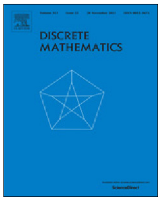
Discrete Mathematics 341 (2018) 1873–1884

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc



# Additive cyclic codes over finite commutative chain rings

Edgar Martinez-Moro [a,*], Kamil Otal [b], Ferruh Özbudak [b]

[a] Mathematics Research Institute, University of Valladolid, Castilla, Spain
[b] Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, Dumlupınar BulvarıNo. 1, 06800, Ankara, Turkey

ARTICLE INFO

*Article history:*
Received 9 September 2017
Received in revised form 8 January 2018
Accepted 17 March 2018

*Keywords:*
Cyclic codes
Additive codes
Codes over rings
Finite commutative chain rings
Galois rings

ABSTRACT

Additive cyclic codes over Galois rings were investigated in Cao et al. (2015). In this paper, we investigate the same problem but over a more general ring family, finite commutative chain rings. When we focus on non-Galois finite commutative chain rings, we observe two different kinds of additivity. One of them is a natural generalization of the study in Cao et al. (2015), whereas the other one has some unusual properties especially while constructing dual codes. We interpret the reasons of such properties and illustrate our results giving concrete examples.

## 1. Introduction

Additive codes are a direct and useful generalization of linear codes, and they have applications in quantum error correcting codes. There are several studies using different approaches on them and their applications (see, for example, [1,4,12,21]).

Cyclic codes are one of the most attractive code families thanks to their rich algebraic structure and easy implementation properties. There are many generalizations of cyclic codes in different directions, e.g., [7,14–16].

Codes over rings have been of interest in the last twenty years, after the discovery that some linear codes over $\mathbb{Z}_4$ are related to non-linear optimal codes over finite fields (see, for example, [3,5,8,18,19]). The first family of the rings used in this perspective was $\mathbb{Z}_{p^n}$, where $p$ is a prime and $n$ is a positive integer. The most important property of such rings is that their ideals form a chain under inclusion. Therefore, generalizations to Galois rings, or moreover finite chain rings are immediate. Some recent works on codes over such rings are [6,7,10,22].

Finite chain rings, besides their practical importance, are quite rich mathematical objects, and so they have also theoretical attraction (see, for example, [11]). They have connections in both geometry (Pappian Hjelmslev planes) and algebraic number theory (quotient rings of algebraic integers). These connections have also been interpreted in applications (as an example of applications in coding theory, see [10]). Some main sources about finite commutative chain rings in the literature are [2,17,20,24].

### 1.1. Related work and our contribution

Additive cyclic codes over Galois rings were investigated in [6]. In this paper, we investigate the same problem but over a more general ring family, finite commutative chain rings. When we focus on non-Galois finite commutative chain rings, we observe two different kinds of additivity.

[*] Corresponding author.
*E-mail addresses:* edgar.martinez@uva.es (E. Martinez-Moro), kamil.otal@gmail.com (K. Otal), ozbudak@metu.edu.tr (F. Özbudak).

https://doi.org/10.1016/j.disc.2018.03.016
0012-365X/© 2018 Elsevier B.V. All rights reserved.

The first one, so-called Galois-additivity, is a natural generalization of the study in [6], anyway our way of construction in this generalization is slightly different from the one in that paper. The authors in [6] were using some linear codes over the base ring and their generator matrices, but we just make use of ideals and do not utilize generator matrices. Our main result with this approach is Theorem 4.9. Also we have some further results related to the code size relations ( Corollary 4.11) and self-duality (Corollary 4.12) as well as we illustrate these results in a concrete example (Example 4.13).

The second one, so-called Eisenstein-additivity, is set up in Theorem 5.2. Eisenstein-additivity has some unusual properties especially as constructing dual codes. It is because, some chain rings are not free over their coefficient rings and hence we cannot define a trace function for some elements over the base ring (Lemma 5.1). Hence, one cannot make use of the equivalence of Euclidean orthogonality and duality via the trace map (see [23, Lemma 6]). Therefore, we use the general idea of duality constructed via annihilators of characters (see [25]). We have adapted this character theoretic duality notion to Eisenstein-additive codes (see Section 5.1) and hence we observe one-to-oneness between a code and its dual code (a MacWilliams identity), as expected. We again provide a concrete example for our result regarding the character theoretic duality (see Example 5.5).

Note that the idea in [6] has been generalized recently also in [22]. However, the generalization in [22] is from Galois rings to free $R$-algebras, where $R$ is a finite commutative chain ring. Recall that we consider also non-free algebras (a finite commutative chain ring does not have to be a free module over a subring of itself). On the other hand, our paper does not cover [22] since every free $R$-algebra does not have to be a chain ring.

### 1.2. Organization of the paper

In Section 2, we introduce finite commutative chain rings constructing them step by step, as from $\mathbb{Z}_{p^n}$ to Galois rings and then to arbitrary finite commutative chain rings. Section 3 provides basic definitions, notations and facts of a code concept over rings, by focusing mainly on cyclic codes and additive codes.

In Section 4, firstly we give some lemmas and then construct the main theorem (Theorem 4.9) of Galois-additivity. We also give some corollaries regarding the code size relations between dual codes (Corollary 4.11), and characterization of self-duality (Corollary 4.12). We also provide an illustration (Example 4.13) about our results.

In Section 5, we directly give the main result (Theorem 5.2) about Eisenstein-additive codes, since it comes from the lemmas in Section 4. A direct character theoretic duality is constructed in Section 5.1 separately. Also an example (Example 5.5) is available to illustrate our results.

## 2. Finite commutative chain rings

A ring $R$ with identity is called *local* if it has only one maximal ideal. A local ring $R$ is called a *chain ring* if its ideals form a chain under inclusion. Saying "finite" we refer to having finitely many elements (not being a finitely generated structure). A finite chain ring is a principal ideal ring, and its maximal ideal is its nil-radical (i.e. the set of nil-potent elements). Hence, the chain of ideals of a finite chain ring $R$ is of the form

$$R \supsetneq NilRad(R) = \langle x \rangle \supsetneq \cdots \supsetneq \langle x^{m-1} \rangle \supsetneq \langle x^m \rangle = \langle 0 \rangle$$

for some nil-potent $x \in R$ and a positive integer $m$ (see, for example [20, Theorem 3.2]). The simplest example of finite chain rings is $\mathbb{Z}_{p^n}$ with the maximal ideal $\langle p \rangle$, where $p$ is a prime and $n$ is a positive integer. We may construct all finite chain rings using $\mathbb{Z}_{p^n}$.

### 2.1. Galois rings

The ring homomorphism $\mathbb{Z}_{p^n} \rightarrow \mathbb{F}_p$ given by $a \mapsto \bar{a}$, where $\bar{a}$ is the remainder of $a$ modulo $p$ and $\mathbb{F}_p$ denotes the finite field of $p$ elements, is called *canonical homomorphism*. We may extend the canonical homomorphism in a natural way from the polynomial ring $\mathbb{Z}_{p^n}[X]$ to the polynomial ring $\mathbb{F}_p[X]$ by $\overline{(\sum_i a_i X^i)} = \sum_i \overline{a_i} X^i$. A polynomial over $\mathbb{Z}_{p^n}$ is called *basic irreducible (primitive)* if its image under the canonical homomorphism is irreducible (primitive) over $\mathbb{F}_p$. We also assume that all polynomials are monic and their constant terms are unit elements unless otherwise stated, since we mainly focus on and utilize such polynomials.

Let $f(X) \in \mathbb{Z}_{p^n}[X]$ be a basic irreducible polynomial of degree $r$. The quotient ring $\mathbb{Z}_{p^n}[X]/\langle f(X) \rangle$ is a finite chain ring with the maximal ideal $\langle p \rangle$. This kind of rings are known as *Galois rings* and denoted by $GR(p^n, r)$. In a Galois ring $GR(p^n, r)$, $p^n$ is called *characteristic* and $r$ is called *rank*. Galois rings are unique up to isomorphism for a given characteristic and rank. We will use the notation $\mathbb{Z}_{p^n}[\omega]$ to denote Galois rings, taking $\omega = X + \langle f(X) \rangle$. Note that $f(X)$ is the unique monic polynomial of degree less than or equal to $r$ such that $f(\omega) = 0$. We may extend the canonical homomorphism as from $\mathbb{Z}_{p^n}[\omega]$ to $\mathbb{F}_{p^r}$ such that $\overline{\omega}$ satisfies $\overline{f}(\overline{\omega}) = 0$ and so $\mathbb{F}_{p^r} = \mathbb{F}_p[\overline{\omega}]$. Moreover, in a Galois ring $GR(p^n, r)$, there exists an element of multiplicative order $p^r - 1$, which is a root of a basic primitive polynomial of degree $r$ over $\mathbb{Z}_{p^n}$ and dividing $X^{p^r-1} - 1$ in $\mathbb{Z}_{p^n}[X]$. If $\omega$ is this kind of "basic primitive element", then the set

$$T = \{0, 1, \omega, \omega^2, \ldots, \omega^{p^r-2}\}$$