On Linear Codes Over a Non-Chain Ring

Abdullah Dertli[1], Yasemin Cengellenmis[2], Senol Eren[1]

1. Ondokuz Mayıs University, Faculty of Arts and Sciences, Mathematics Department, Samsun, Turkey

2. Trakya University, Faculty of Arts and Sciences, Mathematics Department, Edirne, Turkey

E-mail:abdullah.dertli@gmail.com, seren@omu.edu.tr, ycengellenmis@gmail.com

Abstract: In this paper, we study skew cyclic and quasi cyclic codes over the ring $S = F_2 + uF_2 + vF_2$ where $u^2 = u, v^2 = v, uv = vu = 0$. We investigate the structural properties of them. Using a Gray map on S we obtain the MacWilliams identities for codes over S. The relationships between Symmetrized, Lee and Hamming weight enumerator are determined.

Key Words: Line code, chain ring, non-chain ring, Gray map, MacWilliams identity.

AMS(2010): 94B05.

§1. **Introduction**

Since the revelation in 1994 [10], there are a lot of works on codes over finite rings. The structure of certain type of codes over many finite rings are determined such as cyclic, quasi-cyclic. Recently, it is introduced the class of skew codes which are generalized the notion cyclic, quasi-cyclic in [5,6,12,14].

In [1], T. Abualrub, P. Seneviratre studied skew cyclic codes over $F_2 + vF_2$, $v^2 = v$. In [2], T. Abualrub, A. Ghrayeb, N. Aydın, I. Siap introduced skew quasi-cyclic codes. They obtained several new codes with Hamming distance exceeding the distance of the previously best known linear codes with comparable parameters.

In [4], they investigated the structures of skew cyclic and skew quasi-cyclic of arbitrary length over Galois rings. They shown that the skew cyclic codes are equivalent to either cyclic and quasi-cyclic codes over Galois rings. Moreover, they gave a necessary and sufficient condition for skew cyclic codes over Galois rings to be free.

Jian Gao, L.Shen, F. W. Fu studied a class of generalized quasi–cyclic codes called skew generalized quasi-cyclic codes. They gave the Chinese Remainder Theorem over the skew polynomial ring which lead to a canonical decomposition of skew generalized quasi-cyclic codes. Moreover, they focused on 1-generator skew generalized quasi-cyclic code in [7]. J.Gao also presented skew cyclic codes over $F_p + vF_p$ in [8].

The MacWilliams identity supplies the relationship between the weight enumerator of a linear code and that of its dual code [11]. The distribution of weights for a linear code is important for its performance analysis such as linear programming bound, error correcting

---

capabilities, etc. There are a lot of work about the MacWilliams identities in [3,9,15].

This paper is organized as follows. In section 2, we give some basic knowledges about the finite ring S. In section 3, we define a new Gray map from S to F_2^3, Lee weights of elements of S and Lee distance in the linear codes over S. In section 4, we define a new non trivial automorphism and we introduce skew codes over S. In section 5, we obtain the MacWilliams identities and give an example.

§2. Preliminaries

Let S be the ring $F_2 + uF_2 + vF_2$ where $u^2 = u$, $v^2 = v$, $uv = vu = 0$ and $F_2 = \{0,1\}$, a finite commutative ring with 8 elements. S is semi local ring with three maximal ideals and a principal ideal ring. It is not finite chain ring.

The ideals are follows;

$$
\begin{aligned}
I_0 &= \{0\}, \ I_1 = S \\
I_u &= \{0,u\}, \ I_v = \{0,v\}, \ I_{1+u+v} = \{0,1+u+v\} \\
I_{u+v} &= \{0,u,v,u+v\}, \ I_{1+u} = \{0,v,1+u,1+u+v\} \\
I_{1+v} &= \{0,u,1+v,1+u+v\}
\end{aligned}
$$

A linear code C over S length n is a $S-$submodule of S^n. An element of C is called a codeword.

For any $x = (x_0, x_1, \cdots, x_{n-1})$, $y = (y_0, y_1, \cdots, y_{n-1})$ the inner product is defined as

$$
x.y = \sum_{i=0}^{n-1} x_i y_i
$$

If $x.y = 0$ then x and y are said to be orthogonal. Let C be linear code of length n over S, the dual code of C

$$
C^\perp = \{x : \forall y \in C, x.y = 0\},
$$

which is also a linear code over S of length n. A code C is self orthogonal if $C \subseteq C^\perp$ and self dual if $C = C^\perp$.

A cyclic code C over S is a linear code with the property that if $c = (c_0, c_1, \cdots, c_{n-1}) \in C$ then $\sigma(C) = (c_{n-1}, c_0, \cdots, c_{n-2}) \in C$. A subset C of S^n is a linear cyclic code of length n iff it is polynomial representation is an ideal of $S[x]/\langle x^n - 1 \rangle$.

Let C be code over F_2 of length n and $\acute{c} = (\acute{c}_0, \acute{c}_1, \cdots, \acute{c}_{n-1})$ be a codeword of C. The Hamming weight of $\acute{c}$ is defined as $w_H(\acute{c}) = \sum_{i=0}^{n-1} w_H(\acute{c}_i)$ where $w_H(\acute{c}_i) = 1$ if $\acute{c}_i = 1$ and $w_H(\acute{c}_i) = 0$ if $\acute{c}_i = 0$. Hamming distance of C is defined as $d_H(C) = \min d_H(c, \acute{c})$, where for any $\acute{c} \in C$, $c \neq \acute{c}$ and $d_H(c, \acute{c})$ is Hamming distance between two codewords with $d_H(c, \acute{c}) = w_H(c - \acute{c})$.

Let $a \in F_2^{3n}$ with $a = (a_0, a_1, \cdots, a_{3n-1}) = (a^{(0)} | a^{(1)} | a^{(2)})$, $a^{(i)} \in F_2^n$ for $i = 0, 1, 2$. Let φ be a map from F_2^{3n} to F_2^{3n} given by $\varphi(a) = (\sigma(a^{(0)}) | \sigma(a^{(1)}) | \sigma(a^{(2)}))$ where σ is a cyclic

shift from F_2^n to F_2^n given by $\sigma\left(a^{(i)}\right) = ((a^{(i,n-1)}), (a^{(i,0)}), (a^{(i,1)}), \cdots, (a^{(i,n-2)}))$ for every $a^{(i)} = (a^{(i,0)}, \cdots, a^{(i,n-1)})$ where $a^{(i,j)} \in F_2$, $0 \le j \le n-1$. A code of length $3n$ over F_2 is said to be quasi cyclic code of index 3 if $\varphi(C) = C$.

§3. Gray Map

Let $x = a + ub + uc$ be an element of S where $a, b, c \in F_2$. We define Gray map Ψ from S to F_2^3 by

$$\Psi \quad : \quad S \to F_2^3$$
$$\Psi(a + ub + vc) \quad = \quad (a, a+b, a+c)$$

The Lee weight of elements of S are defined $w_L(a + ub + vc) = w_H(a, a+b, a+c)$ where w_H denotes the ordinary Hamming weight for binary codes. Hence, there is one element whose weight is 0, there are $u, v, 1+u+v$ elements whose weights are 1, there are $1+u, 1+v, u+v$ elements whose weights are 2, there is one element whose weight are 3.

Let C be a linear code over S of length n. For any codeword $c = (c_0, \cdots, c_{n-1})$ the Lee weight of c is defined as $w_L(c) = \sum_{i=0}^{n-1} w_L(c_i)$ and the Lee distance of C is defined as $d_L(C) = \min d_L(c, \acute{c})$, where for any $\acute{c} \in C$, $c \ne \acute{c}$ and $d_L(c, \acute{c})$ is Lee distance between two codewords with $d_L(c, \acute{c}) = w_L(c - \acute{c})$. Gray map Ψ can be extended to map from S^n to F_2^{3n}.

Theorem 3.1 *The Gray map Ψ is a weight preserving map from $(S^n,$ Lee weight$)$ to $(F_2^{3n}, Ham-$ ming weight$)$. Moreover it is an isometry from S^n to F_2^{3n}.*

Theorem 3.2 *If C is an $[n, k, d_L]$ linear codes over S then $\Psi(C)$ is a $[3n, k, d_H]$ linear codes over F_2, where $d_H = d_L$.*

§4. Skew Codes over S

We are interested in studying skew codes using the ring $S = F_2 + uF_2 + vF_2$ where $u^2 = u, v^2 = v, uv = vu = 0.$. We define non-trivial ring automorphism θ on the ring S by $\theta(a + ub + vc) = a + vb + uc$ for all $a + ub + vc \in S$.

The ring $S[x, \theta] = \{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} : a_i \in S, n \in N\}$ is called a skew polynomial ring. This ring is a non-commutative ring. The addition in the ring $S[x, \theta]$ is the usual polynomial addition and multiplication is defined using the rule, $(ax^i)(bx^j) = a\theta^i(b)x^{i+j}$. Note that $\theta^2(a) = a$ for all $a \in S$. This implies that θ is a ring automorphism of order 2.

Definition 4.1 *A subset C of S^n is called a skew cyclic code of length n if C satisfies the following conditions,*

(i) C is a submodule of S^n;

(ii) If $c = (c_0, c_1, \cdots, c_{n-1}) \in C$, then $\sigma_\theta(c) = \left(\theta(c_{n-1}), \theta(c_0), \cdots, \theta(c_{n-2})\right) \in C$.

Let $(f(x) + (x^n - 1))$ be an element in the set $S_n = S[x, \theta] / (x^n - 1)$ and let $r(x) \in S[x, \theta]$. Define multiplication from left as follows:

$$r(x)(f(x) + (x^n - 1)) = r(x)f(x) + (x^n - 1)$$

for any $r(x) \in S[x, \theta]$.

Theorem 4.2 S_n is a left $S[x, \theta]$-module where multiplication defined as in above.

Theorem 4.3 A code C in S_n is a skew cyclic code if and only if C is a left $S[x, \theta]$-submodule of the left $S[x, \theta]$-module S_n.

Theorem 4.4 Let C be a skew cyclic code in S_n and let $f(x)$ be a polynomial in C of minimal degree. If $f(x)$ is monic polynomial, then $C = (f(x))$ where $f(x)$ is a right divisor of $(x^n - 1)$.

Theorem 4.5 Let n be odd and C be a skew cyclic code of length n. Then C is equivalent to cyclic code of length n over S.

Proof Since n is odd, $gcd(2, n) = 1$. Hence there exist integers b, c such that $2b + nc = 1$. So $2b = 1 - nc = 1 + zn$ where $z > 0$. Let $a(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$ be a codeword in C. Note that $x^{2b} a(x) = \theta^{2b}(a_0) x^{1+zn} + \theta^{2b}(a_1) x^{2+zn} + \cdots + \theta^{2b}(a_{n-1}) x^{n+zn} = a_{n-1} + a_0 x + \cdots + a_{n-2} x^{n-2} \in C$. Thus C is a cyclic code of length n. $\square$

Corollary 4.6 Let n be odd. Then the number of distinct skew cyclic codes of length n over S is equal to the number of ideals in $S[x] / (x^n - 1)$ because of Theorem 7. If $x^n - 1 = \prod_{i=0}^{r} p_i^{s_i}(x)$ where $p_i(x)$ are irreducible polynomials over F_2. Then the number of distinct skew cyclic codes of length n over S is $\prod_{i=0}^{r}(s_i + 1)^2$.

Example 4.7 Let $n = 15$ and $g(x) = x^4 + x^3 + x^2 + x + 1$. Then $g(x)$ generates a skew cyclic codes of length 15. This code is equivalent to a cyclic code of length 15. Since $x^{15} - 1 = (x + 1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)$, it follows that there are 2^8 skew cyclic code of length 15.

Definition 4.8 A subset C of S^n is called a skew quasi-cyclic code of length n if C satisfies the following conditions:

(i) C is a submodule of S^n;

(ii) If $e = (e_{0,0}, \cdots, e_{0,l-1}, e_{1,0}, \cdots, e_{1,l-1}, \cdots, e_{s-1,0}, \cdots, e_{s-1,l-1}) \in C$, then $\tau_{\theta,s,l}(e) = (\theta(e_{s-1,0}), \cdots, \theta(e_{s-1,l-1}), \theta(e_{0,0}), \cdots, \theta(e_{0,l-1}), \theta(e_{s-2,0}), \cdots, \theta(e_{s-2,l-1})) \in C$.

We note that $x^s - 1$ is a two sided ideal in $S[x, \theta]$ if $m | s$ where $m = 2$ is the order of θ. So $S[x, \theta] / (x^s - 1)$ is well defined.

The ring $M_s^l = (S[x, \theta] / (x^s - 1))^l$ is a left $M_s = S[x, \theta] / (x^s - 1)$ module by the following multiplication on the left $f(x)(g_1(x), \cdots, g_l(x)) = (f(x)g_1(x), \cdots, f(x)g_l(x))$. If the map γ is defined by

$$\gamma : S^n \longrightarrow M_s^l$$

$(e_{0,0}, \cdots, e_{0,l-1}, e_{1,0}, \cdots, e_{1,l-1}, \cdots, e_{s-1,0}, \cdots, e_{s-1,l-1}) \mapsto (c_0(x), \cdots, c_{l-1}(x))$ such that $e_j(x) = \sum_{i=0}^{s-1} e_{i,j} x^i \in M_s^l$ where $j = 0, 1, \cdots, l-1$ then the map γ gives a one to one correspondence S^n and the ring M_s^l.

Theorem 4.9 *A subset C of S^n is a skew quasi-cyclic code of length $n = sl$ and index l if and only if $\gamma(C)$ is a left S_s-submodule of M_s^l.*

§5. MacWilliams Identities

Let the elements of S be represented as $S = \{f_1, f_2, \cdots, f_8\} = \{0, 1, u, v, 1+u, 1+v, u+v, 1+u+v\}$ where the order of elements is fixed.

Definition 5.1 *Define $\chi : S \longrightarrow \mathbb{C}^*$ by $\chi(a+ub+vc) = (-1)^{a+b+c}$. χ is a non-trivial character of each non-zero ideal I of S. Hence we have $\sum_{a \in I} \chi(a) = 0$.*

Lemma 5.2 *Let C be a linear code over S of length n. Then for any $m \in S^n$,*

$$\sum_{c \in C} \chi(c.m) = \begin{cases} 0, & \textit{if } m \notin C^\perp \\ |C|, & \textit{if } m \in C^\perp \end{cases}$$

Theorem 5.3([11]) *Let C be a linear code over S of length n and $\widehat{f}(c) = \sum_{m \in S^n} \chi(c.m) f(m)$. Then $\sum_{m \in C^\perp} f(m) = \frac{1}{|C|} \sum_{c \in C} \widehat{f}(c)$.*

Let A is a 8×8 matrix. A matrix defined by $A(i,j) = \chi(f_i f_j)$. The matrix A is given as follows

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 \end{bmatrix}$$

Definition 5.4 *Let C be a linear code of length n over S, then $Lee_C(x,y) = \sum_{c \in C} x^{3n-w_L(c)} y^{w_L(c)}$ can be called as the Lee weight enumerator of C and $Ham_C(x,y) = \sum_{c \in C} x^{n-w_H(c)} y^{w_H(c)}$ can be called as the Hamming weight enumerator of C. Besides,*

$$Swe_C(x,y,z,w) = \sum_{c \in C} x^{n_0(c)} y^{n_1(c)} z^{n_2(c)} w^{n_3(c)}$$

is the symmetric weight enumerator where $n_i(c)$ denote the number of elements of c with Lee

weight $0, 1, 2, 3$, respectively.

Definition 5.5   *The complete weight enumerator of a linear code C over R is defined as $cwe_C(x_1, x_2, \cdots, x_8) = \sum_{c \in C} x_1^{n_{f_1}(c)} \cdots x_8^{n_{f_8}(c)}$ where $n_{f_i}(c)$ is the number of appearances of f_i in the vector c.*

The complete weight enumerator gives us a lot of information about the code, such as the size of the code, the minimum weight of the code and the weight enumerator of the code for any weight function.

We can define the symmetrized weight enumerator as follows.

Definition 5.6   *Let C be a linear code of length n over S. Then define the symmetrized weight enumerator of C as*

$$Swe_C(x, y, z, w) = cwe_C(x, w, y, y, z, z, z, y)$$

Here x represents the elements that have weight 0 (the 0 element), y represents the elements with weight 1 (the elements $u, v, 1+u+v$), z represents the elements with weight 2 (the elements $1 + u, 1 + v, u + v$), w represents the elements with weight 3 (the element 1).

Theorem 5.7   *Let C be a linear code of length n over S and let $C^{\perp}$ be its dual. Then $cwe_{C^{\perp}}(x_1, x_2, \cdots, x_8) = \frac{1}{|C|} cwe_C(A.(x_1 \ x_2 \ \cdots \ x_8)^{\top})$ where $()^{\top}$ denotes the transpose.*

Theorem 5.8   *Let C be a linear code of length n over S and let $C^{\perp}$ be its dual. Then $Swe_{C^{\perp}}(x, y, z, w) = \frac{1}{|C|} Swe_C(x + w + 3y + 3z, x - w - 3y + 3z, x - w + y - z, x + w - y - z).$*

Proof The proof follows simply from calculating the matrix product

$$A.(x \ w \ y \ y \ z \ z \ z \ y)^{\top}$$

where $()^{\top}$ denotes the transpose.   □

Theorem 5.9   *Let C be a linear code of length n over S. Then,*

(i) $Lee_C(x, y) = Swe_C(x^3, x^2y, y^2x, y^3);$

(ii) $Lee_{C^{\perp}}(x, y) = \frac{1}{|C|} Lee_C(x + y, x - y).$

Proof (i) Let $w_L(c) = n_1(c) + 2n_2(c) + 3n_3(c)$ where $n_i(c)$ denote the number of elements of c with Lee weight $0, 1, 2, 3$, respectively. Since $n = n_0(c) + n_1(c) + n_2(c) + n_3(c)$, $3n - w_L(c) = 3n_0(c) + 2n_1(c) + n_2(c)$. From the definition,

$$
\begin{aligned}
Lee_C(x, y) &= \sum_{c \in C} x^{3n - w_L(c)} y^{w_L(c)} = \sum_{c \in C} x^{3n_0(c) + 2n_1(c) + n_2(c)} y^{n_1(c) + 2n_2(c) + 3n_3(c)} \\
&= \sum_{c \in C} x^{3n_0(c)} (x^2 y)^{n_1(c)} (y^2 x)^{n_2(c)} y^{3n_3(c)} = Swe_C(x^3, x^2 y, y^2 x, y^3)
\end{aligned}
$$

(ii) From Theorems 5.7 and 5.8,

$$
\begin{aligned}
Lee_{C^\perp}(x,y) &= \frac{1}{|C|}Swe_C(x^3 + 3x^2y + 3y^2x + y^3, x^3 - y^3 - 3x^2y + 3xy^2, \\
&\quad x^3 - y^3 + x^2y - xy^2, x^3 + y^3 - x^2y - xy^2) \\
&= \frac{1}{|C|}Swe_C((x+y)^3, (x+y)^2(x-y), (x-y)^2(x+y), (x-y)^3) \\
&= \frac{1}{|C|}Lee_C(x+y, x-y). \qquad \square
\end{aligned}
$$

Theorem 5.10 *Let C be a linear code of length n over S. Then we have*

(i) $Ham_{C^\perp}(x,y) = \frac{1}{|C|}Ham_C(x + 7y, x - y);$
(ii) $Ham_C(x,y) = Swe_C(x,y,y,y).$

Proof (i) It is straightforward from [13].

(ii) The Hamming weight $w_H(c)$ is defined as $w_H(c) = n_0(c) + n_1(c) + n_2(c) + n_3(c)$.

$$
\begin{aligned}
Ham_C(x,y) &= \sum_{c \in C} x^{n-w_H(c)}y^{w_H(c)} = \sum_{c \in C} x^{n_0(c)}y^{n_1(c)+n_2(c)+n_3(c)} \\
&= Swe_C(x,y,y,y). \qquad \square
\end{aligned}
$$

Example 5.11 Let $C = \{(0,0), (v,v)\}$ be a linear code of length 2 over S. The Lee weight enumerator is $Lee_C(x,y) = x^6 + x^4y^2$; the Hamming enumerator is $Ham_C(x,y) = x^2 + y^2$. Lee weight enumerator of $C^\perp$ is $Lee_{C^\perp}(x,y) = x^6 + 4x^5y + 7x^4y^2 + 8x^3y^3 + 7x^2y^4 + 5xy^5 + y^6$; Hamming weight enumerator of $C^\perp$ is

$$
Ham_{C^\perp}(x,y) = x^2 + 6xy + 25y^2.
$$

References

[1] T.Abualrub, P.Seneviratne, On θ-cyclic codes over $F_2 + vF_2$, *Australasian Journal of Com.*, 54(2012), 115-126.

[2] T.Abualrub, A.Ghrayeb, N.Aydın, I.Siap, On the construction of skew quasi-cyclic codes, *IEEE Transsactions on Information Theory*, Vol 56, No.5(2010), 2081-2090.

[3] R.K.Bandi, M.Bhaintwal, Codes over $Z_4 + vZ_4$, *IEEE*, (2014), 978-14799-3080-7.

[4] M.Bhaintwal, Skew quasi-cyclic codes over Galois rings, *Des. Codes Cryptogr.*, DOI.10.1007/ s10623-011-9494-0.

[5] D.Boucher, W.Geiselmann, F.Ulmer, Skew cyclic codes, *Appl. Algebra. Eng.Commun Comput.*, Vol.18, No.4(2007) 379-389.

[6] D.Boucher, F.Ulmer, Coding with skew polynomial rings, *Journal of Symbolic Computation*, 44(2009), 1644-1656.

[7] J.Gao, L.Shen, F.W.Fu, Skew generalized quasi-cyclic codes over finite fields, *arXiv:*1309, 1621v1.

[8] J.Gao, Skew cyclic codes over $F_p + vF_p$, *J. Appl. Math. & Informatics*, 31(2013), 337-342.

[9] J.Gao, Y.Gao, Some Results on Linear Codes over $Z_4 + vZ_4$, *arXiv:* 1402.6 771v1, 2014.

[10] A.R.Hammons, V.Kumar, A.R.Calderbank, N.J.A.Sloane, P. Sole, The Z_4-linearity of Kerdock, Preparata, Goethals and related codes, *IEEE Trans. Inf. Theory*, 40 (1994) 301-319.

[11] F.J.MacWilliams and N.J.A.Sloane, *The Theory of Error Correcting Codes*, North-Holland, Amsterdam, The Netherlands, 1977.

[12] I.Siap, T.Abualrub, N.Aydın, P.Seneviratne, Skew cyclic codes of arbitrary length, *Int. Journal of Information and Coding Theory*, 2010.

[13] J.Wood, Duality for modules over finite rings and applications to coding theory, *Amer. J. Math.*, 121(1993), 555-575.

[14] M.Wu, Skew cyclic and quasi-cyclic codes of arbitrary length over Galois rings, *International Journal of Algebra*, Vol.7, No.17(2013), 803-807.

[15] B.Yildiz, S.Karadeniz, Linear codes over $Z_4 + uZ_4$, MacWilliams identities, projections and formally self-dual codes, *Finite Fields and Their Applications*, 27(2014), 24-40.