Free Cyclic Codes as Invariant Submodules over Finite Chain Rings

Mingzhong Wu

Department of Mathematics, China West Normal University
Nanchong, Sichuan, 637002, P.R. China
m.z.wu@163.com

Copyright © 2013 Mingzhong Wu. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract

By applying the theory of linear algebra, one can obtain some properties of these codes which generalize several well known results for free cyclic codes represented in [1, 4].

Mathematics Subject Classification: 94B05, 11T71, 47A15

Keywords: finite chain rings, free cyclic codes, invariant submodules

1 Preliminary Notes

Let R be a finite chain ring and R^n the R -module of rank n consisting of row vectors over R . We write $R^n = \{(a_0, a_1, \dots, a_{n-1}) \mid a_i \in R, i = 0, 1, \dots, n-1\}$. An R -submodule $\mathcal{C}$ of R^n is called a cyclic code of length n if $(a_{n-1}, a_0, \dots, a_{n-2}) \in \mathcal{C}$, for all $(a_0, a_1, \dots, a_{n-1}) \in \mathcal{C}$.

We set $T = \begin{pmatrix} 0 & I_{n-1} \\ 1 & 0 \end{pmatrix} \in M_n(R)$, where I_{n-1} is the identity matrix of order $n-1$, and denote by ε_i the vector in R^n with zeros everywhere but in position i that holds, $i = 0, 1, \dots, n-1$. Then $\{\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1}\}$ is the standard R -basis of R^n . We denote by $\mathcal{T}$ the set of R -linear transformation of R^n . Then $\mathcal{T}$ is an R -algebra with operations of linear transformations and scalar multiplications with elements of R .

Let

$$\begin{aligned}\tau : \quad R^n &\rightarrow R^n \\ (a_0, a_1, \dots, a_{n-1}) &\mapsto (a_{n-1}, a_0, \dots, a_{n-2})\end{aligned}$$

Then $\tau \in \mathcal{T}$ and it has the matrix T with respect to the basis $\{\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1}\}$. Note that the minimal polynomial of T is $f(x) = x^n - 1$. Let $\gcd(n, p) = 1$, where p is the characteristic of R . Let $f(x) = f_1(x)f_2(x)\dots f_r(x)$ be the factorization of $f(x)$ into coprime monic basic irreducible factors over R . According to the Theorem Cayley-Hamilton, the matrix T satisfies $f(T) = 0$. Consider the homogeneous set of equations $f_i(A)X = 0, X \in R^n$, for $i = 1, 2, \dots, r$. If U_i stands for the solution module of $f_i(A)X = 0, X \in R^n$, then we write $U_i = \text{Ker } f_i(\tau)$. One can verify that each U_i is a free R -module.

Lemma 1.1 *The submodules U_i of R^n satisfy the following statements:*

- (1) U_i is a free τ -invariant submodule of R^n ;
- (2) if W is a free τ -invariant submodule of R^n and $W_i = W \cap U_i$ for $i = 1, 2, \dots, r$, then W_i is free τ -invariant and $W = \bigoplus_{j=1}^r W_j$;
- (3) $R^n = \bigoplus_{j=1}^r U_j$;
- (4) $\text{rank}(U_i) = \deg(f_i)$;
- (5) $f_i(x)$ is the minimal polynomial of τ over U_i ;
- (6) U_i is the minimal free τ -invariant submodule of R^n ;
- (7) for any free submodule U of R^n , U is the direct sum of some of minimal free τ -invariant submodules U_i of R^n .

2 Main Results

Theorem 2.1 *Let $\mathcal{C}$ be a free cyclic code of length n over R . Then the following facts hold.*

- (1) $\mathcal{C} = U_{i_1} \oplus U_{i_2} \oplus \dots \oplus U_{i_s}$ for some free minimal τ -invariant submodules of R^n and the $\text{rank}(\mathcal{C}) = \sum_{j=1}^s k_{i_j}$, where k_{i_j} is the rank of U_{i_j} ;
- (2) $g(x) = f_{i_1}(x)f_{i_2}(x)\dots f_{i_s}(x)$ is the minimal polynomial of τ over $\mathcal{C}$;
- (3) $\text{rank}(g(T)) = n - \text{rank}(\mathcal{C})$;
- (4) $c \in \mathcal{C}$ if and only if $g(T)c = 0$.

Proof (1), (2), (3) These follow immediately from Lemma 1.1.

(4) Let $c \in \mathcal{C}$. Then $c = u_{i_1} + u_{i_2} + \dots + u_{i_s}$ for some $u_{i_j} \in U_{i_j}, j = 1, 2, \dots, s$, and $g(T)c = g(T)u_{i_1} + g(T)u_{i_2} + \dots + g(T)u_{i_s} = 0$. Conversely, suppose that $g(T)c = 0$ for some $c \in R^n$. According to Lemma 1, $c = u_1 + u_2 + \dots + u_r, u_i \in U_i$. Then $g(T)c = (f_{i_1}f_{i_2}\dots f_{i_s})u_1 + (f_{i_1}f_{i_2}\dots f_{i_s})u_2 + \dots + (f_{i_1}f_{i_2}\dots f_{i_s})u_r = 0$. Therefore, $g(T)(u_{j_1} + u_{j_2} + \dots + u_{j_k}) = 0$, where $\{j_1, j_2, \dots, j_k\} = \{1, 2, \dots, r\} \setminus \{i_1, i_2, \dots, i_s\}$. Let $w = u_{j_1} + u_{j_2} + \dots + u_{j_k}$ and $f(x) = g(x)h(x)$. Since $\gcd(g(x), h(x)) = 1$, there exist $a(x), b(x) \in R[x]$

such that $a(x)g(x) + b(x)h(x) = 1$. Then $w = a(T)g(T)w + b(T)h(T)w = 0$. Thus $c \in \mathcal{C}$.

Let $f_1(x), f_2(x), \dots, f_r(x)$ be pairwise coprime monic basic irreducible polynomials over R and $f(x) = f_1(x)f_2(x)\dots f_r(x)$. Denote $\widehat{f_i}(x)$ be the product of $f_j(x)$ except $f_i(x)$, for $i = 1, 2, \dots, r$. Then $\widehat{f_i}(x)$ and $f_i(x)$ are coprime over R . Therefore there exist unique polynomials $u_i(x), v_i(x) \in R[x]$ such that $u_i(x)f_i(x) + v_i(x)\widehat{f_i}(x) = 1$. It follows that $v_i(x)\widehat{f_i}(x)[u_i(x)f_i(x) + v_i(x)f_i(x)] = v_i(x)\widehat{f_i}(x)$. Let $e_i(x) = v_i(x)\widehat{f_i}(x)$ and the corresponding matrix $e_i(T) = v_i(T)\widehat{f_i}(T)$. Since $f(T) = f_i(T)\widehat{f_i}(T) = 0$, $e_i^2(T) = e_i(T)$. We call $e_i(T)$ the idempotent matrix.

Theorem 2.2 *The matrix $e_i(T), i = 1, 2, \dots, r$, satisfy the following relations:*

- (1) $e_i^2(T) = e_i(T)$;
- (2) $e_i(T)e_j(T) = 0$ for $i \neq j$;
- (3) $\sum_{i=1}^r e_i(T) = E$;
- (4) Let $\mathcal{C} = U_i$. Then $c \in U_i$ if and only if $e_i(T)c = c$;
- (5) Let $\mathcal{C} = U_j, j \neq i$. Then $e_i(T)c = 0$.

Proof (1) It follows immediately from the definition of $e_i(T)$.

(2) $e_i(T)e_j(T) = v_i(T)v_j(T)\widehat{f_i}(T)\widehat{f_j}(T) = 0$, for $i \neq j$.

(3) One can verify that $e_1(T) + e_2(T) + \dots + e_r(T) = E = 0$.

(4) Let $c \in U_i$. Since $u_i(x)f_i(x) + v_i(x)\widehat{f_i}(x) = 1$, $u_i(T)f_i(T)c + v_i(T)\widehat{f_i}(T)c = e_i(T)c = c$. Conversely, suppose that $e_i(T)c = c$ for some $c \in R^n$. Then $f_i(T)c = f_i(T)e_i(T)c = v_i(T)f(T)c = 0$, so $c \in U_i$.

(5) Let $c \in U_j, j \neq i$. Then $e_i(T)c = v_i(T)\widehat{f_i}(T)e_j(T)c = v_i(T)v_j(T)\widehat{f_i}(T)\widehat{f_j}(T)c = 0$.

Corollary 2.3 *Let $\mathcal{C} = U_{i_1} \oplus U_{i_2} \oplus \dots \oplus U_{i_s}$ be a free cyclic code of length n over R . Then the following facts hold:*

- (1) $c \in \mathcal{C}$ if and only if $e(T)c = c$;
- (2) $e(T) = e_{i_1}(T) + e_{i_2}(T) + \dots + e_{i_s}(T)$;
- (3) the cyclic code $U_{j_1} \oplus U_{j_2} \oplus \dots \oplus U_{j_l}$ has the idempotent matrix $E - e(T)$, where $\{j_1, j_2, \dots, j_l\} = \{1, 2, \dots, r\} \setminus \{i_1, i_2, \dots, i_s\}$.

References

- [1] M. Bhaintwal, On the quasi-cyclic codes over Z_q , *Appl. Algebra Engrg. Comm. Comput.*, **20**(2009), 459-480.
- [2] Y. Cao, J. Gao, Constructing quasi-cyclic codes from linear algebra theory, *Designs, Codes and Cryptography*, **67** (2013), 59-75.

- [3] D. Radkova, A.J. Van Zanten, Constacyclic codes as invariant subspaces, *Linear Algebra and its Applications*, **430**(2009), 855-864.
- [4] Z. X. Wan, Cyclic codes over Galois rings, *Alg. Coll.*, **3** (1999), 291-304.

Received: October 15, 2013