Journal of Algebra and Related Topics
Vol. 4, No 2, (2016), pp 1-8

SOME NOTES ON THE CHARACTERIZATION OF TWO DIMENSIONAL SKEW CYCLIC CODES

Z. SEPASDAR

Abstract. A natural generalization of two dimensional cyclic code (TDC) is two dimensional skew cyclic code. It is well-known that there is a correspondence between two dimensional skew cyclic codes and left ideals of the quotient ring

$$R_n := \mathbb{F}[x, y; \rho, \theta]/ < x^s - 1, y^\ell - 1 >_l.$$

In this paper we characterize the left ideals of the ring R_n with two methods and find the generator matrix for two dimensional skew cyclic codes.

1. Introduction

There are many generalizations of cyclic codes. One of them is two dimensional cyclic code, which was first introduced by Ikai et al. in [2] and Imai in [3]. After that many authors has worked in this area.

The other generalization of cyclic code is skew cyclic code was introduced by Boucher et al. in [1]. They considered skew cyclic codes as left ideals over skew polynomial rings. After that Xiuli et al. in [4] combined these two generalizations and introduced two dimensional skew cyclic codes. They studied some properties of two dimensional skew cyclic codes and built relation between two dimensional skew cyclic codes and other known codes.

In this paper we characterize two dimensional skew cyclic codes by two different methods. Also we find the generator matrix for these codes.

MSC(2010): Primary: 12E20; Secondary: 94B05, 94B15, 94B60
Keywords: cyclic code, two dimensional skew cyclic code, generator matrix.
Received: 22 October 2016, Accepted: 23 November 2016.

Now, we recall some basic definitions. Let $\mathbb{F}=\mathbb{F}_q$ be the finite field with q elements, where q is a power of a prime number. Assume that ρ and θ are two automorphisms of $\mathbb{F}$. We consider a set of bivariate skew polynomials $\mathbb{F}[x,y;\rho,\theta]=\{\Sigma\Sigma a_{ij}x^iy^j : a_{ij}\in\mathbb{F},(i,j)\in\mathbb{Z}_+^2\}$. The addition in $\mathbb{F}[x,y;\rho,\theta]$ is defined to be the usual addition of polynomials and the multiplication is defined by the basic rule

$$ax^iy^j * bx^ry^t = a\rho^i\theta^j(b)x^{i+r}y^{j+t}$$

and extended to all elements of $\mathbb{F}[x,y;\rho,\theta]$ by associativity and distributivity. Hence $\mathbb{F}[x,y;\rho,\theta]$ is a ring.

Definition 1.1. Suppose that C is a linear code over $\mathbb{F}$ of length $s\ell$ whose codewords are viewed as $s\times\ell$ arrays, i.e. $c\in C$ is written as

$$c=\begin{pmatrix} c_{0,0} & \cdots & c_{0,\ell-1} \\ c_{1,0} & \cdots & c_{1,\ell-1} \\ & \vdots & \\ c_{s-1,0} & \cdots & c_{s-1,\ell-1} \end{pmatrix}.$$

If C is closed under row ρ-skew shift and column θ-skew shift of codewords, then we call C a two dimensional skew cyclic code of size $s\ell$ over $\mathbb{F}$ under ρ and θ.

Suppose that $R_n := \mathbb{F}[x,y;\rho,\theta]/ < x^s-1, y^\ell-1 >_l$ denotes the set of all polynomials over $\mathbb{F}$ of degree less than s with respect to x and of degree less than ℓ with respect to y, where $< x^s-1,y^\ell-1>_l$ is the left ideal generated by x^s-1 and $y^\ell-1$ in $\mathbb{F}[x,y;\rho,\theta]$.

The combinatorial structure of a two dimensional skew cyclic code converts into the algebraic one by the following theorem.

Theorem 1.2. [4, Theorem 3.5].) *Suppose that* $|<\rho>| \mid s$ *and* $|<\theta>| \mid \ell$. *The nonempty subset* C *of* $\mathbb{F}^{s\ell}$ *is a two dimensional skew cyclic code if and only if* C *is a left ideal of* $\mathbb{F}[x,y;\rho,\theta]/ < x^s-1, y^\ell-1 >_l$.

So if one wants to characterize two dimensional skew cyclic codes, it is more convenient to characterize the ideals of the ring $\mathbb{F}[x,y;\rho,\theta]/ < x^s-1,y^\ell-1>_l$. We assume that $|<\rho>| \mid s$ and $|<\theta>| \mid \ell$ and use two methods to characterize the ideals of this ring.

2. First method

Suppose that I is an ideal of the ring $R_n := \mathbb{F}[x,y;\rho,\theta]/ < x^s - 1, y^\ell-1>_l$. Every element $f(x,y)\in I$ can be written uniquely as $f(x,y)=\Sigma_{i=0}^{\ell-1}f_i(x)y^i$, where each $f_i(x)\in R_1 := \mathbb{F}[x,\theta]/ < x^s-1 >$. In [1], it was shown that the ring R_1 is a principal ideal ring, so any left ideal of R_1 can be generated by a right divisor of x^s-1 in $\mathbb{F}[x,\theta]$. Put

$I_0=\{g_0(x)\in R_1:$ there exists g(x, y) ∈ I such that

$$g(x,y)=\Sigma_{i=0}^{\ell-1}g_i(x)y^i\}\ .$$

Clearly I_0 is a left ideal of R_1, so there exists a unique monic polynomial $p_0^0(x)\in R_1$ such that $I_0=<p_0^0(x)>$ and there exists $q_0(x)$ such that $x^s-1=q_0(x)\ p_0^0(x)$. Now, since $f(x,y)\in I$ it is clear that $f_0(x)\in I_0$, and so $f_0(x)=p_0'(x)\ p_0^0(x)$ for some $p_0'(x)\in R_1$. On the other hand, $p_0^0(x)\in I_0$ implies that there exists $\mathbf{p}_0(x,y)\in I$ such that $\mathbf{p}_0(x,y)=\Sigma_{i=0}^{\ell-1}p_i^0(x)y^i$. Set $h_1(x,y)=f(x,y)-p_0'(x)\ \mathbf{p}_0(x,y)$, hence $h_1(x,y)$ is a polynomial in I of the form $h_1(x,y)=\Sigma_{i=1}^{\ell-1}h_i^1(x)y^i$. Put $I_1=\{g_1(x)\in R_1:$ there exists g(x, y) ∈ I such that

$$g(x,y)=\Sigma_{i=1}^{\ell-1}g_i(x)y^i\}.$$

Clearly I_1 is a left ideal of R_1, so there exists a unique monic polynomial $p_1^1(x)\in R_1$ such that $I_1=<p_1^1(x)>$ and there exists $q_1(x)$ such that $x^s-1=q_1(x)\ p_1^1(x)$. Now, since $h_1(x,y)\in I$ it is clear that $h_1^1(x)\in I_1$, and so $h_1^1(x)=p_1'(x)\ p_1^1(x)$ for some $p_1'(x)\in R_1$. On the other hand, $p_1^1(x)\in I_1$ implies that there exists $\mathbf{p}_1(x,y)\in I$ such that $\mathbf{p}_1(x,y)=\Sigma_{i=1}^{\ell-1}p_i^1(x)y^i$. Set $h_2(x,y)=h_1(x,y)-p_1'(x)\ \mathbf{p}_1(x,y)$, hence $h_2(x,y)$ is a polynomial in I of the form $h_2(x,y)=\Sigma_{i=2}^{\ell-1}h_i^2(x)y^i$. Put $I_2=\{g_2(x)\in R_1:$ there exists g(x, y) ∈ I such that

$$g(x,y)=\Sigma_{i=2}^{\ell-1}g_i(x)y^i\}.$$

Clearly I_2 is a left ideal of R_1, so there exists a unique monic polynomial $p_2^2(x)\in R_1$ such that $I_2=<p_2^2(x)>$ and there exists $q_2(x)$ such that $x^s-1=q_2(x)\ p_2^2(x)$. Now, since $h_2(x,y)\in I$ it is clear that $h_2^2(x)\in I_2$, and so $h_2^2(x)=p_2'(x)\ p_2^2(x)$ for some $p_2'(x)\in R_1$. On the other hand $p_2^2(x)\in I_2$ implies that there exists $\mathbf{p}_2(x,y)\in I$ such that $\mathbf{p}_2(x,y)=\Sigma_{i=2}^{\ell-1}p_i^2(x)y^i$. Set $h_3(x,y)=h_2(x,y)-p_2'(x)\ \mathbf{p}_2(x,y)$, hence $h_3(x,y)$ is a polynomial in I of the form $h_3(x,y)=\Sigma_{i=3}^{\ell-1}h_i^3(x)y^i$, now I_3 can be defined. By this method one can construct $\mathbf{p}_i(x,y)\in I$ for $i=0,\dots,\ell-1$. It is easy to see that

$$I=<\mathbf{p}_0(x,y),\dots,\mathbf{p}_{\ell-1}(x,y)>\ .$$

We call $\mathbf{p}_i(x,y)$ as the generating polynomials of I.

By multiply y^j $(j=1,\dots,\ell-1)$ to each $\mathbf{p}_i(x,y)$ $(i=0,\dots,\ell-1)$, we can find some conditions on the terms of generating polynomials. For example we apply the first method for $\ell=4$ and get te conditions. Assume that I is an ideal of the ring $\mathbb{F}[x,y;\rho,\theta]/<x^s-1,y^4-1>_l$ and generated by the set $\{\mathbf{p}_0(x,y),\mathbf{p}_1(x,y),\mathbf{p}_2(x,y),\mathbf{p}_3(x,y)\}$ which obtained from the first method.

$$\begin{aligned}
\mathbf{p}_0(x,y) &= p_0^0(x) + p_1^0(x)y + p_2^0(x)y^2 + p_3^0(x)y^3,\\
\mathbf{p}_1(x,y) &= p_1^1(x)y + p_2^1(x)y^2 + p_3^1(x)y^3,\\
\mathbf{p}_2(x,y) &= p_2^2(x)y^2 + p_3^2(x)y^3,\\
\mathbf{p}_3(x,y) &= p_3^3(x)y^3.
\end{aligned}$$

Conditions on $\mathbf{p}_0(x,y)$:

$$p_0^0(x) \mid \theta(p_3^0(x)),\quad p_0^0(x) \mid \theta^2(p_2^0(x)),\quad p_0^0(x) \mid \theta^3(p_1^0(x)),\quad p_1^1(x) \mid \frac{x^s-1}{p_0^0(x)}p_1^0(x).$$

Conditions on $\mathbf{p}_1(x,y)$:

$$p_0^0(x) \mid \theta(p_3^1(x)),\quad p_0^0(x) \mid \theta^2(p_2^1(x)),\quad p_0^0(x) \mid \theta^3(p_1^1(x)),\quad p_2^2(x) \mid \frac{x^s-1}{p_1^1(x)}p_2^1(x),$$
$$p_1^1(x) \mid \theta^3(\frac{x^s-1}{p_1^1(x)}p_2^1(x)).$$

Conditions on $\mathbf{p}_2(x,y)$:

$$p_0^0(x) \mid \theta(p_3^2(x)),\quad p_0^0(x) \mid \theta^2(p_2^2(x)),\quad p_1^1(x) \mid \theta^3(p_2^2(x)),\quad p_3^3(x) \mid \frac{x^s-1}{p_2^2(x)}p_3^2(x),$$
$$p_1^1(x) \mid \theta^2(\frac{x^s-1}{p_2^2(x)}p_3^2(x)),\quad p_2^2(x) \mid \theta^3(\frac{x^s-1}{p_2^2(x)}p_3^2(x)).$$

Conditions on $\mathbf{p}_3(x,y)$:

$$p_0^0(x) \mid \theta(p_3^3(x)),\quad p_1^1(x) \mid \theta^2(p_3^3(x)),\quad p_2^2(x) \mid \theta^3(p_3^3(x)).$$

Also we can take the following conditions:

$$\begin{aligned}
\deg(p_3^3(x)) &> \deg(p_3^k(x)) \quad k=0,1,2,\\
\deg(p_2^2(x)) &> \deg(p_2^k(x)) \quad k=0,1,\text{and}\\
\deg(p_1^1(x)) &> \deg(p_1^k(x)) \quad k=0.
\end{aligned}$$

By the following theorem, one can easily find the generator matrix and dimension of two dimensional skew cyclic codes.

Theorem 2.1. *Let I be a left ideal of the ring $\mathbb{F}[x,y;\rho,\theta]/ < x^s-1, y^\ell-1 >_l$ (a two dimensional skew cyclic code) with length $n=s\ell$ and is generated by $\{\boldsymbol{p}_0(x,y),\ldots,\boldsymbol{p}_{\ell-1}(x,y)\}$, which* *is obtained from the fisrt method. Then the set*

$$\{\boldsymbol{p}_0(x,y), x\boldsymbol{p}_0(x,y), \ldots, x^{n-a_0-1}\boldsymbol{p}_0(x,y),$$
$$\boldsymbol{p}_1(x,y), x\boldsymbol{p}_1(x,y), \ldots, x^{n-a_1-1}\boldsymbol{p}_1(x,y),$$
$$\vdots$$
$$\boldsymbol{p}_{\ell-1}(x,y), x\boldsymbol{p}_{\ell-1}(x,y), \ldots, x^{n-a_{\ell-1}-1}\boldsymbol{p}_{\ell-1}(x,y)\}$$

where $a_i := \deg(p_i^i(x))$ *for* $i = 0, \ldots, \ell-1$*, is an* $\mathbb{F}$*-basis for* I*.*

Proof. Assume that $k_0(x), \ldots, k_{\ell-1}(x)$ are polynomials in $\mathbb{F}[x,\theta]$, such that $\deg(k_i(x)) < s - a_i$ and $k_0(x)\ \mathbf{p}_0(x,y) + \cdots + k_{\ell-1}(x)\ \mathbf{p}_{\ell-1}(x,y) = 0$. This implies that

$$k_0(x)\ p_0^0(x) = 0 \text{ in } \mathbb{F}[x,\theta]/ < x^s - 1 > .$$

Hence $k_0(x)\ p_0^0(x) = s(x)\ (x^s - 1)$, for some $s(x) \in \mathbb{F}[x,\theta]$. Since $\deg(p_0^0(x)) = a_0$ and $\deg(k_0(x)) < s - a_0$, $k_0(x) = 0$. Similar arguments can be applied to show that $k_i(x) = 0$ for $i = 1, \ldots, \ell-1$. □

3. Second method

Let I be a left ideal of the ring $R_n := \mathbb{F}[x,y;\rho,\theta]/ < x^s - 1, y^\ell - 1 >_l$. Every element $f(x,y) \in I$ can be written uniquely as $f(x,y) = \Sigma_{i=0}^{\ell-1} f_i(x) y^i$, where each $f_i(x) \in R_1 := \mathbb{F}[x,\theta]/ < x^s - 1 >$. Put

$I_0 = \{g_{\ell-1}(x) \in R_1 :$ there exists g(x, y) $\in$ I such that

$$g(x,y) = \Sigma_{i=0}^{\ell-1} g_i(x) y^i\}.$$

Clearly I_0 is a left ideal of R_1. Thus there exists a unique monic polynomial $p_{\ell-1}^0(x) \in R_1$ such that $I_0 =< p_{\ell-1}^0(x) >$ and there exists $q_0(x) \in R_1$ such that $x^s - 1 = q_0(x)\ p_{\ell-1}^0(x)$. Now, since $f(x,y) \in I$ it is clear that $f_{\ell-1}(x) \in I_0$. So $f_{\ell-1}(x) = p'_{\ell-1}(x)\ p_{\ell-1}^0(x)$ for some $p'_{\ell-1}(x) \in R_1$. On the other hand, $p_{\ell-1}^0(x) \in I_0$ implies that there exists $\mathbf{p}_0(x,y) \in I$ such that $\mathbf{p}_0(x,y) = \Sigma_{i=0}^{\ell-1} p_i^0(x) y^i$. Set $h_1(x,y) = f(x,y) - p'_{\ell-1}(x)\ \mathbf{p}_0(x,y)$, hence $h_1(x,y)$ is a polynomial in I of the form $h_1(x,y) = \Sigma_{i=0}^{\ell-2} h_i^1(x) y^i$. Put

$I_1 = \{g_{\ell-2}(x) \in R_1$ there exists g(x, y) $\in$ I such that

$$g(x,y) = \Sigma_{i=0}^{\ell-2} g_i(x) y^i\}.$$

Clearly I_1 is a left ideal of R_1. Thus there exists a unique monic polynomial $p_{\ell-2}^1(x) \in R_1$ such that $I_1 =< p_{\ell-2}^1(x) >$ and there exists $q_1(x) \in R_1$ such that $x^s - 1 = q_1(x)\ p_{\ell-2}^1(x)$. Now, since $h_1(x,y) \in I$ it is obvious that $h_{\ell-2}^1(x) \in I_1$, and so $h_{\ell-2}^1(x) = p'_{\ell-2}(x)\ p_{\ell-2}^1(x)$ for some $p'_{\ell-2}(x) \in R_1$. On the other hand, $p_{\ell-2}^1(x) \in I_1$ implies that there exists $\mathbf{p}_1(x,y) \in I$ such that $\mathbf{p}_1(x,y) = \Sigma_{i=0}^{\ell-2} p_i^1(x) y^i$. Set

$h_2(x,y) = h_1(x,y) - p'_{\ell-2}(x)\ \mathbf{p}_1(x,y)$, hence $h_2(x,y)$ is a polynomial in I of the form $h_2(x,y) = \Sigma_{i=0}^{\ell-3} h_i^2(x) y^i$. Put

$I_2 = \{g_{\ell-3}(x) \in R_1$ there exists g(x, y) $\in$ I such that

$$g(x,y) = \Sigma_{i=0}^{\ell-3} g_i(x) y^i\}.$$

Clearly I_2 is a left ideal of R_1. Thus there exists a unique monic polynomial $p^2_{\ell-3}(x) \in R_1$ such that $I_2 =< p^2_{\ell-3}(x) >$ and there exists $q_2(x) \in R_1$ such that $x^s - 1 = q_2(x)\ p^2_{\ell-3}(x)$. Now, since $h_2(x,y) \in I$ it is obvious that $h^2_{\ell-3}(x) \in I_2$, and so $h^2_{\ell-3}(x) = p'_{\ell-3}(x)\ p^2_{\ell-3}(x)$ for some $p'_{\ell-3}(x) \in R_1$. On the other hand, $p^2_{\ell-3}(x) \in I_2$ implies that there exists $\mathbf{p}_2(x,y) \in I$ such that $\mathbf{p}_2(x,y) = \Sigma_{i=0}^{\ell-3} p_i^2(x) y^i$. Set $h_3(x,y) = h_2(x,y) - p'_{\ell-3}(x)\ \mathbf{p}_2(x,y)$, hence $h_3(x,y)$ is a polynomial in I of the form $h_3(x,y) = \Sigma_{i=0}^{\ell-4} h_i^3(x) y^i$. By this method we can construct $\mathbf{p}_i(x,y) \in I$ for $i = 0, \ldots, \ell-1$. It is easy to see that

$$I =< \mathbf{p}_0(x,y), \ldots, \mathbf{p}_{\ell-1}(x,y) > .$$

We call $\mathbf{p}_i(x,y)$ as the generating polynomials of I.

By multiply y^j $(j = 1, \ldots, \ell-1)$ to each $\mathbf{p}_i(x,y)$ $(i = 0, \ldots, \ell-1)$ we can find conditions on the terms of the generating polynomials. For convenience we obtain the conditions for generating polynomials of the ideal I of the ring $\mathbb{F}[x, y; \rho, \theta]/ < x^s - 1, y^4 - 1 >_l$. Assume that $\{\mathbf{p}_0(x,y), \mathbf{p}_1(x,y), \mathbf{p}_2(x,y), \mathbf{p}_3(x,y)\}$ is the set of generating polynomial of I which obtained from the second method

$$\begin{aligned}
\mathbf{p}_0(x,y) &= p_0^0(x) + p_1^0(x)y + p_2^0(x)y^2 + p_3^0(x)y^3, \\
\mathbf{p}_1(x,y) &= p_0^1(x) + p_1^1(x)y + p_2^1(x)y^2, \\
\mathbf{p}_2(x,y) &= p_0^2(x) + p_1^2(x)y, \\
\mathbf{p}_3(x,y) &= p_0^3(x).
\end{aligned}$$

Conditions on $\mathbf{p}_0(x,y)$:

$$p_3^0(x) \mid \theta(p_2^0(x)),\quad p_3^0(x) \mid \theta^2(p_1^0(x)),\quad p_3^0(x) \mid \theta^3(p_0^0(x)),\quad p_2^1(x) \mid \frac{x^s-1}{p_3^0(x)} p_2^0(x).$$

Conditions on $\mathbf{p}_1(x,y)$:

$$p_3^0(x) \mid \theta(p_2^1(x)),\quad p_3^0(x) \mid \theta^2(p_1^1(x)),\quad p_3^0(x) \mid \theta^3(p_0^1(x)),\quad p_1^2(x) \mid \frac{x^s-1}{p_2^1(x)} p_1^1(x),$$

$$p_2^1(x) \mid \theta(\frac{x^s-1}{p_2^1(x)} p_1^1(x)).$$

Conditions on $\mathbf{p}_2(x,y)$:

$$p_2^1(x) \mid \theta(p_1^2(x)), \;\; p_3^0(x) \mid \theta^2(p_1^2(x)), \;\; p_3^0(x) \mid \theta^3(p_0^2(x)), \;\; p_0^3(x) \mid \frac{x^s-1}{p_1^2(x)}p_0^2(x),$$

$$p_1^2(x) \mid \theta(\frac{x^s-1}{p_1^2(x)}p_0^2(x)), \;\; p_2^1(x) \mid \theta^2(\frac{x^s-1}{p_1^2(x)}p_0^2(x)), \;\; p_3^0(x) \mid \theta^3(\frac{x^s-1}{p_1^2(x)}p_0^2(x)).$$

Conditions on $\mathbf{p}_3(x,y)$:

$$p_1^2(x) \mid \theta(p_0^3(x)), \qquad p_2^1(x) \mid \theta^2(p_0^3(x)), \qquad p_3^0(x) \mid \theta^3(p_0^3(x)).$$

Also we can take the following conditions:

$$\deg(p_0^3(x)) > \deg(p_0^k(x)) \quad k=0,1,2.$$
$$\deg(p_1^2(x)) > \deg(p_1^k(x)) \quad k=0,1.$$
$$\deg(p_2^1(x)) > \deg(p_2^k(x)) \quad k=0.$$

By a method similar which is used in the proof of Theorem 2.1, the following result holds.

Theorem 3.1. *Let I be a left ideal of the ring $\mathbb{F}[x,y;\rho,\theta]/<x^s-1,y^\ell-1>_l$ (a two dimensional skew cyclic code) with length $n=s\ell$ and is generated by $\{\boldsymbol{p}_0(x,y),\ldots,\boldsymbol{p}_{\ell-1}(x,y)\}$, which is obtained from the second method. Then the set*

$$\begin{aligned}\{&\boldsymbol{p}_0(x,y), x\boldsymbol{p}_0(x,y),\ldots,x^{n-a_0-1}\boldsymbol{p}_0(x,y),\\ &\boldsymbol{p}_1(x,y), x\boldsymbol{p}_1(x,y),\ldots,x^{n-a_1-1}\boldsymbol{p}_1(x,y),\\ &\vdots\\ &\boldsymbol{p}_{\ell-1}(x,y), x\boldsymbol{p}_{\ell-1}(x,y),\ldots,x^{n-a_{\ell-1}-1}\boldsymbol{p}_{\ell-1}(x,y)\}\end{aligned}$$

where $a_i := \deg(p_{\ell-1-i}^i(x))$ for $i=0,\ldots,\ell-1$, is an $\mathbb{F}$-basis for I.

References

1. D. Boucher, W. Geiselmann, F. Ulmer, *Skew-cyclic codes,* Appl. Algebra Engrg. Comm. Comput., **18** (2007), 379-389.
2. T. Ikai, H. Kosako, and Y. Kojima, *Two-Dimensional cyclic codes*, Electronics and Communications in Japan, **4** 57-A (1975), 27-35.
3. H. Imai, *Theory of two-dimensional cyclic codes*, Information and Control, **34** (1977), 1-21.
4. L. Xiuli, L. Hongyan, *2-D skew cyclic codes over $\mathbb{F}_q[x,y;\rho,\theta]$,* Finite Fields Appl., **25** (2014), 49-63.

Zahra Sepasdar

Department of pure Mathematics, Ferdowsi University of Mashhad,

P.O.Box 1159-91775, Mashhad, Iran.
Email: zahra.sepasdar@gmail.com