Finite Fields and Their Applications 37 (2016) 108–130

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Constacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$

Bocong Chen [a,e], Hai Q. Dinh [b], Hongwei Liu [c,*], Liqi Wang [d]

[a] *School of Mathematics, South China University of Technology, Guangzhou, Guangdong, 510641, China*
[b] *Department of Mathematical Sciences, Kent State University, 4314 Mahoning Avenue, Warren, OH 44483, USA*
[c] *School of Mathematics and Statistics, Central China Normal University, Wuhan, Hubei, 430079, China*
[d] *School of Mathematics, Hefei University of Technology, Hefei, Anhui, 230009, China*
[e] *Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore, 637616, Singapore*

ARTICLE INFO

Article history:
Received 24 March 2015
Received in revised form 22 September 2015
Accepted 23 September 2015
Available online 11 November 2015
Communicated by Chaoping Xing

MSC:
94A55
94B05

Keywords:
Constacyclic codes
Dual codes
Repeated-root codes

ABSTRACT

The aim of this paper is to determine the algebraic structures of all λ-constacyclic codes of length $2p^s$ over the finite commutative chain ring $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, where p is an odd prime and $u^2 = 0$. For this purpose, the situation of λ is mainly divided into two cases separately. If the unit λ is not a square and $\lambda = \alpha + u\beta$ for nonzero elements α, β of $\mathbb{F}_{p^m}$, it is shown that the ambient ring $(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})[x]/\langle x^{2p^s} - (\alpha + u\beta)\rangle$ is a chain ring with the unique maximal ideal $\langle x^2 - \alpha_0\rangle$, and thus $(\alpha + u\beta)$-constacyclic codes are $\langle (x^2 - \alpha_0)^i\rangle$ for $0 \le i \le 2p^s$. If the unit λ is not a square and $\lambda = \gamma$ for some nonzero element γ of $\mathbb{F}_{p^m}$, such λ-constacyclic codes are classified into 4 distinct types of ideals. The detailed structures of ideals in each type are provided. Among other results, the number of codewords and the dual of every λ-constacyclic code are obtained.

* Corresponding author.
E-mail addresses: bocong_chen@yahoo.com (B. Chen), hdinh@kent.edu (H.Q. Dinh), hwliu@mail.ccnu.edu.cn (H. Liu), liqiwangg@163.com (L. Wang).

http://dx.doi.org/10.1016/j.ffa.2015.09.006
1071-5797/

1. Introduction

The class of constacyclic codes plays a very significant role in the theory of error-correcting codes. It includes as subclass the important class of cyclic codes, which has been well studied since the late 1950's. Constacyclic codes also have practical applications as they can be efficiently encoded with simple shift registers. This family of codes is thus interesting for both theoretical and practical reasons.

Given a unit λ of a finite field $\mathbb{F}$, λ-constacyclic codes of length n over $\mathbb{F}$ are ideals of the quotient ring $\mathbb{F}[x]/\langle x^n - \lambda\rangle$. In the literature, most of the research is concentrated on the situation where the code length n is relatively prime to the characteristic of $\mathbb{F}$. The case where the code length n is not relatively prime to the characteristic of $\mathbb{F}$ yields the so-called repeated-root codes. It was first studied by Berman [5], and then by several authors, such as Massey et al. [27], Falkner et al. [21] and Roth and Seroussi [32]. Repeated-root cyclic codes were investigated in the most generality by Castagnoli et al. [11] and van Lint [37], where they showed that repeated-root cyclic codes have a concatenated construction and are asymptotically bad. Nevertheless, it turns out that such codes are optimal in a few cases, which motivates researchers to further study this class of codes (see, for example, [12,25,29,35,39]).

After the realization in the 1990's [9,22,28] that many important yet seemingly non-linear binary codes, such as Kerdock and Preparata codes, are actually closely related to linear codes over the ring of integers modulo four via the Gray map, codes over finite rings have received a great deal of attention. Since 2003, special classes of repeated-root codes over certain classes of finite chain rings have been studied by many authors (see, for example, [1,6,10,20,30]). Negacyclic codes as an important class of constacyclic codes were first initiated by Berlekamp in the early 1960's [4]. In 1999, Wolfmann [38] studied negacyclic codes of odd length over $\mathbb{Z}_4$ and gave some important results of such codes. More generally, the structure of negacyclic codes over a finite chain ring with the code length relatively prime to the characteristic of its residue field was obtained by Dinh and López-Permouth [18]. Meanwhile, much attention has also been paid to repeated-root negacyclic codes over finite rings. Blackford [7] used a transform approach to classify negacyclic codes of even length over $\mathbb{Z}_4$. The structures of negacyclic codes of length 2^s over the Galois ring $GR(2^a, m)$ as well as their dual codes were determined in [13]. After that, Sălăgean [33] showed that negacyclic codes of even length over the Galois ring $GR(2^a, m)$ are principally generated.

The class of finite commutative rings of the form $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, where $u^2 = 0$, has been widely used as alphabets of certain constacyclic codes. For example, the structure of $\mathbb{F}_2 + u\mathbb{F}_2$ is interesting, because it is lying between $\mathbb{F}_4$ and $\mathbb{Z}_4$ in the sense that it is additively analogous to $\mathbb{F}_4$ and multiplicatively analogous to $\mathbb{Z}_4$. Linear codes over $\mathbb{F}_2 + u\mathbb{F}_2$ have been studied by a lot of researchers (see, for example, [2,3,8,23,34,36]). The classification of codes plays an important role in studying their structures. However, in general, it is a very difficult task, and only some codes of special lengths over certain finite fields or finite chain rings are classified. All constacyclic codes of length 2^s over