Journal of Pure and Applied Algebra • • • (• • • •) • • •–• • •

Contents lists available at ScienceDirect

Journal of Pure and Applied Algebra

www.elsevier.com/locate/jpaa

Multivariable codes in principal ideal polynomial quotient rings with applications to additive modular bivariate codes over $\mathbb{F}_4$

E. Martínez-Moro [a,*,1], A. Piñera-Nicolás [a,2], I.F. Rúa [b,3]

[a] *Mathematics Research Institute (IMUVa), Universidad de Valladolid, Spain*
[b] *Departamento de Matemáticas, Universidad de Oviedo, Spain*

ARTICLE INFO

Article history:
Received 9 July 2015
Received in revised form 16 March 2017
Available online xxxx
Communicated by I.M. Duursma

MSC:
11T71; 94B99; 81P70; 13M10

ABSTRACT

In this work, we study the structure of multivariable modular codes over finite chain rings when the ambient space is a principal ideal ring. We also provide some applications to additive modular codes over the finite field $\mathbb{F}_4$.

1. Introduction

Multivariable codes over a finite field $\mathbb{F}_q$ are a natural generalization of several classes of codes, including cyclic, negacyclic, constacyclic, polycyclic and abelian codes. Since these particular families have also been considered over finite chain rings (e.g., over Galois rings), we proposed in [16,17] constructions of multivariable codes over them. As with classical cyclic codes over finite fields, the modular case (i.e., codes with repeated roots) is much more difficult to handle than the semisimple case (i.e., codes with non-repeated roots). In this sense, different authors have studied the properties of cyclic, negacyclic, constacylic and polycyclic modular codes over finite chain rings. Among these codes, those contained in an ambient space which is a principal ideal ring admit a relatively simple description, quite close to that of semisimple codes. This feature has been recently used in the description of abelian codes over a finite field [9], and in the description of modular additive cyclic codes over $\mathbb{F}_4$ [8]. As a natural continuation of these works, in this paper we consider the structure of multivariable modular codes over finite chain rings when the ambient space is a principal ideal ring.

* Corresponding author.
E-mail addresses: Edgar.Martinez@uva.es (E. Martínez-Moro), alejandro.pinera@uva.es (A. Piñera-Nicolás), rua@uniovi.es (I.F. Rúa).

[1] Partially supported by the Spanish MINECO under grants MTM2015-65764-C3-1-P and MTM2015-69138-REDT.
[2] Partially supported by MINECO-13-MTM2013-45588-C3-1-P.
[3] Partially supported by MINECO-13-MTM2013-45588-C3-1-P and Principado de Asturias Grant GRUPIN14-142.

http://dx.doi.org/10.1016/j.jpaa.2017.04.007
0022-4049/

2. Finite chain rings and codes over them

An associative, commutative, unital, finite ring R is called *chain ring* if it has a unique maximal ideal M and it is principal (i.e., generated by an element a). This condition is equivalent [5, Proposition 2.1] to the fact that the set of ideals of R is the chain (hence its name) $\langle 0\rangle = \langle a^t\rangle \subsetneq \langle a^{t-1}\rangle \subsetneq \cdots \subsetneq \langle a^1\rangle = M \subsetneq \langle a^0\rangle = R$, where t is the nilpotency index of the generator a. The quotient ring $\overline{R} = R/M$ is a finite field $\mathbb{F}_q$ where $q = p^l$ is a prime number power. Examples of finite chain rings include Galois rings $GR(p^n, l)$ of characteristic p^n and p^{nl} elements (here $a = p$, and $t = n$) and, in particular, finite fields ($\mathbb{F}_q = GR(p, l)$) [18].

Multivariable codes over finite chain rings, i.e., ideals of the ring $\mathcal{R} = R[X_1, \ldots, X_r]/\langle t_1(X_1), \ldots, t_r(X_r)\rangle$, where $t_i(X_i) \in R[X_i]$ are monic polynomials, were introduced in [16,17]. These codes generalize the notion of multivariable codes over a finite field $\mathbb{F}_q$, as presented in [21], and include well-known families of codes over a finite chain ring alphabet. For instance *cyclic* ($r = 1, t_1(X_1) = X_1^{e_1} - 1$), *negacyclic* ($r = 1, t_1(X_1) = X_1^{e_1} + 1$), *constacyclic* ($r = 1, t_1(X_1) = X_1^{e_1} + \lambda$), *polycyclic* ($r = 1$) and *abelian codes* ($t_i(X_i) = X_i^{e_i} - 1, \forall i = 1, \ldots, r$) [5,12]. Properties of multivariable codes over a finite chain ring depend on the structure of the ambient ring $\mathcal{R}$. So, in [16] a complete account of codes was given when the polynomials $\overline{t_i}(X_i) \in \mathbb{F}_q[X_i]$ have no repeated roots (the so-called *semisimple* or *serial* case). On the other hand, as a first approach to the *repeated-root* (or *modular*) case, Canonical Generating Systems [19] were considered in [17]. Unfortunately, the description is not as satisfactory as in the semisimple case. This situation agrees with that of cyclic, negacyclic, constacyclic and polycyclic repeated-root codes. Different authors have dedicated their efforts to provide a better understanding of these codes over finite chain rings (see, for instance [6,1,22,12]).

One important feature of semisimple codes is that all of them can be generated by a single codeword, i.e., they can be regarded as principal ideals in $\mathcal{R}$. This property is not generally true in the modular case, and it partly explains the reason why these codes are more difficult to describe. However, that of all the ideals in $\mathcal{R}$ are principal is not equivalent to the semisimple condition. Instead, it is equivalent to the fact that its nilradical is principal [4, Lemma 3]. As it was shown in [4, Theorem 2], we have the following characterization (see also [12, Theorem 5.2], [22, Theorem 3.2], [17, Theorem 1]).

Theorem 1. *The ring* $\mathcal{R} = R[X_1, \ldots, X_r]/\langle t_1(X_1), \ldots, t_r(X_r)\rangle$ *is a* principal ideal ring (PIR) *if and only if one of the following conditions is satisfied:*

1. *If* R *is a Galois ring* $GR(p^n, l)$*, then the number of polynomials for which* $\overline{t}_i(X_i)$ *is not square-free is at most one. Moreover, if* R *is not a finite field (i.e.,* $n > 1$*), and* $\overline{t}_i(X_i)$ *is not square-free with*

$$t_i(X_i) = g(X_i)h(X_i) + au(X_i)$$

   where $\overline{g}(X_i)$ *is the square-free part of* $\overline{t}_i(X_i)$*, then* $\overline{u}(X_i)$ *and* $\overline{h}(X_i)$ *are coprime polynomials.*
2. *If* R *is not a Galois ring, then* $r = 1$*, and* $\overline{t}_1(X_1)$ *is square-free.*

Example 1. Let us consider the ring $R = \mathbb{Z}/4\mathbb{Z}$, which is the Galois ring $GR(4, 1)$, and the polynomials $t_1(X_1) = X_1^2 + 1$ and $t_2(X_2) = X_2^7 - 1$. Following Theorem 1, $t_1(X_1)$ can be written as $t_1(X) = (X_1 - 1)^2 + 2X_1$. Since $\overline{h}(X_1) = X_1 + 1$ and $\overline{u}(X_1) = X_1$ are coprime polynomials, then $\mathcal{R} = R[X_1, X_2]/\langle X_1^2 + 1, X_2^7 - 1\rangle$ is a principal ideal ring. Notice that the ring $R[X_1]/\langle X_1^2 + 1\rangle$ is also a principal ideal ring and its ideals are negacyclic codes.

The principal ideal property has been recently used in the description of modular abelian codes over a finite field [9], and in the description of modular *additive* cyclic codes over $\mathbb{F}_4$ (i.e., additive subgroups of the ambient ring $\mathbb{F}_4[X_1]/\langle X_1^{e_1} - 1\rangle$, e_1 even) [8]. As a natural continuation of these works, in this paper we consider the structure of multivariable modular codes over finite chain rings when the ambient space is a

Please cite this article in press as: E. Martínez-Moro et al., Multivariable codes in principal ideal polynomial quotient rings with applications to additive modular bivariate codes over $\mathbb{F}_4$, J. Pure Appl. Algebra (2017), http://dx.doi.org/10.1016/j.jpaa.2017.04.007