Finite Fields and Their Applications 43 (2017) 86–105

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On structure and distances of some classes of repeated-root constacyclic codes over Galois rings

Hai Q. Dinh [a], Hongwei Liu [b,*], Xiu-sheng Liu [c], Songsak Sriboonchitta [d]

[a] *Department of Mathematical Sciences, Kent State University, 4314 Mahoning Avenue, Warren, OH 44483, USA*
[b] *School of Mathematics and Statistics, Central China Normal University, Wuhan, Hubei, 430079, China*
[c] *School of Mathematics and Physics, Hubei Polytechnic University, Huangshi, 435003, China*
[d] *Faculty of Economics, Chiang Mai University, Chiang Mai 52000, Thailand*

ARTICLE INFO

Article history:
Received 21 May 2016
Received in revised form 18 September 2016
Accepted 19 September 2016
Available online xxxx
Communicated by W. Cary Huffman

MSC:
primary 94B15, 94B05
secondary 11T71

Keywords:
Constacyclic codes
Repeated-root codes
Dual codes
Codes over rings
Hamming distance
Homogeneous distance
Rosenbloom–Tsfasman distance

ABSTRACT

The structure of λ-constacyclic codes of length 2^s over the Galois ring $\mathrm{GR}(2^a, m)$ is obtained, for any unit λ of the form $4z - 1$, $z \in \mathrm{GR}(2^a, m)$. The duals codes and necessary and sufficient conditions for the existence of a self-dual λ-constacyclic code are provided. Among others, this structure is used to establish the Hamming, homogeneous, and Rosenbloom–Tsfasman distances, and Rosenbloom–Tsfasman weight distribution of all such constacyclic codes.

* Corresponding author.
E-mail addresses: hdinh@kent.edu (H.Q. Dinh), hwliu@mail.ccnu.edu.cn (H. Liu), lxs6682@163.com (X. Liu), songsakecon@gmail.com (S. Sriboonchitta).

http://dx.doi.org/10.1016/j.ffa.2016.09.004
1071-5797/

Chain rings
Galois rings

1. Introduction

Constacyclic codes over finite fields play a very significant role in algebraic coding theory. The most important class of these codes is the class of cyclic codes, which has been well studied since the late 1950's. However, most of the research is concentrated on the situation when the code length n is relatively prime to the characteristic of the field F. In this case, cyclic codes of length n are classified as ideals $\langle f(x)\rangle$ of $\frac{F[x]}{\langle x^n-1\rangle}$, where $f(x)$ is a divisor of x^n-1. 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 [6], and then in the 1970's and 1980's by several authors such as Massey et al. [40], Falkner et al. [28], Roth and Seroussi [47]. However, repeated-root codes over finite fields were investigated in the most generality in the 1990's by Castagnoli et al. [15], and van Lint [51], 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 (see, for example, [50,43]).

In the early 1990's, Nechaev [42], and Hammons et al. [13,31] established the celebrated result that many well-known seemingly nonlinear codes over finite fields such as Kerdock and Preparata codes are actually closely related to linear codes over the ring $\mathbb{Z}_4$. Since then, codes over $\mathbb{Z}_4$ in particular, and codes over finite rings in general, have proved their importance, and they have received a great deal of attention.

The Galois ring of characteristic p^a and dimension m, denoted by $\mathrm{GR}(p^a, m)$, is the Galois extension of degree m of the ring $\mathbb{Z}_{p^a}$, for some prime number p. In particular, rings of the form $\mathbb{Z}_{p^a}$ such as $\mathbb{Z}_4$ are Galois rings. The class of Galois rings has been used widely as an alphabet for cyclic and negacyclic codes, for instance [14,52,3,8,35,10]. Various decoding schemes for codes over Galois rings have also been addressed [9–12]. Since 2003, special classes of repeated-root constacyclic codes over certain classes of finite chain rings and Galois rings have been studied by numerous other authors (see, for example, [1,8,21,37,44,48]).

In recent years, we have been working on the description of several classes of constacyclic codes, such as cyclic and negacyclic codes, over various types of Galois rings. In 2005 [20], we investigated negacyclic codes of length 2^s over the Galois ring $\mathrm{GR}(2^a, m)$. We showed that the ring $\frac{\mathrm{GR}(2^a,m)[x]}{\langle x^{2^s}+1\rangle}$ is indeed a chain ring, and the negacyclic codes of length 2^s over $\mathrm{GR}(2^a, m)$ are precisely the ideals generated by $(x+1)^i$ of this chain ring, for $i = 0, 1, \dots, 2^s a$. Using this structure, Hamming distances of such negacyclic codes were obtained. In 2007, we computed the Hamming, Lee, homogeneous, and Euclidean distances of all those negacyclic codes for the case when the alphabet is $\mathbb{Z}_{2^a}$ [22], i.e., the Galois ring $\mathrm{GR}(2^a, m)$ with dimension $m = 1$.