ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 9, September 2017

Some Results on Cyclic Codes over the ring of integers modulo 8

[1] Jasbir Kaur, [2] Ranjeet Sehmi, [3] Sucheta Dutt
[1][2][3] Department of Applied Sciences
[1][2][3] PEC University of Technology, Chandigarh, India

Abstract **- Let $\mathfrak{R}$ be a Galois ring of characteristic p^a and cardinality p^{am}. Let C be a cyclic code of arbitrary length n over $\mathfrak{R}$, viewed as ideals of $\mathfrak{R}[x]/< x^n - 1 >$. The generators of C in terms of minimal degree polynomials of certain subsets of C have been obtained by Kaur et al. [6]. In this paper, using the structure of cyclic codes over a Galois ring given in [6], the generators of cyclic code of arbitrary length n over $\mathbb{Z}_8$, the ring of integers modulo 8 have been obtained in a unique form. Further, using the p-adic representation for the coefficients of these generators of cyclic codes over $\mathbb{Z}_8$, some results involving the generators have been proved. Cyclic codes over modular rings have applications in code- division multiple access (CDMA) cellular radio communication systems and M-PSK (M-ary Phase Shift Keying) channel.**

Keywords: **--- Cyclic codes, Unique form**

INTRODUCTION

Let R be a commutative ring with identity. A subset $C \subseteq R^n$ is called a linear code of length n over R if C is an R-submodule of R^n. A cyclic code C of length n over R is a linear code such that $(c_{n-1}, c_0, .., c_{n-2}) \in C$ whenever $(c_0, c_1, .., c_{n-1}) \in C$. Identifying the codeword $(c_0, c_1, .., c_{n-1}) \in R^n$ with the polynomial $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} \in R_n = R[x]/< x^n - 1 >$, cyclic codes over a ring R can be recognized as ideals of R_n. Further, a cyclic shift $(c_{n-1}, c_0, .., c_{n-2})$ of the codeword $(c_0, c_1, .., c_{n-1})$ can be identified with the polynomial $xc(x)$ modulo $x^n - 1$.

A finite ring with identity is a Galois ring if its zero divisors including zero form a principal ideal $< p >$ for some prime p. A Galois ring $\mathfrak{R}$ is a Galois extension of $\mathbb{Z}_{p^a}$ of degree m, where p is a prime and a, m are natural numbers. The characteristic of the Galois ring $\mathfrak{R}$ is p^a and cardinality is p^{am}. Further, $\mathfrak{R}$ is isomorphic to the ring $\mathbb{Z}_{p^a}[y]/< f(y) >$ where $f(y)$ is a monic basic irreducible polynomial of degree m in $\mathbb{Z}_{p^a}[y]$. It is easy to see that $\xi = y + < f(y) >$ is a root of $f(y)$ and $a_0 + a_1y + \cdots + a_{m-1}y^{m-1} + < f(y) > = a_0 + a_1\xi + \cdots + a_{m-1}\xi^{m-1}$, where $a_i \in \mathbb{Z}_{p^a}$ for $0 \le i \le m-1$. Therefore, $\mathfrak{R} = \mathbb{Z}_{p^a}[y]/< f(y) > = \mathbb{Z}_{p^a}[\xi]$. A Galois ring of characteristic p^a and cardinality p^{am} is denoted by $GR(p^a, m)$. The Galois ring $GR(p^a, m)$ is isomorphic to a finite field F_{p^m} with p^m elements for $a = 1$, and, is isomorphic to a finite ring $\mathbb{Z}_{p^a}$ with p^a elements for $m = 1$ ([12]).

The codewords of $\mathbb{Z}_4$ linear codes are associated with some complex valued sequences. If the complex correlation of the complex valued sequences is low so that the minimum Euclidean distance of the code is large then the family of such sequences has applications in code-division multiple access (CDMA) cellular radio communication systems and the code has potentially good error correction. For further reference, see [8].

Further in communication systems, cyclic codes over $\mathbb{Z}_8$ are employed in 8-PSK (8-ary Phase Shift Keying) channels, where 8 possible channel signals are different phases of a given basic signal. The 8 channel signals are associated with integers modulo 8 and this association gives the motivation to study cyclic codes over $\mathbb{Z}_8$. For further reference, see [10]. Thus a profound characterization of such an important class of codes is needed.

It is well known that cyclic codes over finite fields are in one to one correspondence with the monic divisors of $x^n - 1$. However, the description of cyclic codes over a finite ring R in terms of the divisors of $x^n - 1$ is much more intricate, as the polynomial ring $R[x]$ ceases to be a unique factorization domain. In literature, mostly the structure of cyclic codes has been determined in terms of the divisors of $x^n - 1$. For reference see ([1], [4], [5] and [9]). Kaur *et al.* [6] have employed a completely different approach to obtain the structure of cyclic codes of arbitrary

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 9, September 2017

length over a Galois ring. Using this structure, we have obtained a unique form for the generators of cyclic codes over $\mathbb{Z}_8$. Further some results related to the generators of cyclic codes of arbitrary length over $\mathbb{Z}_8$ have been obtained. These results characterize the generators of the cyclic codes of arbitrary length over $\mathbb{Z}_8$. This is a generalization of the results given by Sobhani and Molakarimi [11]. For further references, see Abualrub and Siap [2] and; Al-Ashker and Hamoudeh [3].

II. PRELIMINARIES

Let $\mathfrak{R}$ be a Galois ring of characteristic p^a and cardinality p^{am} and $\mathfrak{R}_n = \mathfrak{R}[x]/< x^n - 1 >$. We give below some preliminary results which shall be used in this paper.

Lemma 1. ([12]) Let $\mathcal{T} = \{0, 1, \xi, \xi^2, \dots, \xi^{p^m-2}\}$ where ξ is a root of $f(y)$ which is a monic basic irreducible polynomial in $\mathbb{Z}_{p^a}[y]$. Then every element $c \in \mathfrak{R} = \mathbb{Z}_{p^a}[y]/< f(y) >$ can be written uniquely as

$$c = c_0 + c_1 p + \cdots + c_{a-1}p^{a-1}, \qquad (1)$$

where $c_0, c_1, \dots, c_{a-1} \in \mathcal{T}$. Moreover, c is a unit if and only if $c_0 \neq 0$.

The representation given in equation (1) is called the p-adic representation of the element c.

Let C be an ideal in $\mathfrak{R}_n$. Let $g_e(x)$ be a minimal degree polynomial in C with minimum power of p in its leading coefficient. Suppose the leading coefficient of $g_e(x)$ is $p^{i_e}u_e$ where u_e is a unit and $0 \leq i_e \leq a-1$. If $i_e = 0$ then $g_e(x)$ is a monic polynomial; otherwise for $0 \leq j \leq e-1$, successively define $g_j(x)$ to be a minimal degree polynomial with minimum power of p in the leading coefficient among all polynomials in C having the power of p in the leading coefficient less than i_{j+1}, where i_j is the power of p in the leading coefficient of $g_j(x)$ and i_0 is the minimum power of p among the leading coefficients of all polynomials in C. Clearly $0 \leq i_0 < i_1 < \cdots < i_j < i_{j+1} < \cdots < i_e$. For $i_0 = 0$, $g_0(x)$ is a monic polynomial. Let t_j be the degree of the polynomial $g_j(x)$. Clearly $t_j > t_{j+1}$.

Theorem 1. ([6]) *Let C be an ideal in $\mathfrak{R}_n$ and $g_j(x)$ be polynomials as defined above. Then $C = < g_0(x), g_1(x), \dots, g_e(x) >$.*

Theorem 2. ([6]) *Let $g_j(x)$ be the polynomials as defined earlier. Then*

1) $p^{i_{j+1}-i_j}g_j(x) \in < g_{j+1}(x), g_{j+2}(x), \dots, g_e(x) >$ *for* $0 \leq j \leq e-1$.
2) $g_j(x) = p^{i_j}h_j(x)$, *where* $h_j(x)$ *is a monic polynomial in* $\mathfrak{R}^j[x]/< x^n - 1 >$, $\mathfrak{R}^j$ *is a Galois ring of characteristic* p^{a-i_j} *for* $0 \leq j \leq e$.
3) $h_{j+1}(x) | h_j(x) \pmod{p^{i_{j+2}-i_{j+1}}}$ *for* $0 \leq j \leq e-2$.
4) $h_e(x) | h_{e-1}(x) \pmod{p^{a-i_e}}$.
5) $p^{i_0}(x^n - 1) \in < g_0(x), g_1(x), \dots, g_e(x) >$ *and* $h_0(x) | (x^n - 1) \pmod{p^{i_1-i_0}}$.

Consider the map
$\Phi: \mathfrak{R}[x]/< x^n - 1 > \to F_{p^m}[x]/< x^n - 1 >$ defined as $\Phi(f(x)) = \overline{f(x)}$, where $\overline{f(x)} = f(x) \pmod{p}$. Clearly, Φ is a surjective ring homomorphism.

Definition 1. For $0 \leq j \leq a-1$, the i^{th}- torsion code of a cyclic code C of length n over $\mathfrak{R}$ is

$$Tor_i(C) = \{ \Phi(v(x)) \mid p^i v(x) \in C, v(x) \in \mathfrak{R}_n \}.$$

Theorem 3. ([7]) *Let $C = < g_0(x), g_1(x), \dots, g_e(x) >$ be an ideal in $\mathfrak{R}_n$ where $g_j(x) = p^{i_j}h_j(x)$ are polynomials as defined earlier. Then $Tor_{i_j}(C) = < \overline{h_j(x)} >$ and $i_j{}^{th}$-torsional degree of $C = deg\left(h_j(x)\right) = t_j$.*

Remark 1. ([7]) *Let $C = < g_0(x), g_1(x), \dots, g_e(x) >$ be a cyclic code of length n over $\mathfrak{R}$, where $g_j(x) = p^{i_j}h_j(x)$ are polynomials as defined earlier. Let $i_{j+1} - i_j = k_j$ for $0 \leq j \leq e-1$ and $a - i_e = k_e$. Clearly, $Tor_0(C) = Tor_1(C) = \cdots = Tor_{i_0-1}(C) = < 0 > = < x^n - 1 >$, $Tor_{i_j}(C) = Tor_{i_{j+1}}(C) = \cdots = Tor_{i_j+k_j-1}(C) \subset Tor_{i_{j+1}}(C)$ for $0 \leq j \leq e-1$ and $Tor_{i_e}(C) = Tor_{i_e+1}(C) = \cdots = Tor_{i_e+k_e-1}(C) = Tor_{a-1}(C)$.*

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 9, September 2017

III. MAIN RESULT

In this section, we shall use the $p-$adic representation for the coefficients of the generators of cyclic codes over $\mathbb{Z}_8$ to prove the main result.

The following result is easy to prove.

Lemma 2. *Let $C = < g_0(x), g_1(x), g_2(x)$ be a cyclic code of length n over $\mathbb{Z}_8$, where $g_j(x)$ are polynomials as defined earlier in Section 2. The generators $g_r(x)$ of C can be reduced to a unique form given by $g_r(x) = 2^r h_{r,0}(x) + 2^{r+1}h_{r,1}(x) + 2^{r+2}h_{r,2}(x)$ where $h_{i,j}(x)$ are polynomials in $\mathbb{Z}_2[x]$ such that $deg\left(h_{0,1}(x)\right) < deg\left(h_{1,0}(x)\right)$, $deg\left(h_{0,2}(x)\right) < deg\left(h_{2,0}(x)\right)$ and $deg\left(h_{1,1}(x)\right) < deg\left(h_{2,0}(x)\right)$.*

We shall now give the main result of this paper. Assume that $Tor_i(C) = < f_i(x) >$ where $f_i(x)$ can be determined using Remark 1and Theorem 3.

Theorem 4. *Let $C = < g_0(x), g_1(x), g_2(x)$ be a cyclic code of length n over $\mathbb{Z}_8$, where $g_1(x) \neq 0$, $g_0(x) = h_{0,0}(x) + 2h_{0,1}(x) + 4h_{0,2}(x)$, $g_1(x) = 2h_{1,0}(x) + 4h_{1,1}(x)$ and $g_2(x) = 4h_{2,0}(x)$ as defined earlier in Lemma 2. Then over $\mathbb{Z}_2$ we have*

1) $h_{i,0}(x)|(x^n - 1)$ *for* $i = 0, 1, 2$.
2) $h_{i,0}(x)|h_{i-1,0}(x)$ *for* $i = 1, 2$.
3) $f_i(x)|\frac{(x^n-1)}{h_{i-1,0}(x)}h_{i-1,1}(x)$ *for* $i = 1, 2$.
4) $f_i(x)|\frac{(x^n-1)}{h_{i-2,0}(x)}(h_{i-2,1}(x) + h_{i-2,2}(x) + \frac{h_{i-2,1}(x)h_{i-1,1}(x)}{h_{i-1,0}(x)})$ *for* $i = 2$.
5) $f_i(x)|(h_{i-2,0}(x) + h_{i-2,1}(x) + \frac{h_{i-2,0}(x)h_{i-1,1}(x)}{h_{i-1,0}(x)}$ *for* $i = 2$.

Proof. Using parts (3), (4) and (5) of Theorem 2, conditions (1) and (2) of the theorem hold. The polynomial $\frac{(x^n-1)}{h_{i,0}(x)}g_i(x)$ is in C. For $i = 0$, $\frac{(x^n-1)}{h_{00}(x)}g_0(x) = \frac{(x^n-1)}{h_{00}(x)}\left(h_{0,0}(x) + 2h_{0,1}(x) + 4h_{0,2}(x)\right)$ is in C. Therefore

$$2(x^n - 1)\frac{h_{0,1}(x)}{h_{0,0}(x)} + 4(x^n - 1)\frac{h_{0,2}(x)}{h_{0,0}(x)}$$

is in C. This gives that

$$\Phi((x^n - 1)\frac{h_{0,1}(x)}{h_{0,0}(x)} + 2(x^n - 1)\frac{h_{0,2}(x)}{h_{0,0}(x)})$$

is in $Tor_1(C) =< f_1(x) >$. Hence

$$f_1(x)|\frac{(x^n-1)}{h_{0,0}(x)}h_{0,1}(x) \bmod 2,$$

which proves condition (3) of the theorem. Similarly for $i = 2$ the condition (3) holds.

Using condition (3) of the Theorem along with the fact that $f_1(x) = h_{1,0}(x) \neq 0$, we get that the polynomial

$$A(x) = \frac{(x^n - 1)}{h_{0,0}(x)}g_0(x) + \frac{(x^n - 1)h_{0,1}(x)}{h_{0,0}(x)h_{1,0}(x)}g_1(x)$$

is in C. Now

$$\begin{aligned} A(x) = {} & 2\frac{(x^n - 1)}{h_{0,0}(x)}h_{0,1}(x) + 4\frac{(x^n - 1)}{h_{0,0}(x)}h_{0,2}(x) \\ & + 2\frac{(x^n - 1)}{h_{0,0}(x)}h_{0,1}(x) \\ & + 4\frac{(x^n - 1)\,h_{0,1}(x)}{h_{0,0}(x)\,h_{1,0}(x)}h_{1,1}(x) \\ = {} & 4\frac{(x^n-1)}{h_{0,0}(x)}(h_{0,1}(x) + h_{0,2}(x) + \frac{h_{0,1}(x)}{h_{1,0}(x)}h_{1,1}(x)) \end{aligned}$$

is in C. This implies that

$$\Phi(\frac{(x^n-1)}{h_{0,0}(x)}(h_{0,1}(x) + h_{0,2}(x) + \frac{h_{0,1}(x)}{h_{1,0}(x)}h_{1,1}(x)))$$

is in $Tor_2(C) =< f_2(x) >$. This gives $f_2(x)|\frac{(x^n-1)}{h_{0,0}(x)}(h_{0,1}(x) + h_{0,2}(x) + \frac{h_{0,1}(x)}{h_{1,0}(x)}h_{1,1}(x))$ mod 2, which proves condition (4) of the theorem.

Further, using condition (2) of the theorem the polynomial $B(x) = 2g_0(x) + \frac{h_{0,0}(x)}{h_{1,0}(x)}g_1(x)$ is in C. Now $B(x) = 4(h_{0,0}(x) + h_{0,1}(x) + \frac{h_{0,0}(x)}{h_{1,0}(x)}h_{1,1}(x))$ is in C. This implies that $\Phi(h_{0,0}(x) + h_{0,1}(x) + \frac{h_{0,0}(x)}{h_{1,0}(x)}h_{1,1}(x))$ is in $Tor_2(C) =< f_2(x) >$. Hence $f_2(x)|(h_{0,0}(x) + h_{0,1}(x) + \frac{h_{0,0}(x)}{h_{1,0}(x)}h_{1,1}(x))$ mod 2, which proves condition (5) of the theorem.

Theorem 5. *Let $C = < g_0(x), g_2(x) >$ be a cyclic code of length n over $\mathbb{Z}_8$, where $g_0(x) = h_{0,0}(x) + 2h_{0,1}(x) +$*

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 9, September 2017

$4h_{0,2}(x)$ *and* $g_2(x) = 4h_{2,0}(x)$ *as defined earlier in Lemma 2. Then over* $\mathbb{Z}_2$ *we have*

1) $h_{i,0}(x)|(x^n - 1)$ *for* $i = 0, 2$.
2) $h_{i,0}(x)|h_{i-2,0}(x)$ *for* $i = 2$.
3) $f_i(x)|\frac{(x^n-1)}{h_{i-1,0}(x)}h_{i-1,1}(x)$ *for* $i = 1$.
4) $f_i(x)|\frac{(x^n-1)}{h_{i-2,0}(x)}(h_{i-2,1}(x) + h_{i-2,2}(x) + \frac{h^2{}_{i-2,1}(x)}{h_{i-1,0}(x)})$ *for* $i = 2$.

Proof. Following the same steps as in the proof of the above theorem and using the fact $2h_{0,0}(x) + 4h_{0,1}(x) \in C$ along with Remark 1, we get the required result.

CONCLUSION

In this paper, we have characterized the generators of cyclic codes of arbitrary length over $\mathbb{Z}_8$. This characterization can be employed to obtain certain good codes suitable for the 8-PSK communication systems and CDMA cellular radio communication systems. Further using these results, a closed formula on the number of distinct cyclic codes over $\mathbb{Z}_8$ can be obtained.

REFERENCES

[1] Abualrub T., Oehmke R., Cyclic codes of length 2^e over $\mathbb{Z}_4$, Discrete Appl. Math., 128(1), 3--9 (2003).

[2] Abualrub T., Siap I., Cyclic codes over $\mathbb{Z}_2 + u\mathbb{Z}_2$ and $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$, Des. Codes. Cryptogr., 14, 273--287 (2007).

[3] Al-Ashker M., Hamoudeh M., Cyclic codes over $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2 + \cdots + u^{k-1}\mathbb{Z}_2$,Turkish J. Math., 35, 737--749 (2011).

[4] Calderbank A. R., Sloane N. J. A., Modular and p −adic cyclic codes, Des. Codes Cryptogr., 6(1), 21--35 (1995).

[5] Dougherty S. T., Park Y. H., On modular cyclic codes, Finite Fields Appl., 13, 31--57 (2007).

[6] Kaur J., Dutt S., Sehmi R., Cyclic codes over Galois rings, In: Govindarajan S., Maheshwari A. (eds) Algorithms and Discrete Applied Mathematics, Lecture Notes in Computer Science (LNCS) 9602, 233--239 (2016).

[7] Kaur J., Dutt S., Sehmi R., On cyclic codes over Galois rings, Communicated.

[8] Kumar P. V., Large families of quaternary sequences with low correlation. IEEE Transactions on Information Theory, 42(2), 579-592 (1996).

[9] Lӧpez-Permouth S. R., Özadam H., Özbudak F., Szabo S., Polycyclic codes over Galois rings with applications to repeated-root constacyclic codes. Finite Fields Appl., 19(1), 16-38 (2012).

[10] Piret P. M., Algebraic construction of cyclic codes over $\mathbb{Z}_8$ with a good Euclidean minimum distance, IEEE Transactions on Information Theory, 41(3), 815-818 (1995).

[11] Sobhani R., Molakarimi M., Some results on cyclic codes over the ring $R_{2,m}$, Turkish J. Math., 37, 1061--1074 (2013).

[12] Wan Z. X., Finite fields and Galois rings, World Scientific Publishing Company, (2011).