Finite Fields and Their Applications 38 (2016) 27–39

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Cyclic and some constacyclic codes over the ring $\frac{\mathbb{Z}_4[u]}{\langle u^2-1\rangle}$

Mehmet Özen [a,*], Fatma Zehra Uzekmek [a], Nuh Aydin [b], N. Tuğba Özzaim [a]

[a] *Department of Mathematics, Sakarya University, Sakarya, Turkey*
[b] *Department of Mathematics and Statistics, Kenyon College, Gambier, OH, 43022, United States*

A R T I C L E   I N F O

Article history:
Received 28 May 2015
Received in revised form 24 November 2015
Accepted 10 December 2015
Available online 21 December 2015
Communicated by W. Cary Huffman

MSC:
94B05
94B15

Keywords:
Codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$, where $u^2 = 1$
Cyclic codes
Constacyclic codes

A B S T R A C T

In this paper, we study cyclic codes and constacyclic codes with shift constant $(2 + u)$ over $R = \mathbb{Z}_4 + u\mathbb{Z}_4$, where $u^2 = 1$. We determine the form of the generators of the cyclic codes over this ring and their spanning sets. Considering their $\mathbb{Z}_4$ images, we prove that the $\mathbb{Z}_4$-image of a $(2 + u)$-constacyclic code of odd length is a cyclic code over $\mathbb{Z}_4$. We also present many examples of cyclic codes over R whose $\mathbb{Z}_4$-images have better parameters than previously best-known $\mathbb{Z}_4$-linear codes.

1. Introduction and motivation

Cyclic codes have a prominent place in algebraic coding theory. They are among the most intensively studied classes of codes. Another class of codes that attracted the

* Corresponding author.
E-mail addresses: ozen@sakarya.edu.tr (M. Özen), zehra.uzekmek@ogr.sakarya.edu.tr (F.Z. Uzekmek), aydinn@kenyon.edu (N. Aydin), tugbaozzaim@gmail.com (N.T. Özzaim).

http://dx.doi.org/10.1016/j.ffa.2015.12.003

attention of many coding theory researchers in the last two decades is codes over rings. The interest in codes over rings started with the seminal work [10] and expanded in many directions. Rings of order 16 are of special importance. Among other things it is known that the smallest local finite Frobenius commutative, non-chain ring has order 16 [11]. Many rings of order 16 that are of interest in coding theory are extensions of $\mathbb{Z}_4$. For example, codes over the ring $\frac{\mathbb{Z}_4[u]}{\langle u^2\rangle}$ which can also be expressed as $\mathbb{Z}_4+u\mathbb{Z}_4$, where $u^2=0$, are introduced recently in [1], and cyclic codes over this ring are studied more recently in [2].

Tables and databases of best known linear codes over small finite fields have been available for a long time [3]. Due to the importance of codes over $\mathbb{Z}_4$ and intensive work on $\mathbb{Z}_4$-codes, a database of $\mathbb{Z}_4$-codes was created in [4] which is available online [5]. One of the contributions of [2] was to find new $\mathbb{Z}_4$-linear codes that were not known before.

Cyclic codes have many generalizations. One of these is the class of constacyclic codes. There has been much work on constacyclic codes since their introduction in [7]. Constacyclic codes over various rings are also extensively studied in recent years (e.g. [6,12,13,15]). Negacyclic codes are a special case of constacyclic codes with shift constant -1. Negacyclic codes over $\mathbb{Z}_4$ were initially investigated by Wolfmann [9] where he proved that binary Gray image of a linear negacyclic code over $\mathbb{Z}_4$ is a binary cyclic code.

In this article, we focus on cyclic codes over the ring $R=\frac{\mathbb{Z}_4[u]}{\langle u^2-1\rangle}\cong\mathbb{Z}_4+u\mathbb{Z}_4$, where $u^2=1$. This is one of the seven local Frobenius non-chain rings (LFNCR) of order 16 classified in [11] that is isomorphic to $\frac{\mathbb{Z}_4[u]}{\langle u^2+2u\rangle}$, via $u\to u+1$. This is the unique (up to isomorphism) local Frobenius non-chain ring R of order 16 whose group of units is isomorphic to $C_2\times C_2\times C_2$ and $2\notin soc(R)$ [11]. We also consider constacyclic codes over this ring with a specific shift constant. Note that the ring $\mathbb{Z}_4+u\mathbb{Z}_4$, where $u^2=0$, over which cyclic codes are studied recently is another ring in the list of seven LFNCR's of order 16.

2. Preliminaries

Let R be the ring $\mathbb{Z}_4+u\mathbb{Z}_4=\{0,1,2,3,u,2u,3u,1+u,2+u,3+u,1+2u,2+2u,3+2u,1+3u,2+3u,3+3u\}$, where $u^2=1$. This ring is isomorphic to the quotient ring $\mathbb{Z}_4[u]/\langle u^2-1\rangle$. The set of units of R is $\{1,3,u,3u,2+u,1+2u,3+2u,2+3u\}$. There are 7 ideals in this ring of characteristic 4 which are $\langle 0\rangle$, $\langle 2u\rangle$, $\langle 1+u\rangle$, $\langle 3+u\rangle$, $\langle 2+2u\rangle$, $\langle 2u,1+u\rangle$ and R. It is a local ring with the maximal ideal $\langle 2u,1+u\rangle$.

A linear code C of length n over R is an R-submodule of R^n. Elements of C are called codewords. Since R is not a chain ring, there is no canonical form for the generator matrix of a linear code over R, however, one can still find a generating set for it. We will be interested in $\mathbb{Z}_4$-images of codes over R. Any $z\in R$ can be written in the form $z=b+(a-b)u$ for $a,b\in\mathbb{Z}_4$. Then we define the map $\phi: R\to\mathbb{Z}_4^2$ by $\phi(z)=(b,a+b)$, which is then extended to a map from R^n to $\mathbb{Z}_4^{2n}$. For $\vec{v}=(v_0,v_1,\dots,v_{n-1})=(b_0+u(a_0-b_0),\dots,b_{n-1}+u(a_{n-1}-b_{n-1}))$, the natural way of extending ϕ gives us