

 (b) G_2 is an Abelian group of order $p^{(k-1)r} - 1$.

4. The group of automorphisms of $GR(p^k, r)$ is a cyclic group of order r.

5. In general, factorization in rings with zero divisors is not unique. But when $(n, p) = 1$, the polynomial $(x^n - 1)$ factors uniquely in $GR^*(p^k, r)$.

6. Every subring of $GR(p^k, r)$ is a Galois ring of the form $GR(p^k, d)$, where d divides r. Conversely if d divides r then $GR(p^k, r)$ contains a unique subring isomorphic to $GR(p^k, d)$.

Example 5. Let $m = 8$ and $r = 2$, $\phi(x) = x^2 + x + 1$ is an irreducible polynomial of degree 2 in $Z_2[x]$. $GR(8, 2) = Z_8[x]/(x^2 + x + 1)$. Ideals of $GR(8, 2)$ are $\{0\}$, $\{0, 4, 4x, 4 + 4x\} = 2^2GR(8, 2)$, $\{0, 2, 6 + 2x, 6 + 6x, 2 + 4x, 4 + 4x, 2x, 4, 6x, 2 + 6x, 6 + 4x, 2 + 2x, 6, 4 + 6x, 4x, 4 + 2x\} = 2GR(8, 2)$ and $GR(8, 2)$. Subrings of $GR(8, 2)$ are $\{0\}$, $\{0, 1, 2, 3, 4, 5, 6, 7\} = GR(8, 1)$ and $GR(8, 2)$. The only cyclic subgroup of order relatively prime to 8 in $GR^*(8, 2)$, i.e., G_1 is $\{1, x, 7 + 7x\}$. The generator of the automorphism group is $\sigma: x \to 7 + 7x$.

In what follows we introduce the notion of degree of an element of a Galois ring. Consider the Galois ring $GF(p^k, s)$. If r divides s, then $GR(p^k, s)$ contains a subring which is isomorphic to $GR(p^k, r)$. For our purposes it is required to identify the elements of $GR(p^k, s)$, which constitute the subring $GR(p^k, r)$. We shall use the fact that there is a one-to-one correspondence between the subgroups of the automorphism group of a Galois ring and the set of subrings of the Galois ring [12]. The subgroup of the automorphism group that corresponds to a particular subring of the Galois ring consists of those automorphisms which leave the elements of the subring invariant. Let the generator of the automorphism group be $\sigma: \sigma(\alpha) = \alpha^p$. It follows that if β in $GR(p^k, r)$ but not in any subring $GR(p^k, r_1)$, where $r_1 < r$ then the least integer t such that $\sigma^t(\beta) = \beta$ is equal to r.

Definition 5. Let β be an element of the Galois ring $GR(p^k, s)$. The degree of β is defined as the least integer r such that $\sigma(\beta) = \beta$, where σ is a generator of the group of automorphisms of $GR(p^k, s)$.

Since the set $\{0, 1, 2, \ldots, p^k - 1\}$ is invariant under the group of automorphisms of $GR(p^k, s)$, it consists of elements of degree 1. Moreover the subring of $GR(p^k, s)$ which is isomorphic to $GR(p^k, r)$, where r divides s, consists of the elements of $GR(p^k, s)$ whose degree divides r.

Example 6. Consider $GR(4, 4) = Z_4[x]/(x^4 + x + 1)$. Every element is of the form $a_0 + a_1x + a_2x^2 + a_3x^3$. The mapping $\sigma: \sigma(x) = 2 + 2x + 3x^2$ is a generator of the automorphism group of $GR(4, 4)$. Degree of an element can be $1, 2$ or 4.

(a) The elements of degree 1 are $0, 1, 2$ and 3.

(b) The elements of degree 2 are

$1 + 2x + 2x^2$, $2x + 2x^2$, $2 + 2x + 2x^2$, $3 + 2x + 2x^2$, $3 + x^2 + 2x^3$, $1 + 3x + x^2 + 2x^3$, $2 + 3x + x^2 + 2x^3$, $3 + 3x + x^2 + 2x^3$, $x + 3x^2 + 2x^3$, $1 + x + 3x^2 + 2x^3$, $2 + x + 3x^2 + 2x^3$, and $3 + x + 3x^2 + 2x^3$.

(c) All other elements are of degree 4.

Appendix 2: DFT Over Finite Rings

A finite commutative ring with identity, denoted by R, is said to support a discrete Fourier transform of length n if there exists a transform of the form

$$A_j = \sum_{i=0}^{n-1} \alpha^{ij} a_i, \quad j = 0, 1, \ldots, n-1$$

where $a_i, A_j \in R$, and α is a unit of order n in the group of units of R and n is invertible in R. The element α is called the transform factor of the DFT. This DFT defines an isomorphism between convolution algebra $R[x]/(x^n - 1)$ and pointwise product algebra of n-tuples of R, denoted by R^n.

The following theorems [8] give the necessary and sufficient conditions for finite rings to support a DFT of a given length.

Theorem 12. If R is a direct sum of local rings $R_1, R_2, \ldots, R_t$ then R supports a DFT of length n iff R_i, $i = 0, 1, \ldots, t$, supports a DFT of length n.

Theorem 13. Let $R = R_1 \oplus R_2 \oplus \cdots \oplus R_t$ where $R_i, i = 1, 2, \ldots, t$, is a local ring. Then R supports a DFT of length n iff

(i) R_i contains an element α_i of order n.

(ii) n is invertible in R_i, i.e., n is a unit in R_i.

It follows that a Galois ring $GR(p^k, r)$ to support a DFT of length n it is required that n and p must be relatively prime, i.e., $(n, p) = 1$, and n should divide $p^r - 1$. Also $\oplus_{i=1}^{s} GR(p_i^{k_i})$ can support a DFT of length n iff the following conditions are satisfied.

(i) $(n, p_i) = 1$ for $i = 1, 2, \ldots, s$.

(ii) $n \,|\, g.c.d.\ ((p_1^r - 1), (p_2^r - 1), \ldots, (p_s^r - 1))$.

Let $(a_0, a_1, \ldots, a_{n-1})$ be an n-tuple over Z_{p^k} and $(A_0, A_1, \ldots, A_{n-1}) \in GR^n(p^k, r)$ be its transform vector, where $GR(p^k, r)$ is the extension ring of Z_{p^k} which supports the DFT. The automorphism group of $GR(p^k, r)$ is a cyclic group of order r and the generator automorphism is $\sigma(\alpha) = \alpha^p$. The following relation known as conjugate symmetry property holds

$$A_{pj} = \sigma(A_j) \quad \text{for all } j.$$

All the n-tuples of $GR(p^k, r)$ which are DFT vectors of some n-tuple over Z_{p^k} satisfy this condition.

Definition 6. Given a positive integer n and a prime p relatively prime to n, the conjugacy class containing j, $(0 \leq i \leq k)$, denoted by $C_{p,n}(j)$ is the set $\{j, pj, p^2 j, \ldots, p^{(e-1)} j\}$ where e is the least integer such that $p^e j = j (\bmod n)$. The integer e is called the exponent of the conjugacy class $C_{p,n}(j)$ and is denoted by $\exp(C_{p,n}(j))$.

The conjugacy class structure for a given n and p^k, which is a partition of $\{0, 1, 2, \ldots, n-1\}$ depends only on n and the prime p, and not on k.

Given a prime p and an integer n the number of conjugacy classes, denoted by t, is given by,

$$t = \sum_{d|n} \frac{\phi(d)}{e(d)}$$

where $e(d)$ is the least integer such that $d^e = 1 (\bmod q)$, $\phi(d)$ is the Euler's totient function and $q = n/d$ [9].

References

1. Berlekamp, E. R.: Algebraic Coding Theory. New York: McGraw Hill 1968
2. Blahut, R. E.: Theory and Practice of Error Control Codes. California: Addision-Wesley 1983
3. Blake, I. F.: Codes over certain rings. Inform. Control **20**, 296–404 (1972)
4. Blake, I. F.: Codes over integer residue rings. Inform. Control **29**, 295–300 (1975)
5. Britten, J. D., Lemire, E. W.: A structure theorem for rings supporting a discrete Fourier transform. SIAM J. Appl. Math. **41**, 222–226 (1981)
6. Chiang, J., Wolf, J. K.: On channels and codes for the Lee metric. Inform. Control **19**, 159–173 (1971)
7. Delsarte, P.: Bounds for unrestricted codes by linear programming. Philips Research Dev. J. **27**, 272–289 (1972)
8. Dubios, E., Venetsanopoulos, A. N.: The discrete Fourier transform over finite rings with application to fast convolution. IEEE Trans. Computers, C-27, 586–593 (1978)
9. Madhusudhana, H. S.: On Abelian codes which are closed under cyclic shifts, M. Tech Thesis, Indian Institute of Tech. Kanpur (India), 1987
10. Martens, J. B., Vanwormhoudt, M. C.: Convolution using a conjugate symmetry property for number theoretic transforms over rings of regular integers. IEEE Trans. ASSP, ASSP-**31**, 1121–1124 (1983)
11. Massey, J. L., Mittelholzer, T. M.: Convolutional codes over rings. Proceedings of the Fourth Joint Swedish-USSR Int. Workshop in Information Theory, 27, Gotland, Sweden, 1989
12. McDonald, B. R.: Finite Rings with identity, New York: Marcel-Decker 1974
13. Murakami, H., Reed, I. S., Welch, L. R.: A tranform decider for Reed-Solomon codes in multiple user communication systems. IEEE Trans. Inform. Theory **IT-23**, 1745–1753 (1977)
14. Nemirovskiy, E. E.: Codes on residue class rings with multi-freequency phase telegraphy. Radiotechnika i electronika **9**, 1745–1753 (1984)
15. Prithi Shankar: On BCH codes over arbitrary integer rings. IEEE Trans. Inform. Theory, **IT-25**, 480–483 (1979)
16. Reeds, J. A., Sloane, N. J. A.: Shift Register Synthesis (modulo *m*). SIAM J. Computing, 505–513 (1985)
17. Spiegel, E.: Codes over Z_m. Inform. Control **35**, 48–52 (1977)
18. Spiegel, E.: Codes over Z_m-Revisited. Inform. Control **37**, 100–104 (1978)
19. Sundar Rajan, B., Siddiqi, M. U.: Transform decoding of BCH codes over Z_m (To appear in Internat. J. Electronics)