A Note on Dual Codes of Pseudo-cyclic Codes

PhD Thesis Periodic Report-5
PhD Candidate: Sümeyra BEDIR
Supervisor: Prof. Dr. Bayram Ali ERSOY
Date: 8 June 2018

Contents

1 Objective

In this report, as a result of our recent studies, we introduce a method to obtain a direct construction for the dual codes of pseudo-cyclic codes.

2 Introduction

Pseudo-cyclic codes over finite fields were first introduced by (Peterson and Weldon, 1972). Although every pseudo-cyclic code corresponds to a shortened cyclic code over finite fields, in terms of introducing a direct construction, pseudo-cyclic codes have attracted many researchers with their rich algebraic structure. Figure 1 shows a generalization schema of cyclic codes.

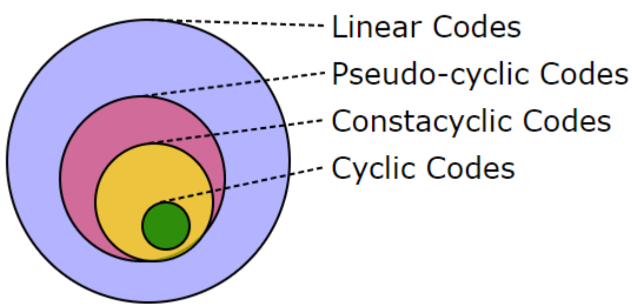

Figure 1: Generalization of Cyclic Codes

3 Preliminaries

3.1 Pseudo-cyclic Codes

Let F_q be a finite field with q elements and let F_q^n be the $n-$dimensional vector space over F_q.

Let $c = (c_0, c_1, \ldots, c_{n-1})$ be any vector in F_q^n. We fix a shift vector $v = (v_0, v_1, \ldots, v_{n-1})$ and define the following linear transformation

$$\begin{aligned} \tau_v : F^n &\to F^n \\ (c_0, c_1, \ldots, c_{n-1}) &\mapsto (v_0 c_{n-1}, c_0 + v_1 c_{n-1}, \ldots, c_{n-2} + v_{n-1} c_{n-1}) \end{aligned}$$

It has the following representation matrix as $\tau_v(c) = c.T_v$ and T_v is exactly the companion matrix for $f(x) = x^n - v(x)$.

$$T_v = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ 0 & 0 & \ddots & \ddots & 0 \\ \vdots & 0 & \cdots & 0 & 1 \\ v_0 & v_1 & \cdots & v_{n-2} & v_{n-1} \end{bmatrix}_{nxn}$$

Example 1. *Let $c = (c_0, c_1, c_2)$ be a vector in some vector space F_q^3. Let $v = (v_0, v_1, v_2)$ be the shift vector.*

Thus we have

$$T_v = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ v_0 & v_1 & v_2 \end{bmatrix}$$

And the transformation τ_v moves $c = (c_0, c_1, c_2)$ to the vector $\tau_v(c) = (v_0c_2, c_0 + v_1c_2, c_1 + v_2c_2)$ as follows;

$$\tau_v(c) = c \cdot T_v = \begin{bmatrix} c_0 \, c_1 \, c_2 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ v_0 & v_1 & v_2 \end{bmatrix} = \begin{bmatrix} v_0c_2 \; c_0 + v_1c_2 \; c_1 + v_2c_2 \end{bmatrix}$$

T_v is the companion matrix for $f(x) = x^3 - (v_0 + v_1x + v_2x^2)$.

Definition 2 (Pseudo-cyclic Codes)**.** *A linear code C with length n over a finite field F_q is called $pseudo-cyclic$ with respect to the vector $v = (v_0, v_1, \dots, v_{n-1})$, if whenever $c = (c_0, c_1, \dots, c_{n-1})$ is in C, so is its $v-$pseudo-cyclic shift $(v_0c_{n-1}, c_0 + v_1c_{n-1}, \dots, c_{n-2} + v_{n-1}c_{n-1})$.*

A pseudo-cyclic code with respect to v is invariant under τ_v.

Any cyclic code is $pseudo-cyclic$ with respect to $v = (1, 0, \dots, 0)$ and $v(x) = 1$.

Any constacyclic code with respect to α, is $pseudo-cyclic$ with respect to $v = (\alpha, 0, \dots, 0)$ and $v(x) = \alpha$.

Figure 2 shows the inclusion properties with respect to the usual polynomial correspondence between linear codes as subspaces of vector spaces and linear codes as ideals of polynomial rings.

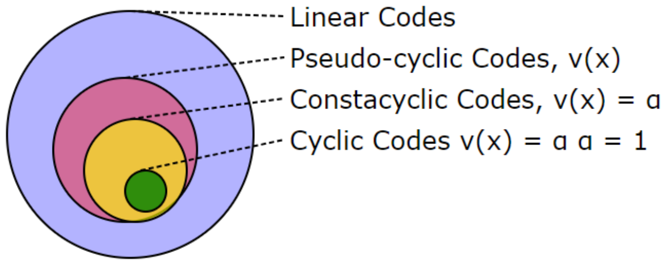

Figure 2: Polynomial Correspondence

For pseudo-cyclic codes we have $C \lhd F_q[x]/(f(x))$, $f(x) = x^n - v(x)$, for constacyclic codes we have $C \lhd F_q[x]/(f(x))$, $f(x) = x^n - \alpha, \alpha \in F_q^*$ and for cyclic codes we have $C \lhd F_q[x]/(f(x))$, $f(x) = x^n - 1$.In terms of this correspondence to the polynomial ring $F_q[x]/(x^n - v(x))$, multiplying a polynomial by x corresponds to a pseudo-cyclic shift with respect to v, therefore a $pseudo-cyclic$ code over F_q^n corresponds to an ideal in $F_q[x]/(x^n - v(x))$.

Example 3. *Consider $c(x) = c_0 + c_1x + c_2x^2$. Let $v(x) = v_0 + v_1x + v_2x^2$, so we are in $F_q[x]/(x^3 - v(x))$.*

Multiplying $c(x)$ by x, we get;

$$\begin{aligned}(c_0 + c_1x + c_2x^2).x &= c_0x + c_1x^2 + c_2x^3 \\ &= c_0x + c_1x^2 + c_2(v(x)) \\ &= c_0x + c_1x^2 + c_2(v_0 + v_1x + v_2x^2) \\ &= c_2v_0 + (c_0 + c_2v_1)x + (c_1 + c_2v_2)x^2\end{aligned}$$

So this gives us the pseudo-cyclic shift,

$$(c_0, c_1, c_2) \to (c_2v_0, c_0 + c_2v_1, c_1 + c_2v_2)$$

4 Formulation of the Problem

Pseudo-cyclic codes are fully characterized over finite fields and finite chain rings (Lopez et al., 2013; Bedir and Siap, 2015; Alahamdi et al., 2016). They have been constructed as module $\theta-$codes over skew polynomial rings (Boucher and Ulmer, 2011). However, the problem of finding a concrete generator for the dual code was open both over the commutative and noncommutative cases.

For the commutative case, the following theorem gives an indirect method for generating the dual code;

Theorem 4 (Bedir and Siap, 2015). *If $g(x) = f(x)/h(x)$ is the generating polynomial of a pseudo-cyclic code C, then $G = g(T_v)$ is a generator matrix for C and $H = h^R((T_v^{-1})^{tr})$ is a parity check matrix for C, where $h^R(x)$ is the reciprocal polynomial of $h(x)$ ($h^R(x) = h(1/x)x^{\deg(h(x))}$).*

4.1 The Dual Code and Sequential Codes

The dual code of a polycyclic code is a type of "sequential code" (Lopez et al., 2009).

Definition 5 (Sequential Codes). *A linear code C with length n over a finite field F is called sequential with respect to the the vector $\omega = (\omega_0, \omega_1, \ldots, \omega_{n-1})$, if there is a function $\varphi_\omega : F^n \longrightarrow F$ such that whenever $c = (c_0, c_1, \ldots, c_{n-1})$ is in C, so is $(\varphi_\omega(c_0, c_1, \ldots, c_{n-1}), c_0, c_1, \ldots, c_{n-2})$.*

Let C be a pseudo-cyclic code with respect to $v = (v_0, v_1, \ldots, v_{n-1})$, with generating polynomial $g(x) = g_0 + g_1x + \cdots + g_{n-1}x^{n-1}$, and let $h(x) = (x^n - v(x))/g(x)$.

Set $\omega = (v_0^{-1}, -v_{n-1}/v_0, -v_{n-2}/v_0, \ldots, -v_1/v_0)$. And consider the following transformation;

$$\begin{aligned} \rho_\omega : F^n &\to F^n \\ (c_0, c_1, \ldots, c_{n-1}) &\mapsto (\omega_{n-1}c_0 + \omega_{n-2}c_1 + \cdots + \omega_0 c_{n-1}, \\ &\qquad c_0, c_1, .., c_{n-2}) \end{aligned}$$

The matrix represenation for ρ_ω is exactly $(T_v^{-1})^{tr}$, and note that v_0 should be invertible in any case.

The dual code of a pseudo-cyclic code with respect to $v = (v_0, v_1, \ldots, v_{n-1})$ is therefore a sequential code with respect to $\omega = (v_0^{-1}, -v_{n-1}/v_0, \ldots, -v_1/v_0)$, where $\varphi_\omega(c_0, c_1, \ldots, c_{n-1}) = \omega_{n-1}c_0 + \omega_{n-2}c_1 + \cdots + \omega_0 c_{n-1}$.

The placement of sequential codes in the previous diagram is shown in Figure 3.

Notice that, negacyclic codes live at the intersection like in Figure 4.

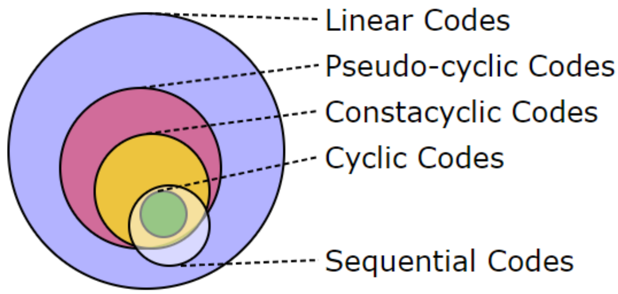

Figure 3: Sequential Codes

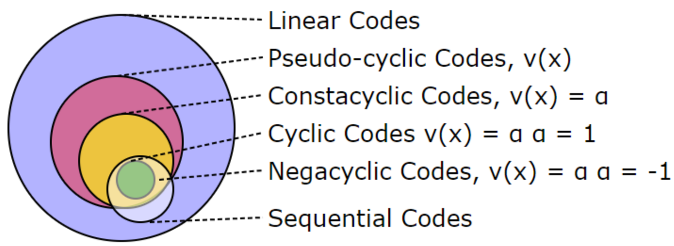

Figure 4: Negacyclic Codes

4.2 Pseudo-cyclic Codes vs Sequential Codes

Pseudo-cyclic codes have an ideal structure, and over the corresponding polynomial ring, we are able to find a generating polynomial; which gives a generating vector and provides constructing a vector-circulant generating matrix.

However, sequential codes do not have an ideal structure. The transformation does not correspond to multiplication by x in the polynomial correspondence.

So, the question is: how can we obtain a generating polynomial/ generating vector a for sequential codes (as the dual code of pseudo-cyclic codes), so that we obtain a direct construction as follows;

$$H = \begin{bmatrix} \cdots & a & \cdots \\ \cdots & \rho_\omega(a) & \cdots \\ \cdots & \rho_\omega^2(a) & \cdots \\ & \vdots & \\ \cdots & \rho_\omega^{n-1}(a) & \cdots \end{bmatrix}_{nxn} \quad \Longrightarrow \quad a = ???$$

5 Construction Method and Examples

Shortening Method

Let C' be an $[n, k, d]$-linear code over F_q. For a fixed $1 \leq i \leq n$, form the subset A of C' consisting of the codewords with the i^{th} position equal to 0. Delete the i^{th} position from all the words in A to form a code C. Then C is an $[n-1, k, d]$-linear code over F_q with $k-1 \leq k \leq k$, $d \geq d$. (Ling and Xing, 2004).

A pseudo-cyclic code with generating polynomial $g(x) = g_0 + g_1x + \cdots + g_{n-1}x^{n-1}$ can be obtained by shortening a cyclic code C' generated by $g(x)$.

Puncturing Method

Let D' be an $[n+r, k, d+r]$-linear code over F_q. Choose a set B of codewords in D' with distance $d+r$. Choose r non-zero coordinates, and delete these coordinates from all the codewords of D'. Then the new code D, is an $[n, k, d]$-linear code over F_q (Ling and Xing, 2004).

The dual code of a pseudo-cyclic code with generating polynomial $g(x) = g_0 + g_1x + \cdots + g_{n-1}x^{n-1}$ can be obtained by puncturing the dual code of a cyclic code C' generated by $g(x)$.

5.1 From Shortening and Puncturing to Pseudo-cyclic Codes and Their Duals

Following the intiutions we get from the above correspondences, we derived a formula to obtain a generating vector for the dual codes of pseudo-cyclic codes. We used the cyclic code with the smallest length N for which $f(x)$ divides $x^N - 1$.

Theorem 6. *Let $h(x)g(x) = f(x)$, $\deg(g(x)) = n-k$, $p(x) = \frac{x^N-1}{f(x)} = \sum_{i=0}^{N-n} p_i x^i$ and let C be the pseudo-cyclic code generated by $g(x)$. Then the dual code D is generated by the vector $a = (a_0, a_1, \ldots, a_{n-1})$ and its $n-k-1$ sequential shifts, where*

$$a_0 = p_0 h_0, a_i = \sum_{j=0}^{i-1} p_{N-n-j} h_{n-i+j}, 1 \leq i \leq n-1$$

Example 7. *Let F be the finite field with 4 elements; $F_4 = \{0, 1, \alpha, \alpha^2 = \alpha+1\}$. Let $g(x) = \alpha^2+\alpha x^2+x^3, h(x) = 1+\alpha x+x^2$ and $f(x) = g(x)h(x) = x^5+\alpha x^3+x^2+x+\alpha^2$.*

Let T_v be the companion matrix of $f(x)$.

Consider the pseudo-cyclic code C generated by $g(x)$ over F_4.

We obtain the generating matrix of C as follows;

$$G = \begin{bmatrix} \cdots & g & \cdots \\ \cdots & g \cdot T_v & \cdots \end{bmatrix}_{2x5} = \begin{bmatrix} \alpha^2 & 0 & \alpha & 1 & 0 \\ 0 & \alpha^2 & 0 & \alpha & 1 \end{bmatrix}_{2x5}$$

We have $f(x)|x^{15} - 1$ and we set $N = 15$.

In this case we have

$$p(x) = \frac{x^N - 1}{f(x)} = \alpha + \alpha^2 x + \alpha x^2 + \alpha^2 x^3 + \alpha^2 x^5 + \alpha x^6 + x^7 + \alpha x^8 + x^{10}$$

Using the above formula

$$a_0 = p_0 h_0, a_i = \sum_{j=0}^{i-1} p_{N-n-j} h_{n-i+j},$$

we get

$$a = (a, 0, 0, 1, a)$$

So the dual code can be generated as follows;

$$H = \begin{bmatrix} \cdots & a & \cdots \\ \cdots & a \cdot (T_v^{-1})^{tr} & \cdots \\ \cdots & a \cdot ((T_v^{-1})^{tr})^2 & \cdots \end{bmatrix}_{3x5} = \begin{bmatrix} \alpha & 0 & 0 & 1 & \alpha \\ 0 & \alpha & 0 & 0 & 1 \\ 1 & 0 & \alpha & 0 & 0 \end{bmatrix}_{3x5}$$

6 Conclusion and Future Work

We have derived a formula to obtain the generators of the dual codes of pseudo-cyclic codes and we gave an example over a commutative structure. We further improved our result for the non-commutative case over skew polynomial rings as a near future work. We will apply these results to skew quasi-cyclic codes and skew multi-twisted codes.

References

[1] A. Alahamdi, S. Dougherty, A. Leroy, P. Sole (2016). On the duality and the direction of polycyclic codes, Adv. in Math. of Com., 10(4):921-929.

[2] S. Bedir, I. Siap (2015). Polycyclic Quaternary Codes, Proceedings of the International Conference on Coding and Cryptography, 5-10 Nov 2015, Algeria.

[3] D. Boucher, F.Ulmer (2011). A note on the dual codes of module skew codes, 7089:230-243.

[4] S. Jitman (2013). Vector-circulant matrices over finite fields and related codes, arXiv:1408.2059 [math.RA]

[5] S. Ling, C. Xing (2004). Coding Theory: A First Course, Cambridge University Press, New York.

[6] S. R. López-Permouth, H. Özadam, F. Özbudak , S. Szabo (2013). Polycyclic codes over Galois rings with applications to repeated-root constacyclic codes, Finite Fields and Their Applications, 19(2013):16-38.

[7] S.R. Lopez-Permouth, B.R. Parra-Avila, S. Szabo (2009). Dual generalizations of the concept of cyclicity of codes, Adv. in Math. of Com. (2009): 227–234.

[8] W. W. Peterson, E. J. Jr Weldon (1972) Error Correcting codes: second edition, MIT Press, Cambridge, MA.

[9] D. Radkova, A.J. Van Zanten, (2009). Constacyclic codes as invariant subspaces, Linear Algebra and its Applications, 430(2009): 855-864.

[10] M. Wu, (2013). Free cyclic codes as invariant submodules over finite chain rings, International Mathematical Forum, 8(37): 1835 - 1838.