Codes of Constant Lee or Euclidean Weight over The Ring $F_2 + uF_2$

S. Sadek*
M. El-Atrash**
A. K. Nagi***

ملخص البحث

قام Carlet [5] بتحديد الترامیز الخطية ذات وزن Lee الثابت علي الحلقة Z_4. وبعد ذلك قام Wood [9] بتحديد الترامیز الخطية ذات وزن Lee أو Euclid الثابت علي نفس الحلقة ، ولكن بطريقة مختلفة.

اهتم العديد من الباحثين [1] ، [2] ، [3] ، [4] ، [6] بالحلقة $F_2 + uF_2$ وكان ذلك الاهتمام نابعاً من خواص هذه الحلقة والتي تشترك بها مع حلقات أخري تشكل مجال خصباً لدراسة نظرية الترميز الخطي عليها. وفي محاولة لإكمال البحث في الترامیز الخطية علي الحلقة $R = F_2 + uF_2$ سنقدم في هذا البحث وصفاً للترامیز الخطية علي R مستخدمين وزن Lee ووزن Euclid الثابتين.

Abstract

Carlet [5] determined the linear codes over the ring Z_4 of constant Lee weight. Wood [9] has determined linear codes of constant Lee or Euclidean weight over the same ring following a different approach from that of Carlet.

There is interest in the ring $R = F_2 + uF_2$ [1],[2],[3],[4],[6]. This interest arises from the common properties between this ring and other rings like Z_4 and F_4.

In this paper we describe linear codes of constant Lee or Euclidean weight over the ring $F_2 + uF_2$.

Mathematics Subject Classification 2000: Primary 94B05, Secondary 16W70.

---

* *Prof. Dr. of Mathematics, Faculty of Since, Department of Mathematics, Ain Shams University, Egypt.*

** *Assoc. Prof. of Mathematics, department of mathematics, Islamic University-Gaza, Email: matrash@mail.iugaza.edu.*

*** *Lecturer of mathematics, department of mathematics, Al-Aqsa University-Gaza, P.O. Box 4051, Gaza, Palestine.*

Introduction

Recently there has been interest in the ring $\mathbb{F}_2 + u\mathbb{F}_2$. For example [1], [2], [3], [4], [6]. Because of the "nice" properties of this ring, many applications of coding theory have been made, and others are to be given.

Over finite fields, any linear code with constant Hamming weight is a replication of simplex codes. Several proofs have been given to this result (see for example [3]). Carlet [5] has proved a similar result for linear codes of constant Lee weight over $\mathbb{Z}_4$. Wood [9] has generalized these results to codes of constant Lee or Euclidean weight over the rings $\mathbb{Z}_{p^2}$, p prime, giving different proof for Carlet's result when $p = 2$. In these results, coordinate functionals and their orbits under automorphisms of a code C played an essential role, in addition to the extension theorem [11], [13]. Because of this, J. Wood has proved the following theorem:

Theorem [9]

Let $C \subset R^n$, $R = \mathbb{Z}_4$, *be a linear code of constant weight, either Lee or Euclidean weight. If* $\lambda \in C^{\#}$ *occurs as a coordinate functional of C, then (up to* $\pm$ *signs) every other linear functional* μ *in the Aut(C)-orbit of* λ *also occurs as a coordinate functional of* C.

In this paper we prove a similar theorem, as well as some other results of Wood [9] and Carlet [3] when R is the ring $\mathbb{F}_2 + u\mathbb{F}_2$.

1. The ring $\mathbb{F}_2 + u\mathbb{F}_2$

The ring $R = F_2 + uF_2$ is introduced in [1], [2], [3], [4] and [6] (here $F_2 = \{0, 1\}$ is the binary field). $R = \{0, 1, u, 1+u\}$ with $u^2 = 0$. Addition and multiplication in R are given by the following tables:

+	0	1	u	$1+u$
0	0	1	u	$1+u$
1	1	0	$1+u$	u
u	u	$1+u$	0	1
$1+u$	$1+u$	u	1	0

•	0	1	u	$1+u$
0	0	0	0	0
1	0	1	u	$1+u$
u	0	u	0	u
$1+u$	0	$1+u$	u	1

Tables (1)

Example: As a simple example we can view $F_2 + uF_2$ as the ring $Z_2[i]$ where i is the complex number $\sqrt{-1}$ with $u = 1 + i$.

A linear code C over R is simply an R-submodule of R^n. Elements of C are called codewords. The Hamming weight of a codeword $x = (x_1, \ldots, x_n)$ is the number of non-zero components in x. The Lee weight of x is given by the equation [6]

$$wt_L(x) = \sum_{i=1}^{n} wt_L(x_i), \tag{1.1}$$

where

$$wt_L(x_i) = \begin{cases} 0 & \text{if} \quad x_i = 0 \\ 1 & \text{if} \quad x_i = 1 \quad \text{or} \quad 1+u. \\ 2 & \text{if} \quad x_i = u \end{cases}$$

Let $n_0(x)$ be the number of the zero components x_i in x, $n_2(x)$ be the number of components x_i in x which are equal to u, and $n_1(x) = n - n_0(x) - n_2(x)$ i.e. $n_1(x)$ is the number of the components x_i in x which are either 1 or $1 + u$. Then the Lee weight $wt_L(x)$ of x can also be given by

$$wt_L(x) = n_1(x) + 2\, n_2(x), \qquad x \in R^n \tag{1.2}$$

The Euclidean weight is given by the relation

$$wt_E(x) = \sum_{i=1}^{n} wt_E(x_i), \tag{1.3}$$

where

$$wt_E(x_i) = \begin{cases} 0 & if \quad x_i = 0 \\ 1 & if \quad x_i = 1 \quad or \quad 1+u. \\ 4 & if \quad x_i = u \end{cases}$$

As above, we have

$$wt_E(x) = n_1(x) + 4n_2(x),\ x \in R^n \tag{1.4}$$

2. Chain Rings and Module Decomposition

A ring R is local if for every $a \in R$, either a or $1 - a$ is a unit in R. As in [12] chain rings are local rings R whose maximal ideal M is principal, say $M = (m)$. It follows that every ideal in R is principal and of the form $M^j = (m^j)$ for some j. The ideals form a chain

$$R = (m^0) \supset (m) \supset (m^2) \supset \ldots \supset (m^{\beta-1}) \supset (m^\beta) = 0, \tag{2.1}$$

where $m^\beta = 0$, but $m^{\beta-1} \neq 0$.

When R is a chain ring as in (2.1), every module C over R admits a decreasing filtration

$$C \supset mC \supset m^2C \supset \ldots \supset m^{s-1}C \supset m^sC = 0, \tag{2.2}$$

for some $s \leq \beta$, as well as a direct sum decomposition

$$C \cong \bigoplus_{j=1}^{\beta} \left(R/(m^j)\right)^{\gamma_j}. \tag{2.3}$$

The ring $R = F_2 + uF_2$ is obviously a local ring, so we have

$$M = uR = \{0, u\}, \tag{2.4}$$

and so, (2.1) becomes

$$R = (u^0) \supset uR \supset u^2R = 0,$$

with $\beta = 2$, and (2.3) becomes

$$C \cong (R/(u))^{l_1} \oplus (R/(u^2))^{l_2} \tag{2.5}$$

Note: In [7, definition 3.6 and corollary 3.8] Norton and sălăgean have proved that

$$C \cong (R/(u))^{l_1} \oplus (R/(u^2))^{l_2} \cong (uR)^{l_1} \oplus (R)^{l_2} \tag{2.6}$$

where l_i is the number of rows divisible by u^i in a generating matrix G in standard form for C, and that $l_1 + l_2$ is the number of rows in G.

3. Extension Theorem

Definition [11]: A right linear automorphism f: $R^n \to R^n$ is a right monomial transformation if there exist units $u_1, \ldots, u_n$ in the group $\mathcal{U}$ of units of R and a permutation σ of $\{1, \ldots, n\}$ such that, for any $x \in R^n$

$$f(x) = f(x_1, \ldots, x_n) = (u_1 x_{\sigma(1)}, \ldots, u_n x_{\sigma(n)}). \tag{3.1}$$

If U is a subgroup of $\mathcal{U}$ and $u_1, \ldots, u_n \in U$, we say that f is a U-monomial transformation.

If U is defined as above, and if we view the additive group of R as a finite abelian group G, then left multiplication by $r \in U$ defines an automorphism of G.

We write $v \approx s$ if $s = rv$ for some $r \in U$. The orbit of v under U is.

$$\text{orb}(v) = \{s \in R: s \approx v\}.$$

The *symmetrized weight composition* determined by the subgroup U is the function *swc*: $R^n \times R \to Z$ given by

$$swc_v(x) = \sum_{s \in orb(v)} n_s(x),$$

where

$$n_s(x) = |\{i: x_i = s\}|, x \in R^n, s \in R.$$

If $s \in \text{orb}(v)$, then $swc_s = swc_v$. The function $f: R^n \to R^n$ preserves *swc* if $swc_v(f(x)) = swc_v(x)$ for all $x \in R^n$, $v \in R$.

The Extension Theorem [11]:

Suppose that R *is a finite Frobenius ring and that* $C \subset R^n$ *is a right linear code. Fix a subgroup* U *of the group of units of* R, *which gives rise to a symmetrized weight linear composition swc. Then any injective right linear homomorphism* $f: C \to R^n$ *which preserves swc extends to a right* U-*monomial transformation.*

Note: (i) Other versions of the extension theorem can be seen in [13].

(ii) For the definition of a Frobenius ring see for example [10].

Now, the ring $R = F_2 + uF_2$ is a finite Frobenius ring and satisfies the conditions of the extension theorem with Lee weight and Euclidean weight as the required weight compositions, so the extension theorem is valid for $R = F_2 + uF_2$, with $U = \{1, 1 + u\} = \mathcal{U}$.

Main Results

4. Orbit Structures

The linear automorphism group Aut(C) acts on C and $C^{\#} = \mathrm{Hom}_R(C, R)$, the linear dual of C. Our main interest is the action on $C^{\#}$. However $C^{\#} \cong C$ so we will work directly with the action on C [9].

In the next results, we will denote elements of C as pairs , $x = (x_{(1)}, x_{(2)})$, where $x_{(i)} \in (u^i R)^{l_i}$ as in (2.6). An astrisk $*$ means that the entry can assume any value; $u*$ means that every component of the entry is a multiple of u; u means that at least one component of the entry is u; v means that at least one component of the entry is a unit (either 1 or $1 + u$).

Theorem 1

For any linear code over $F_2 + uF_2$, the orbits of Aut(C) on C are given by the table:

Orbit	Representative	Size
$(*, v)$	$(0, e)$	$2^{l_1+l_2}(2^{l_2}-1)$
$(u, u*)$	$(e, 0)$	$(2^{l_1}-1)2^{l_2}$
$(0, vu)$	$(0, ue)$	$2^{l_2}-1$
$(0, 0)$	$(0, 0)$	1

Table (2)

Proof:

For the first case of the table (2), $*$ represents the entry in $(uR)^{l_1}$. So we have 2^{l_1} possibilities (including the 0-entry). Every one of these

possibilities will appear with the $2^{l_2}(2^{l_2}-1)$ possibilities of appearance of a unit in some component of the entry represented by v.

For other cases we can follow the same way of counting to complete the table. □

Now we state our first result on constant weight codes over $R = F_2 + uF_2$. We view a linear code C as an abstract R-module as in (2.6), equipped with an embedding in R^n. The embedding is given by n-coordinate functionals $\lambda_1, \ldots, \lambda_n \in C^{\#}$. If C has a generator matrix G, then the columns of G are the values of the λ_i evaluated on a set of generators for C.

Theorem 2

Let $C \subset R^n$ *be a linear code of constant weight, either Lee or Euclidean weight. If* $\lambda \in C^{\#}$ *occurs as a coordinate functional of* C *then every other linear functional* μ *in the Aut*(C)*-orbit of* λ *also occurs as a coordinate functional of* C (*up to possibly permuting* 1 *and* $1 + u$).

Proof: Given any μ in the orbit of λ, there exists $f \in$ Aut(C) carrying λ to μ. Then f preserves weight since C has constant weight. Since R is a Frobenius ring, and f: $C \to R^n$ is an injective homomorphism, then by the extension theorem [11], (up to permuting 1 and $1 + u$) f extends to an automorphism of R^n, thus μ is another coordinate functional of C.□

Definition [9]. A linear code is called non-degenerate if it has no zero-coordinate functionals.

Example: The code C with generator matrix G = [1 $1+u$ u] is a non-degenerate code of cardinality 4, length 3 and constant Lee weight 4.

Remark: Following Wood [9], two linear codes of length n and constant Lee or Euclidean weight over R are equivalent if one can be obtained from the other by an automorphism of R^n with possible permuting 1 and $1+u$. This means that the two codes have the same collections of coordinate functionals (up to permuting 1 and $1+u$). The code C is an m-fold replication of the code D if each functional of D has multiplicity m in C.

Theorem 3

Let C *be a non-degenerate linear code of constant Lee weight over* $R = F_2 + uF_2$. *Then* C *is equivalent to the replication of a code* D *whose coordinate functionals consist of all the non-zero linear functionals on* D.

The linear codes C *and* D *are isomorphic as R-modules, each of cardinality* $2^{l_1+2l_2}$. *The code* D *has length* $|D| - 1 = 2^{l_1+2l_2} - 1$, *while the code* C *has length* $m(2^{l_1+2l_2} - 1)$, *for some positive integer m.*

Every non-zero element of D has Lee weight $L = |D| = 2^{l_1+2l_2}$ *while every non-zero element of* C *has Lee weight* mL.

Proof: By Theorem 2, the orbits of linear functionals (up to permuting 1 and $1+u$) must occur in the collection of coordinate functionals of C. Because C is non-degenerate, no zero functionals occur.

Let α, β, γ denote the number of times the orbits $(*,v)$, $(u, u*)$, $(0, vu)$ (up to permuting 1 and $1+u$ in pairs $(*, v)$ only) occur in the coordinate functionals of C.

Let $n_1(x)$ and $n_2(x)$ be as in (1.2). We have $wt_L(ux) = 2n_1(x)$, since $u^2 = 0$.

In C we have two types of non-zero elements

(a) elements having only 0's and u's as components, in which case $ux = 0$ for every such element x, so $wt_L(ux) = 0$ and $wt_L(x) = 2n_2(x)$, since $n_1(x) = 0$.

(b) elements having 1's and $(1+u)$'s, among their components. In this case we have $wt_L(x) = wt_L(ux)$ (because C is of constant Lee weight, and $ux \neq 0$). It then follows that $n_1(x) + 2\,n_2(x) = 2n_1(x)$, and hence $n_1(x) = 2\,n_2(x)$ (i.e. the number of occurrences of 1's and $(1+u)$'s is twice the number of occurrences of u in x).

Let $x = (0, e)$ and $y = (e, 0)$ be as in table (2). Therefore, $u.y = 0$ (since only u's and 0's appear in y).

Now, following the calculations of table (2), we have

$$\begin{aligned} n_1(x) &= 2^{l_1+2l_2-2}\,\alpha, \\ n_2(x) &= 2^{l_1+l_2-2}(2^{l_2-1}-1)\alpha + (2^{l_1}-1)\,2^{l_2-1}\beta + 2^{l_2-1}\gamma, \\ n_2(y) &= 2^{l_1+l_2-2}(2^{l_2}-1)\alpha + 2^{l_1+l_2-1}\beta. \end{aligned} \tag{4.1}$$

From the constant weight conditions $wt_L(x) = wt_L(ux) = wt_L(y)$, it follows that $n_1(x) = 2n_2(x) = n_2(y)$. Then solving the system of equations (4.1) with this information, we get that $\alpha = 2\beta$ and $\beta = \gamma$ and $wt_L(x) = 2^{l_1+2l_2}\,\beta = wt_L(y)$ (since $wt_L(x) = n_1(x) + 2\,n_2(x)$), i.e. the constant weight of C is a β-multiple of $2^{l_1+2l_2}$. C has length $(2^{l_1+2l_2}-1)\beta$, and so C is a β-fold replication of D, where D is a code of minimum constant weight $2^{l_1+2l_2}$, and minimal length $2^{l_1+2l_2}-1$. This completes the proof for the Lee weight case. □

Example: For $l_1 = l_2 = 1$, the smallest example occurs where $\beta = 1$, hence $\alpha = 2, \gamma = 1$. Therefore our replicated code D is of length 7, constant Lee weight 8 and cardinality 8. A generating matrix has the form

$$G = \begin{pmatrix} 0 & u & 0 & u & u & u & 0 \\ 1 & 1 & 1 & 1 & 0 & u & u \end{pmatrix}.$$

For Euclidean weight we have:

Theorem 4

Let C *be a non-degenerate linear code of constant Euclidean weight over* $R = F_2 + uF_2$. *Then* C *is equivalent to the replication of a code* D *whose coordinate functionals consist of all the non-zero linear functionals on* D.

Proof:

For elements $x, y \in C$, where x is of type (b) and y is of type (a) we have $wt_E(y) = 4\, n_2(y)$, $wt_E(x) = n_1(x) + 4\, n_2(x)$,(by 1.4).

As C is of constant Euclidean weight, and $ux \neq 0$,

$$wt_E(x) = wt_E(ux) = wt_E(y).$$

Then

$$n_1(x) + 4\, n_2(x) = 4n_1(x) = 4\, n_2(y),$$

and so

$$n_2(x) = (3/4)n_1(x) \text{ and } n_1(x) = n_2(y).$$

Thus considering again the elements $x = (0, e), y = (e, 0)$ and referring to the system of equations (4.1), we have $\alpha = 2\beta$ and $\gamma = (2^{l_1+l_2-2}+1)\beta$ (as was given by J. Wood [9]).

Also, calculating the Euclidean weight of x and y, we have that C is the replication of a code D of minimum length $2^{l_1+2l_2} - 1 + 2^{l_1+l_2-2}(2^{l_2} - 1)$ and constant Euclidean weight $L = 2|D| = 2^{l_1+2l_2+1}$. Thus C is a β-fold replication of D. □

Example: If $l_1 = l_2 = 1$, then $\alpha = \gamma = 2\beta$. The smallest example has $\beta = 1$, $\alpha = \gamma = 2$. A generating matrix has the form

$$G = \begin{pmatrix} 0 & u & 0 & u & u & u & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & u & u & u \end{pmatrix}.$$

The resulting code has cardinality 8, length 8 and constant Euclidean weight 16.

Conclusion

What we have introduced in this work is that results examined by J. Wood [9] over the ring $\mathbb{Z}_4$ are still valid over the ring $R = F_2 + uF_2$. The question is: Do these results, or possibly relevant results, still hold for other Galois rings?

References

[1] Bachoc C., *Application of Coding Theory to the Construction of Modular Lattices,* J. Combin. Theory Ser. A **78** pp. 92-119, (1997).

[2] Betsumiya K., Gulliver A. T. and Harada M., *Extremal Self-Dual Codes Over* $F_2 \times F_2$,

[3] Bonisoli A., *Every Equidistant Linear Code is A sequence of Dual Hamming Codes,* Ars Combin. **18** pp. 181-186, (1984).

[4] Bonnecaze A. and Udaya P., *Cyclic Codes and Self-Dual Codes Over* $F_2 + uF_2$, IEEE, IT, Vol. 45, No. 4, pp 1250-1254, Mar. 1999.

[5] Carlet C., *One-weight Z_4-Linear Codes,* Coding Theory, Cryptography and Related Areas (J. Buchmann, T. Hϕholdt, H. Stichtenoth, and H. Tapia-Recillas, eds.), Springer, Berlin, 2000, pp. 57-72.

[6] El-Atrash M. and Al-Ashker M., *Linear Codes Over the Ring* $F_2 + uF_2$, Islamic University Journal.

[7] Norton G. H. and Sălăgean A., *On the Structure of Linear and Cyclic Codes Over A finite Chain Ring.* Applicable algebra in engineering, communication and computing, **10** pp. 489-506, (2000)

[8] Udaya P. and Bonnecaze A., *Decoding of Cyclic Codes over* $F_2 + uF_2$, IEEE, IT, Vol. 45, No. 6, pp 2148-2156, Sept. 1999.

[9] Wood Jay A., *Codes of Constant Lee or Euclidean Weight,* extended abstract for the workshop on coding and cryptography, Paris, (1999).

[10] Wood Jay A., *Duality for Modules Over Finite Rings and Applications to Coding Theory,* Amer. J. Math. **121**, pp. 555-575, (1999).

[11] Wood Jay A., *Extension Theorems for Linear Codes Over Finite Rings,* Applied Algebra, Algorithms and Error-Correcting Codes (T. Mora and

H. Mattson, eds.), Lecture Notes in Comput. Sci., **1255**, Springer-Verlag, Berlin, pp. 329-340, (1997).

[12] Wood Jay A., *The Structure of Linear Codes of Constant Weight*, Trans. Amer. Math. Soc. **354**, pp. 1007-1026, (2002).

[13] Wood Jay A., *Weight Functions and the Extension Theorem for Linear Codes Over Finite Rings*, Contemp. Math. **225**, Providence: Amer. Math. Soc. pp. 231-243, (1999).