Finite Fields and Their Applications 43 (2017) 22–41

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Repeated-root constacyclic codes of prime power lengths over finite chain rings

Hai Q. Dinh [a,*], Hien D.T. Nguyen [b], Songsak Sriboonchitta [c], Thang M. Vo [d]

[a] *Department of Mathematical Sciences, Kent State University, 4314 Mahoning Avenue, Warren, OH 44483, USA*
[b] *Department of Mathematics, Vinh University, Vinh city, Nghe An, Viet Nam*
[c] *Faculty of Economics, Chiang Mai University, Chiang Mai 52000, Thailand*
[d] *Department of Personnel and Organization, Vinh University of Technology Education, Vinh city, Nghe An, Viet Nam*

ARTICLE INFO

Article history:
Received 24 February 2016
Received in revised form 22 May 2016
Accepted 29 July 2016
Available online xxxx
Communicated by W. Cary Huffman

MSC:
primary 94B15, 94B05
secondary 11T71

Keywords:
Cyclic codes
Negacyclic codes
Constacyclic codes
Repeated-root codes
Chain rings

ABSTRACT

We study the algebraic structure of repeated-root λ-constacyclic codes of prime power length p^s over a finite commutative chain ring R with maximal ideal $\langle\gamma\rangle$. It is shown that, for any unit λ of the chain ring R, there always exists an element $r \in R$ such that $\lambda - r^{p^s}$ is not invertible, and furthermore, the ambient ring $\frac{R[x]}{\langle x^{p^s}-\lambda\rangle}$ is a local ring with maximal ideal $\langle x-r, \gamma\rangle$. When there is a unit λ_0 such that $\lambda = \lambda_0^{p^s}$, the nilpotency index of $x - \lambda_0$ in the ambient ring $\frac{R[x]}{\langle x^{p^s}-\lambda\rangle}$ is established. When $\lambda = \lambda_0^{p^s} + \gamma w$, for some unit w of R, it is shown that the ambient ring $\frac{R[x]}{\langle x^{p^s}-\lambda\rangle}$ is a chain ring with maximal ideal $\langle x^{p^s} - \lambda_0\rangle$, which in turn provides structure and sizes of all λ-constacyclic codes and their duals. Among other things, situations when a linear code over R is both α- and β-constacyclic, for different units α, β, are discussed.

* Corresponding author.
E-mail addresses: hdinh@kent.edu (H.Q. Dinh), nguyenthiduchiendhv@gmail.com (H.D.T. Nguyen), songsakecon@gmail.com (S. Sriboonchitta), vomanhthang@vute.edu.vn (T.M. Vo).

http://dx.doi.org/10.1016/j.ffa.2016.07.011
1071-5797/

1. Introduction

The constacyclic codes play a very significant role in the theory of error-correcting codes as they are a direct generalization of the important family of cyclic codes. Cyclic codes have been the most studied of all codes. Many well known codes, such as BCH, Kerdock, Golay, Reed–Muller, Preparata, Justesen, and binary Hamming codes, are either cyclic codes or constructed from cyclic codes. Due to their rich algebraic structure, constacyclic codes can be efficiently encoded using shift registers, which explains their preferred role in engineering.

Given a nonzero element λ of the finite field F, λ-constacyclic codes of length n are classified as ideals as the ideals $\langle f(x)\rangle$ of the quotient ring $\frac{F[x]}{\langle x^n-\lambda\rangle}$, where $f(x)$ is a divisor of $x^n-\lambda$. In the early history of error-correcting codes, most of the research was concentrated on the situation when the code length n is relatively prime to the characteristic of the field F. This ensures that $x^n-\lambda$, and hence the generator polynomial of any λ-constacyclic code, will have no multiple factors, and hence no repeated roots in an extension field. The case when the code length n is divisible by the characteristic p of the field yields the so-called repeated-root codes, which were first studied since 1967 by Berman [3], and then in the 1970's and 1980's by several authors such as Massey et al. [28], Falkner et al. [22], Roth and Seroussi [32]. Repeated-root codes were first investigated in the most generality in the 1990's by Castagnoli et al. [11], and van Lint [34], where they showed that repeated-root cyclic codes have a concatenated construction, and are asymptotically bad. Nevertheless, such codes are optimal in a few cases, that motivates researchers to further study this class of codes.

After the celebrated results in the 1990's [9,23,30] by Nechaev and Hammons et al. that many important yet seemingly non-linear codes over finite fields are actually closely related to linear codes over the ring of integers modulo four, codes over $\mathbb{Z}_4$ in particular, and codes over finite commutative chain rings in general, have received a great deal of attention. Certain repeated-root constacyclic codes over a class of finite chain rings have been extensively studied over the last few years by many researchers, such as Abualrub and Oehmke [1,2], Blackford [4,5], Dinh [12,13,15,16,20], Ling et al. [21,27,25], Sălăgean et al. [31,33], etc. (See Examples 3.13–3.16 and 3.23 for more details.) To distinguish the two cases, codes where the code-length is not divisible by the characteristic p of the residue field $\overline{R}$ are called *simple-root codes*. In this paper, we concentrate on repeated-root constacyclic codes of length p^s over finite chain rings in general.

The rest of this paper is organized as follows. Section 2 presents some preliminary materials about chain rings and constacyclic codes. In Section 3, we show that, given a finite commutative chain ring R of characteristic p^a with unique maximal ideal $\langle\gamma\rangle$, any unit λ of R can expressed as $\lambda = \lambda_0^{p^s} + \gamma w$, for some $w \in R$. Moreover, the ambient ring $\frac{R[x]}{\langle x^{p^s}-\lambda\rangle}$ is a local ring with maximal ideal $\langle x-\lambda_0, \gamma\rangle$. Two cases are studied in details, namely, $w = 0$, and w is a unit. When $w = 0$, i.e., $\lambda = \lambda_0^{p^s}$, the nilpotency index of $x - \lambda_0$ is completely determined. When w is a unit, i.e., $\lambda = \lambda_0^{p^s} + \gamma w$ for units λ_0, w of R, we prove that $\gamma \in \langle x-\lambda_0\rangle$, and so the ambient ring $\frac{R[x]}{\langle x^{p^s}-\lambda\rangle}$ is a chain