Finite Fields and Their Applications 42 (2016) 1–22

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Enumeration formulas for self-dual cyclic codes

Bocong Chen [a,b], San Ling [b], Guanghui Zhang [c,*]

[a] *School of Mathematics, South China University of Technology, Guangzhou, Guangdong, 510641, China*
[b] *Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore 637616, Singapore*
[c] *School of Mathematical Sciences, Luoyang Normal University, Luoyang, Henan, 471022, China*

ARTICLE INFO

Article history:
Received 6 December 2014
Received in revised form 18 January 2016
Accepted 22 June 2016
Available online 18 July 2016
Communicated by Jacques Wolfmann

MSC:
94B15
11T71

Keywords:
Cyclic code
Dual code
Self-dual cyclic code
Finite chain ring

ABSTRACT

Let R be a finite commutative chain ring with unique maximal ideal $\langle\gamma\rangle$, and let n be a positive integer relatively prime to the characteristic of $R/\langle\gamma\rangle$. In this paper, some new necessary and sufficient conditions for the existence of nontrivial self-dual cyclic codes of length n over R are provided. Explicit enumeration formulas for self-dual cyclic codes over R are studied. In particular, several main results of [21] are special cases of the present paper.

[*] Corresponding author.
E-mail addresses: bocong_chen@yahoo.com (B. Chen), lingsan@ntu.edu.sg (S. Ling), zghui2012@126.com (G. Zhang).

http://dx.doi.org/10.1016/j.ffa.2016.06.007
1071-5797/© 2016 Elsevier Inc. All rights reserved.

1. Introduction

The study of codes over finite rings has grown tremendously since the seminal work of Hammons et al. [9]. It is shown in [9] that some of the best nonlinear codes over $\mathbb{F}_2$ can be viewed as linear codes over $\mathbb{Z}_4$. Wood [25,26] pointed out that only finite Frobenius rings are suitable for coding alphabets, in the sense that several fundamental properties of codes over finite fields still hold for codes over such rings. This has motivated numerous authors to do research on codes over finite chain rings, as chain rings are Frobenius rings with good algebraic structures.

On the other hand, the class of cyclic codes plays a very significant role in the theory of error-correcting codes. One is that they can be efficiently encoded using shift registers. There is a lot of literature about cyclic codes over finite chain rings (e.g., see [1,7,8,14, 19–22]). Generally, cyclic codes over finite chain rings can be divided into two classes: simple-root cyclic codes, if the code lengths are relatively prime to the characteristic of the ring; otherwise, we have the so-called repeated-root cyclic codes. In this paper, we study simple-root cyclic codes over finite chain rings.

Pless and Qian [19] showed that cyclic codes of odd length n over $\mathbb{Z}_4$ have generators of an interesting form: $\langle fh, 2gh\rangle$, where $f, g, h \in \mathbb{Z}_4[X]$ satisfy $fgh = X^n - 1$. Pless, Solé and Qian in [20] considered the existence conditions for nontrivial self-dual cyclic codes of odd length over $\mathbb{Z}_4$. Results of [19,20] were then extended to simple-root cyclic codes over $\mathbb{Z}_{p^m}$ [15]. Following that line of research, Wan continued to consider simple-root cyclic codes over Galois rings [23]. Extending the main results of [15] and [23], Dinh and López-Permouth in [7] completely described simple-root cyclic codes over finite commutative chain rings; several necessary and sufficient conditions for the existence of nontrivial self-dual cyclic codes were provided. Very recently, Qian et al. in [21] studied self-orthogonal and self-dual cyclic codes of odd length over $\mathbb{Z}_{2^m}$; enumeration formulas for self-dual cyclic codes of odd length over $\mathbb{Z}_{2^m}$ were presented.

Let R be a finite commutative chain ring with unique maximal ideal $\langle\gamma\rangle$. Then $\langle\gamma\rangle$ is nilpotent and its nilpotency index is denoted by t. Let n be a positive integer relatively prime to the characteristic of $\mathbb{F}_q = R/\langle\gamma\rangle$. First, we generalize the methods of [13] to obtain the algebraic structure of cyclic codes of length n over R, which is different from that given in [7]. Using this structure theorem, we show that self-dual cyclic codes of length n over R exist if and only if t is even. Some new necessary and sufficient conditions for the existence of nontrivial self-dual cyclic codes are also derived. We show that, when the nilpotency index t is even, the number of self-dual cyclic codes is fully determined by $|\Delta_n|$, the number of reciprocal polynomial pairs in the monic irreducible factorization of $X^n - 1$ over $\mathbb{F}_q$. Several main results of [21] are thus special cases of the present paper. Comparing with [7] and [21], one of the main contributions of our paper lies in showing that the existence of nontrivial self-dual cyclic codes of length n over R is equivalent to the existence of nontrivial self-dual cyclic codes of length n over $\mathbb{F}_q = R/\langle\gamma\rangle$.

The counting problem for $|\Delta_n|$ naturally reduces to an equivalent question about counting $|\Omega_n|$, the number of self-reciprocal monic irreducible factors of $X^n - 1$ over $\mathbb{F}_q$.