Commun. Korean Math. Soc. **28** (2013), No. 1, pp. 39–54
http://dx.doi.org/10.4134/CKMS.2013.28.1.039

CYCLIC CODES OF LENGTH 2^n OVER $\mathbb{Z}_4$

Sung Sik Woo

Abstract. The purpose of this paper is to find a description of the cyclic codes of length 2^n over $\mathbb{Z}_4$. We show that any ideal of $\mathbb{Z}_4[X]/(X^{2^n}-1)$ is generated by at most two polynomials of the standard forms. We also find an explicit description of their duals in terms of the generators.

1. Introduction

The purpose of this paper is to find all cyclic codes of length 2^n over $\mathbb{Z}_4$. A cyclic code of length m over $\mathbb{Z}_4$ is, by definition, a submodule of $\mathbb{Z}_4^m$ which is stable under cyclic shift. Hence a cyclic code of length m over $\mathbb{Z}_4$ can be identified with an ideal of $\mathbb{Z}_4[X]/(X^m-1)$.

The cyclic codes of odd length over $\mathbb{Z}_4$ is described in [3]. To find the descriptions of the ideals of $R=\mathbb{Z}_4[X]/(X^{2^n}-1)$ we show that the ring R is isomorphic to a seemingly simpler ring namely a ring of the form $S=\mathbb{Z}_4[x]$ where $x^n=0$ for some n, namely a nilpotent algebra.

To find the description of the ideals of a nilpotent algebra S we endow an order structure on S. As for the case of a polynomial ring over a field, 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 $\mathbb{Z}_4$ which is a key to find the ideals of S (§2).

In §3 we derive formulae for counting the number of elements of the ideals. To find the dual of the cyclic codes we find polynomials which annihilates the generators of the ideals of S in most economical way (§4). In §5 we relate the ideals of a nilpotent algebra with the cyclic codes of length 2^n and then we show that the dual of the cyclic codes are basically given by the polynomials which annihilates the generator of the ideal which corresponds to a cyclic codes of length 2^n over $\mathbb{Z}_4$ (§5). In §7, we give some examples.

This paper was referred in the papers [5, 6] and was not published. And there are papers whose contents are overlapping with this paper [2, 6]. Still

Received January 12, 2012.
2010 *Mathematics Subject Classification.* 94B15.
Key words and phrases. cyclic code over $\mathbb{Z}_4$.

there are people who want to see this paper and I think it is worth to publish it whose method is purely algebraic.

2. Euclidean algorithm modulo 4 and the ideals of nilpotent algebra

We consider a ring of the form $S = \mathbb{Z}_4[X]/(p(X))$, where $p(X)$ is a monic polynomial of degree m such that $X^n \in (p(X))$ for some n, i.e., $S = \mathbb{Z}_4[x]$ with $x^n = 0$ for some n. If l is the smallest integer, then we will say that the nilpotency of x is l. We will call such ring as *finite nilpotent $\mathbb{Z}_4$-algebra with nilpotency l*.

Typical examples we have in mind are $S = \mathbb{Z}_4[X]/(X^{2n} - 2X^n)$ and $S = \mathbb{Z}_4[X]/(X^{2^n} - 2X^{2^{n-1}})$. Later we show that the ring $R = \mathbb{Z}_4[X]/(X^{2^n} - 1)$ is isomorphic to a ring of this type.

Throughout this paper a ring S will mean a nilpotent $\mathbb{Z}_4$ algebra of the form $S = \mathbb{Z}_4[X]/(p(X))$ unless otherwise stated. Whenever we talk about a polynomial $f(X)$ in $S = \mathbb{Z}_4[X]/(p(X))$ we shall choose a representative with degree less than m. In this section we fix the degree of $p(X)$ say, $\deg(p(X)) = m$.

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.

Proposition 1. *The ring S is a local ring with the maximal ideal $(2, X)$. Every ideal J of S is primary with the radical $rad(J) = (2, X)$.*

Proof. Let $\mathfrak{m}$ be a maximal ideal. Any nilpotent element is contained in every prime ideal [1]. Since 2 is also nilpotent we see 2 and X belong to $\mathfrak{m}$. On the other hand, $(2, X)$ is a maximal ideal since $S/(2, X) \cong \mathbb{F}_2$. Therefore $\mathfrak{m} = (2, X)$.

Let J be an ideal of S. Then 2 and X, being nilpotent, belong to the radical $\mathrm{rad}(J)$ of J. Therefore $\mathrm{rad}(J) = (2, X)$. 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. Let u be a unit. Then $u + n$ is a unit if $n \in R$ is nilpotent.*

We define an order on the set $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ in the usual way

$$0 < 1 < 2 < 3$$

where we omitted the bars as we will do from now on. On the set $C = \{(a_0, a_1, \ldots, a_{m-1}) \mid a_i \in \mathbb{Z}_4\}$ 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 $\mathbb{Z}_4[X]$ with $\deg(f), \deg(g) < m$. Then we define

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

Proposition 2. *Let J be an ideal of S contained in (2). Then J is of the form $(2X^r)$ for some r.*

Proof. Let $f(X) = \sum_{i=0}^{m-1} a_i X^i \in J$. Since $J \subseteq (2)$ all of the coefficients of f are in $2\mathbb{Z}_4$. By noting that X is nilpotent we see that $f(X)$ is of the form $2X^j\cdot$(unit). Now let $2X^r$ be the lowest degree among such expression. Now it is obvious that $J = (2X^r)$. □

Definition. Let us call the element of the form $2X^r$ a 2xr form.

We now prove existence of elements of some special form if the ideal is not contained in the ideal (2) generated by $2 \in S$.

Proposition 3. *Let S be a nilpotent algebra. Let J be a nonzero ideal of S which is not contained in the ideal (2) generated by $2 \in S$. Then there are nonzero elements of the form $X^k + 2h(X)$ where $h \in S$ of degree $< k$.*

Proof. Let $f(X) = \sum_{i<m} a_i X^i$ be a nonzero polynomial in J. If $a_0 \in \mathbb{Z}_4$ is a unit, then f is a unit since $X \in S$ is nilpotent. Hence we may assume a_0 is 0 or 2. If the coefficients of the lowest degree terms are all units, then f is of the form $X^i \times$ (unit). Therefore X^i is an element of J which is of the required form.

Now suppose the coefficient of the nonzero term of lowest degree is 2. Let a_i be the unit coefficient of the lowest degree, i.e., $a_{i-1}, a_{i-2}, \dots$ are in $2\mathbb{Z}_4$. Let l be the smallest integer such that $X^l = 0$. Then $X^{l-i-1} f(X)$ is a desired form. □

Definition. Let us call the polynomials of the form

$$g(X) = X^k + 2X^{h_1} + 2X^{h_2} + \cdots + 2X^{h_t}$$

with $h_t < \cdots < h_1 < k < m$ an xk2 form. And we will often denote the polynomial $2X^{h_1} + 2X^{h_2} + \cdots + 2X^{h_t}$ by $2h(X)$.

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

Theorem 1 (Euclidean algorithm modulo 4)**.** *Let J be an ideal of S which is not contained in the ideal (2) generated by $2 \in S$. Let $g(X) = X^k + 2h(X) \in J$ be an xk2 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 $r(X) \in 2\mathbb{Z}_4[X]$.

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 are in $2\mathbb{Z}_4$.

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 contradict to the fact that $g(X) = X^k + 2h(X)$ is a minimal element. Hence we may assume that the coefficient of the lowest degree term is 2.

Let $r(X) = a_j X^j + a_{j-1}X^{j-1} + \cdots + 2X^l$ with $j < k$ and $a_j \neq 0$. Let $a_s X^s$ be the lowest degree term with a_s a unit, that is $a_{s-1}, a_{s-2}, \ldots \in 2\mathbb{Z}_4$. If $s = j$, then $r(X)$ is a xk2 form which is smaller than $g(X)$. Hence $j > s$.

Then we see that $X^{k-j}r(X) - a_j g(X) \in J$ is a polynomial of degree $< k$ with the parity of the coefficients of $X^{s+k-j-1}, X^{s+k-j-2}, \ldots$ remain the same as those of $a_{s-1}, a_{s-2}, \ldots$ since the coefficient of terms of degree $< k$ in $a_j g(X)$ is in $2\mathbb{Z}_4$.

Let $2h(X) = \sum_i 2h_i X^i$. If the coefficients of $X^{k-1}, X^{k-2}, \ldots, X^{s+k-j+1}$ in $X^{k-j}r(X) - a_j g(X)$ happen to vanish namely $X^{k-j}r(X) - a_j g(X) = (a_s + 2a_j h_s)X^{s+k-j} + (a_{s-1} + 2a_j h_{s-1})X^{s+k-j-1} + \cdots + (2 + 2a_j h_l)X^l$. Then $a_s + 2a_j h_s$ is a unit and $a_{s-i} + 2a_j h_{s-i} \in 2\mathbb{Z}_4$ for $i \geq 1$. But this gives us an element in J which is smaller than $g(X)$ after multiplying -1 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 parity of the coefficients of the last $(s - l)$ terms to get an element of J with degree $< \deg(X^{k-j}r(X) - a_j g(X))$. Then obviously, the resulting element is an xk2 form which is smaller than $g(X)$ belonging to J. □

Let J be a nonzero ideal of S which is not contained in (2). Choose an element of the form $g(X) = X^k + 2h(X)$ with $h(X) \in S$ with $\deg(h) < k$ which is the smallest with respect to the ordering defined above. We will show that J is generated by $g(X)$ and $2X^r$ for some r.

Theorem 2. *Let J be an ideal of S which is not contained in* (2). *Let $g(X) = X^k + 2h(X) \in J$ be the smallest xk2 form in J and $2X^r$ be the smallest 2xr form in J. Then $J = (g(X), 2X^r)$ where $-\infty \leq r < l$.*

Proof. Obviously $J \supseteq (g(X), 2X^r)$. Now let $f \in J$ and write $f(X) = g(X)q(X) + 2r(X)$. Then $2r(X)$ is of the form $2r(X) = 2X^t(1 + X^{i_1} + \cdots + X^{i_s})$. That is $2r(X) = 2X^t \cdot u$ for some unit u. Hence we can write $f(X) = g(X)q(X) + 2X^t \cdot u$ for some unit u. Since $f(X)$ and $g(X)$ belong to J we see that $2X^t \in J$. As $2X^r$ is the smallest 2xr form in J we have $t \geq r$. Therefore $f(X) = g(X)q(X) + uX^{t-r}(2X^r)$. Thus $J \subseteq (g(X), 2X^r)$. □

Corollary 1. *The proper ideals of S are of the form $(2X^i)$ for some i; or $(g(X), 2X^r)$ for some xk2 form $g(X)$ and some r with $-\infty \leq r < \deg(g)$.*

Now we count the number of possible distinct ideals of a nilpotent algebra.

Proposition 4. *The principal ideals of S are of the forms*
(i) *$(2X^r)$ for some 2xr form $2X^r$ with $(0 \leq r < m)$;*
(ii) *$(g(X))$ for some xk2 form $g(X)$.*

The number of ideals of the first type is m; the number of ideals of the second type does not exceed $\sum_{k=1}^{m-1} 2^k = 2^m - 2$.

Proof. May be the last statement worth checking. For each degree k of $g(X)$ we can choose $\{h_1, h_2, \ldots, h_t\}$ with $k > h_1 > h_2 > \cdots > h_t \geq 0$ for the degrees of nonzero terms of $h(X)$. And therefore there are 2^k xk2 forms of degree k for each $0 < k < m$. Hence the number of ideals generated by an xk2 form does not exceed

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

□

Proposition 5. *The set of nonprincipal ideals of S are of the form $(g(X), 2X^r)$ where $g(X) = X^k + 2X^{h_1} + \cdots + 2X^{h_t}$ is an xk2 form with $k < r < h_1$. Then the number of nonprincipal ideals does not exceed*

$$\sum_{m>k>j\geq 0} (k - j - 1)2^j.$$

Proof. For each k choose the highest degree of nonzero term h_1. Once we choose k and h_1 then there are $k - h_1 - 1$ possible choices of 2xr form $2X^r$ $(k < r < h_1)$. For each such choice we choose arbitrary subset of $\{1, \ldots, (h_1 - 1)\}$ which corresponds to the degrees of nonzero terms of $h(X)$. Therefore the number of all possible nonprincipal ideals is $\sum_{m>k>j\geq 0}(k-j-1)2^j$ by letting $h_1 = j$. □

Remark. (1) Not all distinct expressions of $(g(X), 2X^r)$ give distinct ideals. For example, if we take $S = \mathbb{Z}_4[X]/(X^4 - 2X^2)$, then one can easily check that $(X^3 + 2X^2) = (X^3, 2X^2)$. Also $(X^3 + 2, 2X) = (X^3 + 2)$.

(2) Let $g(X) = X^k + 2X^{h_1} + \cdots + 2X^{h_t}$ be an xk2 form and $k > r > h_1$. Then $g(X)$ is not, in general, the smallest element of the ideal $(g(X), 2X^r)$.

3. Number of elements of the ideals

With applications to cyclic codes in mind we specialize our ring S. Accordingly we let $S = \mathbb{Z}_4[X]/(X^{2l} - 2X^l)$ throughout this section. Note that $X^{3l} = 2X^l \cdot X^l = 0$. Hence S is a nilpotent algebra with nilpotency $3l$.

For $f(X) \in S$ with $\deg(f(X)) < 2l$ let us write $\deg_L(f(X))$ for the degree of the lowest nonzero degree term.

Let $g(X) = X^k + 2h(X)$ where $2h(X) = 2X^{h_1} + \cdots + 2X^{h_{t-1}} + 2X^{h_t}$ with $h_t < \cdots < h_1 < k < 2l$ or $h(X) = 0$. For each basis element $\{1, X, \ldots, X^{2l-1}\}$ (in this order) of S express $X^i g(X)$ as a linear combination of the basis $\{X^{2l-1}, \ldots, X, 1\}$ (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 $(2l-k)\times(2l-k)$ 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 consists of the elements of $2\mathbb{Z}_4$. The matrix B consist of 0's and 2's of size $(2l-k)\times k$. And C is a $(2l-k)\times(2l-k)$ matrix of the form

$$C=\begin{pmatrix}0&\cdots&2&\cdots&2\\0&\cdots&*&*&2\\2&\cdots&*&\cdots&0\\*&\cdot&2&0&0\\*&2&0&0&0\end{pmatrix}$$

with 2's along the opposite diagonal of a square submatrix on the right lower corner. And D is a $k\times k$ matrix of the form

$$D=\begin{pmatrix}*&*&\cdots&2&0&\cdots&0\\&\cdots&2&0&\ldots\ldots&&0\\*&\cdot&0&\ldots\ldots\ldots&&&0\\2&0&0&\ldots\ldots\ldots&&&0\\0&0&0&\ldots\ldots\ldots&&&0\\&&\ldots\ldots\ldots\ldots&&&&\\0&0&\ldots\ldots\ldots\ldots&&&0\end{pmatrix}$$

where $*$'s are in $2\mathbb{Z}_4$; and the upper left corner of D is a square matrix whose opposite diagonals are 2's.

We consider two cases. The first case is when $D=0$. This is equivalent to $\deg_L(X^{2l-k}g(X))\geq k$.

The second case we consider is when $D\neq 0$. This is equivalent to that $\deg_L(X^{2l-k}g(X)<k$. For $D\neq 0$, we consider three cases. The first case is when $\deg_L(X^{2l-k}g(X))<l$ (i.e., $l+h_t<k$) in which case the lowest degree of $X^{2l-k}g(X)$ is $2l-k+h_t$. The second case is when $\deg_L(X^{2l-k}g(X))=l$ (i.e., $l+h_t=k$) in which case the lowest degree of $X^{2l-k}g(X)$ is $2l-k+h_{t-1}$. Finally we can consider the case when $\deg_L(X^{2l-k}g(X))>l$ (i.e., $l+h_t>k$) in which case the lowest degree of $X^{2l-k}g(X)$ is l.

We will use the notation $\lceil a,b\rceil$ for $\max\{a,b\}$.

Theorem 3. *Let $S=\mathbb{Z}_4[X]/(X^{2l}-2X^l)$ and let*

$$g(X)=X^k+2X^{h_1}+2X^{h_2}+\cdots+2X^{h_t}$$

with $h_t<\cdots<h_1<k<2l$. Then the number of elements in the principal ideal generated by $g(X)$ is given by

(i) *if $\deg_L(X^{2l-k}g(X)\geq k)$, then the number of elements is 4^{2l-k},*

(ii) *if* $\deg_L(X^{2l-k}g(X) < k)$, *then the number of elements is*

$$\begin{cases} 4^{2l-k-h_t}2^{2k-2l-h_t} & \text{if } l+h_t < k \\ 4^{2l-k}2^{2k-2l-h_{t-1}} & \text{if } l+h_t = k \\ 4^{2l-k}2^{\lceil k-l,0\rceil} & \text{if } k < h_t + l \end{cases}$$

where $\lceil a, b\rceil = \max\{a, b\}$.

Remark. It is understood that there is no factor of 2 in the first two numbers of (ii) when there is no h_t or h_{t-1}.

Proof. First consider the case when $D = 0$, i.e., $\deg_L X^{2l-k}g(X) \geq k$. And in this case, the number of 1's is $2l-k$. And using these 1's we can get rid of 2's in C. Hence the ideal generated by $g(X)$ is free over $\mathbb{Z}_4$ of rank $2l-k$.

Now assume $\deg_L X^{2l-k}g(X) < k$. The number of 1's in the opposite diagonal of A is $2l-k$. As before we can get rid of 2's in C without changing D. Now we need to count the number of 2's on the opposite diagonal of a square submatrix in the upper left corner of D. The first case is when $\deg_L(X^{2l-k}g(X)) < l$ (i.e., $l + h_t < k$) in which case the lowest degree of $X^{2l-k}g(X)$ is $2l-k+h_t$. Therefore the number of 2's on the opposite diagonal in a square submatrix of D is $k-(2l-k+h_t) = 2k-2l-h_t$. Thus, in this case, the number of elements in the ideal generated by $g(X)$ is $4^{2l-k}2^{2k-2l-h_t}$.

We omit the proof of the other cases which can be proved in the same manner. □

Corollary 2. *Let* $S = \mathbb{Z}_4[X]/(X^{2l} - 2X^l)$. *Then the ideal* $(g(X))$ *is* $\mathbb{Z}_4$*-free if and only if the exponent of 2 is zero in the formula for the number of elements of the ideal* $(g(X))$. *In particular, the ideal* $(g(X))$ *is* $\mathbb{Z}_4$*-free only when one of the following cases holds*:

$$\begin{cases} \deg_L(X^{2l-k}g(X)) \geq k, \\ 0 < h_t = k-l \text{ and } 2h_t = h_{t-1}, \\ 0 < h_t = k-l \text{ and there is no } h_{t-1}. \end{cases}$$

Proof. We know that the ideal $(g(X))$ is $\mathbb{Z}_4$-free if there is no 2-part which is the case when $\deg_L(X^{2l-k}g(X)) \geq k$. For the case (ii) in Theorem 3, one can check easily that the first and third case cannot happen. The only possible case where the exponent of 2 becomes 0 is the second case of (ii). It happens exactly when $0 < h_t = k-l, 2h_t = h_{t-1}$; or $0 < h_t = k-l$ and there is no h_{t-1}. □

Remark. It can be shown [5] that the ideal $(g(X))$ is free if and only if $g(X)$ divides $X^{2l} - 2X^l$.

Proposition 6. *Let* $S = \mathbb{Z}_4[X]/(X^{2l} - 2X^l)$. *Then the number of elements in the ideal* $(2X^r)$ *generated by* $2X^r$ *is* 2^{2l-r}.

Proof. Easy to show and we omit its proof. □

Theorem 4. *Let* $S = \mathbb{Z}_4[X]/(X^{2l} - 2X^l)$ *and let*

$$g(X) = X^k + 2X^{h_1} + 2X^{h_2} + \cdots + 2X^{h_t}$$

with $h_t < \cdots < h_1 < k < 2l$. *Then the number of elements in the ideal* $(g(X), 2X^r)$ *generated by* $g(X)$ *and* $2X^r$ *is given by*

(i) *if* $\deg_L(X^{2l-k}g(X)) \geq k$, *then the number of elements is* $4^{2l-k}2^{\lceil k-r,0\rceil}$,

(ii) *if* $\deg_L(X^{2l-k}g(X)) < k$, *then the number of elements is*

$$\begin{cases} 4^{2l-k}2^{\lceil 2k-2l-h_t,k-r\rceil} & \text{if } l + h_t < k \\ 4^{2l-k}2^{\lceil 2k-2l-h_{t-1},k-r\rceil} & \text{if } l + h_t = k \\ 4^{2l-k}2^{\lceil k-l,0\rceil} & \text{if } k < h_t + l \end{cases}$$

where $\lceil a, b\rceil = \max\{a, b\}$.

Proof. The generator matrix for $(g(X), 2X^r)$

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

where F is a matrix of the same form as D of size $(2l - r) \times 2l$. Now it is easy to check that the number of elements in the ideal is given as in the theorem and we omit the detail. □

4. 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 turn out to be the generators for the dual of the cyclic codes.

Proposition 7. *Let* $S = \mathbb{Z}_4[X]/(X^{2l} - 2X^l)$. *Then the annihilator of the ideal* $(2X^r)$ *is given by* $(X^{2l-r}, 2)$.

Proof. By Theorem 2 we need to find the smallest xk2 form and 2xr form which annihilate $2X^r$. Now we have $X^{2l-r}(2X^r) = 2X^{2l} = 0$ and $2(2X^r) = 0$. It is clear that X^{2l-r} is a minimal xk2 form which annihilates $g(X)$ and 2 is the smallest 2xr form which annihilates $2X^r$. □

Theorem 5. *Let* $S = \mathbb{Z}_4[X]/(X^{2l} - 2X^l)$ *and let*

$$g(X) = X^k + 2X^{h_1} + 2X^{h_2} + \cdots + 2X^{h_t}$$

with $h_t < \cdots < h_1 < k < 2l$. *Then the annihilator of the ideal* $(g(X))$ *is given by*

(i) *if* $\deg_L(X^{2l-k}g(X)) \geq k$, *then* $\mathrm{Ann}(g(X))$ *is generated by*

$$g^{\perp}(X) = X^{2l-k} + \sum_{i=1}^{t} 2X^{h_i+2l-2k} + 2X^{l-k}.$$

(ii) *if* $\deg_L(X^{2l-k}g(X)) < k$, *then* $\mathrm{Ann}(g(X))$ *is generated by* $g^\perp(X)$ *and* $2X^{2l-k}$ *where* $g^\perp(X)$ *is given by*

$$\begin{cases} X^{k-h_t} + 2X^{h_1-h_t} + 2X^{h_2-h_t} + \cdots + 2 + 2X^{k-h_t-l} & \text{if } l + h_t < k \\ X^{k-h_{t-1}} + 2X^{h_1-h_{t-1}} + 2X^{h_2-h_{t-1}} + \cdots + 2 & \text{if } l + h_t = k \\ X^l + 2X^{l-k+h_1} + \cdots + 2X^{l-k+h_t} + 2 & \text{if } l < k < h_t + l. \end{cases}$$

Proof. (i) We need to find the smallest xk2 form $X^m + 2h'(X)$ such that $X^m g(X) = 2h'(X)g(X)$. Hence we need to find the smallest m such that $X^m g(X) \in 2\mathbb{Z}_4[X]$ and $\deg_L(X^m g(X)) \geq k$.

Since $\deg_L(X^{2l-k}g(X)) \geq k$ we see that $h_i + 2l - k \geq k$ and $l \geq k$ whenever they appear as an exponent of a nonzero term of $X^{2l-k}g(X) = \sum 2X^{h_i+2l-k} + 2X^l$. And we see that $m = 2l - k$ is the smallest such and

$$\begin{aligned} X^{2l-k}g(X) &= \sum 2X^{h_i+2l-k} + 2X^l \\ &= 2g(X)\sum X^{h_i+2l-2k} + 2g(X)X^{l-k}. \end{aligned}$$

Therefore we see that $g^\perp(X) = X^{2l-k} + \sum_{i=1}^{t} 2X^{h_i+2l-2k} + 2X^{l-k}$ is the smallest xk2 form that annihialtes $g(X)$.

The smallest 2xr form that annihilates $g(X)$ is $2X^{2l-k}$ but it already belongs to the ideal $(g^\perp(X))$. Therefore $\mathrm{Ann}(g(X)) = (g^\perp(X))$.

(ii) Now suppose $\deg_L(X^{2l-k}g(X)) < k$. There are three cases we need to consider.

First consider the case $\deg_L(X^{2l-k}g(X)) < k$ and $(2l-k) + h_t < l$, i.e., $l + h_t < k$. In this case the degree of the lowest nonzero term of $X^{2l-k}g(X)$ is $2l - k + h_t$.

$$\begin{aligned} X^{k-h_t}g(X) &= X^{2k-h_t} + 2X^{k-h_t+h_1} + \cdots + 2X^k \\ &= 2X^{k-h_t+h_1} + \cdots + 2X^k + 2X^l \cdot X^{2k-2l-h_t} \\ &= 2X^{-h_t+h_1}g(X) + \cdots + 2g(X) + 2X^{k-h_t-l}g(X), \end{aligned}$$

where $(k - h_t - l) > 0$. Therefore

$$(X^{k-h_t} + 2X^{-h_t+h_1} + 2X^{-h_t+h_2} + \cdots + 2 + 2X^{k-h_t-l})g(X) = 0.$$

Second consider the case when $\deg_L(X^{2l-k}g(X)) < k$ and $2l - k + h_t = l$. That is $l + h_t = k$ and $h_{t-1} < 2k - 2l$.

$$\begin{aligned} & X^{k-h_{t-1}}g(X) \\ &= X^{2k-h_{t-1}} + 2X^{k-h_{t-1}+h_1} + \cdots + 2X^k + 2X^{k-h_{t-1}+h_t} \\ &= 2X^{k-h_{t-1}+h_1} + \cdots + 2X^k + 2X^{k-h_{t-1}+h_t} + 2X^l \cdot X^{2k-2l-h_{t-1}} \\ &= 2X^{-h_{t-1}+h_1}g(X) + \cdots + 2X^{-h_{t-1}+h_{t-2}}g(X) + 2g(X). \end{aligned}$$

Therefore $(X^{k-h_{t-1}} + 2X^{-h_{t-1}+h_1} + 2X^{-h_{t-1}+h_2} + \cdots + 2)g(X) = 0$. Hence $g^\perp(X) = (X^{k-h_{t-1}} + 2X^{-h_{t-1}+h_1} + 2X^{-h_{t-1}+h_2} + \cdots + 2) \in \mathrm{Ann}(g(X))$.

Thirdly consider the case when $k > \deg_L(X^{2l-k}g(X)) > l$. Hence we have $k < h_t + l$ and

$$\begin{aligned} X^{(2l-k)+(k-l)}g(X) &= X^l g(X) \\ &= X^{l+k} + 2X^{l+h_1} + \cdots + 2X^{l+h_t} \\ &= 2X^{l-k+h_1}g(X) + \cdots + 2X^{l-k+h_t}g(X) + 2X^l X^{k-l} \\ &= 2X^{l-k+h_1}g(X) + \cdots + 2X^{l-k+h_t}g(X) + 2g(X). \end{aligned}$$

Hence $g^\perp(X) = X^l + 2X^{l-k+h_1} + \cdots + 2X^{l-k+h_t} + 2 \in \mathrm{Ann}(g(X))$.

In any one of these cases we have $2X^{2l-k}g(X) = 0$. Hence we see that $2X^{2l-k} \in \mathrm{Ann}(g(X))$.

As in (i) we see that $g^\perp(X)$ is the smallest xk2 form and $2X^{2l-k}$ is the smallest 2xr form that annihilate $g(X)$ in each cases. Therefore $\mathrm{Ann}(g(X)) = (g^\perp(X), X^{2l-k})$. □

Theorem 6. *Let $R = \mathbb{Z}_4[X]/(X^{2l} - 2X^l)$ and let*

$$g(X) = X^k + 2X^{h_1} + 2X^{h_2} + \cdots + 2X^{h_t}$$

with $h_t < \cdots < h_1 < k < 2l$. Then the annihialtor of the ideal $(g(X), 2X^r)$ is given by

(i) *if $\deg_L(X^{2l-k}g(X)) \geq k$), then $\mathrm{Ann}(g(X), 2X^r)$ is generated by $2X^{2l-k}$ and $X^{\lceil k-r,0\rceil}g^\perp(X)$ where $g^\perp(X)$ is given in Theorem 5.*

(ii) *if $\deg_L(X^{2l-k}g(X)) < k$), then $\mathrm{Ann}(g(X), 2X^r)$ is generated by $g_1^\perp(X)$ and $2X^{2l-k}$ where $g_1^\perp(X)$ is given by*

$$\begin{cases} X^{\lceil 2l-k+h_t-r,0\rceil}g^\perp(X) & \text{if } l + h_t < k \\ X^{\lceil 2l-k+h_{t-1}-r,0\rceil}g^\perp(X) & \text{if } l + h_t = k \\ X^{\lceil l-r,0\rceil}g^\perp(X) & \text{if } l < k < h_t + l \end{cases}$$

where $g^\perp(X)$ is given in Theorem 5 in each respective case.

Proof. (i) As before, we need to find the smallest xk2 form and 2xr form which annihilate $g(X)$ as well as $2X^r$. We saw in Theorem 5 that $g^\perp(X)$ is the smallest xk2 form of degree $2l - k$ which annihilates $g(X)$. If $r \geq k$, then $2X^r g^\perp(X) = 0$ since all the coefficients of $X^r g^\perp(X)$ are in $2\mathbb{Z}_4$. If $r < k$, then $X^{k-r}g^\perp(X)$ annihilates $g(X)$ as well as $2X^r$. It is obvious that $X^{k-r}g^\perp(X)$ is the smallest such. Since any 2xr form annihilates $2X^r$ we need the smallest 2xr form which annihilates $g(X)$ which should be $2X^{2l-k}$.

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

5. Nilpotent algebras and cyclic codes over $\mathbb{Z}_4$

To apply the results on nilpotent algebras of the previous sections we will show that the nilpotent algebra $S = \mathbb{Z}_4[X]/(X^{2^n} - 2X^{2^{n-1}})$ is isomorphic to the ring $R = \mathbb{Z}_4[X]/(X^{2^n} - 1)$ whose ideals can be considered as the cyclic codes of length 2^n.

First we need a lemma.

Lemma 2. *Let $n \geq 2$. Modulo 4 we have the equality*

$$\binom{2^n}{r} \equiv \begin{cases} 0 \pmod 4 \text{ if } r \neq 2^{n-1}, \\ 2 \pmod 4 \text{ if } r = 2^{n-1}. \end{cases}$$

Proof. We recall

$$\binom{2^n}{r} = \frac{2^n(2^n-1)(2^n-2)\cdots(2^n-r+1)}{1\cdot 2\cdots r}.$$

By the relation

$$\binom{2^n}{r} = \binom{2^n}{2^n-r}$$

we may assume $r \leq 2^{n-1}$.

First let $r < 2^{n-1}$. Note that for any $k \leq 2^{n-1}$ the highest power of 2 diving k is the same as the highest power of 2 dividing $2^n - k$. Write $r = 2^a t$ with t odd. Let $\{2, 2^2, 2, \ldots, 2^a\}$ be the set of powers of 2 in the set of numbers $\{1, 2, 3, \ldots, r\}$. Then since $r < 2^{n-1}$ we have $a \leq n-2$. Now the power of 2 in the denominator of $\binom{2^n}{r}$ is $2 \cdots 2^a$. On the other hand, the power of 2 in the numerator of $\binom{2^n}{r}$ is $\frac{1}{2^a} 2^n \cdot 2 \cdots 2^a$. Therefore the power of 2 in $\binom{2^n}{r}$ is $2^n/2^a$ which is divisible by 4 since $a \leq n-2$.

Now let $r = 2^{n-1}$. Then the power of 2 in the numerator of $\binom{2^n}{r}$ is $\frac{1}{2^{n-1}} 2^n \cdot 2 \cdot 2^2 \cdots 2^{n-1}$. On the other hand, the power of 2 in the denominator of $\binom{2^n}{r}$ is $2^n \cdot 2 \cdot 2^2 \cdots 2^{n-1}$. Therefore the power of 2 in $\binom{2^n}{r}$ is $2^n/2^{n-1}$ which is 2. □

Proposition 8. *Let $n \geq 1$. Let $X^{2^n} - 1 \in \mathbb{Z}_4[X]$. Then we can write*

$$X^{2^n} - 1 = (X-1)^{2^n} - 2(X-1)^{2^{n-1}}.$$

Proof. For $n \geq 2$ we have

$$(X-1)^{2^n} = X^{2^n} - 2X^{2^{n-1}} + 1$$

by Lemma 2. Therefore, in $\mathbb{Z}_4[X]$, we have

$$\begin{aligned} X^{2^n} - 1 &= (X-1)^{2^n} - 2X^{2^{n-1}} - 2 \\ &= (X-1)^{2^n} - 2(X^{2^{n-1}} + 1) \\ &= (X-1)^{2^n} - 2(X^{2^{n-1}} - 2X^{2^{n-2}} + 1) \\ &= (X-1)^{2^n} - 2(X-1)^{2^{n-1}}. \end{aligned}$$

For $n = 1$, we check: $X^2 - 1 = (X-1)^2 - 2(X-1)$. □

Corollary 3. *There is an isomorphism*

$$\phi : \mathbb{Z}_4[T]/(T^{2^n} - 2T^{2^{n-1}}) \longrightarrow \mathbb{Z}_4[X]/(X^{2^n} - 1)$$

of rings which maps $f(T)$ to $f(X-1)$. The inverse of ϕ maps $f(X)$ to $f(X+1)$.

Corollary 4. *The ring $\mathbb{Z}_4[X]/(X^{2^n}-1)$ is a local ring with the maxiaml ideal $(2, X-1)$ for all $n \geq 1$.*

Proof. By Corollary 1, $R = \mathbb{Z}_4[X]/(X^{2^n}-1)$ is a local ring. By Proposition 1, $S = \mathbb{Z}_4[T]/(T^{2^n} - 2T^{2^{n-1}})$ is a local ring with the maximal ideal $\mathfrak{m} = (2, T)$. Hence $\phi(\mathfrak{m}) = (2, X-1)$ is the maximal ideal of the local ring R. □

Note that $X^{2^n} - 1 = (X-1)^{2^n} - 2(X-1)^{2^{n-1}}$ is a primary polynomial with the basic irreducible polynomial $X - 1$ [4].

Combining Proposition 8 with Theorem 2 and by a change of variable we can find all cyclic codes of length 2^n over $\mathbb{Z}_4$.

Theorem 7. *The cyclic codes of length 2^n over $\mathbb{Z}_4$ are given by the ideals $(2(X-1)^s)$ for some s or $(g(X-1), 2(X-1)^r)$ where $g(T)$ is a xk2 form of degree $< 2^n$ and some $r \leq \deg(g)$.*

Proof. By Corollary 1 to Proposition 8, we have an isomorphism

$$\phi : \mathbb{Z}_4[T]/(T^{2^n} - 2T^{2^{n-1}}) \longrightarrow \mathbb{Z}_4[X]/(X^{2^n} - 1).$$

The ideals of $\mathbb{Z}_4[X]/(X^{2^n}-1)$ are precisely of the form $\phi(J)$ where J is an ideal of $\mathbb{Z}_4[T]/(T^{2^n} - 2T^{2^{n-1}})$. Now the result follows from Theorem 2. □

6. Duality of cyclic codes over $\mathbb{Z}_4$

To find the dual of cyclic codes we use the isomorphism

$$\phi : \mathbb{Z}_4[T]/(T^{2^n} - 2T^{2^{n-1}}) \longrightarrow \mathbb{Z}_4[X]/(X^{2^n} - 1)$$

which maps $f(T)$ to $f(X-1)$.

We will use the following obvious facts.

Lemma 3. *Let $S = \mathbb{Z}_4[X]/(X^{2^n} - 2X^{2^{n-1}})$ and $R = \mathbb{Z}_4[X]/(X^{2^n} - 1)$ and $\phi : S \to R$ be the isomorphism defined above.*

(i) *If J is an ideal of S, then $\phi(J)$ is an ideal of R with the same number of elements.*

(ii) *If $g_1(X), g_2(X) \in S$ with $g_1(X)g_2(X) = 0$, then $\phi(g_1(X))\phi(g_2(X)) = 0$ and conversely.*

We need a well known fact.

Lemma 4. *Let C be a $\mathbb{Z}_4$-submodule of $\mathbb{Z}_4^n$. Define*

$$C^{\perp} = \{b \in \mathbb{Z}_4^n \mid a \cdot b = 0 \text{ for all } a \in C\},$$

where $a = (a_1, \ldots, a_n), b = (b_1, \ldots, b_n)$ and $a \cdot b = a_1b_1 + \cdots + a_nb_n$. Then the number of elements of C is of the form $\#C = 4^{k_1}2^{k_2}$ and then $\#C^{\perp} = 4^{n-k_1-k_2}2^{k_2}$.

For a polynomial $f(X) = a_nX^n + \cdots + a_1X + a_0$ be a polynomial over a commutative ring. As usual we define the reciprocal polynomial $f^*(X)$ as $f^*(X) = X^n f(X^{-1})$.

Lemma 5. (i) *Let $g(T) = T^k + 2h(T)$ be a xk2 form and $r(T) = 2T^r$ be a 2xr form. Then $g^{**}(X-1) = g(X-1)$ and $r^{**}(X-1) = r(X-1)$.*

(ii) *Let g, h be the generator polynomials for a cyclic code C and if g' and h' are polynomilas with nonzero polynomilas with nonzero constant terms annihilating the ideal (g, h). If (g', h') has the same number of elements as $C^\perp$ which is given in Lemma 4, then $C^\perp$ is generated by g' and h'.*

Proof. For (i) it is enough to show that the constant terms of $g(X-1)$ and $r(X-1)$ is nonzero. Since $g(X-1) = (X-1)^k + 2(X-1)^{h_1} + \cdots + 2(X-1)^{h_t}$, the constant term of $g(X-1)$ is a unit. And the constant term of $r(X) = 2(X-1)^r$ is 2. Hence in either case we see that the constant terms of $g(X-1)$ and $r(X-1)$ are nonzero.

(ii) For this we simply note that $(g')^{**} = g'$ and $(h')^{**} = h'$ since g' and h' have nonzero constants. □

For the sake of notational convenience let us write $2l = 2^n$ and $l = 2^{n-1}$.

Proposition 9. *Let $S = \mathbb{Z}_4[X]/(X^{2^n} - 1)$ and let $T = X - 1$ and $l = 2^{n-1}$. Let C be the cyclic code generated by $2T^r$. Then the dual $C^\perp$ is given by the ideal $(T^{2l-r}, 2)$ generated by T^{2l-r} and 2.*

Proof. By Lemma 3 and by the results of the previous sections we see that the polynomials $g^\perp(T)$ and $2T^{2l-k}$ annihilate $g(T)$. Hence $g^\perp(T)$ and $2T^{2l-k}$ annihilate $g(T)$. By Lemma 5 we need to show that the ideals generated by $g^\perp(T)$ and $2T^{2l-k}$ have the right number of elements. By Lemma 3 we can use Theorem 4 to count the number of elements in the ideal $(T^{2l-r}, 2)$ which gives $4^r 2^{2l-r}$. Now that is the right number of elements for the dual. As desired. □

Theorem 8. *Let $R = \mathbb{Z}_4[X]/(X^{2^n} - 1)$. Let $T = X - 1$ and*

$$g(T) = T^k + 2T^{h_1} + 2T^{h_2} + \cdots + 2T^{h_t}$$

with $h_t < \cdots < h_1 < k < 2l$, $l = 2^{n-1}$. Let C be the cyclic code generated by $g(T)$ then the dual $C^\perp$ is generated by;

(i) *if $\deg_L(T^{2l-k}g(T)) \geq k$, then $C^\perp$ is generated by*

$$g^\perp(T) = T^{2l-k} + \sum_{i=1}^{t} 2T^{h_i+2l-2k} + 2T^{l-k},$$

(ii) *if $\deg_L(T^{2l-k}g(T)) < k$), then $C^\perp$ is generated by $g^\perp(T)$ and $2T^{2l-k}$ where $g^\perp(T)$ is given by*

$$\begin{cases} T^{k-h_t} + 2T^{h_1-h_t} + 2T^{h_2-h_t} + \cdots + 2 + 2T^{k-h_t-l} & \text{if } l + h_t < k \\ T^{k-h_{t-1}} + 2T^{h_1-h_{t-1}} + 2T^{h_2-h_{t-1}} + \cdots + 2 & \text{if } l + h_t = k \\ T^l + 2T^{l-k+h_1} + \cdots + 2T^{l-k+h_t} + 2 & \text{if } l < k < h_t + l. \end{cases}$$

Proof. By the results of §4, we see that the polynomials $g^{\perp}(X)$ and $2X^{2l-k}$ annihilate $g(X)$. Hence $g^{\perp}(T)$ and $2T^{2l-k}$ annihilate $g(T)$ by Lemma 3. By Lemma 4 we need to show that the ideals generated by $g^{\perp}(T)$ and $2T^{2l-k}$ have the right number of elements. By Lemma 3, the number of elements in the ideal $(g^{\perp}(T), 2T^{2l-k})$ is the same as $(g^{\perp}(X), 2X^{2l-k})$. Now we compute the number of elements in each case by using Theorem 4.

(i) Since $X^k g^{\perp}(X) = X^{2l} + \sum 2X^{h_i+2l-2k} + 2X^l = \sum 2X^{h_i+2l-2k}$ we see that $\deg_L(X^k g^{\perp}(X)) \geq 2l-k$. Therefore we can apply (i) of Theorem 3 to see that the number of element of $(g^{\perp}(X))$ is $4^{2l-(2l-k)} = 4^k$. By Lemma 5 we have that $C^{\perp} = (g^{\perp}(T))$.

(ii) Consider the first case of (ii). Since $k - h_t - l > 0$ the lowest degree of $g^{\perp}(X) = X^{k-h_t} + 2X^{-h_t+h_1} + 2X^{-h_t+h_2} + \cdots + 2 + 2X^{k-h_t-l}$ is 0, i.e., $\deg_L(g^{\perp}(X)) = 0$. Since $\deg(g^{\perp}(X)) = k - h_t$ we have that $l \deg_L(g^{\perp}) < \deg(g^{\perp})$. Hence we can apply the first case of Theorem 3(ii) to see that the number of elements of $(g^{\perp}(X))$ is $4^{(2l-k)+h_t}2^{2k-2l-2h_t}$. On the other hand, by writing out the generator matrix for $(g^{\perp}(X), 2X^{2l-k})$ we see that the number of elements of $(g^{\perp}(X), 2X^{2l-k})$ is $4^{(2l-k)+h_t}2^{2k-2l-2h_t}2^{h_t} = 4^{(2l-k)+h_t}2^{2k-2l-h_t}$. Now we see that this is the right number of elements for $C^{\perp}$. Hence $C^{\perp} = (g^{\perp}(T), 2T^{2l-k})$.

The second case is similar to the case considered above and we omit its proof.

Now consider the third case. By Theorem 3, we see that the number of elements of $(g^{\perp}(T))$ is 4^l. Now by writing out the generator matrix for $(g^{\perp}(T), 2T^{2l-k})$ we see that the number of elements of $(g^{\perp}(T), 2T^{2l-k})$ is $4^l 2^{k-l}$. Now it is immediate to show that it is the right number of elements for $C^{\perp}$. Hence $C^{\perp} = (g^{\perp}(T), 2T^{2l-k})$. □

Theorem 9. *Let $R = \mathbb{Z}_4[X]/(X^{2^n} - 1)$ and let $T = X - 1$. Let*

$$g(T) = T^k + 2T^{h_1} + 2T^{h_2} + \cdots + 2T^{h_t}$$

with $h_t < \cdots < h_1 < k < 2l$ and $l = 2^{n-1}$. Let C be the cyclic code $(g(T), 2T^r)$ generated by $g(T)$ and $2T^r$ then the dual $C^{\perp}$ is generated by;

(i) *if $\deg_L(T^{2l-k}g(T)) \geq k$), then $C^{\perp}$ is given by*

$$C^{\perp} = (T^{\lceil k-r,0 \rceil} g^{\perp}(T), 2T^{2l-k}),$$

(ii) *if $\deg_L(T^{2l-k}g(T)) < k$), then $C^{\perp}$ is given by*

$$C^{\perp} = \begin{cases} (T^{\lceil 2l-k+h_t-r,0 \rceil} g^{\perp}(T), 2T^{2l-k}) & \text{if } l + h_t < k \\ (T^{\lceil 2l-k+h_{t-1}-r,0 \rceil} g^{\perp}(T), 2T^{2l-k}) & \text{if } l + h_t = k \\ (T^{\lceil l-r,0 \rceil} g^{\perp}(T), 2T^{2l-k}) & \text{if } l < k < h_t + l \end{cases}$$

where $g^{\perp}(T)$ is given in Theorem 5 in each respective case.

Proof. We need to check that $C^{\perp}$ has the right number of elements by using Theorem 4.

(i) It is easy to show that $(T^{k-r}g^{\perp}(T), 2T^{2l-k})$ annihilate $g(T)$ and $2T^r$. Hence it suffices to show that $(T^{k-r}g^{\perp}(T), 2T^{2l-k})$ has the right number of elements. By Theorem 4, we see $(T^{k-r}g^{\perp}(T), 2T^{2l-k})$ has 4^r2^{k-r} elements. On the other hand, the number of elements of $(g(T), 2T^r)$ is $4^{2l-k}2^{k-r}$ as expected.

(ii) Consider the first case when $l + h_t < k$. If $2l - k + h_t < r$, then $g^{\perp}(T) \cdot 2T^r = 0$. Hence $g^{\perp}(T)$ and $2T^{2l-k}$ annihilates $g(T)$ and $2T^r$. To see $(g(T), 2T^r)^{\perp} = (g^{\perp}(T), 2T^{2l-k})$ we need to show that $(g(T), 2T^r)$ and $(g^{\perp}(T), 2T^{2l-k})$ have the right number of elements. Now the number of elements of $(g(T), 2T^r)$ is seen to be $4^{2l-k}2^{2k-2l-h_t}$. On the other hand, the number of elements of $(g^{\perp}(T), 2T^{2l-k})$ is $4^{2l-k+h_t}2^{2k-2l-h_t}$ which shows that $(g(T), 2T^r)^{\perp} = (g^{\perp}(T), 2T^{2l-k})$. If $2l - k + h_t \geq r$, then we have that $T^{2l-k+h_t-r}\ g^{\perp}(T) \cdot 2T^r = 0$. Therefore $T^{2l-k+h_t-r}g^{\perp}(T)$ and $2T^{2l-k}$ annihilate $(g(T), 2T^r)$. To see $(g(T), 2T^r)^{\perp} = (T^{2l-k+h_t-r}g^{\perp}(T), 2T^{2l-k})$ we need to check they have the right number of elements. In fact, the number of elements of $(g(T), 2T^r)$ is $4^{2l-k}2^{k-r}$ and the number of elements of $(T^{2l-k+h_t-r}g^{\perp}(T), 2T^{2l-k})$ is 4^r2^{k-r} as desired.

We omit the proof of the second case.

For the third case, if $r \geq l$, then $2T^r \cdot g^{\perp}(T) = 0$. Hence $g^{\perp}(T)$ and $2T^{2l-k}$ annihilates $(g(T), 2T^r)$. We claim that $(g(T), 2T^r)^{\perp} = (g^{\perp}(T), 2T^{2l-k})$. For this one checks that the number of elements of $(g(T), 2T^r)$ is $4^{2l-k}2^{k-l}$ and the number of elements of $(g^{\perp}(T), 2T^{2l-k})$ is 4^l2^{k-l} as desired. On the other hand, if $r < l$, then $T^{l-r}g^{\perp}(T)$ and $2T^{2l-k}$ annihilate $(g(T), 2T^r)$. To see in fact $(g(T), 2T^r)^{\perp} = (T^{l-r}g^{\perp}(T), 2T^{2l-k})$ we count the number of elements in each ideal. The number of elements of $(g(T), 2T^r)$ is $4^{2l-k}2^{k-r}$ and the number of elements of $(T^{l-r}g^{\perp}(T), 2T^{2l-k})$ is 4^r2^{k-r} as contented. □

7. Examples

Example 1. A nilpotent $\mathbb{Z}_4$ algebra with nilpotency 3.

Let $S = \mathbb{Z}_4[X]/(X^2 - 2X)$. It can be shown by direct computation or by using Propositions 4 and 5 that there are exactly 5 distinct proper ideals

$$(2), (X), (2X), (X + 2), (2, X).$$

In particular, the maximal ideal is the only one which is not principal.

The number of elements in the ideals and the duality among these ideals are given as follows.

$$\#(X + 2) = 4,\ (X + 2)^{\perp} = (X),\ \#(X) = 4;$$
$$\#(2X) = 2,\ (2X)^{\perp} = (X, 2),\ \#(X, 2) = 4 \cdot 2;$$
$$\#(2) = 2^2,\ (2)^{\perp} = (2).$$

Example 2. A nilpotent $\mathbb{Z}_4$ algebra with nilpotency 6.

Let $S = \mathbb{Z}_4[X]/(X^4 - 2X^2)$. Consider the possible choice for xr2 form $g(X)$ in terms of degree.

If $\deg g = 1$, then there are two possible xr2 form are $\{X, X+2\}$. For $g(X) = X$ the only possible 2xr form to adjoin is 2 to form the maximal ideal $(X, 2)$.

If $\deg g = 2$, then the possible xk2 forms are

$$\{X^2, X^2+2, X^2+2X, X^2+2X+2\}.$$

The possible 2xr forms we can adjoin to X^2 are $\{2X, 2\}$; and we can adjoin $2X$ to X^2+2.

If $\deg g = 3$, then the possible xk2 forms are

$$\{X^3, X^3+2, X^3+2X+2, X^3+2X^2+2, X^3+2X^2+2X, X^3+2X^2+2X+2\}.$$

The possible 2xr forms we can adjoin to X^3 are $\{2X^2, 2X, 2\}$; the possible 2xr form we can adjoin to X^3+2X+2 is $\{2X^2\}$; the possible 2xr form we can adjoin to X^3+2 are $\{2X^2, 2X\}$.

Let $g(X) = X^3+2X+2$. Then $l + h_t = 2 + 0 < k = 3$. Hence the number of elements of $(g(X))$ is $4 \cdot 2^2$. And $g^{\perp}(X) = X^3 + 2$ with $\#(g^{\perp}(X)) = 4 \cdot 2^2$.

Consider $I = (g(X), 2X^2)$ with $g(X) = X^3 + 2X$. Then $\#I = 4 \cdot 2$. $\mathrm{Ann}(g(X)) = X^3 + 2X + 2$ and $\mathrm{Ann}(g(X), 2X^2) = (X^3 + 2X + 2, 2X) = (X^3 + 2, 2X)$.

Example 3. A cyclic code of length 8 over $\mathbb{Z}_4$.

Let C be the cyclic code generated by $g(T) = T^5+2T^2+2T$ and $r(T) = 2T^4$. Then by Theorem 3, we see that the number of elements of C is $4^3 \cdot 2$. By Theorem 6(i), we see that the dual $C^{\perp}$ of C is generated by $T^4 + 2T$ and $2T^3$. By Theorem 3, the number of elements of $C^{\perp}$ is $4^4 \cdot 2$.

References

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

[2] S. T. Dougherty and Y. H. Park, *On modular cyclic codes*, Finite Fields Appl. **13** (2007), no. 1, 31–57.

[3] P. Kanwar and S. R. López-Permouth, *Cyclic codes over the integers modulo p^m*, Finite Fields Appl. **3** (1997), no. 4, 334–352.

[4] Bernard R. McDonald, *Finite Rings with Identity*, Marcel Dekker, 1974.

[5] S. S. Woo, *Free cyclic codes over finite local rings*, Bull. Korean Math. Soc. **43** (2006), no. 4, 723–735.

[6] ———, *Ideals of $\mathbb{Z}_{p^n}[X]/(X^l - 1)$*, Commun. Korean Math. Soc. **26** (2011), no. 3, 427–443.

[7] ———, *Cyclic codes of even length over $\mathbb{Z}_4$*, J. Korean Math. Soc. **44** (2007), no. 3, 697–706.

Department of Mathematics
Ewha Women's University
Seoul 120-750, Korea
E-mail address: sswoo@ewha.ac.kr