Virtual Linear Codes of Constant Weight Over the Ring $\mathbb{Z}/(p)[u]/(u^2)$

Prof. S. Sadek*
Dr. M. El-Atrash**
Mr. A. K. Nagi***

الملخص

في [8] وود Wood عرف دوال التعدد multiplicity functions بقيم حقيقية لا تنتمي إلى مجموعة الأعداد الصحيحة ، من أجل أن يقدم وصفاً للترميز الخطية التقديرية (الواقعية) virtual linear codes ذات الوزن الثابت علي الحلقات Z_N. في بحثه هذا قدم وود دراسة كاملة لبنية الترميز الخطية الكلاسيكية ذات الوزن الثابت علي الحلقات ذات السلاسل المنتهية finite chain rings باستخدام دوال وزنية قبل المتجانسة pre-homogeneous weight functions.

في هذا البحث سوف نقوم بتعريف دالة تعدد η علي الداليات الخطية linear functionals لموديول M علي الحلقة $R = Z/(p)[u]/(u^2)$ حيث p عدد أولي فردي ، وسوف نثبت أن الترميز التقديري virtual code الخطي الناتج له وزن ثابت تحت تأثير η ، وذلك بعد تعريف دالة وزن معينة علي الحلقة R.

Abstract

In [8] Wood has defined multiplicity functions with non-integer values, to determine *virtual* linear codes of constant weight over the rings $\mathbb{Z}_N$. In his paper, he also gave a full study of the structure of *classical* linear codes of constant weight over finite chain rings using *pre-homogeneous weight* functions.

In this paper we define a multiplicity function η on the linear functionals of a module M over the ring $R = \mathbb{Z}/(p)[u]/(u^2)$, p an odd prime, and show that the resulting virtual linear code has constant weight under this η, after defining a suitable weight function on R.

Mathematics Subject Classification: Primary 94B05, Secondary 16W70

* **Prof. of Mathematics, Department of Mathematics, Ain Shams University, Egypt.**
** **Assoc. Prof. of Mathematics, Department of Mathematics, Islamic University-Gaza, Palestine .**
*** **Lecturer. of Mathematics, Department of Mathematics, Al-Aqsa University-Gaza, P.O. Box 4051, Palestine.**

1. Introduction

In [8] Wood has classified the structure of linear codes of constant weight over $\mathbb{Z}_N$. The classification of Wood reproves the classical result about linear codes of constant Hamming weight over a finite field. This classical result can be seen in [1].

Wood's classification also reproves a theorem given by Carlet [2] on linear codes of constant Lee weight over $\mathbb{Z}_4$.

Wood also has described linear codes from the linear functional point of view of [5], and used the following definitions, which will be used also in this paper:

Definitions 1.1 [8]

A *linear code* C over a ring R is a pair (M, η), where M is an R-module, the module *underlying* the code, and η: $M^{\#} \to \mathbb{N}$ is a multiplicity function where $M^{\#}$ is the linear dual of M. The *length* n of the linear code C is $n = \sum_{\lambda \in M^{\#}} \eta(\lambda)$. A linear code is *non-degenerate* if the multiplicity of the zero functional $\eta(0)$ is 0.

The code C = (M, η) is a *virtual linear* code if η has values in $\mathbb{Z}$ or $\mathbb{Q}$, that is, if we allow functionals to occur with negative or rational multiplicities. In case η takes values in $\mathbb{N}$, C is *classical*.

A *weight function* w on the ring R is a function which assigns real number weights a_r to every $r \in R$. We assume that $a_0 = 0$ and that $a_r > 0$ for $r \neq 0$. This choice of weight function on R allows us to define a *weight* function w_η: $M \to \mathbb{R}$ on any linear code C = (M, η):

$$w_\eta(x) = \sum_{\lambda \in \hat{M}^\#} \eta(\lambda) a_{\lambda(x)}, \qquad x \in \mathrm{M} \tag{1.1}$$

Chain rings are *local* rings R whose maximal ideal **m** is principal, say **m** = (m). This implies that every ideal in R is principal and of the form $\mathbf{m}^j = (m^j)$, for some j. The ideals form a chain

$$\mathrm{R} = (m^0) \supset (m) \supset (m^2) \supset \ldots \supset (m^{\beta-1}) \supset (m^\beta) = 0, \tag{1.2}$$

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

Then R/**m** $\cong \mathsf{F}_p$, a finite field. The class of m^j is a basis of $(m^j)/(m^{j+1})$ as an R/**m**-vector space. It follows that

$$|(m^j)| = p|(m^{j+1})| = p^{\beta-j} \tag{1.3}$$

(Information and examples of these rings can be seen in [3, 7, 9]).

When R is a chain ring as in (1.2), every module M over R admits a decreasing filtration

$$\mathrm{M} \supset m\mathrm{M} \supset m^2\mathrm{M} \supset \ldots \supset m^{\gamma-1}\mathrm{M} \supset m^\gamma\mathrm{M} = 0, \tag{1.4}$$

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

$$\mathrm{M} \cong \bigoplus_{j=1}^{\beta} \left(R/(m^j)\right)^{k_j}. \tag{1.5}$$

From (1.3), we see that

$$|\mathrm{M}| = p^{\sum_{j=1}^{\beta} j k_j}. \tag{1.6}$$

If $k_\beta = 0$, then M is the pullback of a module defined over R/$(m^{\beta-1})$. To avoid this, we assume that $k_\beta \geq 1$. In that case $\gamma = \beta$ in (1.4).

Note: In [4], Norton and Sălăgean gave a slightly different form of the decomposition (1.5).

Example

Let $p = 3$, $n = 1$, $r = 2$ in definition 2.1, we have R = {0, 1, 2, u, $2u$ $1+u$, $2+u$, $1+2u$, $2+2u$} and $w(0) = 0$, $w(1) = w(2) = 1$, $w(u) = w(2u)$, $w(1+u) = w(2+2u)$, $w(1+2u) = w(2+u)$.

If we fix the value of $w(u)$ to be 3, then the rest of the values of w will be 2 and 4. One can use $w(1+2u) = w(2+u) = 2$ and $w(1+u) = w(2+2u) = 4$.

Note: There is an analogue between this weight function w and the Lee weight function w_L defined on $Z_N = \{x: -\frac{N-1}{2} \le x \le \frac{N-1}{2}\}$ as $w_L(x) = |x|$, (see[6]).

3. A special Case

Now for an arbitrary odd prime p, with n = 1, r = 2, we apply definition 2.1 to the ring $R = Z/(p)[u]/(u^2) = \{0, 1, 2, \ldots, p-1, u, 1+u, 2+u, \ldots, (p-1)+u, 2u, 1+2u, 2+2u, \ldots, (p-1)+2u, \ldots, (p-1)u, 1+(p-1)u, 2+(p-1)u, \ldots, (p-1)+(p-1)u\}$.

The ring R is a chain ring as in (1.2) with $\beta = 2$. Its maximal ideal is $uR = \{0, u, 2u, \ldots, (p-1)u\}$. By (1.3) $|R/(uR)| = p$. We assign specific weights for the elements $0, 1, \ldots, p-1, u, 2u, \ldots, (p-1)u$ as follows:

$$a_x = w(x) = \begin{cases} |x|, & x \in \{0, \pm 1, \cdots, \pm (p-1)/2\} \\ |r| p, & x = \pm ru, \quad r \in \{0, \pm 1, \cdots, \pm (p-1)/2\} \end{cases}, \qquad (3.1)$$

For the rest of the elements of R we use part (b) of definition 2.1.

Note: In (3.1) we used the notation: $Z/(p) = \{0, \pm 1, \ldots, \pm (p-1)/2\}$ instead of $\{0, 1, \ldots, p-1\}$, and it will be used in the proof of the next theorem.

In the next theorem we use (1.5) to decompose any module over the ring $R = Z/(p)[u]/(u^2)$, with $\beta = 2$ and non-negative integers k_1, k_2.

Theorem

Let R be the ring $\mathbb{Z}/(p)[u]/(u^2)$, and suppose that M is an R-module. For every nonzero $\lambda \in M^{\#}$, assign the multiplicity

$$\eta(\lambda) = \begin{cases} 1, & \lambda \in M^{\#} - uM^{\#} \\ 1 - p^{k_1+k_2-2}, & \lambda \in uM^{\#} \end{cases} . \qquad (3.2)$$

The resulting *virtual linear code* has constant weight $\frac{|M|}{4}(p^2-1)$.

Note: $M^{\#} - uM^{\#}$ means the set theoretic defference.

Proof:

Consider any nonzero $x \in M$. Since $a_0 = 0$, there is no harm in including $\lambda = 0$ in any summation. Write $k = k_1 + k_2$, where k_1 and k_2 are the integers of (1.5). By definition 1.1 we have

$$w_\eta(x) = \sum_{\lambda \in M^{\#} - uM^{\#}} a_{\lambda(x)} + (1-p^{k-2}) \sum_{\lambda \in uM^{\#}} a_{\lambda(x)}$$

$$= \sum_{\lambda \in M^{\#}} a_{\lambda(x)} - p^{k-2} \sum_{\lambda \in uM^{\#}} a_{\lambda(x)} . \qquad (3.3)$$

The element x determines a linear map $\breve{x} : M^{\#} \to R$ by $\lambda \mapsto \lambda(x)$. The image $\operatorname{im}\breve{x}$ of $\breve{x}$ is a nonzero ideal in R, say $\operatorname{im}\breve{x} = (u^i)$, $i = 0$ or 1. It now follows that $\operatorname{im}(\breve{x}|_{uM^{\#}}) = (u^{i+1})$. Therefore $p^{k_1+2k_2} = |M| = p^k|uM|$. From (1.3) and (1.6), we see that $|\ker\breve{x}| = \frac{|M^{\#}|}{|\operatorname{im}\breve{x}|} = p^{k_1+2k_2-2+i}$, while $|\ker(\breve{x}|_{uM^{\#}})| = |uM^{\#}|/|(u^{i+1})| = p^{k_1+2k_2-k-2+i+1} = p^{k_2+i-1}$.

Also, $\sum_{r \in (u^i)} a_r = \frac{p^4 - (w(u^i))^2}{4w(u^i)} = \begin{cases} \frac{p^4-1}{4}, & i = 0 \\ \frac{p(p^2-1)}{4}, & i = 1 \end{cases}$.

Therefore $w_\eta(x) = |\ker \tilde{x}| \sum_{r\in(u^i)} a_r - p^{k-2}|\ker(\tilde{x}\,|_{uM^\#})| \sum_{r\in(u^{i+1})} a_r$.

(a) For $i = 0$, we have $w_\eta(x) = p^{k_1+2k_2-2}\,\frac{p^4-1}{4} - p^{k-2}\,p^{k_2-1}\,p\,\frac{p^2-1}{4}$

$$= \frac{p^{k_1+2k_2}}{4}(p^2-1) = \frac{|M|}{4}(p^2-1).$$

(b) For $i = 1$, in this case $(u^{i+1}) = 0$ so we get,

$$w_\eta(x) = p^{k_1+2k_2-1}\,p\,\frac{p^2-1}{4} = \frac{p^{k_1+2k_2}}{4}(p^2-1) = \frac{|M|}{4}(p^2-1).$$

In either case we get a constant weight independent of the choice of the nonzero x.

4. Conclusion

Over the ring $Z/(2^k)$ Wood has determined linear codes of constant weight (Lee or Euclidean). Also virtual linear codes of constant Lee or Euclidean weight have been studied by Wood over the ring $Z/(N)$, N arbitrary.

In this paper, virtual linear codes of constant weight over the ring $Z/(p)[u]/(u^2)$ are determined. Do virtual linear codes of constant weight over a more general ring $Z/(p)[u]/(u^r)$ or $Z/(p^n)[u]/(u^r)$ exist and have a similar structure?. Difficulties arise when one tries to define weight and multiplicity functions.

2. The Ring $\mathbb{Z}/(p^n)[u]/(u^r)$

In this paper we first define a general weight function on the ring R = $\mathbb{Z}/(p^n)[u]/(u^r)$, $n \geq 1$, $r \geq 2$, for a general odd prime p, then we determine the constant weight of a virtual linear code M over the ring R = $\mathbb{Z}/(p)[u]/(u^2)$ as a special case, after defining a suitable multiplicity function η on the linear dual $M^{\#} = \mathrm{Hom}_R(M, R)$ of M, and under the assumption that M does in fact exist.

Definition 2.1

We view any linear code over a ring R as a submodule C of the free R-module R^n. Let R be the ring $\mathbb{Z}/(p^n)[u]/(u^r)$, where $\mathbb{Z}/(p^n)[u]$ is the ring of polynomials in u with coefficients from the ring $\mathbb{Z}/(p^n) = \{x: -(p^n-1)/2 \leq x \leq (p^n-1)/2\}$.

We define the function w on R as follows:

(a) for every x such that $-(p^n-1)/2 \leq x \leq (p^n-1)/2$, $w(x) = |x|$,

(b) for the rest of the elements of R, w assigns to each element x and its additive inverse $-x$ a real number $l_x = l_{(-x)}$ such that the values of l_x start from $(p^n-1)/2 + 1 = (p^n+1)/2$ (i.e., the values of l_x are arranged as: $(p^n+1)/2$, $(p^n+1)/2+1$, ...) and end with $(p^{nr}-1)/2$.

Note

(i) Definition 2.1 seems to be arbitrary and very general since one can assign any value to w in the given range of l_x when applied to the elements of the set $\mathbb{Z}/(p^n)[u]/(u^r) - \mathbb{Z}/(p^n)$.

(ii) We call $w(x)$ the *weight* of x.

References

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

[2] 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.

[3]McDonalds,B.R.,*Finite Rings with Identity*, Marcel Dekker,(1974).

[4] 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** ,(2000) pp. 489-506.

[5] Ward H. N., *An introduction to divisible codes*, Des. Codes Cryptogr. **17** (1999), pp. 73-79.

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

[7] 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**,(1997) pp. 329-340, , Berlin Springer-Verlag,.

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

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