Finite Fields and Their Applications 39 (2016) 233–250

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On double cyclic codes over $\mathbb{Z}_4$

Jian Gao [a], Minjia Shi [b,c,d], Tingting Wu [e,*], Fang-Wei Fu [e]

[a] *School of Science, Shandong University of Technology, Zibo, 255091, PR China*
[b] *Key Laboratory of Intelligent Computing & Signal Processing, Ministry of Education, Anhui University, Hefei, 230039, PR China*
[c] *School of Mathematical Sciences, Anhui University, Hefei, 230601, PR China*
[d] *National Mobile Communications Research Laboratory, Southeast University, Nanjing, 210096, PR China*
[e] *Chern Institute of Mathematics and LPMC, Nankai University, Tianjin, 300071, PR China*

ARTICLE INFO

Article history:
Received 6 January 2015
Received in revised form 3 February 2016
Accepted 4 February 2016
Communicated by Chaoping Xing

MSC:
11T71
94B05
94B15

Keywords:
Double cyclic codes
Generator polynomials
Minimal generating sets
Good nonlinear binary codes

ABSTRACT

Let $R = \mathbb{Z}_4$ be the integer ring mod 4. A double cyclic code of length (r, s) over R is a set that can be partitioned into two parts that any cyclic shift of the coordinates of both parts leaves invariant the code. These codes can be viewed as $R[x]$-submodules of $R[x]/(x^r - 1) \times R[x]/(x^s - 1)$. In this paper, we determine the generator polynomials of this family of codes as $R[x]$-submodules of $R[x]/(x^r - 1) \times R[x]/(x^s - 1)$. Further, we also give the minimal generating sets of this family of codes as R-submodules of $R[x]/(x^r - 1) \times R[x]/(x^s - 1)$. Some optimal or suboptimal nonlinear binary codes are obtained from this family of codes. Finally, we determine the relationship of generators between the double cyclic code and its dual.

* Corresponding author.
E-mail address: wutingting@mail.nankai.edu.cn (T. Wu).

http://dx.doi.org/10.1016/j.ffa.2016.02.003

1. Introduction

Error-correcting codes play an important role in applications ranging from data networking to satellite communication to compact disks. Classical coding theory concerns linear codes since they have clear structure that makes them easy to discover, to understand and to encode and decode.

Codes over finite rings have been studied since the early 1970s. There are a lot of works on codes over finite rings after the discovery that certain good nonlinear binary codes can be constructed from cyclic codes over $\mathbb{Z}_4$ via the Gray map [14]. Since then, many researchers have paid more and more attention to study the codes over finite rings. In these studies, the group rings associated with codes are finite chain rings. Recently, the Spanish coding group Borges et al. introduced a class of new codes called $\mathbb{Z}_2\mathbb{Z}_4$-additive codes (see [6]). This family of codes are important from theory to application, and some generalizations are also studied deeply in the last years (see [2,4,5]). For $\mathbb{Z}_2\mathbb{Z}_4$-additive codes, the set of coordinates is partitioned into two parts, the first one of binary coordinates and the second one of quaternary coordinates. The generator matrices and duality of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes were studied (see [6]), and $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes first were studied by Abualrub et al. (see [1]). The methods given in [1] and [6] have been used efficiently to study some generalizations of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes [2,4,5].

Recently, Borges et al. [7] studied the algebraic structures of $\mathbb{Z}_2$-double cyclic codes and determined the generator polynomials of this family of codes and their duals. In fact, the double cyclic codes were generalized quasi-cyclic (GQC) codes with index two introduced by Siap and Kulhan [16] and were studied deeply by many other researchers [9–12]. However, the points of view between [7] and [9–12,16] are different. In [9–12,16], authors mainly studied structural properties of GQC codes including enumerators, minimum generating sets and minimum Hamming distance bounds of GQC codes. However, the problem of determining the explicit generators of GQC codes has not been discussed until the appearance of the literature [7].

An important motivation to study linear codes, for example cyclic codes and their generalizations, over $\mathbb{Z}_4$ is that some good nonlinear binary codes can be obtained by these codes (see [3,14]). Naturally, as a special class of linear codes, we ask whether some good nonlinear binary codes can be obtained from the double cyclic codes over $\mathbb{Z}_4$. In this paper, following the approaches given in [1] and [7], we investigate some algebraic structures of double cyclic codes over $\mathbb{Z}_4$. Some good nonlinear binary codes are obtained from this family of codes.

The paper is organized as follows. In Section 2, we introduce some definitions and give some structural properties of double cyclic codes over $\mathbb{Z}_4$. In Section 3, we determine the minimal generating sets of double cyclic codes over $\mathbb{Z}_4$. Moreover, some good nonlinear binary codes are obtained from this family of codes. In Section 4, we determine the relationship of generators between the double cyclic code and its dual.