Kuwait J. Sci. **43 (1)** pp. 15-24, 2016

Cyclic codes of length p^n over $\mathbb{Z}_{p^3}$

Mehdi Alaeiyan[1,*], Mohammad Hyrizadeh[2]

[1]*Department of Mathematics, Iran University of Science and Technology, Narmak, Tehran 16844, Iran.*

[2]*Department of Mathematics, Iran University of Science and Technology, Narmak, Tehran 16844, Iran.*

[*]*Corresponding Author: Email: Alaeiyan@iust.ac.ir*

Abstract

The purpose of this paper is to find a description of the cyclic codes of length p^n over $\mathbb{Z}_{p^3}$, such that p is a prime. It is known that cyclic codes of length p^n over $\mathbb{Z}_{p^3}$ are ideals of the ring $S := \mathbb{Z}_{p^3}[X]/(X^{p^n} - 1)$. In this paper we prove that the S is a local ring with unique maximal ideal $(p, X - 1)$. We also prove that cyclic codes of length p^n over $\mathbb{Z}_{p^3}$ are generated as ideals by at most three elements.

Keywords: Cyclic codes over $\mathbb{Z}_{p^3}$; primary analysis; local ring.

1. Introduction

Let S be a commutative finite ring with identity. A linear code C over S of length n is defined as an $S-$ $submodule$ of S^n. An element of C is called acodeword. A cyclic code C over S of length n is a linear code such that any cyclic shift of a codeword is also a codeword, i.e whenever $(c_0, c_1, \dots, c_{n-1})$ is in C then so is $(c_{n-1}, c_0, \dots, c_{n-2})$. Cyclic codes of order n are ideals of the ring S^n.

Let $\mathbb{Z}_{p^3}$ denote the ring of integers modulo p^3. Cyclic codes over ring $\mathbb{Z}_{p^m}$ of length n such that $(n, p) = 1$ are studied by Calderbank & Sloane (1995) and Kanwar & Lopez-permouth (1997). Most of the work has been done on the generators of cyclic code of length n over $\mathbb{Z}_4$ such that $2|n$. In Abualrub & Oehmke (2003), gave the structure of cyclic codes over $\mathbb{Z}_4$ of length 2^k, Blackford (2003) classified all cyclic codes over $\mathbb{Z}_4$ of length $2n$ where n is odd, and Dougherty & ling (2006) gave the generator polynomial of cyclic codes over $\mathbb{Z}_4$ for arbitrary even length. The structure of cyclic codes over $\mathbb{Z}_{p^2}$ of length p^e is given by Minjia & Shixin (2008).

In this paper we prove that the ring $S = \mathbb{Z}_{p^3}\frac{[X]}{X^{p^n}-1}$ is a local ring with unique maximal ideal $(p, X - 1)$. Thereby implying that S is not a principal ideal ring (PIR) Garg & Dutt (2012), also the generators of a cyclic code need not divide $X^{p^n} - 1$ over $\mathbb{Z}_{p^3}$. More over, we prove that cyclic codes of length p^n over $\mathbb{Z}_{p^3}$ are generated as ideals by at most three elements.

2. Primary analysis

In this part we want to find the ideals of the ring $R_{\alpha(X)} = \mathbb{Z}_{p^3}[X]/(X^{p^n} + p\alpha(X))$, where $\alpha(X)\epsilon\mathbb{Z}_{p^3}[X]$ of degree less than p^n. Set $A(X) := X^{p^n} + p\alpha(X)$.We will show that there exist an $\alpha_0(X)\epsilon\mathbb{Z}_{p^3}[X]$ such that $S \cong R_{\alpha_0(X)}$. Since two rings $R_{\alpha_0(X)}$ and S are isomorphic, we can get the ideals of the ring S by obtaining the ideals of the ring $R_{\alpha_0(X)}$.

Definition 1. Let $\overline{f(X)}\epsilon R_{\alpha(X)}$, where $f(X)\epsilon\mathbb{Z}_{p^3}[X]$. The degree of $\overline{f(X)}$ over $R_{\alpha(X)}$ is equal to the degree of $r(X)$ over $\mathbb{Z}_{p^3}[X]$, such that

$$f(X) = A(X)\,q(X) + r(X),$$

where $\deg r(X) < \deg A(X)$.

Lemma 1. If $f(X)\,\epsilon\mathbb{Z}_{p^3}[X]$, then $deg kf(X) \leq deg f(X)$ over $\mathbb{Z}_{p^3}[X]$, such that $k\epsilon\mathbb{Z}_{p^3}$.

Lemma 2. If $\overline{f(X)}\epsilon R_{\alpha(X)}$, then $deg k\overline{f(X)} \leq deg\overline{f(X)}$ over $R_{\alpha(X)}$, where $k\epsilon\mathbb{Z}_{p^3}$.

Proof. Since $A(X)$ is a monic polynomial, the division algorithm by $A(X)$ is valid over$\mathbb{Z}_{p^3}[X]$, and if

$$f(X) = A(X)q(X) + r(X),$$

where $deg r(X) < deg A(X)$, and

$$kf(X) = A(X)q'(X) + r'(X),$$

where $deg r'(X) < deg A(X)$, are the division algorithms of $f(X)$ and $kf(X)$ by $A(X)$, respectively, then we will have

$$kf(X) = A(X)\,kq(X) + kr(X),$$

where $deg kr(X) \leq deg r(X) < deg A(X)$ (we conclude $\deg kr(X) \leq deg r(X)$ by Lemma*1*). Since $\deg kr(X) < deg A(X)$, we conclude that

$$kf(X) = A(X)\,kq(X) + kr(X),$$

where $deg kr(X) < deg A(X)$, is the division algorithm of $kf(X)$ *by* $A(X)$. Therefore, by using Definition 1 we have

$$deg\overline{kf(X)} \leq deg\overline{f(X)} \text{ over } R_{\alpha(X)}.$$

The following result is similar to Proposition 1 in Woo (2013).

Proposition 1. The ring $R_{\alpha(X)}$ is a local ring with the maximal ideal (p, X). Every nonzero ideal J of $R_{\alpha(X)}$ is primary with the radical $rad\,(J) = (p, X)$.

Proof. Let m be a maximal ideal. Any nilpotent element is contained in every prime ideal, Atiyah & Macdonald (1965). Since p is also nilpotent we see p and X

belong to m. On the other hand, (p, X) is a maximal ideal since $R_{\alpha(X)} \,/\, (p, X) \cong F_p$. Therefore, $m = (p, X)$.

Let J be an ideal of $R_{\alpha(X)}$. Then p and X, being nilpotent, belong to the radical $rad(J)$ of J. Therefore $rad(J) = (p, X)$. It is well known that if the radical of J is a maximal ideal, then J is primary, (Atiyah & Macdonald (1965)) Proposition 4.2).

Lemma 3. (Atiyah & Macdonald, 1965) Suppose R is a commutative ring with unity, and $u \epsilon R$ is a unit of R. Then $u + n$ is unit if n is nilpotent.

We will use Lemma 3 in this paper freely.

Proposition 2. $R_{\alpha(X)}$ is not PIR.

Let J refer to an arbitrary ideal of R and M denote the set of ideals of R. We can partition M into three parts:

(i) $J \subseteq (p^2)$

(ii) $J \nsubseteq (p^2)$ &$J \subseteq (p)$

(iii) $J \nsubseteq (p)$.

We analyze each of these three cases.

First case: $\boldsymbol{J \subseteq (p^2)}$.

Theorem 1. If J is a nonzero ideal of $R_{\alpha(X)}$ such that $J \subseteq (p^2)$, then $J = (p^2X^r)$ for some r.

Proof .Let $f(x)\, \epsilon J$, then all of coefficients of $f(X)$ belong to $p^2\mathbb{Z}_{p^3}[X]$.

We assume $f(X) = p^2 \sum_{i=0} f_i X^i$, such that f_i is equal to zero or is a unit in Z_{p^3}. Let $deg_L f(X) = t$ then $f(X) = p^2X^t.u$,such that u is aunit in $R_{\alpha(X)}$.

We conclude that $p^2X^t \epsilon J$. Suppose r is the smallest t that mentioned. It is clear that $J = (p^2X^r)$ because each nonzero polynomial in J takes the form of $p^2X^a.u$, where u is an unit in $R_{\alpha(X)}$ and $r \leq a$.

Definition 2. Let us call the element of the form p^2X^r an p^2Xr form.

Second case: $\mathbf{J \nsubseteq (p^2)}$ &$\mathbf{J \subseteq (p)}$

Theorem 2. If J is a nonzero ideal of $R_{\alpha(X)}$ such that $J \nsubseteq (p^2)$ &$J \subseteq (p)$, then J contains a nonzero element in form of $pX^k + p^2K(X)$, where $K(X) = \sum_{i=0}^{k-1} k_i X^i$. All of coefficients of $K(X)$ are zero or unit in $\mathbb{Z}_{p^3}$.

Proof. Suppose l be the smallest integer such that $X^l = 0$ in $R_{\alpha(X)}$. In addition, since $J \nsubseteq (p^2)$ &$J \subseteq (p)$, there is a polynomial $f(X) = p \sum_{i=0} f_i X^i$ such that one of its coefficients doesn't belong to $p^2\mathbb{Z}_{p^3}$. Let s denote the smallest nonzero i which $f_i \notin p\mathbb{Z}_{p^3}$. Therefore $X^{l-s-1} f(X)$ is the polynomial we desired.

Definition 3. We call the element of the form $pX^k + p^2K(X)$, where $K(X) = \sum_{i=0}^{k-1} k_i X^i$, and $k_i \notin pZ_{p^3}$ or $k_i = 0, 0 \le i \le k-1$ an $pXkp^2$ form.

Let us agree that the degree of the zero polynomial to be $-\infty$ and $X^k = 0$ if $k = -\infty$.

Theorem 3. If J is a nonzero ideal of $R_{\alpha(X)}$, where $J \nsubseteq (p^2)$ & $J \subseteq (p)$, then $J = (p^2X^r, g(X))$, where $g(X)$ and p^2X^r have the lowest degree between $pXkp^2$ forms and p^2Xr forms respectively.

Proof. As we proved in theorem 2 there is an $pXkp^2$ form in J. We call the $pXkp^2$ form with the lowest degree $g(X)$. Therefore $g(X) = pX^k + p^2K(X)$, where $K(X) = \sum_{i=0}^{k-1} k_i X^i$, and $k_i \notin p\mathbb{Z}_{p^3}$ or $k_i = 0, 0 \le i \le k-1$. It is clear that $(p^2X^r, g(X)) \subseteq J$. We show that $J \subseteq (p^2X^r, g(X))$.

Suppose that $T'(X)$ & $T(X) \in J, T(X) = p\sum_{i=0} t_i X^i$ and $T'(X) = \sum_{i=0} t_i X^i$. Then the division algorithm states that

$$T'(X) = g'(X)\, q(X) + r'(X),$$

where $deg\overline{r'(X)} < deg\overline{g'(X)}$ over $R_{\alpha(X)}$, and $g'(X) = X^k + pK(X)$.

We conclude that

$$pT'(X) = pg'(X)\, q(X) + pr'(X)$$

$$\Rightarrow T(X) = g(X)q(X) + pr'(X).$$

Lemma 2 Implies that $deg\, pr'(X) < deg\, r'(X)$. *Let* $r(X)$ denote $pr'(X)$, i.e. $r(X) = pr'(X)$. We will have

$$T(X) = g(X)\, q(X) + r(X), \text{where } deg r(X) < deg g(X)$$

We will show $r(X) \in (p^2)$.

In a proof by contradiction, we assume the opposite: $r(X) \notin (p^2)$. suppose $r(X) = p\sum_{i=0}^{t} r_i X^i, r'(X) = \sum_{i=0}^{t} r_i X^i$.

First, we assume s is the smallest i such that r_i is unit. Therefore $r(X) = pX^s u$ for some unit u.We see that $pX^s \in J$, an $pXkp^2$ form. It is a contradiction, because $s < deg g(X)$.

Second, we assume s is the index of the leading coefficient of $r(X)$. Then $r'(X) = r_s X^s + ph(X)$. Therefore $pX^s + p^2uh(X) \in J$, for some unit u. This is contradiction, because $s < \deg g(X)$ and $pX^s + p^2uh(X)$ is an $pXkp^2$ form.

Thirdly, we assume s is an arbitrary index of a coefficient of $r(X)$, except the smallest or the greatest one. Up to the end of the paper we consider a coefficient zero if its index become negative.

We define the sequence of $\psi_i(X)$ of polynomials as the following:

$$\psi_0(X) = X^{k-t}r(X) - r_t g(X) \Rightarrow \psi_0(X) = \sum_{i=0}^{k-1} p(r_{i+t-k} - pr_t k_i)X^{\mathrm{i}}.$$

$$\psi_1(X) = X\psi_0(X) - (r_{t-1} - pk_{k-1}r_t)g(X)$$

$$\Rightarrow \psi_1(X) = \sum_{i=0}^{t-2} (r_{i+t-k} - p(k_i r_t + r_{t-1}))X^{\mathrm{i}+1} + p^2 f_0.$$

$$\psi_2(X) = X\psi_1(X) - (r_{t-2} - p(k_{k-2}r_t + r_{t-1}))g(X)$$

$$\Rightarrow \psi_2(X) = \sum_{i=0}^{t-2} p(r_{i+t-k} - p(k_i r_t + r_{t-1} + r_{t-2}))X^{\mathrm{i}+2} + p^2 f_2(X),$$

where $\deg f_2(X) \leq 1$.

We define $\psi_z(X)$ inductively such as

$$\psi_z(X) = X\psi_{z-1}(X) - \delta_z g(X),$$

where $\delta_z = (r_{t-z} - p(k_{k-z}r_t + r_{t-1} + r_{t-2} + \cdots + r_{t-z-1}))$

$$\Rightarrow \psi_z(X) = \sum_{i=0}^{k-z-1} p\big(r_{i+t-k} - p(k_i r_t + r_{t-1} + r_{t-2} + \cdots + r_{t-z})\big)X^{\mathrm{i}+\mathrm{z}} + p^2 f_z(X),$$

where $\deg f_z(X) \leq z - 1$.

By taking $z = t - s - 1$ we have

$$\psi_{t-s-1}(X) = \sum_{i=0}^{k-t+s} p\big(r_{i+t-k} - p(k_i r_t + r_{t-1} + r_{t-2} + \cdots + r_{s+1})\big)X^{\mathrm{i}+\mathrm{t}-\mathrm{s}-1} + p^2 f_{t-s-1}(X)$$

The leading coefficient of $\psi_{t-s-1}(X)$ is equal to

$$B = p(r_s - p(k_{k-t+s}r_t + r_{t-1} + r_{t-2} + \cdots + r_{s+1}))$$

Clearly, there exists a unit u in $R_{\alpha(X)}$ such that $B = pu$. Other coefficients of $\psi_{t-s-1}(X)$ are also in form of p^2u $(uisunit)$. Considering $\deg\psi_{t-s-1}(X) \leq k - 1$, we see a contradiction. Since $r(X) \in (p^2)$. Therefore $r(X) = p^2X^t u$ for some unit u, where u is unit. It means $T(X) \in (p^2X^r, g(X))$, so $J = (p^2X^r, g(X))$.

Third case: $\boldsymbol{J \not\subseteq (p)}$.

Theorem 4. Let J be a nonzero ideal of $R_{\alpha(X)}$ such that $J \not\subseteq (p)$. Then J contains a nonzero element in form of $X^t + pt_1(X) + p^2t_2(X)$, where $deg t_1(X), deg t_2(X) < t$, and all of the coefficients of $t_1(X)$ and $t_2(X)$ are unit in $\mathbb{Z}_{p^3}$.

Proof. Since$J \nsubseteq (p)$, there exists polynomial $f(X)$ of J which one of its coefficients doesn't belong to pZ_{p^3}. We consider s to be the smallest positive integer such that f_s is unit. Therefore $X^{l-s-1}f(X)$ is the polynomial as desired, where l is the lowest positive integer such that $X^l = 0$ in $R_{\alpha(X)}$.

Definition 4. Let J be a nonzero ideal of $R_{\alpha(X)}$, where $J \nsubseteq (p)$. Then we define an element $X^t + pt_1(X) + p^2t_2(X)$ as an $Xtpp^2$ form, where $degt_1(X) < t, degt_2(X) < t$, and all of coefficients of $t_1(X)$ and $t_2(X)$ are unit in $\mathbb{Z}_{p^3}$.

Theorem 5. .Let J be a nonzero ideal of $R_{\alpha(X)}$ and $J \nsubseteq (p)$. Then $J = (p^2X^r, g(X), f(X))$, where $f(X)$ is an element of J with the lowest degree and an $Xtpp^2$ form, and $g(X)$ is an element of J with the lowest degree and $pXkp^2$ form, and an p^2X^r is an element of J with the lowest degree and an p^2Xr form.

Proof. It is obvious that $(p^2X^r, g(X), f(X)) \subseteq J$. We will show that $J \subseteq (p^2X^r, g(X), f(X))$.

Let $f(X) = X^t + pt_1(X) + p^2t_2(X)$ is an $Xtpp^2$ form, where $t_j(X) = \sum_{i=0}^{t-1} t_j^{(i)} X^i$, $j = 1,2$, and $t_j^{(i)}$'s are unit or zero, $j = 1,2$ & $0 \leq i \leq t-1$.

We consider $T(X) \in J$. As polynomial $f(X)$ is monic, we can use the division algorithm for $T(X)$ and $f(X)$ in $R_{\alpha(X)}$. We will have

$$T(X) = f(X)q(X) + r(X),$$

where $degr(X) < degf(X)$, and we can assume $r(X) = \sum_{i=0}^{w} r_i X^i$.

We will show that $r(X) \in (p)$.

In a proof by contradiction, we assume the opposite: $r(X) \notin (p)$ and $r(X) = \sum_{i=0}^{w} r_i X^i$. Suppose that s denotes the smallest i where r_i is unit. If r_s is the leading coefficient of $r(X)$, then $w = s$ and $r(X) = uX^w + pw_1(X) + p^2w_2(X)$ for some u and for some $w_1(X), w_2(X)$. Therfore $r(X)$ is an $Xtpp^2$ form. It is a contradiction.

If r_s is the coefficient of the lowest degree term, then $r(X) = uX^s$ for some u, where u is unit.Therefore $r(X)$ is an $Xtpp^2$ form. Again it is a contradiction.

We consider r_w as an arbitraty coefficients of $r(X)$, except two cases mentioned. We define the sequence of $\psi_i(X)$ of polynomials as the following:

$$\psi_0(X) = X^{t-w}r(X) - r_wf(X)$$

$$\Rightarrow \psi_0(X) = \sum_{i=0}^{t-1}\left(r_{i-t+w} - pr_wt_i^{(1)} - p^2r_wt_i^{(2)}\right)X^{\mathrm{i}}.$$

We remember that we consider a coefficient zero if its index become negative.

$$\psi_1(X) = X\psi_0(X) - \left(r_{w-1} - pr_w t_{t-1}^{(1)} - p^2 r_w t_{t-2}^{(2)}\right) f(X).$$

For the sake of notational convenience let us use $\alpha_i^{(j)}$ instead of some coefficients and $\beta_i(X), \gamma_i(X)$ instead of some polynomials. Moreover, the coefficients of $\beta_i(X)$ and $\gamma_i(X)$ are unit.

$$\psi_1(X) = \sum_{i=0}^{t-2} (r_{i-t+w} + p\alpha_i^{(1)}) X^{\mathrm{i}+1} + p\beta_1(X) + p^2\gamma_1(X),$$

where $\deg \beta_1(\mathrm{X}) = \deg \gamma_1(X) = 0$.

$$\psi_2(X) = X\psi_1(X) - \left(r_{w-2} + p\alpha_{t-2}^{(1)}\right) f(X)$$

$$\Rightarrow \psi_2(X) = \sum_{i=0}^{t-3} (r_{i-t+w} + p\alpha_i^{(2)}) X^{\mathrm{i}+2} + p\beta_2(X) + p^2\gamma_2(X),$$

where $\deg \beta_2(X) \leq 1, \deg \gamma_2(X) \leq 1$.

We define $\psi_h(X)$ inductivly such as

$$\psi_h(X) = X\psi_{h-1}(X) - \left(r_{w-h} + p\alpha_{t-h}^{(\mathrm{h}-1)}\right) f(X)$$

$$\Rightarrow \psi_h(X) = \sum_{i=0}^{t-h-1} (r_{i-t+w} + p\alpha_i^{(\mathrm{h})}) X^{\mathrm{i}+\mathrm{h}} + p\beta_{\mathrm{h}}(X) + p^2\gamma_{\mathrm{h}}(X),$$

where $\deg \beta_{\mathrm{h}}(X) \leq h-1, \deg \gamma_{\mathrm{h}}(X) \leq h-1$.

By taking $h = w - s - 1$, we have

$$\psi_{w-s-1}(X) = \sum_{i=0}^{t-w+s} (r_{i-t+w} + p\alpha_i^{(\mathrm{w-s-1})}) X^{\mathrm{i+w-s-1}} + p\beta_{\mathrm{w-s-1}}(X) + p^2\gamma_{\mathrm{w-s-1}}(X),$$

where $\deg \beta_{\mathrm{w-s-1}}(X)\, w - s - 2, \deg \gamma_{\mathrm{w-s-1}}(X) \leq w - s - 2$.

The leading coefficient of $\psi_{w-s-1}(X)$ is equal to B= $r_s + p\alpha_{t-w+s}^{(\mathrm{w-s-1})}$. Since r_s is unit, B is unit too. It is a contradiction because $\psi_{w-s-1}(X)$ is an $Xtpp^2$ form and its degree is less than $k-1$. Therefore $r(X) \in (p)$. Consequently $(r(X)) \subseteq (p^2X^r, g(X))$. Hence we see that

$$J = \left(p^2X^r, g(X), f(X)\right).$$

3. The main results

In this part we contact between $R_{\alpha(X)}$ and S by using an isomorphism to find the ideals of S.

Lemma 4. Let $n \geq 2$. Then

$$\binom{p^n}{r} \equiv \begin{cases} a_r p, r = ip^n, i = 1,2,\dots,p^2-1, \exists a_r \notin p^2\mathbb{Z}_{p^3}, a_r \in \mathbb{Z}_{p^3}, & \\ & (mod p^3) \\ 0 & o.w. \end{cases}$$

Proof. Consider the mapping $t_p\colon \mathbb{N} \longrightarrow \mathbb{N}$ ($p$prime), such that $t_p(r) = p^m$, where m is the greatest positive integer such that $p^m | r$. Clearly $t_p(r) = t_p(p^n - r)$, $t_p(ab) = t_p(a)t_p(b)$ and $t_p(a/b) = t_p(a)/t_p(b)$. So if $r = ip^{n-2}, i = 1,2,\dots,p^2-1$, then $p|\binom{p^n}{r}$. Therefore $\binom{p^n}{r} \not\equiv 0(mod p^3)$, thus for $r = ip^{n-2}, i = 1,2,\dots,p^2-1$, there exists an element a_r such that $\binom{p^n}{r} \equiv pa_r(mod p^3)$. Otherwise, $\binom{p^n}{r} \equiv 0(mod p^3)$.

Lemma 5. Let $(X^{p^n} - 1) \in \mathbb{Z}_{p^3}[X]$, where $n \geq 2$. Then

$$X^{p^n} - 1 = (X-1)^{p^n} + p\sum_{r\in\Gamma} a_r(X-1)^r,$$

where $\Gamma = \{ip^{n-2} | i = 1,2,\dots,p^2-1\}$.

Proof. We know $X^{p^n} - 1 = ((X-1)+1)^{p^n} - 1$.

By taking $T = X - 1$, we have $(T+1)^{p^n} - 1 = \sum_{i=0}^{p^n}\binom{p^n}{i}T^i - 1$. By Lemma 4, $(T+1)^{p^n} - 1 = T^{p^n} + p\sum_{r\in\Gamma} a_r T^r$. Therefore

$$X^{p^n} - 1 = (X-1)^{p^n} + p\sum_{r\in\Gamma} a_r(X-1)^r,$$

where we know $\sum_{r\in\Gamma} a_r(X-1)^r = \alpha_0(X-1)$ in advance.

By Lemma 5 we have the following result.

Proposition 4. There is an isomorphism $\varphi\colon R_{\alpha_0(X)} \to S$ of rings which maps $f(X)$ to $f(X-1)$.

We have the following main result.

Proposition 5. $(p, X-1)$ is the unique maximal of S. Moreover, the only ideals of S are

$I_0 = (0)$,

$I_1 = (p^2(X-1)^r)$, for some r,

$I_2 = \left(p^2(X-1)^r, g(X-1)\right)$, for some $g(X)$ where is an $pXkp^2$ form, and $deg\, g(X) \geq r$, for some r,

$I_3 = \left(p^2(X-1)^r, g(X-1), f(X-1)\right)$, for some $g(X)$, $f(X)$ and r which are the form $pXkp^2$, $Xtpp^2$ respectively, and $deg\, f(X) \geq deg\, g(X) \geq r$.

Proof. We know the mapping $\varphi: R_{\alpha_0(X)} \longrightarrow S$ is an isomorphism $R_{\alpha_0(X)}$ onto S. Therefore, the mapping $\varphi^{-1}: S \longrightarrow R_{\alpha_0(X)}$ given by $\varphi^{-1}(X) = X + 1$ is an isomorphism S onto $R_{\alpha_0(X)}$. If I is an ideal of S, then $\varphi^{-1}(I) = J$ will be an ideal of $R_{\alpha_0(X)}$, and if J is an ideal of $R_{\alpha_0(X)}$, then $\varphi(J) = I$ will be an ideal of S. Therefore maximal ideal of S is unique, and is equal to $(p, X - 1)$. In addition, I_0, I_1, I_2, and I_3 mentioned above are the only ideals of S.All cyclic codes of length p^n over $\mathbb{Z}_{p^3}$ are defined by I_0, I_1, I_2, and I_3.

References

Atiyah, M.F. & Macdonald, I.G. (1969) Introduction to Commutative Algebra. AddisonWesley.

Abualrub, T. & Oehmke, R. (2003) Cyclic codes of length 2^e over $\mathbb{Z}_4$. Discrete Applied Mathematics, **128:**3-9.

Blackford, T. (2003) Cyclic codes over $\mathbb{Z}_4$ of oddly even length. Discrete Applied Mathematics, **128:**27-46.

Calderbank, N.J.A. & Sloane, A.R. (1995) Modular and p-adic cyclic codes. Designs, Codes and Cryptography, **6:**21-35.

Dougherty, S.T. & Ling, S. (2006) Cyclic codes over $\mathbb{Z}_4$ of even length. Designs, Codes and Cryptography, **39:**127-153.

Garg, A. & Dutt, S. (2012) Cyclic codes of length 2^k over $\mathbb{Z}_8$. Open Journal of Applied Sciences, **2**(4B)**:**104-107.

Kanwar, P. & Lopez-permouth, S.R. (1997) Cyclic codes over the integers modulo p^m. Finite Fields and Their Applications, **3**(4)**:**334-352.

Minjia, S. & Shixin, Z. (2008) Cyclic codes over the ring $\mathbb{Z}_{p^2}$ of length p^e. Journal of Electronics (China), **25**(5)**:**636-640.

Woo, S.S. (2013) Cyclic codes of length 2^n over $\mathbb{Z}_4$. Communications of the Korean Mathematical Society, **28**(1)**:**39-54.

Submitted **:** 17/03/2014

Revised **:** 26/08/2014

Accepted **:** 05/01/2015

شيفرات دورية طولها p^n على $\mathbb{Z}_{p^3}$

مهدي اليان[1]،*، [2]محمد هيرزاد

[1]قسم الرياضيات – جامعة إيران للعلوم والتكنولوجيا، نارمك – طهران 16844– إيران.

[2]قسم الرياضيات – جامعة إيران للعلوم والتكنولوجيا، نارمك – طهران 16844– إيران.

*البريد الإلكتروني للمؤلف: Alaeiyan@iust.ac.i

خلاصة

الغرض من هذا البحث هو إيجاد وصف للشيفرات الدورية التي طولها p^n حيث p هو عدد أولي. ومن المعروف أن الشيفرات الدورية ذات الطول p^n على Z_{P3} هي مثاليات للحلقات $S = Z_{P3}(X) / (X^{PN}-1)$. نثبت في هذا البحث أن S هي حلقة محلية لها مثالية أعظمية وحيدة (P,X -1). كما نثبت أيضاً بأن الشيفرات الدورية التي طولها p^n على Z_{P3} يمكن توليدها كمثاليات بواسطة ثلاثة عناصر على الاكثر.