Discrete Mathematics 341 (2018) 1722–1731

Contents lists available at ScienceDirect

Discrete Mathematics

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

Contraction of cyclic codes over finite chain rings

Alexandre Fotue Tabue [a,*], Christophe Mouaha [b]

[a] Department of Mathematics, Faculty of Science, University of Yaoundé 1, Cameroon
[b] Department of Mathematics, Higher Teachers Training College, University of Yaoundé 1, Cameroon

ARTICLE INFO

Article history:
Received 18 September 2016
Received in revised form 2 January 2018
Accepted 10 March 2018

Keywords:
Finite chain ring
Galois extension
Linear code
Constacyclic code

ABSTRACT

In this paper, R is a finite chain ring with residue field $\mathbb{F}_q$ and γ is a unit in R. By assuming that the multiplicative order u of γ is coprime to q, we give the trace-representation of any simple-root γ-constacyclic code over R of length ℓ, and on the other hand show that any cyclic code over R of length $u\ell$ is a direct sum of trace-representable cyclic codes. Finally, we characterize the simple-root, contractable and cyclic codes over R of length $u\ell$ into γ-constacyclic codes of length ℓ.

1. Introduction

Let R be a finite chain ring with identity element 1_R, and $\mathbb{F}_q$ its residue field. Let $\pi : R \to \mathbb{F}_q$ be the natural ring-epimorphism, and $\gamma \in R$ be a unit with multiplicative order u. An R-linear code $\mathscr{C}$ of length n is γ-*constacyclic*, if $\tau_\gamma(\mathscr{C}) = \mathscr{C}$ where the γ-*shift operator* $\tau_\gamma : R^n \to R^n$ is defined by: $\tau_\gamma(c_0, c_1, \ldots, c_{n-1}) = (\gamma c_{n-1}, c_0, \ldots, c_{n-2})$. Especially, cyclic and negacyclic codes correspond respectively to $\gamma = 1_R$ and $\gamma = -1_R$ (see [5] and the references therein). By considering the map $\pi : R \to \mathbb{F}_q$, we define the *residue* $\pi(\mathscr{C})$ of any R-linear code $\mathscr{C}$ of length n to be

$$\pi(\mathscr{C}) := \left\{ (\pi(c_0), \pi(c_1), \ldots, \pi(c_{n-1})) \ : \ (c_0, c_1, \ldots, c_{n-1}) \in \mathscr{C} \right\}.$$

Obviously, $\pi(\mathscr{C})$ is an $\mathbb{F}_q$-linear code. The equality $\pi(\tau_\gamma(\mathscr{C})) = \tau_{\pi(\gamma)}(\pi(\mathscr{C}))$ allows to see that the residue of any γ-constacyclic code over R is $\pi(\gamma)$-constacyclic.

The class of constacyclic codes over rings was introduced as an extension of the class of cyclic codes over rings. Recently, constacyclic codes over various rings were considered. Historically, Wolfmann J. [13] was the first to study the structural properties of negacyclic codes over $\mathbb{Z}_4$, proving under some conditions that several constacyclic codes are equivalent to cyclic codes. Those results were generalized to γ-constacyclic codes over R, with multiplicative order of γ being a power of the characteristic of R (see [1,2,4,14] and the references therein). In this paper, we study the simple-root constacyclic codes of length ℓ over a finite chain ring R, their length ℓ of which is coprime to the characteristic of R. We give a complete Bierbrauer's approach for any free constacyclic code over R of length ℓ, and we decompose any (non-necessary free) cyclic codes over R of length $u\ell$ into a direct sum of trace-representable cyclic codes over R of length $u\ell$. An R-linear code $\mathscr{K}$ of length ℓ is a *contraction* of an R-linear code $\mathscr{C}$ of length n, if $\ell < n$ and $(c_0, c_1, \ldots, c_{\ell-1}) \in \mathscr{K}$ for all $(c_0, c_1, \ldots, c_{\ell-1}, c_\ell, \ldots, c_{n-1}) \in \mathscr{C}$. Finally, we give a necessary and sufficient condition so that the contraction of a cyclic code over R of length $u\ell$, is a γ-constacyclic code over R of length ℓ.

* Corresponding author.
E-mail addresses: alexfotue@gmail.com (A. Fotue Tabue), cmouaha@yahoo.fr (C. Mouaha).

https://doi.org/10.1016/j.disc.2018.03.008
0012-365X/

The rest of this paper is organized as follows. In Section 2, we give some results, which will be used in the following sections. In Section 3, we explore a Bierbrauer's approach for any free simple-root constacyclic code, and decompose any cyclic code into a direct sum of trace-representable cyclic codes. In Section 4, we characterize the simple-root cyclic codes over R of length $u\ell$, whose contractions are constacyclic codes over R of length ℓ.

2. Preliminaries

Throughout this section, $\mathbb{F}_q$ denote the finite field of order q and characteristic p, R is a *finite chain ring of invariants* (q, s), which is a local ring R with maximal ideal $\mathtt{J}(R)$, such that $\mathtt{J}(R)$ is principal, $R/\mathtt{J}(R) \simeq \mathbb{F}_q$ and $R \supsetneq \mathtt{J}(R) \supsetneq \cdots \supsetneq \mathtt{J}(R)^{s-1} \supsetneq \mathtt{J}(R)^s = \{0_R\}$. The positive integer s is called the *nilpotency index* of R and $\mathbb{F}_q$ is called residue field of R. Obviously, the ideals of R, are precisely $\mathtt{J}(R)^t = R\theta^t$ for $t \in \{0; 1; \cdots; s\}$, and for some fixed generator θ of $\mathtt{J}(R)$. The natural ring-epimorphism $\pi : R \to \mathbb{F}_q$ extends to $R[X] \to \mathbb{F}_q[X]$ of in the following way: $\pi\left(\sum a_i X^i\right) = \sum \pi(a_i)X^i$ for $a_i \in R$. The *multiplicative order* $\mathtt{ord}(\gamma)$ of the unit γ in R, is the smallest positive integer among the positive integers i fulfilling $i \neq 0$ and $\gamma^i = 1$. The following definitions and results on the finite chain rings were extracted from monographs [10,11].

2.1. Galois extension of finite chain rings

Let R be a finite chain ring of invariants (q, s). Let $\Gamma(R)^*$ be the unique cyclic subgroup of $R^\times$ of order $q-1$. The set $\Gamma(R)^* \cup \{0_R\}$ is called the *Teichmüller set* of R, and one just writes $\Gamma(R) = \Gamma(R)^* \cup \{0_R\}$. The subset $1_R + \mathtt{J}(R)$ of R is a multiplicative subgroup of $R^\times$ and $R^\times \simeq \Gamma(R)^* \times (1_R + \mathtt{J}(R))$ (as groups), since $R^\times = R \setminus \mathtt{J}(R)$ and $\mathtt{gcd}(q, q-1) = 1$. Nechaev reveals in [11] that $\Gamma(R)$ is the set of roots of $X^q - X$, which allows us to characterize the subgroups $\Gamma(R)^*$ and $1_R + \mathtt{J}(R)$ of $R^\times$ of the following way.

Proposition 2.1. *If R be a finite chain ring of invariants (q, s), then $\Gamma(R)^* = \left\{\gamma \in R^\times : \mathtt{gcd}(q, \mathtt{ord}(\gamma)) = 1\right\}$ and $1_R + \mathtt{J}(R) = \left\{\gamma \in R^\times : \mathtt{ord}(\gamma)\ \text{divides}\ q^{s-1}\right\}$.*

The cardinality of the residue field and the nilpotency index of R suffice for our study of simple-root constacyclic codes over R.

Example 2.1. The finite field $\mathbb{F}_q$ is the finite chain ring of invariants $(q, 1)$. The rings $\mathbb{Z}_{p^s}$ and $\mathbb{F}_p[X]/\langle X^s \rangle$ are non-isomorphic finite chain rings of invariants (p, s).

The ring S is an *extension* of R, and we denote it by $S|R$, if R is a subring of S and $1_R = 1_S$. If S is an extension of R, then S is an R-module. When S is a free R-module, the rank $[S : R]$ of the R-module S is the cardinality of an R-basis of S. We denote by $\mathtt{Aut}_R(S)$, the group of ring-automorphisms of S fixing the elements of R. A local ring S is a *Galois extension* of R with degree m, if $[S : R] = m$, $\mathtt{J}(S) = \mathtt{J}(R)S$ and $R := \{a \in S : \varrho(a) = a \text{ for all } \varrho \in \mathtt{Aut}_R(S)\}$. A monic polynomial f over R is *basic-irreducible*, if $\pi(f)$ is irreducible over $\mathbb{F}_q$. From [10, Theorem XIV.8 and Corollary XV.4], we have the following result.

Proposition 2.2. *Let R be a finite chain ring. The ring S is a Galois extension of R with degree m, if and only if there exists a monic basic-irreducible polynomial f over R of degree m such that $S \simeq R[X]/\langle f \rangle$ (as R-algebras), where $\langle f \rangle$ is the ideal of $R[X]$ generated by f.*

For instance, the Galois ring with characteristic p^s of cardinality q (recall that $\mathtt{GR}(p^s, r)$ and $q = p^r$) is the Galois extension of $\mathbb{Z}_{p^s}$ with degree r. According to [10, Theorem XV.7], there is a unique (up to R-algebra isomorphism) Galois extensions of R with a specified degree m. The Galois extension S of R with degree m is a free R-module, and S is a finite chain ring of invariants $(q^{[S:R]}, s)$. The recapitulative Theorem XV.7 in [10], stipulates that the group $\mathtt{Aut}_R(S)$ is cyclic of order $[S : R]$ and $S = R[\xi]$ where ξ is a generator of $\Gamma(S)$. From now, $S|R$ is the Galois extension of finite chain rings of degree m where $m := [S : R]$, and σ is a generator of $\mathtt{Aut}_R(S)$. The *trace map* $\mathtt{Tr}_R^S : S \to R$ is defined as: $\mathtt{Tr}_R^S := \mathtt{Id}_S + \sigma + \cdots + \sigma^{m-1}$, where $\mathtt{Id}_S : S \to S$ is the identity map of S. Obviously $\mathtt{Tr}_R^S \circ \sigma = \mathtt{Tr}_R^S$. Several facts about the trace map are already known.

Proposition 2.3 (*[10, Chap. XIV]*)**.** *Let S be a Galois extension of R. The trace map $\mathtt{Tr}_R^S : S \to R$ is an R-module epimorphism.*

2.2. Galois-invariance of linear codes over finite chain rings

Recall that an R-linear code (or linear code over R) of length n is a submodule of the R-module R^n. An R-linear code over R is *free*, if it is free as an R-module. A matrix G is called a *generator matrix* for an R-linear code $\mathscr{C}$, if the rows of G span $\mathscr{C}$ and none of them can be written as an R-linear combination of the other rows of G. A matrix G is in the *standard form* if there exists an s-tuple $(k_0, k_1, \ldots, k_{s-1})$ in $\mathbb{N}^s$ (where s is the nilpotency index of R) such that

$$G = \begin{pmatrix} I_{k_0} & G_{0,1} & G_{0,2} & \cdots & G_{0,s-1} & G_{0,s} \\ 0 & \theta I_{k_1} & \theta G_{1,2} & \cdots & \theta G_{1,s-1} & \theta G_{1,s} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & \theta^{s-1} I_{k_{s-1}} & \theta^{s-1} G_{s-1,s} \end{pmatrix} U, \tag{1}$$