Bull. Korean Math. Soc. **43** (2006), No. 3, pp. 487–497

ALGEBRAS WITH A NILPOTENT GENERATOR OVER $\mathbb{Z}_{p^2}$

SUNG SIK WOO

ABSTRACT. The purpose of this paper is to describe the structure of the rings $\mathbb{Z}_{p^2}[X]/(\alpha(X))$ with $\alpha(X)$ a monic polynomial and $\bar{X}^k = 0$ for some nonnegative integer k. Especially we will see that any ideal of such rings can be generated by at most two elements of the special form and we will find the 'minimal' set of generators of the ideals. We indicate how to identify the isomorphism types of the ideals as $\mathbb{Z}_{p^2}$-modules by finding the isomorphism types of the ideals of some particular ring. Also we will find the annihilators of the ideals by finding the most 'economical' way of annihilating the generators of the ideal.

1. Introduction

The motivation of this paper is to look at the cyclic codes of length 2^n over $\mathbb{Z}_4$. A cyclic code of length 2^n over $\mathbb{Z}_4$ can be identified with an ideal of $\mathbb{Z}_4[X]/(X^{2^n} - 1)$. Now $\mathbb{Z}_4[X]/(X^{2^n} - 1)$ turns out to be isomorphic to the ring $\mathbb{Z}_4[X]/(X^{2^n} - 2X^{2^{n-1}})$ which is one of the type in the title [3]. Descriptions of the ideals of $\mathbb{Z}_{p^n}[X]/(X^m - 1)$ when p is relatively prime to m is given in [2]. But nothing seems to be known for the case when p divides m.

In [3], it was shown that the generators of the ideals and their annihilators is described for the ring $\mathbb{Z}_4[X]/(X^{2^n} - 2X^{2^{n-1}})$. In this paper, we generalize the results to the case of a prime p. Namely we will describe the minimal generators for the ideals of $S = \mathbb{Z}_{p^2}[X]/(\alpha(X))$ with a monic polynomial $\alpha(X)$ in which $\bar{X}^n = 0$ for some nonnegative integer n.

To find the description of the ideals of such algebra S, we endow an order structure on S. As for the case of a polynomial ring over a field,

Received April 18, 2005.
2000 Mathematics Subject Classification: 13C12.
Key words and phrases: cyclic code over $\mathbb{Z}_4$.

to find the generator of an ideal, we find the minimal elements of some special forms with respect to the order structure of S. We show the ideal is generated by those minimal elements. For this we prove something similar to Euclidean algorithm over $\mathbb{Z}_{p^2}$ which is a key to find the ideals of S (§2, §3).

We identify the isomorphism types of the ideals of some specially chosen ring in §4 which indicate the way how to find the isomorphism types for other cases. To find the annihilators of an ideal we find polynomials which annihilates the generators of the ideals of S in most economical way (§5).

Most of the results of §2, §3 are straight forward generalizations of the results in [3], where the prime p is supposed to be even.

2. Algebras over $\mathbb{Z}_{p^2}$ generated by a nilpotent element

We consider a ring of the form $S = \mathbb{Z}_{p^2}[X]/(\alpha(X))$, where $\alpha(X)$ is a monic polynomial of degree m such that $X^n \in (\alpha(X))$ for some n, i.e., $S = \mathbb{Z}_{p^2}[x]$ with $x^n = 0$ for some n and satisfies a monic polynomial. If l is the smallest integer then we will say that the nilpotency of x is l. We will call such ring as *finite cyclic $\mathbb{Z}_{p^2}$-algebra with a nilpotent generator of nilpotency l*. Typical examples we have in mind are $S = \mathbb{Z}_{p^2}[X]/(X^m - pX^n)$ with nonnegative integers $m \geq n$.

Throughout this paper a ring S will mean a cyclic $\mathbb{Z}_{p^2}$- algebra of the form $S = \mathbb{Z}_{p^2}[X]/(\alpha(X))$, where $\alpha(X)$ is a monic polynomial of degree m such that $X^n \in (\alpha(X))$ for some n. Whenever we talk about a polynomial $f(X)$ in $S = \mathbb{Z}_{p^2}[X]/(\alpha(X))$ we shall choose a representative with degree less than m. In this section we fix the degree of $\alpha(X)$, say $\deg(\alpha(X)) = m$.

Our first observation is that the ring we are interested in is a local ring and every ideal of S is primary. See [1] for the definition of primary ideals and the radical of an ideal.

PROPOSITION 1. *The ring $S = \mathbb{Z}_{p^2}[X]/(\alpha(X))$ is a local ring with the maximal ideal (p, X). Every ideal J of S is primary with the radical* $\mathrm{rad}(J) = (p, X)$.

Proof. Let $\mathfrak{m}$ be a maximal ideal. Any nilpotent element is contained in every prime ideal [1]. Since p is also nilpotent, we see p and X belong to $\mathfrak{m}$. On the other hand, (p, X) is a maximal ideal since $S/(p, X) \cong \mathbb{F}_p$, the field with p elements. Therefore $\mathfrak{m} = (p, X)$.

Let J be an ideal of S. Then p and X, being nilpotent, belong to the radical $\mathrm{rad}(J)$ of J. Therefore $\mathrm{rad}(J) = (p, X)$. It is well known that if the radical of J is a maximal ideal, then J is primary [1, Proposition 4.2]. □

We will use the following well known fact freely.

LEMMA 1. *Let R be a commutative ring with the identity. If u be a unit and $\nu \in R$ is nilpotent, then $u + \nu$ is a unit.*

We define an ordering on the set of representatives $\{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{p^2 - 1}\}$ of $\mathbb{Z}_{p^2}$ in the usual way

$$0 < 1 < 2 < \cdots < p^2 - 1,$$

where we omit the bars as we will do from now on. On the set $C = \{(a_0, a_1, \dots, a_{m-1}) | a_i \in \mathbb{Z}_{p^2}\}$, we define an ordering by endowing the lexicographic order.

Let $f(X) = \sum_{i=0}^{m-1} a_i X^i, g(X) = \sum_{i=0}^{m-1} b_i X^i$ be polynomials in $\mathbb{Z}_{p^2}[X]$ with $\deg(f), \deg(g) < m$. Then we define

$$f \leq g \text{ if and only if } (a_0, a_1, \dots, a_{m-1}) \leq (b_0, b_1, \dots, b_{m-1}).$$

If an ideal of $S = \mathbb{Z}_{p^2}[X]/(\alpha(X))$ is contained in a principal ideal (p) generated by p, then J is also a principal ideal as we see in the following proposition.

PROPOSITION 2. *Let J be an ideal of S contained in (p). Then J is of the form (pX^r) for some r.*

Proof. Let $f(X) = \sum_{i=0}^{m-1} a_i X^i \in J$. Since $J \subseteq (p)$, all of the coefficients of f are in $p\mathbb{Z}_{p^2}$. By noting that X is nilpotent, we see that $f(X)$ is of the form $pX^j \cdot (\text{unit})$. Now let pX^r be the lowest degree among such expressions of the elements of J. Now it is obvious that $J = (pX^r)$. □

DEFINITION. Let us call the element of the form pX^r a pxr form.

3. Euclidean algorithm modulo p^2 and the ideals of nilpotent algebra

If the ideal J is not contained in the ideal (p) generated by $p \in S$, we will then prove existence of elements of some special form.

PROPOSITION 3. *Let S be as before. Let J be a nonzero ideal of S which is not contained in the ideal (p). Then there are nonzero elements of the form $X^k + ph(X)$, where $h \in S$ of degree $< k$.*

Proof. If $f(X) = \sum_{i<m} a_i X^i$ is a nonzero polynomial in J with a unit a_0, then f is a unit since $X \in S$ is nilpotent, i.e., J is the unit ideal.

Hence we may assume the constant term of every $f \in J$ is 0 or p. If the coefficient of the lowest degree term of every nonzero $f \in J$ is a unit, then they are of the form $X^i \times$ (unit). Therefore X^i is an element of J which is of the required form. Now suppose there is $f = \sum_{i<m} a_i X^i \in J$ with the coefficient of the lowest degree is p. Let a_i be the unit coefficient of the lowest degree, i.e., $a_{i-1}, a_{i-2}, \ldots$ are in $p\mathbb{Z}_{p^2}$. Let l be the smallest integer such that $X^l = 0$. Then $X^{l-i-1} f(X)$ is a desired form. □

DEFINITION. The polynomials of the form

$$g(X) = X^k + pa_h X^h + pa_{h-1} X^{h-1} + \cdots + pa_0$$

with $a_h, a_{h-1}, \ldots, a_0 \in \mathbb{Z}_{p^2}$ will be called an xkp form. And we will often denote the polynomial $pa_h X^h + pa_{h-1} X^{h-1} + \cdots + pa_0$ by $p \cdot h(X)$.

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

THEOREM 1(EUCLIDEAN ALGORITHM MODULO p^2). *Let J be an ideal of S which is not contained in the ideal (p) generated by $p \in S$. Let $g(X) = X^k + ph(X) \in J$ be an xkp form which is minimal with respect to the ordering defined above. Let $f(X) = \sum_{i<m} a_i X^i \in J$. Then we can write uniquely*

$$f(X) = g(X)q(X) + r(X)$$

with $q(X), r(X) \in S$, $\deg(r) < k$ and $r(X) \in p\mathbb{Z}_{p^2}[X]$.

Proof. Since g is monic, we can write $f = gq + r$ for some $r \in S$ with $\deg(r) < \deg(g) = k$ uniquely by Euclidean algorithm over a commutative ring. We need to prove that the coefficients of $r(X)$ are in $p\mathbb{Z}_{p^2}$.

Assume that this is not true. If the coefficient of the lowest degree term is a unit, then $r(X)$ is of the form $X^i \cdot$(unit) with $i < k$ since X is nilpotent. Hence $X^i \in J$ with $i < k$. But this contradicts to the fact

that $g(X) = X^k + ph(X)$ is a minimal element. Hence we may assume that the coefficient of the lowest degree term is p.

Let $r(X) = a_jX^j + a_{j-1}X^{j-1} + \cdots + pX^l$ with $j < k$ and $a_j \neq 0$. Let a_sX^s be the lowest degree term with a unit a_s, that is, $a_{s-1}, a_{s-2}, \ldots \in p\mathbb{Z}_{p^2}$. If $s = j$, then $r(X)$ is a xkp form which is smaller than $g(X)$ which contradicts to the minimality of $g(X)$. Hence $j > s$.

Then we see that $X^{k-j}r(X) - a_jg(X) \in J$ is a polynomial of degree $< k$ in which the divisibility of the coefficients of $X^{s+k-j-1}, X^{s+k-j-2}, \ldots$ by p remain the same as those of $a_{s-1}, a_{s-2}, \ldots$ since the coefficient of terms of degree $< k$ in $a_jg(X)$ is in $p\mathbb{Z}_{p^2}$.

Let $ph(X) = \sum_i ph_iX^i$. If the coefficients of $X^{k-1}, X^{k-2}, \ldots, X^{s+k-j+1}$ in $X^{k-j}r(X) - a_jg(X)$ happen to vanish namely $X^{k-j}r(X) - a_jg(X) = (a_s + pa_jh_s)X^{s+k-j} + (a_{s-1} + pa_jh_{s-1})X^{s+k-j-1} + \cdots + (p + pa_jh_l)X^l$. Then $a_s + pa_jh_s$ is a unit and $a_{s-i} + pa_jh_{s-i} \in p\mathbb{Z}_{p^2}$ for $i \geq 1$. But this gives us an element in J which is smaller than $g(X)$ after multiplying some unit if necessary. This is a contradiction.

If this is not the case, then we can repeat the same process until all the coefficients of the terms but the last $(s - l)$ terms vanish without changing the divisibility by p of the coefficients of the last $(s - l)$ terms to get an element of J with degree $< \deg(X^{k-j}r(X) - a_jg(X))$. Then, the resulting element is obviously an xkp form which is smaller than $g(X)$ belonging to J. □

Let J be a nonzero ideal of S which is not contained in (p). Choose an element of the form $g(X) = X^k + ph(X)$ with $h(X) \in S$ with $\deg(h) < k$ which is the smallest one with respect to the ordering defined above. We will show that J is generated by $g(X)$ and pX^r for some r.

THEOREM 2. *Let J be an ideal of S which is not contained in (p). Let $g(X) = X^k + ph(X) \in J$ be the smallest xkp form in J and pX^r be the smallest pxr form in J. Then $J = (g(X), pX^r)$, where $-\infty \leq r < l$.*

Proof. Obviously $J \supseteq (g(X), pX^r)$. Now let $f \in J$ and write $f(X) = g(X)q(X) + pr(X)$. Then $pr(X)$ is of the form $pr(X) = pX^t(v + \sum_{i\geq 1} a_iX^i)$ for some unit $v \in \mathbb{Z}_{p^2}$. Since X is nilpotent, $pr(X) = pX^t \cdot u$ for some unit u. Hence we can write $f(X) = g(X)q(X) + pX^t \cdot u$ for some unit u. Since $f(X)$ and $g(X)$ belong to J, we see that $pX^t \in J$. As pX^r is the smallest pxr form in J, we have $t \geq r$. Therefore $f(X) = g(X)q(X) + uX^{t-r}(pX^r)$. Thus $J \subseteq (g(X), pX^r)$. □

COROLLARY. *The proper ideals of S are of the form (pX^i) for some i; or are of the form $(g(X), pX^r)$ for some xkp form $g(X)$ and some r with $-\infty \leq r < \deg(g)$.*

Now we count the number of possible distinct ideals of S.

PROPOSITION 4. *The principal ideals of S are of the following forms:*
(i) *(pX^r) for some pxr form pX^r with $(0 \leq r < m)$;*
(ii) *$(g(X))$ for some xkp form $g(X)$.*
The number of ideals of the first type is m; the number of ideals of the second type does not exceed $\sum_{k=1}^{m-1} p^k = \frac{p^m - p}{p-1}$.

Proof. May be the last statement worth checking. For each degree k of $g(X)$ we can choose the coefficients of $X^{k-1}, \ldots, X, 1$ in the set of multiples $p\mathbb{Z}_{p^2}$ of p, namely $\{p, 2p, \ldots, p(p-1), p^2 = 0\}$ and thus the number of all possible xkp forms are p^k for each fixed k of degree $g(X)$. Hence the number of ideals generated by an xkp form does not exceed

$$p + p^2 + \cdots + p^{m-1} = \frac{p^m - p}{p-1}.$$

□

PROPOSITION 5. *The set of nonprincipal ideals of S are of the form $(g(X), pX^r)$, where $g(X) = X^k + pa_hX^h + \cdots + pa_0$ is an xkp form with $k < r < h$. Then the number of nonprincipal ideals does not exceed*

$$\sum_{0 \leq h < k < m} (k - h - 1)p^h(p-1).$$

Proof. For each k, choose the highest degree of nonzero term h. Once we choose k and h, then there are $k - h - 1$ possible choices of pxr form $2X^r$ $(k < r < h)$. For each choice of k and h, we can choose the coefficient of X^h from $\{p, p+1, \ldots, p(p-1)\}$ since it has to be nonzero and then we can choose the coefficients of $X^{h-1}, \ldots, X, 1$ from $p\mathbb{Z}_{p^2}$. Hence there are $p^h(p-1)(k-h-1)$ of them. Therefore the number of all possible nonprincipal ideals is $\sum_{0 \leq h < k < m} (k - h - 1)p^h(p-1)$. □

REMARK. Not all distinct expressions of $(g(X), pX^r)$ give distinct ideals. For example, if we take $S = \mathbb{Z}_4[X]/(X^4 - 2X^2)$, then one can easily check that $(X^3 + 2X^2) = (X^3, 2X^2)$. The smallest element of the ideal $(g(X), 2X^r)$.

4. Isomorphism types of ideals

Since we are considering a finite ring $S = \mathbb{Z}_{p^2}[X]/(\alpha(X))$, it is isomorphic as abelian groups to m-copies of $\mathbb{Z}_{p^2}$, where $m = \deg \alpha(X)$. Therefore an ideal of S is isomorphic to sum of copies of $\mathbb{Z}_{p^2}$'s and $\mathbb{Z}_p$'s. In this section, we want to find the number of copies of $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p$ of an ideal of S. Thereby we can identify the isomorphism types of the ideals as $\mathbb{Z}_{p^2}$-modules.

It would be too complicate to consider the general monic polynomial $\alpha(X)$. Therefore, in this section we specialize our ring and we let $\alpha(X) = X^m - pX^n$ with nonnegative integers $n < m$ thereby indicating the method for general $\alpha(X)$. For $f(X) \in S$ with $\deg(f(X)) < m$, let us write $\deg_L(f(X))$ for the degree of the lowest nonzero degree term.

Let $g(X) = X^k + pa_hX^h + pa_{h-1}X^{h-1} + \cdots + pa_0$ with $a_h, a_{h-1}, \ldots, a_0 \in \mathbb{Z}_{p^2}$. For each basis element $\{1, X, \ldots, X^{m-1}\}$ (in this order) of S express $X^i g(X)$ as a linear combination of the basis $\{X^{m-1}, \ldots, X, 1\}$ (in this order) of S. Then its matrix expression is of the form

$$G = \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

where A is a $(m-k) \times (m-k)$ matrix of the form

$$A = \begin{pmatrix} 0 & \cdots & \cdots & 1 \\ 0 & \cdots & 1 & * \\ 0 & \cdot & * & * \\ 1 & * & * & * \end{pmatrix}$$

with 1's on the opposite diagonal and $*$'s below the opposite diagonals which consist of the elements of $p\mathbb{Z}_{p^2}$. The matrix B is of size $(m-k) \times k$ over $p\mathbb{Z}_{p^2}$ and C is a $(m-k) \times (m-k)$ matrix over $p\mathbb{Z}_{p^2}$.

And D is a $k \times k$ matrix of the form

$$D = \begin{pmatrix} * & * & \cdots & pa & 0 & \cdots & 0 \\ & \cdots & pa & 0 & \ldots\ldots & & 0 \\ * & \cdot & 0 & \ldots\ldots & & & 0 \\ pa & 0 & 0 & \ldots\ldots & & & 0 \\ 0 & 0 & 0 & \ldots\ldots & & & 0 \\ & & \ldots\ldots & & & & \\ 0 & 0 & \ldots\ldots & & & & 0 \end{pmatrix},$$

where $*$'s are in $p\mathbb{Z}_{p^2}$ with a unit a. Hence the upper left corner of D is a square matrix whose opposite diagonals are multiples of p.

The moral is that adding a constant multiple of a row to another one does not change the submodule generated by the rows.

We consider two cases. The first case is when $D = 0$. This is equivalent to $\deg_L(X^{m-k}g(X)) \geq k$. The second case we consider is when $D \neq 0$. This is equivalent to that $\deg_L(X^{m-k}g(X)) < k$.

THEOREM 3. *Let* $S = \mathbb{Z}_{p^2}[X]/(X^m - pX^n)$ *and let*

$$g(X) = X^k + pa_hX^h + pa_{h-1}X^{h-1} + \cdots + pa_0$$

with $a_h, a_{h-1}, \ldots, a_0 \in \mathbb{Z}_{p^2}$. *Then the ideal* I *generated by* $g(X)$ *is isomorphic, as* $\mathbb{Z}_{p^2}$*-modules, to the following one:*

(i) *if* $\deg_L(X^{m-k}g(X)) \geq k$, *then* I *is* $\mathbb{Z}_{p^2}$*-free of rank* $(m-k)$;
(ii) *if* $l := \deg_L(X^{m-k}g(X)) < k$, *then* I *is isomorphic to the sum of* $(m-k)$ *copies of* $\mathbb{Z}_{p^2}$ *and* $(k-l)$ *copies of* $\mathbb{Z}_p$.

Proof. First, consider the case when $D = 0$, i.e., $\deg X^{m-k}g(X) \geq k$. And in this case, the number of 1's is $m-k$. And, using these 1's, we can get rid of p's in C. Hence the ideal generated by $g(X)$ is free over $\mathbb{Z}_{p^2}$ of rank $m-k$.

Now let $l = \deg_L X^{m-k}g(X) < k$. As before, we can make all entries below the 1's on the opposite diagonal of A. Also we can get rid of multiples p's in C without changing D since the entries in B and C are the multiples of p. We can get rid of all entries above the pa on the opposite diagonal of a square matrix on the upper left corner of D. It is clear that the ideal generated by the rows is isomorphic to the sum of $(m-k)$ copies of $\mathbb{Z}_{p^2}$ which correspond to the 1's in A and $l-k$ copies of $\mathbb{Z}_p$ which correspond to pa's in D. □

COROLLARY. *Let* $S = \mathbb{Z}_{p^2}[X]/(X^m - pX^n)$. *Then the ideal* $(g(X))$ *is* $\mathbb{Z}_{p^2}$*-free if and only if* $\deg_L(X^{m-k}g(X)) \geq k$.

Proof. We know that the ideal $(g(X))$ is $\mathbb{Z}_{p^2}$-free if there is no p-part when $\deg_L(X^{m-k}g(X)) \geq k$. □

For simplicity, we will use the notation

$$\lceil a, b \rceil = \max\{a, b\} \quad \text{and} \quad \lfloor a, b \rfloor = \min\{a, b\}$$

PROPOSITION 6. *Let $S = \mathbb{Z}_{p^2}[X]/(X^m - pX^n)$. Then the ideal (pX^r) generated by pX^r is isomorphic to $(m-r)$ copies of $\mathbb{Z}_p$.*

Proof. It is easy to show and we omit its proof. □

THEOREM 4. *Let $S = \mathbb{Z}_{p^2}[X]/(X^m - pX^n)$ and let*

$$g(X) = X^k + pa_hX^h + pa_{h-1}X^{h-1} + \cdots + pa_0$$

with $a_h, a_{h-1}, \ldots, a_0 \in \mathbb{Z}_{p^2}$. Then the ideal I generated by $g(X)$ and pX^r is isomorphic, as $\mathbb{Z}_{p^2}$-modules, to the following one:

(i) *if $\deg_L(X^{m-k}g(X)) \geq k$, then I is isomorphic to $(m-k)$ copies of $\mathbb{Z}_{p^2}$ and $\lceil k-r, 0\rceil$ copies of $\mathbb{Z}_p$; or*

(ii) *if $l := \deg_L(X^{m-k}g(X)) < k$, then I is isomorphic to $(m-k)$ copies of $\mathbb{Z}_{p^2}$ and $k - \lfloor r, l\rfloor$ copies of $\mathbb{Z}_p$, where $\lceil a, b\rceil = \max\{a, b\}$ and $\lfloor a, b\rfloor = \min\{a, b\}$.*

Proof. The generator matrix for $(g(X), pX^r)$ is

$$G = \begin{pmatrix} A & B \\ C & D \\ & F \end{pmatrix},$$

where F is a matrix of the same form as D of size $(m-r) \times m$. Now it is easy to check that the ideal is isomorphic to the abelian groups in the theorem and we omit the detail. □

5. Annihilating polynomials of the ideals

Recall [1] the annihilator $\mathrm{Ann}(I)$ of an ideal I of a ring R is given by

$$\mathrm{Ann}(I) = \{r \in R \mid rx = 0 \text{ for all } x \in I\}$$

We will find polynomials which annihilates the polynomial $g(X)$ in the 'most economical' way which will be the generators for the annihilator of the ideal. As in §4, we let $S = \mathbb{Z}_{p^2}[X]/(X^m - pX^n)$, throughout this section.

PROPOSITION 7. *Let $S = \mathbb{Z}_{p^2}[X]/(X^m - pX^n)$. Then the annihilator of the ideal (pX^r) is given by (X^{m-r}, p).*

Proof. By Theorem 2, we need to find the smallest xkp form and pxr form which annihilate pX^r. Now we have $X^{m-r}(pX^r) = pX^m = 0$ and $p(pX^r) = 0$. It is clear that X^{m-r} is a minimal xkp form which annihilates $g(X)$ and p is the smallest pxr form which annihilates pX^r.□

THEOREM 5. *Let* $S = \mathbb{Z}_{p^2}[X]/(X^m - pX^n)$ *and let*

$$g(X) = X^k + pa_hX^h + pa_{h-1}X^{h-1} + \cdots + pa_0$$

with $a_h, a_{h-1}, \ldots, a_0 \in \mathbb{Z}_{p^2}$. *Then the annihilator of the ideal* $(g(X))$ *is given by the following:*

(i) *if* $\deg_L(X^{m-k}g(X)) \geq k$, *then* $Ann(g(X))$ *is generated by*

$$g^{\perp}(X) = X^{m-k} - \sum_{i \leq h} pa_iX^{i+m-2k} + pX^{n-k};$$

(ii) *if* $l := \deg_L(X^{m-k}g(X)) < k$ *and let* $X^{m-k}g(X) = pb_tX^t + \cdots + pb_lX^l$, *then the annihilator of the ideal* $(g(X))$ *generated by* $g^{\perp}(X)$ *and* pX^{m-k}, *where* $g^{\perp}(X) := X^{m-l} - pb_tX^{t-l} - \cdots - pb_l$.

Proof. (i) We need to find the smallest xkp form $X^a + ph'(X)$ such that $X^ag(X) = ph'(X)g(X)$. Hence we need to find the smallest a such that $X^ag(X) \in p\mathbb{Z}_{p^2}[X]$ and $\deg_L(X^ag(X) \geq k$. Obviously $a = m-k$ is the smallest such that $X^ag(X) \in p\mathbb{Z}_{p^2}[X]$. And since $\deg_L(X^{m-k}g(X)) \geq k$, we see that

$$\begin{aligned} X^{m-k}g(X) &= \sum_{i \geq h} pa_iX^{i+m-k} - pX^n \\ &= pg(X)\sum_{i \geq h} a_iX^{i+m-2k} - pg(X)X^{n-k}. \end{aligned}$$

Therefore we see that $g^{\perp}(X) := X^{m-k} - \sum_{i \leq h} pa_iX^{i+m-2k} + pX^{n-k}$ is the smallest xkp form that annihilates $g(X)$.

The smallest pxr form that annihilates $g(X)$ is pX^{m-k} but it already belongs to the ideal $(g^{\perp}(X))$. Therefore $\text{Ann}(g(X)) = (g^{\perp}(X))$.

(ii) Now suppose $l := \deg_L(X^{m-k}g(X)) < k$. As before, we need to find the smallest a such that $X^ag(X) \in p\mathbb{Z}_{p^2}[X]$. Let $X^{m-k}g(X) = pb_tX^t + \cdots + pb_lX^l$. Then

$$\begin{aligned} X^{m-l}g(X) &= pb_tX^{t+k-l} + \cdots + pb_lX^k \\ &= g(X)(pb_tX^{t-l} + \cdots + pb_l). \end{aligned}$$

Obviously $a = m-l$ is the smallest integer such that $X^a g(X) \in p\mathbb{Z}_{p^2}[X]$ and

$$g(X)(X^{m-l} - pb_t X^{t-l} - \cdots - pb_l) = 0.$$

Therefore $g^{\perp}(X) := X^{m-l} - pb_t X^{t-l} - \cdots - pb_l$ is the smallest xkp form which annihilates $g(X)$.

It is clear that $pX^{m-k}g(X) = 0$ and pX^{m-k} is the smallest pxr form which annihilates $g(X)$. Therefore $\mathrm{Ann}(g(X)) = (g^{\perp}(X), X^{m-k})$ □

Now, we look at the annihilator of the ideals generated by two elements.

THEOREM 6. *Let* $R = \mathbb{Z}_{p^2}[X]/(X^m - pX^n)$ *and let*

$$g(X) = X^k + pa_h X^h + pa_{h-1}X^{h-1} + \cdots + pa_0$$

with $a_h, a_{h-1}, \ldots, a_0 \in \mathbb{Z}_{p^2}$. *Then the annihilator of the ideal* $I := (g(X), pX^r)$ *is given by the following:*

(i) *if* $\deg_L(X^{m-k}g(X)) \geq k$), *then Ann*$I$ *is generated by* pX^{m-k} *and* $X^{\lceil k-r,0\rceil}g^{\perp}(X)$, *where* $g^{\perp}(X)$ *is given in* Theorem 5 (i);

(ii) *if* $l := \deg_L(X^{m-k}g(X)) < k$), *then Ann*$I$ *is generated by* $X^{\lceil l-r,0\rceil}$ $g^{\perp}(X)$ *and* pX^{m-k}, *where* $g^{\perp}(X)$ *is given in* Theorem 5 (ii).

Proof. (i) As before, we need to find the smallest xkp form and pxr form which annihilate $g(X)$ as well as pX^r. We saw, in Theorem 5, that $g^{\perp}(X)$ is the smallest xkp form of degree $m-k$ which annihilates $g(X)$. If $r \geq k$, then $pX^r g^{\perp}(X) = 0$ since all the coefficients of $X^r g^{\perp}(X)$ are in $p\mathbb{Z}_{p^2}$. If $r < k$, then $X^{k-r}g^{\perp}(X)$ annihilates $g(X)$ as well as pX^r. It is obvious that $X^{k-r}g^{\perp}(X)$ is the smallest such. Since any pxr form annihilates pX^r, we need the smallest pxr form which annihilates $g(X)$ which should be pX^{m-k}.

We omit the proof of (ii) which can be proved in the same way. □

References

[1] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley, 1969.

[2] P. Kanwar and S. R. López-Permouth, *Cyclic codes over the integer modulo* p^n, Finite fields Appl. **3** (1997), no. 2, 334–352.

[3] S. S. Woo, *Cyclic codes of length* 2^n *over* $\mathbb{Z}_4$, preprint, 2004.

DEPARTMENT OF MATHEMATICS, EWHA WOMEN'S UNIVERSITY, SEOUL 120-750, KOREA

E-mail: sswoo@ewha.ac.kr