Malaysian Journal of Science **34** (2): 222 – 226 (2015)

MacWilliams Equivalence Theorem for the Lee Weight over $\mathbb{Z}_{4p+1}$

Aleams Barra*

Fakultas Matematika dan Ilmu Pengetahuan Alam, Institut Teknologi Bandung, Bandung, 40132, Indonesia
*Corresponding Author: barra@math.itb.ac.id

ABSTRACT For codes over fields, the MacWilliams equivalence theorem give us a complete characterization when two codes are equivalent. Considering the important role of the Lee weight in coding theory, one would like to have a similar results for codes over integer residue rings equipped with the Lee weight. We would like to prove that the linear isomorphisms between two codes in $\mathbb{Z}_n^m$ that is preserving the Lee weight are exactly the maps of the form $f(x_1, x_2, \ldots, x_m) = (u_1 x_{\sigma(1)}, u_2 x_{\sigma(2)}, \ldots, u_m x_{\sigma(m)})$ where $u_1, \ldots, u_m \in \{-1, 1\}$ and $\sigma \in S_n$. The problem is still largely open. Wood proved the result for codes over $\mathbb{Z}_n$ where n is a power of 2 or 3. In this paper we prove the result for prime n of the form $4p+1$ where p is prime.

(**Keywords**: MacWilliams equivalence, extension theorem, Lee weight, codes over rings)

INTRODUCTION

Let C and C' be linear codes over finite fields F. The two codes are equivalent if there is a linear isometry between C and C', that is, if there is a linear map $f : \mathrm{C} \to \mathrm{C}'$ that preserves the Hamming weight of every codeword $x \in \mathrm{C}$. The MacWilliams equivalence theorem [1] states that linear isometries are maps of the form

$$f(x_1, \ldots, x_m) = (u_1 x_{\sigma(1)}, \ldots, u_m x_{\sigma(m)}),$$

where $u_i \neq 0$ and $\sigma \in S_n$.

The celebrated results of Hammons, Calderbank, Kumar, Sloane, and Sole [2] show that a class of optimal nonlinear codes called the Kerdock and Preparata can be considered as linear codes over $\mathbb{Z}_4$ equipped with the Lee weight. Since then, the Lee weight had become an important weight in coding theory besides the Hamming weight.

Generalizing Macwilliams Theorem for codes over rings equipped with the Hamming weight proved to be successful. Ward and Wood [3] gave a new proof of the MacWilliams Theorem for codes over fields using a character theory technique. Greferath and Schmidt [4] proved the same result using a combinatorial method. Later, using the same character theory technique, Wood [5] proved that the MacWilliams Theorem holds for a class of rings called the Frobenius rings. In 2008, Wood [6] proved that there was no larger class of rings in which the theorem holds, by showing that to have the MacWilliams theorem over a ring, the ring is necessary to be Frobenius.

Another direction of generalizing Macwilliams theorem is by considering weights other than the Hamming weight. Goldberg [7] proved the theorem for the symmetrized weight composition. Wood [8] gave a sufficient condition when the theorem holds for general weights in terms of invertibility of some matrix A. On the same paper, Wood showed that using this criterion, the MacWilliams theorem for the Lee weight in $\mathbb{Z}_n$, for n is a power of 2 or 3 or prime of the form $n = 2p+1$ where p is also prime.

In this paper, we will show that for n prime, the matrix A in the criterion of Wood above, has a circulant structure. By using this structure, we prove that the Macwilliams theorem for the Lee weight holds for all primes of the form $n = 4p+1$ where p is also prime.

DEFINITIONS

A *linear code* C over a commutative ring $\mathbb{Z}_n$ of length m is an $\mathbb{Z}_n$-submodule of $\mathbb{Z}_n^m$. For $k \in \mathbb{Z}_n$ the Lee weight of k, denoted by $L(k)$ is defined as

$$L(k) := \min\{k, n-k\}.$$

For example for $3, 4, 5 \in \mathbb{Z}_7$ we have $L(3) = L(4) = 3$ and $L(5) = 2$ respectively. We can extend this definition

of the Lee weight to any vector $x=(x_1,\ldots,x_m)\in\mathbb{Z}_n^m$ by defining

$$L(x):=\sum_{i=1}^{m}L(x_i).$$

Let C,C' be codes over $\mathbb{Z}_n$. A linear map $f:\mathrm{C}\to\mathrm{C}'$ is called a *Lee isometry* if for every $x\in\mathrm{C}$ we have $L(x)=L(f(x))$.

We say that the equivalence theorem for the Lee weight holds for $\mathbb{Z}_n$ if for every Lee isometry $f:\mathrm{C}\to\mathrm{C}'$ there is a permutation $\sigma\in S_n$ and $u_1,\ldots,u_n\in\{-1,1\}$ such that

$$f(x_1,x_2,\ldots,x_n)=(u_1x_{\sigma(1)},\ldots,u_nx_{\sigma(n)}).$$

Consider $\mathbb{Z}_n$ as $\{0,1,\ldots,n-1\}$. For $k=1,\ldots,\lfloor n/2\rfloor$, define the Lee class of k by $C_k:=\{k,n-k\}=\{k,-k\}$. Note that C_k is the set of all elements in $\mathbb{Z}_n$ of the Lee weight k, that is $L(x)=k$ if and only if $x\in C_k$. Notice that if $x,y\in C_k$ for some k then $L(xa)=L(ya)$ for every $a\in\mathbb{Z}_n$.

CRITERION OF WOOD

For every ring $\mathbb{Z}_n$ associate a $\lfloor n/2\rfloor\times\lfloor n/2\rfloor$ matrix $A=(a_{ij})$ defined by

$$a_{ij}:=L(a\cdot b)\text{ where }a\in C_i,b\in C_j,$$

where the multiplication $a\cdot b$ is a multiplication in $\mathbb{Z}_n$. It is easy to see that the definition of A is independent of the choice of $a\in C_i$ and $b\in C_j$. For example, the matrix A associated to the ring $\mathbb{Z}_7$ is

$$A=\begin{pmatrix}L(1\cdot1)&L(1\cdot2)&L(1\cdot3)\\L(2\cdot1)&L(2\cdot2)&L(2\cdot3)\\L(3\cdot1)&L(3\cdot2)&L(3\cdot3)\end{pmatrix}=\begin{pmatrix}1&2&3\\2&3&1\\3&1&2\end{pmatrix}.$$

The restriction of the result of Wood [8] to the Lee weight and to the ring $\mathbb{Z}_n$ gives a sufficient condition for $\mathbb{Z}_n$ to have an equivalence theorem for the Lee weight. The criterion is given in terms of the matrix A associated to $\mathbb{Z}_n$.

Teorema 1. Let A be the matrix associated to $\mathbb{Z}_n$. If A is invertible (as matrix over reals) then the equivalence theorem holds for $\mathbb{Z}_n$.

Proof : See [8] (Proposition 12).

For example, the matrix A associated to the ring $\mathbb{Z}_7$ is invertible and hence the equivalence theorem holds for $\mathbb{Z}_7$.

THE STRUCTURE OF MATRIX A

Notice that the invertibility of A is invariant under the row and column permutations. We will show that when n is prime,after several row and column permutations, the A matrix has a circulant structure.

Let $n\geq3$ be prime and r be a primitive root modulo n, write $t=\lfloor n/2\rfloor$. One can obtain the matrix A in two steps. First, we can make a multiplication table over $\mathbb{Z}_n$ where the columns and rows are indexed by $1,2,\ldots,t$. Then the entries of the matrix A are the Lee weight of the inner entries in the multiplication table. For example, for $\mathbb{Z}_7$ the matrix A can be obtained as follows

	1	2	3
1	1	2	3
2	2	4	6
3	3	6	2

$$\to\begin{pmatrix}L(1)&L(2)&L(3)\\L(2)&L(4)&L(6)\\L(3)&L(6)&L(2)\end{pmatrix}=\begin{pmatrix}1&2&3\\2&3&1\\3&1&2\end{pmatrix}.$$

If the rows are instead indexed by $2,1,3$ and the columns are indexed by $3,1,2$, then the multiplication table and the matrix A are given below

	3	1	2
2	1	2	4
1	3	1	2
3	9	3	6

$$\to A=\begin{pmatrix}1&2&3\\3&1&2\\2&3&1\end{pmatrix}.$$

Since the new table can be obtained by row and column permutations of the previous table, then the new matrix A can also be obtained by row and column permutations of the old matrix A. Since we are only interested in the invertibility of the matrix A, we no longer have to differentiate between the old and the new matrix A and simply call them both A.

Proposition 2. Let n be prime. Then the matrix A is circulant.

Proof: Let r be a primitive root modulo n and let $t:=\lfloor n/2\rfloor$. Since $r^t=-1$, for every $k=0,1,\ldots,t-1$ we have $\{r^k,r^{k+t}\}=\{r^k,-r^k\}$ is one of the Lee class C_s for

some s. Hence $1, r, r^2, \ldots, r^{t-1}$ are representatives of $C_1, C_2, \ldots, C_t$ (not necessarily in that order).

Now consider the multiplication table where the rows are indexed by $1, r, \ldots, r^{t-1}$ and the columns are indexed by $r^{t-1}, r^{t-2}, \ldots, 1$

	r^{t-1}	r^{t-2}	$\cdots$	1
1	r^{t-1}	r^{t-2}	$\cdots$	1
r	r^t	r^{t-1}	$\cdots$	r
$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$
r^{t-1}	r^{2t-2}	r^{2t-3}	$\cdots$	r^{t-1}

Using the fact that $r^t = -1$ and $L(a) = L(-a)$ for every $a \in \mathbb{Z}_n$., we have

$$A = \begin{pmatrix} L(r^{t-1}) & L(r^{t-2}) & \cdots & L(1) \\ L(r^t) & L(r^{t-1}) & \cdots & L(r) \\ L(r^{t+1}) & L(r^t) & \cdots & L(r^2) \\ \vdots & \vdots & \cdots & \vdots \\ L(r^{2t-2}) & L(r^{2t-3}) & \cdots & L(r^{t-1}) \end{pmatrix}$$

$$= \begin{pmatrix} L(r^{t-1}) & L(r^{t-2}) & \cdots & L(1) \\ L(1) & L(r^{t-1}) & \cdots & L(r) \\ L(r) & L(1) & \cdots & L(r^2) \\ \vdots & \vdots & \cdots & \vdots \\ L(r^{t-2}) & L(r^{t-3}) & \cdots & L(r^{t-1}) \end{pmatrix}.$$

Therefore A is circulant.

Given a circulant matrix C of size n where the first row of C is $(a_0, \ldots, a_{n-1})$ define a polynomial P_C, called the *presenter* of C by

$$P_C(x) = a_0 x^{n-1} + a_1 x^{n-2} + \cdots + a_{n-1}.$$

The following theorem helps us identifying the invertibility of a circulant matrix.

Proposition 4. (Kra [9], Corollary 10). Let C be a ciruculant matrix with a presenter polynomial P_C. The following are equivalent

1. C is invertible.
2. $P_C(\grave{o}) \neq 0$ for all complex root $\grave{o}$ of $x^n - 1$.
3. $P_C(x)$ and $x^n - 1$ are relatively prime.

In the case where the size of the circulant matrix is prime number, we have the following result.

Proposition 4. (Kra [9], Proposition 23). Let C be a circulant matrix of size p where p is a prime number. Let $(c_0, c_1, \ldots, c_{p-1}) \in \mathbb{Z}^p$ be the first row of C. If $\sum_{j=0}^{p-1} c_j \neq 0$ and $c_0, c_1, \ldots, c_{p-1}$ are not all the same, then C is invertible.

By using the above proposition, we have a new proof of the result discovered by Wood [8].

Corollary 5. If $n = 2p+1$ where p is a prime number, then the equivalence theorem holds for $\mathbb{Z}_{2p+1}$.

Proof: Let A be the circulant matrix associated with $\mathbb{Z}_{2p+1}$. This matrix has size p and the entries of its first row is a permutation of $\{1, 2, \ldots, p\}$. By Proposition 4 we have that A is invertible and hence by the criterion of Wood the result follows.

MAIN RESULT

In this section we will consider the equivalence theorem for $\mathbb{Z}_{4p+1}$ where p is an odd prime number. It is known that when p and $4p+1$ are prime, then 2 is a primitive root modulo $4p+1$ (see [10] page 497 for example). It follows that the first row of the matrix A associated to $\mathbb{Z}_{4p+1}$ is

$$(1, L(2), L(2^2), \ldots, L(2^{2p-1})).$$

Let P_A be the presenter polynomial of A. We will show that A is invertible by showing that $P_A(x)$ and $x^{2p} - 1$ has no common root.

Theorem 6. The equivalence theorem holds for $\mathbb{Z}_{4p+1}$ where p and $4p+1$ are prime.

Proof: The complex roots of $x^{2p} - 1$ form a cyclic group of order $2p$. If η is a root of $x^{2p} - 1$, then the order of η is one of $1, 2, p$ or $2p$. By the previous observation, we know that

$$P_A(x) = x^{2p-1} + L(2)x^{2p-2} + \cdots + L(2^{2p-1})$$

is the presenter matrix of A. We will show that there is no root η of $x^{2p} - 1$ which is also a root of $P_A(x)$. We consider several cases:

- $\text{ord}(\eta) = 1$.
  In this case we have $\eta = 1$. Since the set $\{1, L(2), \ldots, L(2^{2p-1})\}$ is equal to $\{1, 2, \ldots, 2p\}$, then $P_A(1) = \sum_{j=1}^{2p} j = \frac{(2p)(2p+1)}{2} \neq 0$.
- $\text{ord}(\eta) = 2$.
  Then $\eta = -1$ and

$$P_A(-1) = \sum_{i=0}^{2p-1} L(2^i)(-1)^{2p-1-i}$$
$$= -L(1) + L(2) - L(2^2) - \cdots + L(2^{2p-1}).$$

  If $P_A(-1) = 0$ then

$$\sum_{i \text{ odd}} L(2^i) = \sum_{i \text{ even}} L(2^i).$$

  It follows that

$$p(2p+1) = \sum_{j=1}^{2p} L(2^i) = 2 \sum_{j \text{ odd}} L(2^j).$$

  But this is impossible since the left hand side is odd while the right hand side is even.
- $\text{ord}(\eta) = p$.
  Then $\eta^j = \eta^{j+p}$ for all j. If $P(\eta) = 0$ then

$$\sum_{j=0}^{p-1} \left(L(2^j) + L(2^{j+p})\right)\eta^j = 0.$$

  Hence η is a root of $Q(x) = \sum_{j=0}^{p-1} a_j x^j$ where $a_j = L(2^j) + L(2^{j+p})$. Since the minimal polynomial over $\mathbb{Z}$ of η is $m(x) = \sum_{i=0}^{p-1} x^p$, then $m(x) \mid Q(x)$. But $m(x)$ and $Q(x)$ are of the same degree. Hence $Q(x) = K \cdot m(x)$ for some positive integer K. In particular, for all j we have $L(2^j) + L(2^{j+p}) = K$. Now

$$pK = \sum_{j=0}^{p-1} \left(L(2^j) + L(2^{j+p})\right)$$
$$= \sum_{i=1}^{2p} i = p(2p+1).$$

  Hence $1 + L(2^p) = K = 1 + 2p$ and we conclude that $L(2^p) = 2p$. Note that for all $m \in \mathbb{Z}_n$ we have $L(m) \equiv \pm m \pmod{n}$. It follows that

$$\pm 2^p \equiv L(2^p) \equiv 2p \pmod{4p+1}$$
$$2 \cdot (\pm 2^p) \equiv 4p \equiv -1 \pmod{4p+1}.$$

  Squaring both sides we have $2^{2p+2} \equiv 1 \pmod{4p+1}$. Since 2 is a generator of $\mathbb{Z}_{4p+1}^{\times}$, then $4p \mid 2p+2$ which is impossible since $4p > 2p+2$ for odd prime p.
- $\text{ord}(\eta) = 2p$.
  Then $\eta^p = -1$. If $P_A(\eta) = 0$, then

$$0 = \sum_{j=0}^{2p-1} \left(L(2^j) - L(2^{j+p})\right)\eta^j.$$

  Since the minimal polynomial of η in this case is $m(-x)$, then for all j we have

$$L(2^j) - L(2^{j+p}) = L(2^{j+1+p}) - L(2^{j+1}).$$

  In particular for $j = 0$ we have

$$L(2^p) + L(2^{p+1}) = L(1) + L(2) = 3.$$

  Reducing the equation modulo $4p+1$ we have

$$\pm 2^p \pm 2^{p+1} \equiv 3 \pmod{4p+1}.$$

  Squaring both sides,

$$-1 \pm 4 - 4 \equiv 9 \pmod{4p+1}.$$

  So either $-1 \equiv 9 \pmod{4p+1}$ or $-9 \equiv 9 \pmod{4p+1}$. This implies that $4p+1 \mid 10$ or $4p+1 \mid 18$ which is impossible for $p \geq 3$.

In any case we have $p_A(\eta) \neq 0$ and hence A is invertible. Therefore $\mathbb{Z}_{4p+1}$ satisfies the equivalence theorem according to the criterion of Wood.

CONCLUSION AND CONJECTURE

By using Wood's criterion, we are able to show the equivalence theorem holds for the Lee weight for codes over $\mathbb{Z}_{4p+1}$ where p and $4p+1$ are prime. By using the circulant structure of the matrix A, the equivalence theorem holds true for $\mathbb{Z}_p$ if and only if $P_A(x)$ and $x^p - 1$ has no constant common divisor in $\mathbb{Z}[x]$. A computer search on MAPLE shows that for the first 2000 prime numbers the polynomial $P_A(x)$ is irreducible over $\mathbb{Z}$ and hence for those primes, the ring $\mathbb{Z}_p$ satisfies the equivalence theorem. Based on this observation we strongly believe that the equivalence theorem holds for $\mathbb{Z}_p$ and for any prime p.

ACKNOWLEDGEMENT

This research is supported by Riset KK ITB 2015.

REFERENCE

1. MacWilliams, F.J. (1962). Combinatorial Problems of Elementary Abelian Groups, Doctoral dissertation, Radcliffe College.
2. A Roger Hammons Jr, P Vijay Kumar, A Robert Calderbank, Neil JA Sloane, and Patrick Solé. The z 4-linearity of kerdock, preparata, goethals, and related codes. Information Theory, IEEE Transactions on, 40(2):301–319, 1994.
3. Ward, H. N., & Wood, J. A. (1996). Characters and the equivalence of codes. Journal of Combinatorial Theory, Series A, 73(2), 348-352.
4. Greferath, Marcus and Schmidt, Stefan E. Finite-ring combinatorics and MacWilliams' equivalence theorem. In Journal of Combinatorial Theory, Series A, pages 17–28. Elsevier, 2000.
5. Wood, J. A. (1999). Duality for modules over finite rings and applications to coding theory. American journal of Mathematics, 121(3), 555-575.
6. Wood, J. (2008). Code equivalence characterizes finite Frobenius rings. Proceedings of the American Mathematical Society, 136(2), 699-706.
7. Goldberg, D. Y. (1980). A generalized weight for linear codes and a Witt-MacWilliams theorem. Journal of Combinatorial Theory, Series A, 29(3), 363-367.
8. Wood, J. A.. Extension theorems for linear codes over finite rings. In Applied algebra, algebraic algorithms and error-correcting codes, pages 329–340. Springer, 1997.
9. Irwin Kra and Santiago R Simanca. On circulant matrices. Notices of the AMS, 59(3):368–377, 2012.
10. Thomas Koshy. Elementary number theory with applications. Academic press, 2002.