Bull. Korean Math. Soc. **43** (2006), No. 4, pp. 723–735

FREE CYCLIC CODES OVER FINITE LOCAL RINGS

SUNG SIK WOO

ABSTRACT. In [2] it was shown that a 1-generator quasi-cyclic code C of length $n = ml$ of index l over $\mathbb{Z}_4$ is free if C is generated by a polynomial which divides $X^m - 1$. In this paper, we prove that a necessary and sufficient condition for a cyclic code over $\mathbb{Z}_{p^k}$ of length m to be free is that it is generated by a polynomial which divides $X^m - 1$. We also show that this can be extended to finite local rings with a principal maximal ideal.

1. Introduction

For a commutative ring A a *linear code* C of length n over A is an A-submodule of A^n. A linear code of length $n = lm$ is called an *quasi-cyclic code* of index l if it is invariant under cyclic shift by l position. When $l = 1$ we simply say that C is a *cyclic code*. It is well known that a cyclic code can be identified with an ideal of $R := A[X]/(X^m - 1)$ and a quasi-cyclic code with a submodule of R^l.

In [2], it was shown that a quasi-cyclic code over $\mathbb{Z}_4$ generated by a single polynomial which divides $X^m - 1$ is free. In this paper we show that a cyclic code C over a finite commutative local ring T is free if and only if C is generated by a polynomial dividing $X^m - 1$. For its proof we divide into two cases; first we consider the case when $T = \mathbb{Z}_{p^k}$ with $(m, p) = 1$ (§3) and then we consider the case m is divisible by p (§4). Even though the proof for the latter can be used for the former case, we provide separate proofs because they give us better understanding for the free cyclic codes in each case. We then show that these results can be extended to arbitrary finite commutative rings (§5).

Received April 21, 2005.

2000 Mathematics Subject Classification: 13C10.

Key words and phrases: free modules over a finite commutative rings, separable extension of local rings, cyclic codes over $\mathbb{Z}_{p^k}$.

This work was supported by the Intramural Research Grant of Ewha Women's University.

In §6, we consider the dual of free cyclic codes. It turns out that no free cyclic codes are self dual. However, we can construct many quasi-cyclic codes whose duals are equivalent to itself.

Throughout this paper a ring means a commutative ring with the identity element 1. Especially the coefficient ring will be a finite commutative local rings unless otherwise stated.

2. Polynomials over finite rings

In this section we collect the results which we will use in the next sections. We sometimes provide proofs which can be easily derived from the results already known.

Let A be a finite local ring with the maximal ideal $\mathfrak{m}$ and the residue field $A/\mathfrak{m} = k$. Also write the canonical map $\mu : A \to k$. When k is a finite field $\mathbb{Z}_p$ with p elements, we often write $\mathbb{F}_p$ for the field $\mathbb{Z}_p$. A polynomial $f \in A[X]$ is said to be *basic irreducible* if $\mu(f)$ is irreducible in $k[X]$.

Now suppose A is a finite local ring with the maximal ideal $\mathfrak{m}$. We know that the ideal $\mathfrak{m}$ is nilpotent. See for example [6] or [1, Ch.8]. A polynomial $f \in A[X]$ is called *regular* if the coefficients of f generate the unit ideal. A polynomial $f \in A[X]$ is a *primary polynomial* if the ideal generated by f is a primary ideal of $A[X]$.

We have a characterizing property for the primary polynomials.

PROPOSITION 1([6, XIII.12]). *Suppose A is a finite local ring with the maximal ideal $\mathfrak{m}$. A regular polynomial $f \in A[X]$ is primary polynomial if and only if f is of the form $f = \delta\Pi^h + \beta$, where Π is basic irreducible, $\beta \in \mathfrak{m}[X]$ and δ a unit.*

We have an unique factorization theorem for polynomials over a finite local rings similar to the unique factorization of polynomials over a field.

PROPOSITION 2([6, XIII.11]). *Let R be a finite local ring. Let $f \in R[X]$ be a regular polynomial. Then f can be written as a product $f = uf_1f_2\cdots f_k$ where f_i are primary regular coprime polynomials. This expression is unique in the sense that if $f = vg_1g_2\cdots g_l$ then $k = l$ and $(f_i) = (g_i)$ after renumbering if necessary.*

If $\mu(f)$ is a separable polynomial in $\mathbb{F}_p[X]$ (i.e., $\mu(f)$ has no multiple root), then we can use Hensel's lemma to obtain a stronger result.

COROLLARY [4]. *Let R be a finite local ring and let $f \in R[X]$. If $\mu(f)$ has distinct roots, then f can be written as a product $f = uf_1f_2\cdots f_k$*

where f_i are basic irreducible coprime polynomials. This expression is unique in the sense that if $f = vg_1g_2\cdots g_l$, then $k = l$ and $f_i = v_ig_i$ for some unit v_i after renumbering if necessary. In particular, $X^m - 1 \in \mathbb{Z}_{p^k}[X]$ can be written as a product of distinct monic basic irreducible polynomials when $(m, p) = 1$.

When R is finite local and f is a primary polynomial over R, it is easy to show that the quotient ring $R[X]/(f)$ is again local.

LEMMA 1. *Let R be a finite local ring with the principal maximal ideal $\mathfrak{m} = (\pi)$. If $f = \delta\Pi^h + \beta \in R[X]$ is a primary polynomial with $\beta \in \mathfrak{m}[X]$ and Π a basic irreducible, then $R[X]/(f)$ is a local ring.*

Proof. Since π is nilpotent, we see $\pi \in \mathrm{rad}(f)$. Hence $\Pi \in \mathrm{rad}(f)$ also. Hence $\mathrm{rad}(f) \supset (\pi, \Pi)$. But (π, Π) is a maximal ideal. Hence we have that $\mathrm{rad}(f) = (\pi, \Pi)$ is a maximal ideal which we denote by $\mathfrak{M}$. Hence $\bar{\mathfrak{M}}$ is a maximal ideal of $R[X]/(f)$. Suppose $\mathfrak{N}$ is another maximal ideal containing (f). Then $\mathfrak{N} \supset \mathrm{rad}(f) = \mathfrak{M}$. Hence $\mathfrak{M} = \mathfrak{N}$. □

Let R be a finite ring. A polynomial $f \in R[X]$ is said to be *local* if $R[X]/(f)$ is a local extension of R. Therefore a primary polynomial over a finite local ring is a local polynomial by Lemma 1.

Let R, S be commutative rings with $R \subset S$. Let $S^e = S \otimes_R S$. Then S becomes an S^e-module under $(a_1 \otimes a_2)a = a_1aa_2$. We say S is *R-separable* (or S is a *separable extension* of R) if S is a projective S^e-module. A regular polynomial $f \in R[X]$ is said to be *separable* if $R[X]/(f)$ is a local separable extension of R.

We have the equivalent conditions to separability of local extensions.

THEOREM 1([6, XIV 3,6,8]). *Let R, S be a finite local rings with $R \subset S$ and with the maximal ideals $\mathfrak{m}$ and $\mathfrak{M}$ of R and S respectively. Then the following conditions are equivalent.*

(i) *S is a separable extension of R.*

(ii) *$S/\mathfrak{m}S$ is a separable extension of $R/\mathfrak{m}R$.*

(iii) *S is an unramified extension of R, i.e., $\mathfrak{m}S = \mathfrak{M}$.*

(iv) *$S \cong R[X]/(f)$ for some monic basic irreducible polynomial $f \in R[X]$.*

A successive extension of separable extensions is separable.

COROLLARY. *Besides the equivalent conditions of Theorem 1, further assume S' is a separable extension of S. Then S' is a separable extension of R.*

Proof. If $\mathfrak{M}'$ is the maximal ideal of S' then $\mathfrak{M}' = \mathfrak{M}S' = \mathfrak{m}SS' = \mathfrak{m}S'$. □

Note that a finite ring is necessarily Artinian. Hence a finite local ring has nilpotent maximal ideal [1, Proposition 8.6]. See [1] for the details. We have conditions for an Artinian local ring to have a principal maximal ideal.

PROPOSITION 3. [1, p.91] *Let R be an Artinian local ring with the maximal ideal $\mathfrak{m}$ and the residue field $k = R/\mathfrak{m}$. Then the following conditions are equivalent:*

(i) *every ideal of R is principal which is a power of $\mathfrak{m}$.*

(ii) *the maximal ideal $\mathfrak{m}$ is principal.*

(iii) $\dim_k(\mathfrak{m}/\mathfrak{m}^2) \leq 1$.

A separable extension of a local ring having a principal maximal ideal also have a principal maximal ideal.

COROLLARY 1. *Let S be a local extension of a finite local ring R. Let $\mathfrak{M}$ and $\mathfrak{m}$ be the maximal ideals of S and R respectively. Suppose $\mathfrak{m}$ is principal and S is a separable extension of R. Then every ideal of S is principal which is a power of $\mathfrak{M}$ that is also principal.*

Proof. Let $(r) = \mathfrak{m}$. By Theorem 1, $\mathfrak{M} = \mathfrak{m}S = (r)S$ which is the principal ideal (r) of S. Hence by Proposition 3, every ideal of S is a power of $\mathfrak{M}$ which is also principal. □

Combining these results and specializing to $T = \mathbb{Z}_{p^m}$, we have:

COROLLARY 2. *Let T be a finite local ring with the maximal ideal $\mathfrak{m}$ which is principal say $\mathfrak{m} = (\pi)$. Let $f(X) \in T[X]$ be a basic irreducible polynomial. Then every ideal of $T[X]/(f)$ is principal, say a power of (π). In particular, every ideal of $\mathbb{Z}_{p^n}[X]/(f)$ is principal, say a power of (p).*

Proof. Write $R = T[X]/(f)$. Since f is basic irreducible, we see R is a separable extension of T. We know that R is a local ring with the maximal ideal say $\mathfrak{M}$. By Corollary 1, $\mathfrak{M}$ is also principal namely $\mathfrak{M} = (\pi) = \pi R$ for some π. Now by Proposition 3, every ideal of R is a power of the maximal ideal $(\pi) \subset R$. □

Glueing these together by using Chinese Remainder Theorem, we obtain:

COROLLARY 3. *Let T be a finite local ring with the maximal ideal $\mathfrak{m}$ which is principal, say $\mathfrak{m} = (p)$. Let $f \in T[X]$ be a polynomial which can be written as a product of monic basic irreducible polynomials. Then every ideal of $T[X]/(f)$ is principal. In particular, every ideal of $\mathbb{Z}_{p^k}[X]/(X^m - 1)$ is principal if $(m, p) = 1$.*

An explicit formula for the generator g of I in terms of f_i's is given in [4] when $f(X) = X^m - 1$.

3. Free cyclic codes of length m over $\mathbb{Z}_{p^k}$ with $(m, p) = 1$

In this section, we denote the ring $\mathbb{Z}_{p^k}$ by T. We first consider the case when $(m, p) = 1$ in which case the polynomial $X^m - 1$ is a product of basic irreducible polynomials by Corollary to Proposition 2. Then we first show that $R = T[X]/(X^m - 1)$ is a direct sum of separable extensions of T. From this, we show that a cyclic code is free if and only if C is generated by a polynomials which divide $X^m - 1$.

We need a criterion of freeness for a module over a local ring with a nilpotent maximal ideal. The following is an adaption of [3, II.3.2 Proposition 5] for our purpose.

PROPOSITION 4. [3] *Let A be a local ring with the maximal ideal $\mathfrak{m}$ which is nilpotent. Let M be an A-module. Then M is free if and only if the natural map $\mathfrak{m} \otimes_A M \to M$ is injective.*

COROLLARY. *Let A be a local ring with the maximal ideal $\mathfrak{m}$ which is nilpotent. Then $M_1 \oplus M_2$ is free if and only if M_1 and M_2 are free.*

Proof. Simply note that $\mathfrak{m} \otimes (M_1 \oplus M_2) \to M_1 \oplus M_2$ is injective if and only if $\mathfrak{m} \otimes M_i \to M_i (i = 1, 2)$ are injective. □

If $A = \mathbb{Z}_{p^k}$, then this can be also deduced from the theorem of classification of finite abelian groups. Also, note that this is false if A is not local as an easy example shows: Let $A = \mathbb{Z}/6$ which is not local. Then $A \cong \mathbb{Z}/2 \oplus \mathbb{Z}/3$ is free but none of $\mathbb{Z}/2$ or $\mathbb{Z}/3$ is A-free.

For this we look at the modules over a separable extensions of T. Let R be a subring of S and let N be an S-module. Then N can be viewed as an R-module as well. In general it is not true that a free S-module N is R-free when we view N as an R-module. However if S is a separable extension, then we have affirmative answer.

LEMMA 2([6, XIV.4]). *Let S be a local ring containing R. Suppose S is a separable extension of R and N is an S-module which is R-free. Then N is S-free. In particular, if S is R-free, then N is S-free if and only if N is R-free.*

Let $T = \mathbb{Z}_{p^k}$ and let $R = T[X]/(X^m - 1)$ with $(m, p) = 1$. Then we can write $(X^m - 1)$ as a product of monic basic irreducible polynomials, say $(X^m - 1) = f_1 f_2 \cdots f_t$ by Corollary to Proposition 2. Then, by Theorem 1, $S_j = T[X]/(f_j)$ is a separable extension of T for each j.

We first need a simple fact.

LEMMA 3. *Let $T = \mathbb{Z}_{p^k}$ and let $S = T[X]/(f)$ with f a basic irreducible. Then an ideal I of S is T-free only if I is the unit ideal of S.*

Proof. A nonzero ideal I is T-free if and only if I is S-free. But the number of elements of any proper ideal of S contains less elements than the number of elements of S. Hence I cannot be S-free. Accordingly I cannot be T-free either. □

Now we have a necessary and sufficient condition for C to be T-free for the case when $(m, p) = 1$.

THEOREM 2. *Let C be a cyclic code of length m with $(m, p) = 1$. Then C is T-free if and only if there is a polynomial g such that $g|(X^m - 1)$ which generate C. In this case, we have* $\mathrm{rank}_T(C) = m - \deg(g)$.

Proof. Write $R = \bigoplus_{j=1}^{t} S_j$ with $S_j = T[X]/(f_j)$ where $f_1, f_2, \ldots, f_t$ are relatively coprime monic basic irreducibles. Now C being an ideal of $R = \bigoplus S_j$, we have $C = \bigoplus (C \cap S_j)$ where $C \cap S_j$ is an ideal of S_j. By Corollary to Proposition 4, C is T-free if and only if $C \cap S_j$ is T-free for all j. This is equivalent to that $C \cap S_j$ is S_j-free. Since $C \cap S_j$ is an ideal of S_j, it can be S_j-free only if $C \cap S_j = S_j$ by Lemma 4. Therefore for C to be T-free, it is necessary and sufficient that $C \cap S_j$ is either 0 or S_j. That is, $C = S_{i_1} \oplus \cdots \oplus S_{i_l}$ where S_{i_j} is one of the factors of $R = \bigoplus_{j=1}^{t} S_j$. By Corollary 3 to Proposition 3 or by [4], C is a principal ideal, say (g) for some monic polynomial g dividing $X^m - 1$ as desired.

As for the rank, simply note that $\mathrm{rank}_T(R/C) = \mathrm{rank}_T T[X]/(g) = \deg(g)$. □

COROLLARY. *Let $(m,p)=1$. Then a cyclic code C is free if and only if $C \cap S_j$ is either 0 or S_j for all j.*

Proof. We proved this in the course of the proof of Theorem 2. □

4. Free cyclic codes of length n over $\mathbb{Z}_{p^k}$ with $(n,p) \neq 1$

Let $T = \mathbb{Z}_{p^k}$ and let $\mathfrak{m} = (p)$ be the maximal ideal of T. Now consider the case when m is not necessarily relatively prime to p. Let $X^m - 1 = f_1 \cdots f_t$ be a factorization into monic (regular) primary coprime polynomials. Let $S_i = T[X]/(f_i)$. Then S_i is a local extension of T by Lemma 1, but no longer a separable extension of T. We need to look at the ideals of $S = T[X]/(f)$ where f is a primary factor of $X^m - 1$. Let $f = \Pi^e + \beta$ be one of f_i with a basic irreducible Π and $\beta \in \mathfrak{m}[X]$ and let $\mathfrak{M}$ be the maximal ideal of $S = T[X]/(f)$. (See Lemma 1.) Then $pS \subset \mathfrak{M}$ and $\mathfrak{M} = (p, \Pi) = \mathrm{rad}((f))$.

By Proposition 3, *not* every ideal of S is a power of $\mathfrak{M}$ nor principal. However we have the same result as Lemma 4 where we needed the separability. First we will use a simple fact:

LEMMA 4. *If f, g are regular polynomials in $T[X]$, then so is fg. In particular, a product of two regular polynomials is nonzero.*

Proof. We know f is regular if and only if $\mu(f)$ is regular [6, Theorem XIII.2]. But $\mu(fg) = \mu(f)\mu(g) \neq 0$ in $\mathbb{F}_p[X]$. □

Now we need a criterion for an element in a tensor product of two modules to be zero.

LEMMA 5 ([3, I.2.11]). *Let A be a commutative ring and E, F be A-modules. Let $\{e_1, \ldots, e_n\}$ be a set of generators of E. An element $z = \sum_{i=1}^{n} e_i \otimes f_i$ in $E \otimes_A F$ is zero if and only if there is a set $\{a_{ij} | 1 \leq i, j \leq n\}$ in A and $\{x_1, \ldots, x_n\}$ in F such that $\sum_{j=1}^{n} a_{ij} e_j = 0$ and $f_j = \sum_{i=1}^{n} a_{ij} x_i$ for all i, j.*

We will apply this to a module E with a single generator:

COROLLARY. *Let $e \in E$ be a generator and $f \in F$. Then $e \otimes f = 0$ if and only if there are $a \in A$ and $x \in F$ satisfying $ae = 0$ and $ax = f$.*

Now we can prove a key fact:

PROPOSITION 5. *Let $T = \mathbb{Z}_{p^k}$. Let $S = T[X]/(f)$ where $f = \Pi^e + p^i g$ with g regular and Π a monic basic irreducible in $T[X]$. Let I be a proper ideal (nonzero and nonunit ideal) of S. Then I is not T-free.*

Proof. Let $\mathfrak{m} = (p) \subset T$ be the maximal ideal. Since $I \subset \mathfrak{M} = (\Pi, p)$ we see every element of I is of the form $a\Pi + bp$.

First, suppose $p|a$ whenever $a\Pi + pb \in I$. Then $I \subset (p)$. In this case choose the smallest r for which p^r divide all elements of I. Let $0 \neq p^r x \in I$ with $x \notin (p)$ and let $p^{r+a}x = 0$. Then $a < k$ since $r > 0$. Now we see $p^a \otimes p^r x = p \otimes p^{a-1}(p^r x)$ is nonzero element of $\mathfrak{m} \otimes_T I$ by Corollary to Lemma 6. (Apply Corollary to Lemma 6 with $e = p$, $a = p^{k-1}$ and $f = p^{a-1}(p^r x)$. We have then that f is not a multiple of p^{k-1} since $a < k$.) Now $p^a \otimes p^r x$ is mapped to $p^{r+a}x = 0$ in I under the map $\mathfrak{m} \otimes_T I \to I$.

Now suppose there is $a\Pi + pb \in I$ for which $p \nmid a$, i.e., a is regular. Then we have

$$\begin{aligned}(a\Pi + pb)^e &= a^e\Pi^e + p(\text{a polynomial}) \\ &= -a^e(p^i g) + p(\text{a polynomial}).\end{aligned}$$

Since a, g are regular, $a^e g$ is also regular by Lemma 5. In particular, $(a\Pi + pb)^e$ is nonzero and divisible by p. Choose the smallest r for which $p^r|(a\Pi + pb)^e$. Write $(a\Pi + pb)^e = p^r x$ and let $p^{r+a}x = 0$. Then, as before, $p^a \otimes p^r x = p \otimes p^{r+a-1}x$ is a nonzero element of $\mathfrak{m} \otimes_T I$ by Corollary to Lemma 6 which is mapped to $p^{r+a}x = 0$ in I as before.

Therefore in either case the natural map $\mathfrak{m} \otimes I \to I$ is not injective. Hence I is not T-free by Proposition 4. □

REMARK. Since the basic irreducible polynomials are primary, Lemma 4 is a consequence of Proposition 5. However two different proofs gives us better understanding for free cyclic codes.

Now we can characterize the free cyclic codes over $\mathbb{Z}_{p^k}$ of length n for the case $(n, p) \neq 1$. As expected, the conclusion is the same as the case when $(n, p) = 1$.

THEOREM 3. *Let $T = \mathbb{Z}_{p^k}$. Let C be a cyclic code of length m over T. Then C is T-free if and only if there is a polynomial g such that $g|(X^m - 1)$ which generate C. In this case, we have* $\text{rank}_T(C) = m - \deg(g)$.

Proof. The proof is the same as the proof of Theorem 2 except we need to use Proposition 5 instead of Lemma 4. □

Using the same notations as the previous section, we have the following.

COROLLARY. *Let C be a cyclic code of length m over $\mathbb{Z}_{p^k}$ for any n and p. Then C is free if and only if $C \cap S_j$ is either 0 or S_i for all j.*

Proof. It follows from the fact that no proper ideal of S_i is free. □

5. Cyclic codes of length n over finite local rings

The result we obtained so far can be extended to finite local rings with the principal maximal ideals.

PROPOSITION 6. *Let T be a finite local ring with the maximal ideal $\mathfrak{m}$. Suppose $\mathfrak{m}$ is principal, say $\mathfrak{m} = (\pi)$. Let $S = T[X]/(f)$ where $f = \Pi^e + \pi^i g$ with g regular and Π a monic basic irreducible. If I is a proper ideal, then I is not T-free.*

Proof. The proof of Proposition 5 goes through if we replace p by π. Note that $\pi^n = 0$ for some n. □

THEOREM 4. *Let T be a finite local ring whose maximal ideal is principal. Let C be a cyclic code of length m. Then C is T-free if and only if there is a polynomial g where $g|(X^m - 1)$ which generate C. In this case, we have* $\mathrm{rank}_T(C) = m - \deg(g)$.

Proof. We use Proposition 6 and the rest of the proof is the same as the proof of Theorem 3. □

COROLLARY. *Let C be a cyclic code of length m over a finite local ring T. Then C is free if and only if $C \cap S_j$ is either 0 or S_j for all j.*

6. Duality of free cyclic codes

So far we obtained a necessary and sufficient condition for a cyclic code over $\mathbb{Z}_{p^k}$ to be free. With this characterization of free cyclic codes it is easy to find its dual by using the results of [4]. It turns out that no free cyclic code over $\mathbb{Z}_{p^k}$ is self dual. In this section we restrict our attention to $T = \mathbb{Z}_{p^k}$ for simplicity.

As usual for a polynomial f of degree n, we define the reciprocal polynomial f^* by $f^*(X) = X^n f(X^{-1})$. Then we have $f^{**} = f$, $(fg)^* = f^*g^*$ and $(f+g)^* = f^* + g^*$. For a divisor $g(X)$ of $X^m - 1$, we define $\hat{g}$ to be the polynomial $\hat{g}(X) = \frac{X^n-1}{g(X)}$.

First we consider the case of a cyclic code of length m over $\mathbb{Z}_{p^k}$ where $(m,p) = 1$. In this case, the dual code $C^\perp$ can be described explictly in terms of generators [4, Theorem 4.2].

THEOREM 5 [4]. *Let $(n,p) = 1$ and*

$$C = (\hat{F}_1, p\hat{F}_2, \ldots, p^{n-1}\hat{F}_n),$$

where $F_0F_1 \cdots F_n = X^m - 1$. Then

$$C^\perp = (\hat{F}_0^*, p\hat{F}_n^*, p^2\hat{F}_{n-1}^*, \ldots, p^{n-1}\hat{F}_2^*).$$

For our purpose we need just one factor without p-part.

COROLLARY 1. *Let $(m,p) = 1$ and let C be the cyclic code $C = (g)$ generated by the polynomial g with $g|(X^m - 1)$. Then the dual code $C^\perp$ is given by $C^\perp = (\hat{g}^*)$. In particular, a free cyclic code $C = (g)$ is self dual if and only if g is an associate of $\hat{g}^*$.*

COROLLARY 2. *Let $(m,p) = 1$. Let C be a free cyclic code generated by the polynomials $g_1, \ldots, g_l$ with $g_i|(X^m - 1)$, i.e., $C = \bigoplus_{i=1}^{l}(g_i)$. Then we have $C^\perp = \bigoplus_{i=1}^{l}(\hat{g}_i^*)$.*

Even if $p|n$, when a cyclic code C is generated by a factor without p-part, the corollary above still holds.

PROPOSITION 7. *Let $C = (g)$ be the free cyclic code generated by the polynomial g with $g|(X^n - 1)$. Then the dual code $C^\perp$ is given by $C^\perp = (\hat{g}^*)$. Further if C is a free cyclic code generated by the polynomials $g_1, \ldots, g_l$, where $g_i|(X^m - 1)$, i.e., $C = \bigoplus_{i=1}^{l}(g_i)$, then $C^\perp = \bigoplus_{i=1}^{l}(\hat{g}_i^*)$. In particular, a free cyclic code $C = (g)$ is self dual if and only if $(g) = (\hat{g}^*)$.*

Proof. The same proof of [4, Theorem 4.2] works in our case. □

Let $X^n - 1 = f_1 f_2 \cdots f_s$ be a factorization into primary coprime polynomials. Then $(X^n - 1)^* = -(X^n - 1) = f_1^* f_2^* \cdots f_s^*$. By the

uniqueness of factorization (Proposition 2), we let $g_1, \ldots, g_t$ to be those f_i's for which $(g_i^*) = (g_i)$ and we let $h_1, \ldots, h_r, h'_1, \ldots, h'_r$ to be those f_i's for which $(h_j^*) = (h'_j)$. Therefore we can write

$$(*) \qquad X^n - 1 = g_1 \cdots g_t h_1 \cdots h_r h'_1 \cdots h'_r.$$

When C is a cyclic code $C = (g)$ with $g|(X^n - 1)$, then we get an easy criterion for C to be self dual.

COROLLARY 1. *Let $C = (g)$ be a T-free cyclic code of length n with $g|(X^n - 1)$. Let $X^n - 1$ have factorization as in $(*)$ above. Then C is self dual if and only if $t = 0$ and $g = h_1 \cdots h_r$.*

Proof. Let $g = g_1 \cdots g_a h_1 \cdots h_b h'_1 \cdots h'_c$ after renumbering if necessary. Then $\hat{g}^* = g_{a+1} \cdots g_t h'_{b+1} \cdots h'_r h_{c+1} \cdots h_r$. By Proposition 7, we need to find a necessary and sufficient condition for $(g) = (\hat{g}^*)$. Note that these factors are distinct. Now it is clear that $(g) = (\hat{g}^*)$ if and only if $t = 0$, $b = r$ and $c = 0$. □

COROLLARY 2. *There is no self-dual free cyclic code of length n over $\mathbb{Z}_{p^k}$.*

Proof. We simply note that $f(X) = X - 1$ is a divisor of $X^n - 1$ such that f^* is an associate of f. □

On the other hand, we have an abundance of 'quasi' self-dual quasi-cyclic codes. Let T be a commutative ring. A cyclic code of length $n = lm$ over T can be viewed as a linear code over $R = T[X]/(X^m - 1)$ as in the case of a finite field [5].

Let C be a cyclic code over T of length $n = lm$ and index l. Let

$$\mathbf{c} = (c_{00}, c_{01}, \ldots, c_{0,l-1}, c_{10}, \ldots, c_{1,l-1}, \ldots, c_{m-1,0}, \ldots, c_{m-1,l-1})$$

be a coded word in C. We define a map

$$\phi : T^n \to R^l$$

by

$$\phi(\mathbf{c}) = (\mathbf{c}_0(X), \mathbf{c}_1(X), \ldots \mathbf{c}_{l-1}(X))$$

where

$$\mathbf{c}_j(X) = \sum_{i=0}^{m-1} c_{ij} X^i \in R.$$

Then ϕ transforms a cyclic code to a linear code of R^l. Further the correspondence set up a bijection between the cyclic codes of length n with index l and the linear codes of R^l as for the case over a finite field [5]:

LEMMA 6. *The map ϕ defines a one-to-one correspondence between cyclic codes over T of index l and length $n = lm$ and linear codes of length l over R.*

Let $\mathcal{A}$ be the subgroup of all $n \times n$ invertible matrices $\mathrm{GL}(n, \mathbb{Z}_{p^k})$ over $\mathbb{Z}_{p^k}$ generated by transpositions of coordinates and by multiplication of i-th position by elements of $\mathbb{Z}_{p^k}^*$, the group of units of $\mathbb{Z}_{p^k}$. As for the codes over a finite field, we define two codes C and C' are *equivalent* if there is $\alpha \in \mathcal{A}$ such that $C' = \alpha(C)$.

THEOREM 6. *Let $T = \mathbb{Z}_{p^k}$. Let C be a free quasi-cyclic code generated by the polynomials $g_1, \ldots, g_l$ where $g_i | (X^m - 1)$ i.e., $C = \bigoplus_{i=1}^{l} (g_i)$. Then $C^\perp$ is equivalent to C if and only if l is even and $(g_i) = (\hat{g}_j^*)$ (equivalently $(\hat{g}_i) = (g_j^*)$) for distinct indices i and j.*

Proof. By Proposition 7, we have $(\bigoplus_{i=1}^{l} (g_i))^\perp = \bigoplus_{i=1}^{l} (\hat{g}_i^*)$. Hence $\bigoplus_{i=1}^{l} (\hat{g}_i^*)$ is equivalent to $\bigoplus_{i=1}^{l} (g_i)$ if and only if $(g_i) = (\hat{g}_j^*)$ for distinct indices i and j and accordingly l must be even. □

EXAMPLE. A 'quasi' self-dual free cyclic code over $\mathbb{Z}_9$.

Let $R = \mathbb{Z}_9[X]/(X^8 - 1)$ and consider the free cyclic code of R^2 generated by $g_1 = f_0 f_1 f_2$ and $g_2 = f_3 f_4$ in the notations of Example 1. Then $\hat{g}_1 = g_2 = f_3 f_4$ and $g_2^* = (-f_4)(-f_3)$. Hence $\hat{g}_1$ and g_2^* are associates. Hence the cyclic codes generated by g_1 and g_2 are 'quasi' self dual cyclic codes of length 16 and index 2 by Theorem 6.

References

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

[2] N. Aydin and D. K. Ray-Chaudhuri, *Quasi-cyclic codes over $\mathbb{Z}_4$ and some new binary codes*, IEEE Trans. Inform. Theory **48** (2002), no. 7, 2065–2069.

[3] N. Bourbaki, *Elements of Mathematics, Commutative Algebra*, Addison-Wesley, 1972.

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

[5] S. Ling and P. Solé, *On the algebraic structure of cyclic code I: finite fields*, IEEE Transactions on Information Theory **47** (2001), no. 7, 2751–2760.

[6] B. R. McDonald, *Finite rings with identity*, Marcel Dekker, 1974.

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