Scientific Research Publishing

Advances in Linear Algebra & Matrix Theory, 2020, 10, 1-5
https://www.scirp.org/journal/alamt
ISSN Online: 2165-3348
ISSN Print: 2165-333X

Linear Codes over the Finite Ring Z_{15}

Wensheng Li*, Lingyu Wan, Mengtian Yue, Wei Chen, Xuedong Zhang

Langfang Normal University, Langfang, China
Email: *liwensheng@lfnu.edu.cn

How to cite this paper: Li, W.S., Wan, L.Y., Yue, M.T., Chen, W. and Zhang, X.D. (2020) Linear Codes over the Finite Ring Z_{15}. *Advances in Linear Algebra & Matrix Theory*, **10**, 1-5.
https://doi.org/10.4236/alamt.2020.101001

Received: March 3, 2020
Accepted: March 28, 2020
Published: March 31, 2020

Abstract

In this paper, the structure of the non-chain ring Z_{15} is studied. The ideals of the ring Z_{15} are obtained through its non-units and the Lee weights of elements in Z_{15} are presented. On this basis, by the Chinese Remainder Theorem, we construct a unique expression of an element in Z_{15}. Further, the Gray mapping from $\mathbb{Z}_{15}^n$ to $\mathbb{Z}_{15}^{2n}$ is defined and it's shown to be distance preserved. The relationship between the minimum Lee weight and the minimum Hamming weight of the linear code over the ring Z_{15} is also obtained and we prove that the Gray map of the linear code over the ring Z_{15} is also linear.

Keywords

Lee Weight, Hamming Weight, Gray Map, Dual Code

1. Introduction

Error correcting codes and error detection codes play an important role in data networks and satellite applications. Most coding theory is interested. Linear code has a clear structure and it is easy to find, understand, edit and decode for codes over finite rings. Since the 1970s, there are many research papers about codes over the finite ring. Several good nonlinear binary codes have been discovered. The circulation code on Z_4 is composed of a Gary mapping structure [1]. After that, many researchers carried out more and more research on the code of finite ring [2] [3] [4] [5] [6]. The importance of finite rings in algebraic coding theory was established in the early 1990s by observing that some non-linear binary codes actually allow a linear representation of Z_4 (see [1] [7]). It is also noted that the codes on the ring are particularly useful, if the distance function in the alphabet is not given by the usual Hamming metric, but by the homogeneous weight [8]. Examples of homogeneous weights are Hamming weights on finite fields and Lee weights on Z_4. The homogeneous weight can be a natural extension of the Hamming weight of the code over finite rings.

In this paper, we will concern the linear code over the ring Z_{15}, which has $p \cdot q$ elements and $p \neq q$. In the first section, we get the ideals of the ring Z_{15} through its non-units and give the Lee weights of elements in Z_{15}. What's more, we construct a unique expression of an element in Z_{15}. In the second section, we obtain the generate matrix of the dual code of a linear code over the ring $\mathbb{Z}_{15}$, give the definition of Gray mapping from $\mathbb{Z}_{15}^n$ to $\mathbb{Z}_{15}^{2n}$ and show that this Gray mapping is distance preserved. In the third section, we prove that the minimal Lee weight of C is equal to the minimal Hamming weight of its Gray Mapping. Further, the linear property of the Gray mapping of a linear code is obtained.

2. The Ring $\mathbb{Z}_{15}$

The ring $\mathbb{Z}_{15}$ is a non-chain ring, whose units are {1, 2, 4, 7, 8, 11, 13} and non-units are {0, 3, 5, 6, 9, 10, 12}. It has three ideals as follows,

$$I_{(0)} = \{0\},\ I_{(3)} = 3\mathbb{Z}_{15} = \{0,3,6,9,12\},\ I_{(5)} = 5\mathbb{Z}_{15} = \{0,5,10\}$$

The maximal ideal of the ring $\mathbb{Z}_{15}$ are $I_{(3)}$ and $I_{(5)}$, and we have $\mathbb{Z}_{15}/I_{(3)} = F_3$ and $\mathbb{Z}_{15}/I_{(5)} = F_5$. By the Chinese Remainder Theorem, we have

$$\mathbb{Z}_{15} = I_{(3)} \oplus I_{(5)}.$$

Thus, for every $a \in \mathbb{Z}_{15}$, $a = b \cdot 3 + d \cdot 5$. Let $b \in I_{(3)}$ and $d \in I_{(5)}$, then b and d in the expression are unique. The Lee weight of $a \in \mathbb{Z}_{15}$ is defined as $W_L(a) = 2$ if $b \neq 0$ and $d \neq 0$, $W_L(a) = 0$ if $b = 0$ and $d = 0$, and $W_L(a) = 1$ if either $b = 0$ or $d = 0$. Then the Lee weights of elements in $\mathbb{Z}_{15}$ are as follows,

$$W_L(0) = 0;\ W_L(1) = 2;\ W_L(2) = 2;\ W_L(3) = 1;\ W_L(4) = 2;$$

$$W_L(5) = 1;\ W_L(6) = 1;\ W_L(7) = 2;\ W_L(8) = 2;\ W_L(9) = 1;$$

$$W_L(10) = 1;\ W_L(11) = 2;\ W_L(12) = 1;\ W_L(13) = 2;\ W_L(14) = 2.$$

3. Linear Codes over the Ring $\mathbb{Z}_{15}$

A linear code C over the ring $\mathbb{Z}_{15}$ is a additive sub-module. For every code word $x = (x_1, x_2, \cdots, x_n)$ and $y = (y_1, y_2, \cdots, y_n)$ in C, the inner product of x and y is defined as $\langle x, y \rangle = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n$. x is orthogonal to y if $\langle x, y \rangle = 0$.

Let C be a linear code over the ring $\mathbb{Z}_{15}$ with length n. The dual code of C is $C^{\perp} = \{x \in \mathbb{Z}_{15}^n \mid x \cdot y = 0, \text{for every } y \in C\}$. Thus, $C^{\perp}$ is also a linear code over the ring $\mathbb{Z}_{15}$ with length n. For a codeword $x \in C$, the Lee weight of x is defined as $W_L(x) = \sum_{i=1}^{n} W_L(x_i)$. For every two code words $x, y \in C$, the Lee distance between x and y is $d_L(x, y) = W_L(x - y)$. The Hamming weight of x is $W_H(x) = |\{x_i \mid x_i \neq 0, 1 \leq i \leq n\}|$, and the Hamming distance between x and y is $d_H(x, y) = W_H(x - y)$.

By Chinese Reminder Theory, the generate matrix of the linear code C over the ring $\mathbb{Z}_{15}$ is as follows

$$G=\begin{pmatrix} I_{k_1} & 5B_1 & 3A_1 & 3A_1+5B_2 & 3A_3+5B_3 \\ 0 & 3I_{k_2} & 0 & 3A_4 & 0 \\ 0 & 0 & 5I_{k_3} & 0 & 5B_4 \end{pmatrix},$$

in which the elements of A_i and B_i belongs to $\mathbb{Z}_{15}$. Thus, C is a Abel Group of type $15^{k_1}5^{k_2}3^{k_3}$, and $|C|=15^{k_1}5^{k_2}3^{k_3}$.

Let H be the generate matrix of the dual code $C^{\perp}$. Then $GH^{\mathrm{T}}=0$, in which H^{T} is the rotate matrix of H. Since C is a Abel Group of type $15^{k_1}5^{k_2}3^{k_3}$, H is a Abel Group of type $15^{n-(k_1-k_2-k_3)}5^{k_3}3^{k_2}$. Let

$$H=\begin{pmatrix} M_1 & M_2 & M_3 & I_{n-(k_1+k_2+k_3)} \\ Q_1 & 0 & 3I_{k_3} & 0 \\ Q_2 & 5I_{k_2} & 0 & 0 \end{pmatrix}$$

By the linear transformation, M_2 and M_3 have can be changed to be the form as

$$H=\begin{pmatrix} P_1 & 0 & 5R_2 & 0 & I_{n-(k_1+k_2+k_3+k_4)} \\ P_2 & 3R_1 & 0 & I_{k_4} & 0 \\ Q_1 & 0 & 3I_{k_3} & 0 & 0 \\ Q_2 & 5I_{k_2} & 0 & 0 & 0 \end{pmatrix}$$

According to $GH^{\mathrm{T}}=0$, we have

$$H=\begin{pmatrix} 12A_3^{\mathrm{T}}+10B_3^{\mathrm{T}} & 0 & 5B_4^{\mathrm{T}} & 0 & I_{n-(k_1+k_2+k_3+k_4)} \\ 12A_2^{\mathrm{T}}+10B_2^{\mathrm{T}} & 3A_4^{\mathrm{T}} & 0 & I_{k_4} & 0 \\ 6A_1^{\mathrm{T}} & 0 & 3I_{k_3} & 0 & 0 \\ 5B_1^{\mathrm{T}} & 5I_{k_2} & 0 & 0 & 0 \end{pmatrix}$$

For every $x=(x_1,x_2,\cdots,x_n)\in\mathbb{Z}_{15}^n$, let $x=c(x)\cdot 3+d(x)\cdot 5$, in which $c(x)=(c_1,c_2,\cdots,c_n)$, $d(x)=(d_1,d_2,\cdots,d_n)$ and $x_i=c_i\cdot 3+d_i\cdot 5$ ($c_i\in I_{(3)}$ and $d_i\in I_{(5)}$) for $1\le i\le n$. The Gray mapping from $\mathbb{Z}_{15}^n$ to $\mathbb{Z}_{15}^{2n}$ is

$$\Phi\left(c(x)\cdot 3+d(x)\cdot 5\right)=\left(c(x),d(x)\right)$$

It's obvious that the Gray map is a distance preserved mapping from ($\mathbb{Z}_{15}^n$, Lee weight) to ($\mathbb{Z}_{15}^{2n}$, Hamming weight).

4. Main Results

Theorem 1. For every $x,y\in\mathbb{Z}_{15}^n$, we have

$$W_L(x)=W_H\left(\Phi(x)\right),\quad d_L(x,y)=d_H\left(\Phi(x),\Phi(y)\right).$$

Therefore, the minimal Lee weight of C is equal to the minimal Hamming weight of $\Phi(C)$.

Proof: For $x=(x_1,x_2,\cdots,x_n)$, let $x_i=c_i\cdot 3+d_i\cdot 5\left(1\le i\le n\right)$, in which $c_i\in I_{(3)}$ and $d_i\in I_{(5)}$. By the definition of Lee weight and Gray mapping, we have

$$W_L(x_i) = W_H(\Phi(x_i)) = W_H(c_i, d_i),$$

Since $\Phi(x) = \Phi(c(x)\cdot 3 + d(x)\cdot 5) = (c(x), d(x))$, we have

$$\begin{aligned} W_H(\Phi(x)) &= W_H(c(x), d(x)) \\ &= W_H(c(x)) + W_H(d(x)) \\ &= \sum_{i=1}^{n} W_H(c_i) + \sum_{i=1}^{n} W_H(d_i) \\ &= \sum_{i=1}^{n} W_H(c_i, d_i) \\ &= \sum_{i=1}^{n} W_L(x_i) = W_L(x) \end{aligned}$$

and

$$\begin{aligned} d_L(x, y) &= W_L(x - y) \\ &= W_H(\Phi(x - y)) \\ &= W_H(\Phi(x) - \Phi(y)) \\ &= d_H(\Phi(x), \Phi(y)) \end{aligned}$$

Thus we get the conclusion. □

Theorem 2. Let C be a linear code over the ring $\mathbb{Z}_{15}$ with length n and d is the minimum distance over C. Then $\Phi(C)$ is a line of code with the Parameter $[2n, k_1 + k_2 + k_3, d]$.

Proof: For every $x, y \in \mathbb{Z}_{15}^n$ and $t_1, t_2 \in \mathbb{Z}_{15}$, let $x = c(x)\cdot 3 + d(x)\cdot 5$, $y = c(y)\cdot 3 + d(y)\cdot 5$. By the definition of gray mapping, we have

$$\begin{aligned} \Phi(t_1 x + t_2 y) &= \Phi([t_1 c(x) + t_2 c(y)]\cdot 3 + [t_1 d(x) + t_2 d(y)]\cdot 5) \\ &= (t_1 c(x) + t_2 c(y), t_1 d(x) + t_2 d(y)) \\ &= (t_1 c(x), t_1 d(x)) + (t_2 c(y), t_2 d(y)) \\ &= t_1 (c(x), d(x)) + t_2 (c(y), d(y)) \\ &= t_1 \Phi(x) + t_2 \Phi(y) \end{aligned} .$$

Thus $\Phi(C)$ is linear. Since $|C| = 15^{k_1} 5^{k_2} 3^{k_3}$, $\Phi(C)$ is a linear code with the parameter $[2n, k_1 + k_2 + k_3, d]$. □

The property of Theorem 2 also applies to the rings which can be decomposed into direct sum of two ideals.

5. Conclusion

By theoretical analysis and derivation, we prove that the minimum Lee weight of a linear code over the ring $\mathbb{Z}_{15}$ is equal to the minimum Hamming weight of its Gray mapping. Furthermore, the linear property of its Gray mapping is confirmed. In this paper, we have done some preliminary research work, but there are also many other research contents about linear codes over the ring $\mathbb{Z}_{15}$ to be considered, such as weight enumerators, Mac Williams identities and the self-dual codes over the ring $\mathbb{Z}_{15}$.

Acknowledgements

This research is supported by Foundation of Langfang Normal University

(LSLB201707), Scientific Research Innovation Team of Langfang Normal University (Rings and Algebras with their applications on Error correcting theory), the Key Programs of Scientific Research Foundation of Hebei Educational Committee (Grant No.ZD2019056) and the Key Foundation of Hebei Education Department (ZD2017064).

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Hammons, A.R., Kumar, P.V., Calderbank, A.R., Sloane, N.J.A. and Solé, P. (1994) The Z_4-Linearity of Kerdock, Preparata, Goethals and Related Codes. *IEEE Transactions on Information Theory*, **40**, 301-319. https://doi.org/10.1109/18.312154

[2] Dougherty, S.T., Gulliver, T.A. and Wong, J. (2006) Self-Dual Codes over Z_8 and Z_9. *Des. Codes Crypt. Designs*, *Codes and Cryptography*, **41**, 235-249. https://doi.org/10.1007/s10623-006-9000-2

[3] Li, P., Guo, X.M., Zhu, S.X. and Kai, X.S. (2017) Some Results on Linear Codes over the Ring Z_4+u Z_4+vZ_4+uvZ_4. *Journal of Computational and Applied Mathematics*, **54**, 307-324. https://doi.org/10.1007/s12190-016-1011-1

[4] Liu, X.S. and Liu, H.L. (2015) Macwilliams Identities of Linear Codes over the Ring F_2+uF_2+vF_2. *Journal of Systems Science and Complexity*, **28**, 691-701. https://doi.org/10.1007/s11424-015-2246-x

[5] Shi, M.J., Sole, P. and Wu, B. (2013) Cyclic Codes and the Weight Enumerator of Linear Codes over F_2+vF_2+v^2F_2. *Applied Mathematics and Computation*, **2**, 247-255.

[6] Yu, H. and Zhu, S.X. (2006) Identities of Linear Codes and Their Codes over F_2+uF_2. *Journal of University of Science and Technology of Chain*, **12**, 1285-1288.

[7] Nechaev, A.A. (1991) Kerdock Codes in a Cyclic Form. *Discrete Applied Mathematics*, **1**, 365-384. https://doi.org/10.1515/dma.1991.1.4.365

[8] Constantinescu, I. and Heise, W. (1997) A Metric for Codes over Residue Class Rings of Integers. *Problemy Peredachi Informatsii*, **33**, 22-28.