Finite Fields and Their Applications 49 (2018) 94–107

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Codes over affine algebras with a finite commutative chain coefficient ring

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

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

ARTICLE INFO

Article history:
Received 3 December 2016
Received in revised form 14 September 2017
Accepted 17 September 2017
Available online xxxx
Communicated by Dieter Jungnickel

MSC:
11T71
94B99
81P70
13M10

Keywords:
Finite commutative chain ring
Affine algebra
Multivariable codes
Quasi-cyclic codes
Codes over non-chain local Frobenius rings

ABSTRACT

We consider codes defined over an affine algebra $\mathcal{A} = R[X_1, \dots, X_r]/\langle t_1(X_1), \dots, t_r(X_r)\rangle$, where $t_i(X_i)$ is a monic univariate polynomial over a finite commutative chain ring R. Namely, we study the $\mathcal{A}$−submodules of $\mathcal{A}^l$ ($l \in \mathbb{N}$). These codes generalize both the codes over finite quotients of polynomial rings and the multivariable codes over finite chain rings. Some codes over Frobenius local rings that are not chain rings are also of this type. A canonical generator matrix for these codes is introduced with the help of the Canonical Generating System. Duality of the codes is also considered.

[*] 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 funded by MINECO MTM2015-65764-C3-1-P.

[2] Partially supported by MINECO-13-MTM2013-45588-C3-1-P, and Principado de Asturias Grant GRUPIN14-142.

https://doi.org/10.1016/j.ffa.2017.09.008
1071-5797/© 2017 Elsevier Inc. All rights reserved.

1. Introduction

Quasi-cyclic codes over a finite commutative chain ring R can be represented as $(R[x]/\langle x^n - 1\rangle)$-submodules of $(R[x]/\langle x^n - 1\rangle)^l$, generalizing the well known construction for finite fields in, for example, [3]. For finite commutative chain ring, the one-generator codes have been extensively studied (see, for example, the classical paper [21] and the references included in [7]), whereas for finite fields the general situation was studied in [11] and recently generalized in [1] to codes over finite quotients of polynomial rings, i.e., to $\mathbb{F}[x]/\langle f(x)\rangle$-submodules of $(\mathbb{F}[x]/\langle f(x)\rangle)^l$ where $l \in \mathbb{N}$ and $f(x)$ is a monic polynomial. Furthermore, Jitman and Ling studied quasi-abelian codes over finite fields using techniques based on the Discrete Fourier Transform. They also gave a structural characterization, as well as an enumeration, of one-generator quasi-abelian codes in [8].

In this paper we will consider codes defined over an affine algebra $\mathcal{A} = R[X_1, \ldots, X_r]/\langle t_1(X_1), \ldots, t_r(X_r)\rangle$, where each $t_i(X_i)$ is a monic univariate polynomial over a finite commutative chain ring R, i.e., $\mathcal{A}-$submodules of $\mathcal{A}^l$. Therefore, this class of codes includes the codes defined in [1] and also, when $l = 1$, multivariable codes over finite commutative chain rings [15,16]. The proposed approach, which uses the concept of Canonical Generating System introduced in [20], allows the study of quasi-cyclic codes over a finite commutative chain ring and their multivariable generalizations in a broader polynomial way, that is, beyond the one-generator case. Notice that for several generators a trace representation can also be derived from the ideas in [12], see for example Section 4 in [7]. The former approach provides a way for defining codes over some Frobenius local rings which are not chain rings. Some of them, as can be seen in Examples 1, 5 and 6, have not been previously explored in the literature.

The outline of the paper is as follows. In Section 2 we state the basic facts on finite commutative chain rings and some examples of known families of codes that are included in our definition. The construction of a canonical generator matrix for our codes is provided in Section 3. In the final section duality of these codes is considered.

2. Basic definitions and examples

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 $q = p^d$ is a prime number power. Examples of finite commutative chain rings include Galois rings $GR(p^n, d)$ of characteristic p^n and p^{nd} elements (here $a = p$, and $t = n$) and, in particular, finite fields $(\mathbb{F}_q = GR(p, d))$ [19,2]. Any element $r \in R$, can be written as $r = a^i r'$, where $0 \leq i \leq t$ and $0 \neq \overline{r'} \in \mathbb{F}_q$. The exponent i is unique, and it is called the *norm* of r, written $\|r\|$.