Cyclic Codes over Galois Rings

Jasbir Kaur, Sucheta Dutt, and Ranjeet Sehmi(✉)

Department of Applied Sciences, PEC University of Technology, Chandigarh, India
kjasbir03@gmail.com, {suchetapec,rksehmi2003}@yahoo.co.in

Abstract. Let R be a Galois ring of characteristic p^a, where p is a prime and a is a natural number. In this paper cyclic codes of arbitrary length n over R have been studied. The generators for such codes in terms of minimal degree polynomials of certain subsets of codes have been obtained. We prove that a cyclic code of arbitrary length n over R is generated by at most $min\{a, t+1\}$ elements, where $t = max\{deg(g(x))\}$, $g(x)$ a generator. In particular, it follows that a cyclic code of arbitrary length n over finite fields is generated by a single element. Moreover, the explicit set of generators so obtained turns out to be a minimal strong Gröbner basis.

Keywords: Galois ring · Cyclic codes · Gröbner basis · Minimal degree polynomial

1 Introduction

Cyclic codes over finite rings are being studied extensively these days and the literature is abundant with results on cyclic codes over finite rings where the characteristic of the ring under consideration and the length of the code are coprime. For reference see ([4,5,9,14,15]). The methodology used in most of these papers is to focus on irreducible factors of $x^n - 1$ and to obtain in turn, the ideals of the ring $R[x]/\langle x^n - 1\rangle$ by Hensel's lifting. However, this technique cannot be applied to codes of general length n as the ring ceases to be a unique factorization domain in case the length of the code and the characteristic s of the ring are not coprime. A few expositions are available for the study of cyclic codes over finite rings in case $(n, s) \neq 1$. For reference see ([6,7,10,11,16,17,19]). Dougherty et al. in [7] have given a structure theorem for codes over Galois rings and employed Chinese remainder theorem and lifting of irreducible polynomials. Sălăgean in [16] has given an existential proof for the existence of a minimal strong Gröbner basis for cyclic codes of arbitrary length over a finite chain ring. Norton et al. in [13,14] formalized the notion of generating set in standard form for cyclic codes over principal ideal ring and obtained necessary and sufficient conditions for the generating set to be a minimal strong Gröbner basis as defined in [2]. The result for repeated root cyclic codes over chain ring was extended

J. Kaur — Work submitted in partial fulfillment of requirements for the degree of Doctor of Philosophy.

© Springer International Publishing Switzerland 2016
S. Govindarajan and A. Maheshwari (Eds.): CALDAM 2016, LNCS 9602, pp. 233–239, 2016.
DOI: 10.1007/978-3-319-29221-2_20

by Sălăgean in [16]. Abualrub et al. in [1] have given a simpler approach by introducing minimal degree polynomials to find the generators of cyclic codes of length 2^k over $\mathbb{Z}_4$.

In this paper we take further the approach of Abualrub and find the generators of cyclic codes of general length over Galois rings in an explicit constructive manner. Also, the set of generators obtained turns out to be a minimal strong Gröbner basis. The results of Garg and Dutt [8] follow from our results.

2 Preliminaries

A cyclic code over a ring R is a linear code which is closed under cyclic shifts. It is well known that the cyclic codes of length n over a ring R are in correspondence with the ideals of $R[x]/\langle x^n - 1\rangle$ and thus cyclic codes over R, written as vectors, can be recognized as polynomials of degree less than n, that is, $c = (c_0, c_1, \ldots, c_{n-1})$ is identified with the polynomial $c_0 + c_1 x + \ldots + c_{n-1}x^{n-1}$.

A finite ring with identity is called a Galois ring if its zero divisors including zero form a principal ideal $\langle p\rangle$ for some prime p [18]. For any $m \geq 1$, the Galois extension ring of Z_{p^a} can be constructed as $GR(p^a, m) = Z_{p^a}[x]/\langle f(x)\rangle$, where p is a prime, a is a natural number and $f(x) \in Z_{p^a}[x]$ is a monic basic irreducible polynomial of degree m. The ring $GR(p^a, m)$ is called a Galois ring and has p^{am} elements. For $a = 1$, we obtain the finite field $GF(p^m)$ with p^m elements ([12,18]).

Let I be an ideal in $R[x]$ and $A(x)$ be an element of I. Let $lm(A(x))$ denote the leading monomial of $A(x)$. A set $G = \{B_i(x), 1 \leq i \leq \nu\}$ of non zero elements of I is called a Gröbner basis of I if for each $A(x) \in I$ there exists an $i \in \{1, 2, \ldots, \nu\}$ such that $lm(A(x))$ is divisible by $lm(B_i(x))$. An arbitrary subset G of $R[x]$ is called a Gröbner basis if it is a Gröbner basis of $\langle G\rangle$ [3].

3 Generators of Cyclic Codes over a Galois Ring R as Ideals of $R[x]/\langle x^n - 1\rangle$

Let $R = GR(p^a, m)$ be a Galois ring and $R_n = R[x]/\langle x^n - 1\rangle$. The aim of this paper is to find the generators of cyclic codes over Galois rings as ideals of R_n. These generators are found in terms of minimal degree polynomials of certain subsets of the given code.

Let C be an ideal in R_n and $g_e(x)$ be a minimal degree polynomial in C with minimum power of p in the leading coefficient. Let the leading coefficient of $g_e(x)$ be $p^{i_e}u_e$ 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 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 in the leading coefficients among all polynomials in C. Then $0 \leq i_0 < i_1 < \ldots < i_j < i_{j+1} < \ldots < i_e$. For $i_0 = 0$, $g_0(x)$ is a monic polynomial. Let t_j be the degree of the polynomial $g_j(x)$. Clearly $t_j > t_{j+1}$.

Remark 1. It is easy to see that for any polynomial $c(x)$ in C with power of p in the leading coefficient l, there exists a j with $0 \leq j \leq e$ such that $t_j \leq deg(c(x)) < t_{j-1}$. Then $l \geq i_j$ and the polynomial

$$r(x) = c(x) - p^{l-i_j} g_j(x) u x^{deg(c(x))-t_j}$$

is in C for some unit u. Moreover, $r(x) = 0$ or $deg(r(x)) < deg(c(x))$. The polynomial $r(x)$ can be expressed as $r(x) = c(x) - q(x)g_j(x)$ for some $q(x) \in R_n$.

The following theorem gives the generators of a cyclic code over the ring R.

Theorem 1. *Let C be an ideal in R_n and $g_j(x)$ be polynomials as defined above. Then $C = \langle g_0(x), g_1(x), \ldots, g_e(x) \rangle$.*

Proof. Let $c(x)$ be a polynomial in C. By Remark 1, there exists a j and a polynomial $q_1(x) \in R_n$ such that the polynomial

$$r_1(x) = c(x) - q_1(x)g_j(x)$$

is in C. Moreover, $r_1(x) = 0$ or $deg\big(r_1(x)\big) < deg\big(c(x)\big)$. If $r_1(x) = 0$ then $c(x) \in \langle g_j(x) \rangle \subset \langle g_0(x), g_1(x), \ldots, g_e(x) \rangle$. If $deg\big(r_1(x)\big) < deg\big(c(x)\big) < t_{j-1}$ then by Remark 1 there exists a k and a polynomial $q_2(x) \in R_n$ such that the polynomial

$$r_2(x) = r_1(x) - q_2(x)g_k(x)$$

is in C. Moreover, $r_2(x) = 0$ or $deg\big(r_2(x)\big) < deg\big(r_1(x)\big) < deg\big(c(x)\big)$. Clearly $k \geq j$. If $r_2(x) = 0$ then $c(x)$ belongs to $\langle g_j(x), g_k(x) \rangle \subset \langle g_0(x), g_1(x), \ldots, g_e(x) \rangle$. If $deg\big(r_2(x)\big) < deg\big(r_1(x)\big)$, it is evident that after repeating the argument a finite number of times we shall have the remainder equal to zero as the degrees of the remainders form a decreasing sequence of natural numbers which is bounded below by t_e. Therefore back substituting for the remainders it is clear that any polynomial $c(x)$ in C belongs to $\langle g_j(x), \ldots, g_e(x) \rangle$ where j is the smallest value such that $deg\big(c(x)\big) \geq t_j$ for $0 \leq j \leq e$. Consequently we get $C = \langle g_0(x), g_1(x), \ldots, g_e(x) \rangle$. □

The following corollaries are an immediate consequence of Theorem 1.

Corollary 1. *A cyclic code C of arbitrary length n over a Galois ring of characteristic p^a is generated by at most k elements, with $k = min\{a, t+1\}$, where $t = max\{deg(g(x))\}$, $g(x)$ a generator.*

Corollary 2. *A cyclic code C of arbitrary length n over an integer residue ring of characteristic p^a is generated by at most k elements, with $k = min\{a, t+1\}$, where $t = max\{deg(g(x))\}$, $g(x)$ a generator.*

Proof. For $m = 1$, the Galois ring $GR(p^a, m)$ is an integer residue ring of characteristic p^a. □

As finite fields are special case of Galois rings with $a = 1$. We have the following corollary.

Corollary 3. *A cyclic code C of arbitrary length n over finite fields is generated by a single element.*

Theorem 2. *Let $g_e(x)$ be the polynomial as defined above. Then $g_e(x) = p^{i_e}h_e(x)$, where $h_e(x)$ is a monic polynomial in $R^e[x]/\langle x^n - 1\rangle$, R^e is a Galois ring of characteristic p^{a-i_e}.*

Proof. Let $g_e(x) = p^{i_e}u_e x^{t_e} + b_{t_e-1}x^{t_e-1} + \ldots + b_0$. Suppose $b_j \not\equiv 0 \pmod{p^{i_e}}$ for some j, where $0 \leq j \leq t_e - 1$. Now $p^{a-i_e}g_e(x) \in C$ and is a polynomial of degree less than t_e, a contradiction. Hence $b_j \equiv 0 \pmod{p^{i_e}}$ for every j. Thus $g_e(x) = p^{i_e}h_e(x)$ where $h_e(x) \in R^e[x]/\langle x^n - 1\rangle$, R^e is a Galois ring of characteristic p^{a-i_e}. Clearly $h_e(x)$ is a monic polynomial. □

Theorem 3. *Let the polynomials $g_j(x)$ be the polynomials as defined above. Then for $0 \leq j \leq e-1$*

1. $p^{i_{j+1}-i_j}g_j(x) \in \langle g_{j+1}(x), g_{j+2}(x), \ldots, g_e(x)\rangle$.
2. $g_j(x) = p^{i_j}h_j(x)$ *where $h_j(x)$ is a monic polynomial in $R^j[x]/\langle x^n - 1\rangle$, R^j is a Galois Ring of characteristic p^{a-i_j}.*
3. $h_{j+1}(x)|h_j(x)$ *(mod $p^{i_{j+2}-i_{j+1}}$).*

Proof. Let $c(x) = p^{i_{j+1}-i_j}g_j(x) - g_{j+1}(x)x^{t_j-t_{j+1}}$. Then $c(x)$ is in C and $deg(c(x)) < t_j$. Now proceeding as in Theorem 1, it is easy to see that

$$c(x) = p^{i_{j+1}-i_j}g_j(x) - g_{j+1}(x)x^{t_j-t_{j+1}} \in \langle g_k(x), g_{k+1}(x), \ldots, g_e(x)\rangle$$

for some $k > j$. This further implies that

$$p^{i_{j+1}-i_j}g_j(x) \in \langle g_{j+1}(x), g_{j+2}(x), \ldots, g_e(x)\rangle \tag{1}$$

This completes the proof for part 1 of the theorem.

Next, we need to show that

$$g_j(x) = p^{i_j}h_j(x) \tag{2}$$

for $0 \leq j \leq e-1$. From Theorem 2, $g_e(x) = p^{i_e}h_e(x)$, where $h_e(x)$ is a monic polynomial in $R^e[x]/\langle x^n - 1\rangle$, R^e is a Galois ring of characteristic p^{a-i_e}. Suppose $g_{e-1}(x), g_{e-2}(x), \ldots, g_j(x)$ satisfy (2). Then we will show that $g_{j-1}(x)$ satisfies (2). From (1) we have

$$p^{i_j-i_{j-1}}g_{j-1}(x) \in \langle g_j(x), g_{j+1}(x), \ldots, g_e(x)\rangle.$$

This gives

$$\begin{aligned} p^{i_j-i_{j-1}}g_{j-1}(x) &= g_j(x)F_j(x) + \ldots + g_e(x)F_e(x) \\ &= p^{i_j}h_j(x)F_j(x) + \ldots + p^{i_e}h_e(x)F_e(x) \\ &= p^{i_j}K(x). \end{aligned}$$

Suppose there exists a coefficient $g_{l,j-1}$ of the polynomial $g_{j-1}(x)$ such that $g_{l,j-1} \not\equiv 0 \pmod{p^{i_{j-1}}}$. Multiplying both sides by p^{a-i_j} we get, $p^{a-i_{j-1}} g_{j-1}(x) = 0$, a contradiction. Thus $g_{j-1}(x) = p^{i_{j-1}} h_{j-1}(x)$, where $h_{j-1}(x)$ is a monic polynomial. Therefore by principle of mathematical induction (2) holds for all j.

Next, for $1 \leq k \leq a-1$, consider the maps

$$\psi_k : GR(p^a, m) \longrightarrow GR(p^k, m)$$

defined by

$$\psi_k(\alpha) = \alpha \pmod{p^k}.$$

ψ_k is a ring homomorphism for all k which can be extended to

$$\phi_k : GR(p^a, m)[x]/\langle x^n - 1\rangle \longrightarrow GR(p^k, m)[x]/\langle x^n - 1\rangle$$

by defining

$$\phi_k(c_0 + c_1 x + \ldots + c_{n-1}x^{n-1}) = \psi_k(c_0) + \psi_k(c_1)x + \ldots + \psi_k(c_{n-1})x^{n-1}.$$

From (1) and (2) we have

$$p^{i_{j+1}} h_j(x) \in \langle p^{i_{j+1}} h_{j+1}(x), p^{i_{j+2}} h_{j+2}(x), \ldots, p^{i_e} h_e(x)\rangle,$$

which implies

$$p^{i_{j+1}} h_j(x) = p^{i_{j+1}} h_{j+1}(x)F_{j+1}(x) + p^{i_{j+2}} h_{j+2}(x)F_{j+2}(x) + \ldots + p^{i_e} h_e(x)F_e(x),$$

where $F_k(x) \in R_n$ for $j+1 \leq k \leq e$. Therefore

$$\begin{aligned} p^{i_{j+1}}\big(h_j(x) - h_{j+1}(x)F_{j+1}(x)\big) &= p^{i_{j+2}} h_{j+2}(x)F_{j+2}(x) + \ldots + p^{i_e} h_e(x)F_e(x) \\ &= p^{i_{j+2}} F(x), \end{aligned}$$

where $F(x) = h_{j+2}(x)F_{j+2}(x) + \ldots + p^{i_e - i_{j+2}} h_e(x)F_e(x)$. Now

$$p^{i_{j+1}}\big(h_j(x) - h_{j+1}(x)F_{j+1}(x) - p^{i_{j+2}-i_{j+1}} F(x)\big) = 0.$$

It follows that the power of p in each coefficient of the polynomial

$$h_j(x) - h_{j+1}(x)F_{j+1}(x) - p^{i_{j+2}-i_{j+1}} F(x)$$

is greater than or equal to $a - i_{j+1}$. As $\langle p^{a-i_{j+1}}\rangle \subset \langle p^{i_{j+2}-i_{j+1}}\rangle$, the coefficients of the polynomial $h_j(x) - h_{j+1}(x)F_{j+1}(x) - p^{i_{j+2}-i_{j+1}} F(x)$ vanish mod $p^{i_{j+2}-i_{j+1}}$. Thus

$$\phi_{i_{j+2}-i_{j+1}}\big(h_j(x) - h_{j+1}(x)F_{j+1}(x) - p^{i_{j+2}-i_{j+1}} F(x)\big) = 0.$$

As $\phi_{i_{j+2}-i_{j+1}}$ is a homomorphism, we have

$$\phi_{i_{j+2}-i_{j+1}}\big(h_j(x)\big) = \phi_{i_{j+2}-i_{j+1}}\big(h_{j+1}(x)F_{j+1}(x)\big) + \phi_{i_{j+2}-i_{j+1}}\big(p^{i_{j+2}-i_{j+1}} F(x)\big)$$

or

$$\phi_{i_{j+2}-i_{j+1}}\big(h_j(x)\big) = \phi_{i_{j+2}-i_{j+1}}\big(h_{j+1}(x)F_{j+1}(x)\big)$$

which gives $h_{j+1}(x) | h_j(x) \pmod{p^{i_{j+2}-i_{j+1}}}$. □

Theorem 4. *The set* $\{g_0(x), g_1(x), \ldots, g_e(x)\}$ *is a minimal strong Gröbner basis of* C.

Proof. The result follows as an immediate consequence of Theorem 3 above and Theorem 3.2 of [14]. □

Some examples of minimal strong Gröbner basis are given below.

Example 1. Let $G = \{g_0(x), g_1(x), g_2(x)\}$ where $g_j(x) = 2^j h_j(x)$ for $0 \leq j \leq 2$ with $h_0(x) = x^3 + x^2 + x + 1$, $h_1(x) = x^2 + 1$ and $h_2(x) = x + 1$. Let C be the cyclic code of length 8 over $\mathbb{Z}_8$ generated by G. It is easy to see that $x+1|x^2+1$ over $\mathbb{Z}_2$ and $x^2 + 1|x^3 + x^2 + x + 1$ over $\mathbb{Z}_4$. Also, $4(x^2 + 1) \in \langle 4(x + 1)\rangle$ and $2(x^3 + x^2 + x + 1) \in \langle 2(x^2 + 1), 4(x + 1)\rangle$. Therefore by Theorem 3 above, G is a minimal strong Gröbner basis.

Example 2. Let $G_1 = \{g_0(x), g_1(x)\}$ where $g_j(x) = 2^j h_j(x)$ for $0 \leq j \leq 1$ with $h_0(x) = x^5 + x^4 + x^3 + x^2 + x + 1$ and $h_1(x) = x^4 + x^2 + 1$. Let C_1 be the cyclic code of length 6 over $\mathbb{Z}_4$ generated by G_1. Then G_1 is a minimal strong Gröbner basis.

Example 3. Let $G_2 = \{g_0(x), g_1(x)\}$ where $g_j(x) = 2^j h_j(x)$ for $0 \leq j \leq 1$ with $h_0(x) = x^3 - 1$, $h_1(x) = x + 1$. Then G_2 is a minimal strong Gröbner basis for the cyclic code C_2 of length 6 over $\mathbb{Z}_4$.

Example 4. Let $G_3 = \{g_0(x), g_1(x)\}$ where $g_j(x) = 2^j h_j(x)$ for $0 \leq j \leq 1$ with $h_0(x) = x^3 + x^2 + x + 1$ and $h_1(x) = x^2 + 1$. Let C_3 be the cyclic code of length 4 over $\mathbb{Z}_4$ generated by G_3. Then G_3 is a minimal strong Gröbner basis.

Example 5. Let $G_4 = \{g_0(x), g_1(x)\}$ where $g_j(x) = 2^j h_j(x)$ for $0 \leq j \leq 1$ with $h_0(x) = x^2 + 1$ and $h_1(x) = x + 1$. Then G_4 is a minimal strong Gröbner basis for the cyclic code C_4 of length 4 over $\mathbb{Z}_4$.

4 Conclusion

A cyclic code of arbitrary length n over a Galois ring of characteristic p^a is generated by at most $min\{a, t + 1\}$ elements, where $t = max\{deg(g(x))\}$, $g(x)$ a generator. Moreover, the set of generators so obtained is a minimal strong Gröbner basis of the code.

Acknowledgments. The author (Jasbir Kaur) gratefully acknowledges the World Bank funded TEQIP-II for financial support.

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. Adams, W., Loustaunau, P.: An Introduction to Gröbner Basis. American Mathematical Society, Providence (1994)
3. Byrne, E., Fitzpatrick, P.: Gröbner bases over Galois rings with an application to decoding alternant codes. J. Symbolic Comput. **31**, 565–584 (2001)
4. Calderbank, A.R., Sloane, N.J.A.: Modular and p-adic cyclic codes. Des. Codes Cryptogr. **6**(1), 21–35 (1995)
5. Dinh, H.Q., Lopez-Permouth, S.R.: Cyclic and negacyclic codes over finitechain rings. IEEE Trans. Inform. Theory **50**(8), 1728–1744 (2004)
6. Dougherty, S.T., Ling, S.: Cyclic codes over $\mathbb{Z}_4$ of even length. Des. Codes Cryptogr. **39**(2), 127–153 (2006)
7. Dougherty, S.T., Park, Y.H.: On modular cyclic codes. Finite Fields Appl. **13**, 31–57 (2007)
8. Garg, A., Dutt, S.: Cyclic codes of length 2^k over $\mathbb{Z}_{2^m}$.. Int. J. Eng. Res. Dev. **1**(9), 34–37 (2012)
9. Kanwar, P., Lopez-Permouth, S.R.: Cyclic codes over the integers modulo p^m. Finite Fields Appl. **3**(4), 334–352 (1997)
10. Kiah, H.M., Leung, K.H., Ling, S.: Cyclic codes over $GR(p^2, m)$ of length p^k. Finite Fields Appl. **14**(3), 834–846 (2008)
11. Lopez-Permouth, S.R., Ozadam, H., Ozbudak, F., Szabo, S.: Polycyclic codesover Galois rings with applications to repeated-root constacyclic codes. Finite Fields Appl. **19**(1), 16–38 (2012)
12. McDonald, B.R.: Finite Rings with Identity. Marcel Dekker, New York (1974)
13. Norton, G.H., Sălăgean, A.: Strong Gröbner bases for polynomials over a principal ideal ring. Bull. Aust. Math. Soc. **64**(3), 505–528 (2001)
14. Norton, G.H., Sălăgean, A.: Cyclic codes and minimal strong Gröbner bases over a principal ideal ring. Finite Fields Appl. **9**(2), 237–249 (2003)
15. Rajan, B.S., Siddiqi, M.U.: Transform domain characterization of cyclic codes over $\mathbb{Z}_m$.. Appl. Algebra Eng. Commun. Comput. **5**(5), 261–275 (1994)
16. Sălăgean, A.: Repeated-root cyclic and negacyclic codes over a finite chain ring. Discrete Appl. Math. **154**(2), 413–419 (2006)
17. Sobhani, R., Esmaeili, M.: Cyclic and negacyclic codes over the Galois ring $GR(p^2, m)$.. Discrete Appl. Math. **157**(13), 2892–2903 (2009)
18. Wan, Z.X.: Finite fields and Galois rings. World Scientific Publishing Company, Singapore (2011)
19. Woo, S.S.: Ideals of $\mathbb{Z}_{p^n}[x]/\langle x^l - 1\rangle$.. Commun. Korean Math. Soc. **26**(3), 427–443 (2011)