ISSN 0974 - 9373

Vol. 19 No. 2 (2015) **Journal of International Academy of Physical Sciences** pp. 123-130

Cyclic Codes of Length p^k over Z_{p^m}

Arpana Garg and Sucheta Dutt
Department of Applied Sciences
PEC University of Technology
Chandigarh, India.
Email: arpanapujara@gmail.com, suchetapec@yahoo.co.in

(Received May 05, 2015)

Abstract: In this paper, the structure of cyclic codes over Z_{p^m} of length $n=p^k$ for any prime p and natural numbers m and k is studied as ideals of $Z_{p^m}[x]/<x^n-1>$. It is proved that cyclic codes of length $n=p^k$ over Z_{p^m} are generated as ideals of $Z_{p^m}[x]/<x^n-1>$ by at most m elements.

MSC: 94B15, 94B05, 94B60.

Keywords: Cyclic codes, Ideals, Minimal Degree Polynomial, Principal ideal *R*ing.

1. Introduction

Let R be a commutative finite ring with identity. A linear code C over R of length n is defined as an R-submodule of R^n. A cyclic code C over R of length n is a linear code such that any cyclic shift of a codeword is also a codeword, that is, whenever $(c_0, c_1, c_2, \ldots, c_{n-1})$ is in C then so is $(c_{n-1}, c_0, c_1, c_2, \ldots, c_{n-2})$. The one-one correspondence between cyclic codes of length $n=p^k$ over Z_{p^m} and ideals of $Z_{p^m}[x]/<x^n-1>$ is well known (Here p is prime and k and m are natural numbers).

The structure of cyclic codes over Z_4 of length 2^e is given by T. Abualrub[1]. This result is extended to cyclic codes over Z_8 of length 2^k by Arpana Garg and Sucheta Dutt[2], where it is proved that cyclic codes over Z_8 of length 2^k are generated by at most three elements. This result is further generalized to cyclic codes of length 2^k over Z_{2^m} and it is proved that cyclic codes over the ring Z_{2^m} of length 2^k as ideals of $Z_{2^m}[x]/<x^n-1>$, where $n=2^k$ are generated by at most m elements[3].

In this paper, we study the structure of cyclic codes of length $n=p^k$ over Z_{p^m} as ideals of the ring $Z_{p^m}[x]/<x^n-1>$ and prove that cyclic codes of length $n=p^k$ over Z_{p^m} are generated by at most m elements.

2. Preliminaries

Codewords of a cyclic code of length *n* over a ring *R* can be represented by polynomials over *R* modulo x^n-1. Thus any codeword $(c_0, c_1, c_2, \ldots, c_{n-1})$ can be represented by a polynomial $c(x)=c_0+c_1x+c_2x^2+\ldots+c_{n-1}x^{n-1}$ over the ring *R*.

Definition 2.1: The content of the polynomial

$$f(x)=a_0+a_1x+a_2x^2+\ldots+a_lx^l$$

where a_i's belong to Z_{p^m}, is defined as the greatest common divisor of $a_0, a_1, a_2, \ldots, a_l$.

Consider the ring $Z_{p^m}[x]/<x^n-1>$ where *p* is prime and *m, n* are natural numbers. It is known that this ring is a principal ideal domain for *m* = 1. However, for $m>1$ and $n=p^k$, the ideal of $Z_{p^m}[x]/<x^n-1>$ generated by p, $x+p-1$ cannot be generated by a single element. Therefore $Z_{p^m}[x]/<x^n-1>$ is not a principal ideal ring for $m>1$ and $n=p^k$.

3. Generators of cyclic codes over Z_{p^m} of length p^k as ideals of $Z_{p^m}[x]/<x^n-1>$

Lemma 3.1: *Let C be an ideal of the ring* $Z_{p^m}[x]/<x^n-1>$ *where* $n=p^k$ *. If the minimal degree polynomial* $g(x)$ *in C is monic, then C is generated as an ideal by* $g(x)$.

Proof: Let $g(x)$ be the minimal degree polynomial in *C* such that the leading coefficient of *g(x)* is a unit. Let $c(x)$ be a polynomial in *C*. Then, by division algorithm there exists $q(x)$ and $r(x)$ over Z_{p^m} such that

$c(x) = g(x)q(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg g(x)$. Now $r(x) = c(x) - g(x)q(x) \in C$, as C is an ideal. If $r(x) \neq 0$, then $\deg r(x) < \deg g(x)$, which is a contradiction to the choice of degree of $g(x)$. Therefore $r(x) = 0$, that is , every polynomial $c(x)$ in C is a multiple of $g(x)$. Hence C is generated by $g(x)$.

Lemma 3.2: *Let C be an ideal of the ring* $Z_{p^m}[x]/<x^n - 1>$ *where* $n = p^k$. *Let* $g(x)$ *be a minimal degree polynomial in C. If the leading coefficient of g(x) is* $p^s h$ *where* $1 \le s \le m$ *and* $(p,h) = 1$, *then the content of* $g(x)$ *is* p^s, *that is,* $g(x) = p^s q_s(x)$, *where* $q_s(x) \in Z_{p^{m-s}}[x]/<x^n - 1>$.

Proof: Let $g(x)$ be a minimal degree polynomial in C of degree $'t'$ with leading coefficient $p^s h$ where $1 \le s \le m$ and $(p,h) = 1$. Let $g(x) = a_0 + a_1 x + a_2 x^2 + ... + a_t x^t$ be such that $a_t = p^s h$. We claim that $a_i \equiv 0 (\bmod p^s)$ for every *i*. Suppose this is not so. Then there exist some $j < t$ such that $a_i \neq 0 (\bmod p^s)$. Then $p^{m-s} g(x)$ is a nonzero polynomial of degree less than the degree of $g(x)$ and belongs to C, which contradicts the minimality of degree of *g(x)* in C. Hence $a_i \equiv 0 (\bmod p^s)$ for every i and content of $g(x)$ is p^s.Therefore $g(x) = p^s q_s(x)$, where $q_s(x) \in Z_{p^{m-s}}[x]/<x^n - 1>$.

Lemma 3.3*: Let C be an ideal of the ring* $Z_{p^m}[x]/<x^n - 1>$ *where* $n = p^k$. *Let* $g(x)$ *be a minimal degree polynomial in C with leading coefficient* $p^s h$ *where* $1 \le s \le m$ *and* $(p,h) = 1$. *Let all the polynomials in C have leading coefficients of the type* $p^u h$ *such that* $u \ge s$ *and h is a unit. Then* $C = <g(x)> = <p^s q_s(x)>$ *where* $q_s(x) \in Z_{p^m}[x]/<x^n - 1>$.

Proof: As $g(x)$ is a minimal degree polynomial in C of degree $'t'$ with leading coefficient $p^s h$ where $1 \le s \le m$ and $(p,h) = 1$, by Lemma 3.2, the content of $g(x)$ is p^s and $g(x) = p^s q_s(x)$, where $q_s(x) \in Z_{p^{m-s}}[x]/<x^n - 1>$. We claim that all the polynomials in C are multiples of $g(x) = p^s q_s(x)$. If possible, slet there exist polynomials in C which are not divisible by *g(x)*. Out of such polynomials, let $c(x)$ be a minimal degree polynomial. Let $\deg c(x) = v$. As *c(x)* is not divisible by $g(x)$, there exists $r(x) \neq 0$ such that $c(x) = g(x)dx^{v-t} + r(x)$ where $\deg r(x) < \deg c(x)$ and d is an integer. Because C is an ideal, we have $r(x) = c(x) - g(x)dx^{v-t} \in C$. As $\deg r(x) < \deg c(x)$ and $r(x) \in C$ we must have $g(x)/r(x)$. This implies $g(x)/c(x)$, which is a contradiction. Therefore all polynomials in C are multiples of $g(x) = p^s q_s(x)$. Hence $C = < g(x) > = < p^s q_s(x) >$

Lemma 3.4: *Let C be an ideal of the ring* $Z_{p^m}[x]/ < x^n - 1 >$ *where* $n = p^k$. *Let* $p^{s_l} q_l(x)$ *be a minimal degree polynomial in C, where* $q_l(x)$ *is monic. Then* $C = < p^{s_1} q_1(x), p^{s_2} q_2(x), ..., p^{s_{l-1}} q_{l-1}(x), p^{s_l} q_l(x) >$ *where* $0 \leq s_1 \leq s_2 \leq ... \leq s_{l-1} \leq s_l$ *and* $p^{s_i} q_i(x)$ *is a minimal degree polynomial in C among all polynomials in C with leading coefficient of the type* $p^u a$, *where* $(a, p) = 1, u < s_{i+1}$, *and* $q_i(x)$ *is monic for* $1 \leq i \leq 1$.

Proof: Let $c(x)$ be any polynomial in C with leading coefficient of the type $p^u h$ (*h* unit). If $u \geq s_l$, then kill the highest power of $c(x)$ as follows:

(3.1) $$c(x) = p^{s_l} q_l(x).d.x^{\deg(c(x)) - \deg(p^{s_l} q_l(x))} + r(x)$$

where either $r(x) = 0$ or $\deg r(x) < \deg c(x)$. As C is an ideal, $r(x) \in C$. If $r(x) \notin C$ and leading coefficient of $r(x)$ *)* is of the type $p^u h$ (*h* unit) such that $u \geq s_l$, then further go on killing the highest degree term of the remainder till it is zero or it has leading coefficient of the type $p^u h$ (*h* unit) such that $u < s_l$. If remainder become zero at some stage, then *c(x)* is divisible by $p^{s_l} q_l(x)$. Moreover, if during the process degree of remainder becomes less than the degree of $p^{s_l} q_l(x)$, we must have the remainder equal to zero at that stage as $p^{s_l} q_l(x)$ is a minimal degree polynomial in *C*. Therefore without loss of generality, we suppose that either *c(x)* is divisible by $p^{s_l} q_l(x)$ or

(3.2) $$c(x) = p^{s_l} q_l(x) q(x) + r_1(x),$$

where $\deg\deg(r_1(x)) > \deg(p^{s_l}q_l(x))$ and leading coefficient of $r_1(x)$ is of the type $p^u h$ (h unit) such that $u < s_l$. Let $g_1(x)$ be minimal degree polynomial in C among all polynomials in C with leading coefficient of the type $p^u h$ (h unit) such that $u < s_l$. Then all polynomials in C with degree less than degree of $g_1(x)$ should have leading coefficient of the type $p^u h$ (h unit) such that $u < s_l$. Let leading coefficient of $g_1(x)$ be $p^{s_{l-1}}h_1(h_1$ unit). Now, we claim that content of $g_1(x)$ is $p^{s_{l-1}}$. Leading coefficient of $(p^{s_l} - p^{s_{l-1}})g_1(x)$ is $p^{s_l}h_1(h_1$ unit). Therefore

(3.3) $$(p^{s_l} - p^{s_{l-1}})g_1(x) = p^{s_l}q_l(x).d.x^{\deg(g_1(x)) - \deg(p^{s_l}q_l(x))} + r'(x)$$

where $r'(x) = 0$ $\deg r'(x) < \deg\left\{(p^{s_l} - p^{s_{l-1}})g_1(x)\right\} = \deg g_1(x)$. As C is an ideal, $r'(x) \in C$. If $r'(x) \neq 0$, then leading coefficient of $r'(x)$ must be of the type $p^u h$ (h unit) such that $u \geq s_l$. Therefore

(3.4) $$r'(x) = p^{s_l}q_l(x).d_2.x^{\deg(r'(x)) - \deg(p^{s_l}q_l(x))} + r''(x)$$

where either $r''(x) = 0$ or $\deg(r''(x)) < \deg(r'(x)) < \deg(g_1(x))$. As C is an ideal, $r''(x) \in C$. Again, if $r''(x) \neq 0$, then leading coefficient of $r''(x)$ must be of the type $p^u h$ (h unit) such that $u \geq s_l$. Continuing in this way, we can go on killing the highest degree term of the remainder till degree of the remainder becomes less than degree of $p^{s_l}q_l(x)$. The situation that the degree of remainder is less than degree of $p^{s_l}q_l(x)$ cannot arise because $p^{s_l}q_l(x)$ is a minimal degree polynomial in C and the remainder belongs to C. It follows that at some stage the remainder is zero. This implies that content of $(p^{s_l} - p^{s_{l-1}})g_1(x)$ is p^{s_l} and therefore the content of $g_1(x)$ is $p^{s_{l-1}}$ and $g_1(x) = p^{s_{l-1}}q_{l-1}(x)$ (say), where $q_{l-1}(x)$ is a monic polynomial.

Now, if C does not contain any polynomial with leading coefficient of the type $p^u h$ (h unit) such that $u < s_{l-1}$, then leading coefficient of $r_1(x)$ (referring back to equation (3.2)) is of the type $p^u h$ (h unit) such that $s_l > u \geq s_{l-1}$. Now, kill the highest degree term of $r_1(x)$ as follows:

(3.5) $$r_1(x) = p^{s_{l-1}}q_{l-1}(x).d_3x^{\deg(r(x)) - \deg(p^{s_{l-1}}q_{l-1}(x))} + r_2(x)$$

where either $r_2(x)=0$ or $\deg(r_2(x))<\deg(r_1(x))$. As $r_2(x)\in C$ and all polynomials in C have leading coefficient of the type $p^u h$ (h unit) such that $u\geq s_{l-1}$, leading coefficient of $r_2(x)$ is also of the type $p^u h$ (h unit) such that $u\geq s_{l-1}$. Let leading coefficient of $r_2(x)$ be equal to $p^{u_1}t_1 (t_1$ unit) where $u_1\geq s_{l-1}$. If $u_1\geq s_{l-1}$, then kill the highest degree term of $r_2(x)$ by using $p^{s_l}q_l(x)$ and if $s_l>u\geq s_{l-1}$, then kill the highest degree term of $r_2(x)$ by using $p^{s_{l-1}}q_{l-1}(x)$. The successive remainder is either zero or is of the same type. Continuing in the same way, kill the highest power of the remainder by using $p^{s_l}q_l(x)$ or $p^{s_{l-1}}q_{l-1}(x)$ to obtain the various successive remainders as multiples of $p^{s_l}q_l(x)$ or $p^{s_{l-1}}q_{l-1}(x)$. Moreover, at some stage degree of remainder becomes less than degree of $p^{s_l}q_l(x)$, which implies that remainder is zero. This further implies that $c(x)\in<p^{s_l}q_l(x),p^{s_{l-1}}q_{l-1}(x)>$.

If code C contains polynomials with leading coefficient of the type $p^u h$ (h unit) such that $u<s_{l-1}$, then choose minimal degree polynomial in C among all those polynomials in C with leading coefficient of the type $p^u h$ (h unit) such that $u<s_{l-1}$. Let it be $g_2(x)$ with leading coefficient $p^{s_{l-2}}h_2(h_2$ unit$)$. Then all polynomials in C of degree less than degree of $g_2(x)$ have leading coefficient of the type $p^u h$ (h unit) such that $u\geq s_{l-1}$,. We claim that content of $g_2(x)$ is $p^{s_{l-2}}$. Now, $p^{s_{l-1}-s_{l-2}}g_2(x)$ has leading coefficient $p^{s_{l-1}}h_2(h_2$ unit$)$. Therefore

$$p^{s_{l-1}-s_{l-2}}g_2(x)=p^{s_{l-1}}q_{l-1}(x).d_4.x^{\deg(g_2(x)-\deg(p^{s_{l-1}}q_{l-1}(x)))}+r_3(x) \tag{3.6}$$

where either $r_3(x)=0$ or deg $\deg(r_3(x))<\deg(p^{s_{l-1}-s_{l-2}}g_2(x))=\deg(g_2(x))$. As C is an ideal, $r_3(x)\in C$. If $r_3(x)\neq 0$, then leading coefficient of $r_3(x)$ must be of the type $p^u h$ (h unit) such that $u\geq s_{l-1}$. Let leading coefficient of $r_3(x)$ be equal to $p^{u_2}t_2(t_2$ unit$)$. If $u_2\geq s_l$ then kill the highest degree term of $r_3(x)$ by using $p^{s_l}q_l(x)$ and if $s_l>u_2\geq s_{l-1}$ then kill the highest degree term of $r_3(x)$ by using $p^{s_{l-1}}q_{l-1}(x)$. The successive remainder is either zero or is of the same type. Continuing in the same way, kill the highest power of the remainder by using $p^{s_l}q_l(x)$ or $p^{s_{l-1}}q_{l-1}(x)$ to obtain the various successive remainders as multiples of $p^{s_l}q_l(x)$ or $p^{s_{l-1}}q_{l-1}(x)$. Moreover, at some stage degree of remainder becomes less than degree of $p^{s_l}q_l(x)$, which implies that remainder is zero. This further implies that the content of $p^{s_{l-1}-s_{l-2}}g_2(x)$ is $p^{s_{l-1}}$. Therefore the content of $g_2(x)$ is $p^{s_{l-2}}$ and $g_2(x)=p^{s_{l-2}}q_{l-2}(x)$ (say), where $q_{l-2}(x)$ is a monic polynomial.

Now, if *C* does not contain any polynomial with leading coefficient of the type $p^u h$ (*h* unit) such that $u<s_{l-2}$. Then leading coefficient of $r_1(x)$ (referring back to equation (3.2)) is of the type $p^u h$ (*h* unit) such that $u \geq s_{l-2}$.

Let leading coefficient of $r_1(x)$ be equal to $p^{u_3}t_3$ (t_3 unit) where $u_3 \geq s_{l-2}$. If $u_3 \geq s_l$, then kill the highest degree term of $r_1(x)$ by using $p^{s_l}q_l(x)$. If $s_l > u_3 \geq s_{l-1}$, then kill the highest degree term of $r_1(x)$ by using $p^{s_{l-1}}q_{l-1}(x)$. If $s_{l-1} > u_3 \geq s_{l-2}$, then kill the highest degree term of $r_1(x)$ by using $p^{s_{l-2}}q_{l-2}(x)$. The successive remainder is either zero or is of the same type. *C*ontinuing in the same way, kill the highest power of the remainder by using $p^{s_l}q_l(x)$ or $p^{s_{l-1}}q_{l-1}(x)$ or $p^{s_{l-2}}q_{l-2}(x)$ to obtain the various successive remainders as multiples of $p^{s_l}q_l(x)$ or $p^{s_{l-1}}q_{l-1}(x)$ or $p^{s_{l-2}}q_{l-2}(x)$. Moreover, at some stage degree of remainder becomes less than degree of $p^{s_l}q_l(x)$, which implies that remainder is zero. This further implies that $c(x)\in\ < p^{s_l}q_l(x), p^{s_{l-1}}q_{l-1}(x).p^{s_{l-2}}q_{l-2}(x)>$.

If code *C* contains polynomials with leading coefficient of the type $p^u h$ (*h* unit) such that $u<s_{l-2}$, then again choose minimal degree polynomial in *C* among all those polynomials in *C* with leading coefficient of the type $p^u h$ (*h* unit) such that $u<s_{l-2}$. *C*ontinuing in this way, we shall get a sequence of generators $p^{s_{l-3}}q_{l-3}(x), p^{s_{l-4}}q_{l-4}(x),\ldots$ for *C*. This process must come to an end in finite no of steps, because the sequence s_i is a decreasing sequence of non negative numbers. Thus, in a finite number of steps, we obtain that

$C=< p^{s_1}q_1(x), p^{s_2}q_2(x),\ldots, p^{s_{l-1}}q_{l-1}(x), p^{s_l}q_l(x)>$

where $0\leq s_1\leq s_2\leq\ldots\leq s_{l-1}\leq s_l$ and $p^{s_i}q_i(x)$ is a minimal degree polynomial in *C* among all polynomials in *C* with leading coefficient of the type $p^u a$, where $(a,p)=1, u<s_{i+1}$, and $q_i(x)$ is monic for $1\leq i\leq 1$.

We summarize the results of the Lemmas 3.1 to 3.4 in Theorem 3.5. The Theorem follows from these Lemmas because

1) All cyclic codes of length p^k over Z_{p^m} are covered by one of these Lemmas and
2) The number of generators in all the cases is less than or equal to *m*.

Theorem 3.5: *m Cyclic codes of length $n = p^k$ over Z_{p^m} are generated as ideals of $R = Z_{p^m}[x]/ < x^n - 1 >$ by at most elements.*

References

1. T. Abualrub and R. Oehmke, Cyclic codes of length 2^e over Z_4, *Discrete Applied Mathematics*, **128** (2003) 3 - 9.
2. Arpana Garg and Sucheta Dutt, Cyclic codes of length 2^k over Z_8, *Scientific Research Open Journal of Applied Science,* Oct - 2012 world Congress on Engineering and Technology, **2** (2012) 104 - 107.
3. Arpana Garg and Sucheta Dutt, Cyclic codes of length 2^k over Z_{2^m}, *International Journal of Engineering Research and Development,* **1**(2012) 34 - 37.
4. A.R. Calderbank and N.J.A. Sloane, Modular and p-adic cyclic codes, *Designs Codes and Cryptography*, **6** (1995) 21 - 35.
5. T. Blackford, Cyclic codes over Z_4 of oddly even length, *Discrete Applied Mathematics,* **128** (2003) 27 - 46.
6. Steven T. Dougherty and San Ling, Cyclic Codes Over Z_4 of Even Length, *Designs, Codes and Cryptography,* **39** (2006) 127 – 153.
7. S.T. Dougherty and Y. H. Park, On Modular cyclic codes, *Finite Fields and Their Applications*, **13** (2007) 31 - 57.
8. Shi Minjia and Zhu Shixin, Cyclic Codes Over The Ring Z_{p^2} Of Length p^e, *Journal Of Electronics (China)*, **25** (2008) 636 - 640.
9. H.M. Kiah, K.H. Leung and S. Ling, Cyclic codes over $GR(p^2, m)$ of length p^k, *Finite Fields and Their Applications*, **14** (2008) 834 – 846.
10. I.S.Luthar and I.B.S.Passi, *Algebra volume 2 Rings*, Narosa Publishing House, first edition, 2002.
11. F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, Ninth impression, North-Holland, Amsterdam, 1977.