Finite Fields and Their Applications 52 (2018) 67–93

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Negacyclic codes over the local ring $\mathbb{Z}_4[v]/\langle v^2+2v\rangle$ of oddly even length and their Gray images

Yuan Cao, Yonglin Cao *

School of Mathematics and Statistics, Shandong University of Technology, Zibo, Shandong 255091, China

ARTICLE INFO

Article history:
Received 6 December 2017
Received in revised form 22 March 2018
Accepted 26 March 2018
Communicated by Iwan Duursma

MSC:
94B05
94B15
11T71

Keywords:
Negacyclic code
Dual code
Self-dual code
Local ring
Finite chain ring

ABSTRACT

Let $R=\mathbb{Z}_4[v]/\langle v^2+2v\rangle=\mathbb{Z}_4+v\mathbb{Z}_4$ $(v^2=2v)$ and n be an odd positive integer. Then R is a local non-principal ideal ring of 16 elements and there is a $\mathbb{Z}_4$-linear Gray map from R onto $\mathbb{Z}_4^2$ which preserves Lee distance and orthogonality. First, a canonical form decomposition and the structure for any negacyclic code over R of length $2n$ are presented. From this decomposition, a complete classification of all these codes is obtained. Then the cardinality and the dual code for each of these codes are given, and self-dual negacyclic codes over R of length $2n$ are presented. Moreover, all $23\cdot(4^p+5\cdot 2^p+9)^{\frac{2^p-2}{p}}$ negacyclic codes over R of length $2M_p$ and all $3\cdot(4^p+5\cdot 2^p+9)^{\frac{2^{p-1}-1}{p}}$ self-dual codes among them are presented precisely, where $M_p=2^p-1$ is a Mersenne prime. Finally, 36 new and good self-dual 2-quasi-twisted linear codes over $\mathbb{Z}_4$ with basic parameters $(28,2^{28},d_L=8,d_E=12)$ and of type $2^{14}4^7$ and basic parameters $(28,2^{28},d_L=6,d_E=12)$ and of type $2^{16}4^6$ which are Gray images of self-dual negacyclic codes over R of length 14 are listed.

* Corresponding author.
E-mail addresses: ylcao@sdut.edu.cn (Y. Cao), yuancao@sdut.edu.cn (Y. Cao).

https://doi.org/10.1016/j.ffa.2018.03.005
1071-5797/

1. Introduction

The catalyst for the study of codes over rings was the discovery of the connection between the Kerdock and Preparata codes, which are non-linear binary codes, and linear codes over $\mathbb{Z}_4$ (see [3] and [4]). Soon after this discovery, codes over many different rings were studied. This led to many new discoveries and concreted the study of codes over rings as an important part of the coding theory discipline. Since $\mathbb{Z}_4$ is a chain ring, it was natural to expand the theory to focus on alphabets that are finite commutative chain rings and other special rings (see [1,2,5,7–12,14,16,18–20], for examples).

In 1999, Wood in [23] showed that for certain reasons finite Frobenius rings are the most general class of rings that should be used for alphabets of codes. Then self-dual codes over commutative Frobenius rings were investigated by Dougherty et al. [13]. Especially, in 2014, codes over an extension ring of $\mathbb{Z}_4$ were studied in [24] and [25], here the ring was described as $\mathbb{Z}_4 + u\mathbb{Z}_4$ $(u^2 = 0)$ which is a local non-principal ring. Quasi-twisted codes with constacyclic constituent codes were well characterized by Shi et al. in [17]. Recently, Shi et al. in [21] studied $(1+2u)$-constacyclic codes of odd length over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4$ $(u^2 = 1)$. Properties of these codes were investigated and some good $\mathbb{Z}_4$-codes were obtained.

In this paper, all rings are associative and commutative. Let A be an arbitrary finite ring with identity $1 \neq 0$, $A^\times$ the multiplicative group of units of A and $a \in A$. We denote by $\langle a\rangle_A$, or $\langle a\rangle$ for simplicity, the ideal of A generated by a, i.e. $\langle a\rangle_A = aA$. For any ideal I of A, we will identify the element $a + I$ of the residue class ring A/I with $a \pmod I$ in this paper.

For any positive integer N, let $A^N = \{(a_0, a_1, \ldots, a_{N-1}) \mid a_i \in A,\ i = 0, 1, \ldots, N-1\}$ which is an A-module with componentwise addition and scalar multiplication by elements of A. Then an A-submodule $\mathcal{C}$ of A^N is called a *linear code* of length N over A. For any vectors $a = (a_0, a_1, \ldots, a_{N-1}), b = (b_0, b_1, \ldots, b_{N-1}) \in A^N$. The usual *Euclidian inner product* of a and b is defined by $[a, b] = \sum_{j=0}^{N-1} a_j b_j \in A$. Let $\mathcal{C}$ be a linear code over A of length N. The *dual code* of $\mathcal{C}$ is defined by $\mathcal{C}^\perp = \{a \in A^N \mid [a, b] = 0,\ \forall b \in \mathcal{C}\}$, and $\mathcal{C}$ is said to be *self-dual* if $\mathcal{C} = \mathcal{C}^\perp$.

A linear code $\mathcal{C}$ over A of length N is said to be *negacyclic* if

$$(-a_{N-1}, a_0, a_1, \ldots, a_{N-2}) \in \mathcal{C},\ \forall (a_0, a_1, \ldots, a_{N-1}) \in \mathcal{C}.$$

We will use the natural connection of negacyclic codes to polynomial rings, where $c = (c_0, c_1, c_2, \ldots, c_{N-1}) \in A^N$ is viewed as $c(x) = \sum_{j=0}^{N-1} c_j x^j$ and the negacyclic code $\mathcal{C}$ is an ideal in the polynomial residue ring $A[x]/\langle x^N + 1\rangle$.

In this paper, let n be an odd positive integer and denote

$$R = \mathbb{Z}_4[v]/\langle v^2 + 2v\rangle = \{a + bv \mid a, b \in \mathbb{Z}_4\} = \mathbb{Z}_4 + v\mathbb{Z}_4\ (v^2 = 2v)$$

in which the operations are defined by: