Filomat 28:5 (2014), 897–906
DOI 10.2298/FIL1405897O

Published by Faculty of Sciences and Mathematics,
University of Niš, Serbia
Available at: http://www.pmf.ni.ac.rs/filomat

Linear, Cyclic and Constacyclic Codes over $\mathcal{S}_4 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$

Zeynep Ödemiş Özger[a,b], Ümmü Ümare Kara[a], Bahattin Yıldız[a]

[a] *Department of Mathematics, Fatih University, 34500 İstanbul, Turkey*
[b] *Present Address: Department of Engineering Sciences, İzmir Kâtip Çelebi University, 35620 İzmir, Turkey*

Abstract. In this work, linear codes over the ring $\mathcal{S}_4 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$ are considered. The Lee weight and gray map for codes over $\mathcal{S}_4$ are defined and MacWilliams identities for the complete, the symmetrized and the Lee weight enumerators are obtained. Cyclic and $(1 + u^2)$-constacyclic codes over $\mathcal{S}_4$ are studied, as a result of which a substantial number of optimal binary codes of different lengths are obtained as the Gray images of cyclic and constacyclic codes over $\mathcal{S}_4$.

1. Introduction

Cyclic codes are a special family of linear codes that have generated a lot of interest among coding theorists for their rich algebraic structure that allows them to be encoded and decoded in a relatively easier way. With the growing interest on codes over rings in the last two decades, cyclic codes over different types of rings have been studied in the literature. Among the rings studied, finite chain rings are probably the most common type of rings. Cyclic codes over different examples of finite chain rings have been studied in [2], [3], [10], [12], [14], [18]. In [11] and [5] the general structural properties of cyclic codes over finite chain rings have been studied. In [17] and [7], cyclic codes over some families of non-chain Frobenius rings were considered.

Constacyclic codes are a generalization of cyclic codes, and similar to cyclic codes, they have been considered over many different rings. We can refer to [1], [4], [9], [12], [13] and [16] for some of these works.

In this work we will first study some general properties of linear codes over the ring $\mathcal{S}_4 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2 \simeq \mathbb{F}_2[u]/(u^4)$. After studying some general properties of the ring, we will study cyclic and constacyclic codes over $\mathcal{S}_4$. In particular we will obtain a substantial number of optimal binary codes as images of cyclic and constacyclic codes over $\mathcal{S}_4$.

The rest of the paper is organized as follows. In section 2, we will consider the general properties of $\mathcal{S}_4$ and we will introduce a Lee weight and Gray map for codes over $\mathcal{S}_4$. In section 3, we will study the MacWilliams identities. We first deduce the MacWilliams identity for the complete weight enumerators, later extending it to the symmetrized weight enumerator and finally obtaining the MacWilliams identity for the Lee weight enumerator. In section 4, we will consider cyclic codes over $\mathcal{S}_4$. Being a finite chain ring and being similar to the ring studied in [18], we will refer to these works for the theoretical aspects of cyclic

2010 *Mathematics Subject Classification*. Primary 94B05, 94B15; Secondary 11T71, 13M99
Keywords. Finite chain rings, cyclic codes, negacyclic codes, constacyclic codes
Received: 23 September 2013; Accepted: 23 February 2014
Communicated by Eberhard Malkowsky
Email addresses: zynp.odemis@gmail.com (Zeynep Ödemiş Özger), umare_algul@hotmail.com (Ümmü Ümare Kara), byildiz@fatih.edu.tr (Bahattin Yıldız)

codes, instead focusing on one-generator cyclic codes over $\mathcal{S}_4$. We will tabulate some numerical results in which we construct many optimal binary codes from cyclic codes over $\mathcal{S}_4$. In section 5, we will look at constacyclic codes over $\mathcal{S}_4$. After giving the general properties, we will focus on $(1+u^2)$-constacyclic codes over $\mathcal{S}_4$. By proving an isomorphism between two quotient rings, we will establish a strong connection between cyclic codes and $(1+u^2)$-constacyclic codes. We will give some numerical results similar to the ones in section 4.

2. Linear Codes over The Ring $\mathcal{S}_4$

Let $\mathcal{S}_4$ be the ring $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$ with $u^4 = 0$, where $\mathbb{F}_2 = \{0,1\} = \mathbb{Z}_2$. $\mathcal{S}_4$ is a commutative finite chain ring of 16 elements.

The group of units of $\mathcal{S}_4$, is given by

$$\begin{aligned}(\mathcal{S}_4)^* &= \left\{1, 1+u, 1+u^2, 1+u^3, 1+u+u^2, 1+u+u^3, 1+u^2+u^3, 1+u+u^2+u^3\right\}.\\ &= \langle 1+u, 1+u^2+u^3\rangle\end{aligned}$$

The non-units are

$$\left\{0, u, u^2, u^3, u+u^2, u+u^3, u^2+u^3, u+u^2+u^3\right\} = \langle u\rangle$$

The ideals of $\mathcal{S}_4$ are (0), (1),(u),(u^2) and (u^3). We have

$$\mathcal{S}_4 \supset u\mathcal{S}_4 \supset u^2\mathcal{S}_4 \supset u^3\mathcal{S}_4 \supset u^4\mathcal{S}_4 = 0.$$

It is also a local ring with the unique maximal ideal $u\mathcal{S}_4$, moreover $\mathcal{S}_4/u\mathcal{S}_4 \cong \mathbb{F}_2$ is the residue field.

Definition 2.1. *A linear code C of length n over the ring $\mathcal{S}_4$ is an $\mathcal{S}_4$-submodule of $\mathcal{S}_4^n$.*

A non-zero linear code C over $\mathcal{S}_4$, has a generator matrix which after a suitable permutation of the coordinates can be written in the form:

$$G = \begin{bmatrix} I_{k_1} & A_1 & A_2 & A_3 & A_4 \\ 0 & uI_{k_2} & uB_1 & uB_2 & uB_3 \\ 0 & 0 & u^2 I_{k_3} & u^2C_1 & u^2C_2 \\ 0 & 0 & 0 & u^3I_{k_4} & u^3D \end{bmatrix},$$

where A_i, B_j, C_k and D are all matrices over $\mathcal{S}_4$. A linear code that has a such generating matrix is said to be of type $(16)^{k_1}(8)^{k_2}(4)^{k_3}(2)^{k_4}$ and consequently has size $2^{4k_1+3k_2+2k_3+k_4}$.

To define the Lee weights and Gray maps for codes over $\mathcal{S}_4$, we will extend the corresponding definitions from the ring $\mathbb{F}_2 + u\mathbb{F}_2$, in [6].

With w_L denoting the Lee weight for $\mathcal{S}_4$ and w_H denoting the Hamming weight, define

$$w_L\left(a + ub + u^2c + u^3d\right) = w_H\left(a+b+c+d, c+d, b+d, d\right) \forall a,b,c,d \in \mathbb{F}_2.$$

The definition of the weight immediately leads to a Gray map from $\mathcal{S}_4$ to $\mathbb{F}_2^4$ which can naturally be extended to $(\mathcal{S}_4)^n$:

$\phi_L : ((\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2)^n$, Lee weight$) \longrightarrow (\mathbb{F}_2^{4n}$, Hamming weight) is defined as:

$\phi_L : ((\bar{a} + u\bar{b} + u^2\bar{c} + u^3\bar{d})) = (\bar{a}+\bar{b}+\bar{c}+\bar{d}, \bar{c}+\bar{d}, \bar{b}+\bar{d}, \bar{d})$, where $\bar{a}, \bar{b}, \bar{c}, \bar{d} \in \mathbb{F}_2^n$.

It is clear that ϕ_L is a linear distance preserving isometry, leading to the following theorem:

Theorem 2.2. *If C is a linear code over $\mathcal{S}_4$ of length n, size 2^k and minimum Lee weight d, then $\phi_L(C)$ is a binary linear code with parameters $[4n, k, d]$.*

3. MacWilliams Identities For Codes Over $\mathcal{S}_4$

We first start by defining the dual of a code C over $\mathcal{S}_4$. Let $\langle .,. \rangle$ denote the usual Euclidean inner product defined on $\mathcal{S}_4$. Then the dual $C^\perp$ of a linear code C of length n over $\mathcal{S}_4$ is defined as

$$C^\perp = \{\overline{x} \in (\mathcal{S}_4)^n \mid \langle \overline{c}, \overline{x} \rangle = 0, \ \forall \overline{c} \in C\}. \tag{1}$$

$C^\perp$ is also a linear code of length n and since $\mathcal{S}_4$, being a finite chain ring, is Frobenius we have, by [15]:

$$|C|.|C^\perp| = 16^n. \tag{2}$$

Now, let $\mathcal{S}_4 = \{g_1, g_2, \ldots, g_{16}\} = \{0, 1, u, u^2, u^3, 1+u, 1+u^2, \ldots, 1+u+u^2+u^3\}$ be a listing of the elements of $\mathcal{S}_4$. Then we can define the complete weight enumerator for a code C over $\mathcal{S}_4$ as follows:

$$cwe_C(X_1, X_2, \ldots, X_{16}) = \sum_{\overline{c} \in C} X_1^{n_{g_1}(\overline{c})} X_2^{n_{g_2}(\overline{c})} \ldots X_{16}^{n_{g_{16}}(\overline{c})}, \tag{3}$$

where $n_{g_i}(\overline{c})$ is the number of appearances of g_i in the vector $\overline{c}$. The complete weight enumerator of a code carries a lot of information about the code, and almost all other weight enumerators can be obtained from the complete weight enumerator.

By [15], we know that MacWilliams identities for the complete weight enumerator of codes over $\mathcal{S}_4$ exist. To find the exact identities, we need a generating character from the additive group of $\mathcal{S}_4$ to the multiplicative group of complex numbers.

Define $\chi : \mathcal{S}_4 \to \mathbb{C}^\times$ as

$$\chi(a + bu + cu^2 + du^3) = (-1)^{w_H(a,b,c,d)}, \tag{4}$$

where w_H is the Hamming weight on binary codes. Because of the well known $w_H(\overline{x} + \overline{y}) = w_H(\overline{x}) + w_H(\overline{y}) - 2w_H(\overline{x} * \overline{y})$ identity on binary vectors, we see that χ is indeed a character. Since it is non-trivial when restricted to any non-trivial ideal of $\mathcal{S}_4$, it is a generating character. Thus we can use χ to obtain the MacWilliams identity for the complete weight enumerator using χ. For that we need to form the following 16×16 matrix T with $T_{i,j} = \chi(g_i g_j)$:

$$T = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 \\
1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \\
1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 \\
1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 \\
1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 & -1 & -1 \\
1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 & 1 \\
1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 \\
1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 & -1 \\
1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 \\
1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 \\
1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 \\
1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 \\
1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\
1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1
\end{bmatrix}.$$

Now, by [15] we have the following theorem:

Theorem 3.1. *Let C be a linear code over $\mathcal{S}_4$ of length n and suppose $C^\perp$ is its dual. Then we have*

$$cwe_{C^\perp}(X_1, X_2, \ldots, X_{16}) = \frac{1}{|C|} cwe_C(T \cdot (X_1, X_2, \ldots, X_{16})^t),$$

where $()^t$ denotes the transpose.

Table 1: The elements of $\mathcal{S}_4$ together with the Lee weights and the corresponding variables

c	$w_L(c)$	the variable in *cwe*
0	0	X_1
1	1	X_2
u	2	X_3
u^2	2	X_4
u^3	4	X_5
$1+u$	1	X_6
$1+u^2$	1	X_7
$1+u^3$	3	X_8
$u+u^2$	2	X_9
$u+u^3$	2	X_{10}
u^2+u^3	2	X_{11}
$1+u+u^2$	3	X_{12}
$1+u+u^3$	3	X_{13}
$1+u^2+u^3$	3	X_{14}
$u+u^2+u^3$	2	X_{15}
$1+u+u^2+u^3$	1	X_{16}

Our goal is to find a MacWilliams identity for the Lee weight enumerators of codes over $\mathcal{S}_4$. To do this, we will identify the elements that have the same weights in the complete weight enumerator to define the symmetrized weight enumerator. Let's recall the elements of $\mathcal{S}_4$ together with the Lee weights and the corresponding variables:

Thus we define the symmetrized weight enumerator in five variables(there are five different weights) as follows:

$$swe_C(W,X,Y,Z,T) = cwe_C(W,X,Y,Y,T,X,X,Z,Y,Y,Y,Z,Z,Z,Y,X). \tag{5}$$

Thus W represents the elements with zero weight, X represents the elements whose Lee weight is 1, etc. Now combining this with Theorem 3.1, we get the following identity for the symmetrized weight enumerator:

$$\begin{aligned} swe_{C^\perp}(W,X,Y,Z,T) \; &= \tfrac{1}{|C|} swe_C(W+4X+6Y+4Z+T, W+2X-2Z-T, \\ &W-2Y+T, W-2X+2Z-T, W-4X+6Y-4Z+T). \end{aligned} \tag{6}$$

Define the Lee weight enumerator of a code over $\mathcal{S}_4$:

Definition 3.2. *Let C be a linear code over $\mathcal{S}_4$ of length n. The Lee weight enumerator of C is given by*

$$Lee_C(W,X) = \sum_{\overline{c}\in C} W^{4n-w_L(\overline{c})} X^{w_L(\overline{c})}. \tag{7}$$

Considering the weights that the variables W,X,Y,Z,T of the symmetrized weight enumerator represent, we get the following identity:

$$Lee_C(W,X) = swe_C(W^4, W^3X, W^2X^2, WX^3, X^4). \tag{8}$$

Now combining this with 6 we get the following theorem:

Theorem 3.3. *Let C be a linear code over $\mathcal{S}_4$ of length n and $C^\perp$ be its dual. With $Lee_C(W,X)$ denoting its Lee weight enumerator as was given in (7), we have*

$$Lee_{C^\perp}(W,X) = \frac{1}{|C|} Lee_C(W+X, W-X).$$

Proof. The proof follows from observing

$$W^4 + 4W^3X + 6W^2X^2 + 4WX^3 + X^4 = (W + X)^4,$$
$$W^4 + 2W^3X - 2WX^3 - X^4 = (W + X)^3(W - X),$$
$$W^4 - 2W^2X^2 + X^4 = (W + X)^2(W - X)^2,$$
$$W^4 - 2W^3X + 2WX^3 - X^4 = (W + X)(W - X)^3,$$
$$W^4 - 4W^3X + 6W^2X^2 - 4WX^3 + X^4 = (W - X)^4.$$

□

4. One-generator Cyclic Codes Over $\mathcal{S}_4$

Cyclic codes are an important class of codes because of their algebraic structure, which makes them easier to study. Many important codes are of this family. Cyclic codes over rings have been studied recently in many different directions. Cyclic codes over the rings $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ have been studied in [2], [3], [13] and [12]. More generally the structure of cyclic codes over finite chain rings was studied in [5]. Recently Yildiz and Siap studied cyclic codes over the ring $\mathbb{F}_2[u]/(u^4 - 1)$ in connection with DNA-cyclic codes in [18]. The ring $\mathcal{S}_4$ being isomorphic to $\mathbb{F}_2[u]/(u^4 - 1)$, in studying cyclic codes over $\mathcal{S}_4$, for most of the theoretical parts, we will refer to [5] and [18]. In [18], the Lee weight and the Gray map were not defined for $\mathbb{F}_2[u]/(u^4 - 1)$, hence cyclic codes were considered according to the Hamming weight. However, in this section we will consider cyclic codes over $\mathcal{S}_4$ with respect to the Lee weight and the Gray map.

Definition 4.1. *A linear code C of length n over $\mathcal{S}_4$ is cyclic if and only if for any $\bar{c} = (c_0, c_1, \ldots, c_{n-1}) \in C$, we have $\tau(\bar{c}) = (c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$.*

Identifying codewords $(c_0, c_1, \ldots, c_{n-1})$ with polynomials $c_0 + c_1x + \cdots + c_{n-1}x^{n-1} \in \mathcal{S}_4[x]$ we easily see that

Lemma 4.2. *A code C of length n is cyclic if and only if its polynomial representation is an ideal in the ring $\mathcal{S}_4[x]/(x^n - 1)$.*

Thus, to study cyclic codes over $\mathcal{S}_4$, it is necessary to understand the structure of $\mathcal{S}_4[x]/(x^n - 1)$. Now, since $\mathcal{S}_4$ is a finite chain ring, we have the following theorem by [5]:

Theorem 4.3. *Suppose n is odd. Then every ideal in the ring $\mathcal{S}_4[x]/(x^n - 1)$ is principal.*

Thus any cyclic code over $\mathcal{S}_4$ of odd length is principally generated by a generator of the form $g(x)$ where $g(x)|x^n - 1$. This result is not true in general for even lengths.

We are interested in one-generator cyclic codes, i.e. cyclic codes C of the form $C = \langle g(x) \rangle$. Our goal is to construct such cyclic codes of certain lengths and look at their binary images under the Gray map. We will tabulate our results at the end. However, we would like to avoid the cases when $\langle g(x) \rangle$ generates the trivial cyclic code $((\mathcal{S}_4)^n)$. For that we have the following lemma, which can easily be extended from [7] and [17]:

Lemma 4.4. *Let μ be the map $\mu : \mathcal{S}_4 \to \mathbb{F}_2$ such that*

$$\mu(a + bu + cu^2 + du^3) = a.$$

Let $g(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in \mathcal{S}_4[x]/(x^n - 1)$. Then $C = \langle g(x) \rangle$ is a non-trivial cyclic code if and only if

$$GCD(\mu(g(x)), x^n - 1) \neq 1.$$

In what follows, we look at one-generator cyclic codes over $\mathcal{S}_4$ of lengths 2 through 8 and their Gray images. We tabulate these results for each length, where we give the generator polynomial and the parameters of the binary image. The codes with * next to them indicate that they are optimal according to [8]:

Table 2: Some cyclic codes of length 2 and the binary images

$g(x)$	$\phi_L(\langle g(x)\rangle)$
$u+ux$	$[8,3,4]^*$
$1+u^2+u^3+(1+u^2)x$	$[8,4,4]^*$
$1+u^2+u^3+(1+u+u^3)x$	$[8,6,2]^*$

Table 3: Some cyclic codes of length 3 and the binary images

$g(x)$	$\phi_L(\langle g(x)\rangle)$
$u^3+u^3x+u^3x^2$	$[12,1,12]^*$
u^3+u^3x	$[12,2,8]^*$
$u+ux+ux^2$	$[12,3,6]^*$
$u^3+u^2x+u^2x^2$	$[12,5,4]^*$
$u+ux$	$[12,6,4]^*$
$u^3+ux+ux^2$	$[12,7,4]^*$
$1+u+u^2+(1+u^2)x+(u+u^2)x^2$	$[12,9,2]^*$
$1+u+u^2+u^3+ux+(1+u+u^2)x^2$	$[12,11,2]^*$

Table 4: Some cyclic codes of length 4 and the binary images

$g(x)$	$\phi_L(\langle g(x)\rangle)$
$u^3+u^3x+u^3x^2+u^3x^3$	$[16,1,16]^*$
u^3+u^3x	$[16,3,8]^*$
$1+u+u^2+u^3+(1+u+u^3)x+(1+u+u^2+u^3)x^2+(1+u+u^3)x^3$	$[16,4,8]^*$
$1+u+u^2+u^3+(1+u^3)x+(1+u+u^3)x^2+(1+u^2)x^3$	$[16,5,8]^*$
$1+u+u^3+(1+u+u^3)x+(1+u+u^2+u^3)x^2+(1+u+u^2)x^3$	$[16,6,6]^*$
$u^2+u^3+u^2x+(u+u^3)x^2$	$[16,8,4]^*$
$1+u+(1+u^2+u^3)x+(1+u^3)x^2+(1+u+u^2+u^3)x^3$	$[16,9,4]^*$
$u+(1+u+u^2)x^2+(1+u^3)x^3$	$[16,12,2]^*$

Table 5: Some cyclic codes of length 5 and the binary images

$g(x)$	$\phi_L(\langle g(x)\rangle)$
$u^3+u^3x+u^3x^2+u^3x^3+u^3x^4$	$[20,1,20]^*$
$u^2+u^3+u^3x+(u+u^2+u^3)x^2+(u+u^2)x^3+(u^2+u^3)x^2$	$[20,12,4]^*$
$u^3+(u+u^3)x+(u+u^2+u^3)x^2+u^3x^3+(u^2+u^3)x^4$	$[20,13,4]^*$
$u^3+(1+u)x+(u+u^2+u^3)x^2+u^3x^3+(1+u^2)x^4$	$[20,17,2]^*$
$1+(u+u^3)x+(u^2+u^3)x^2+(1+u+u^3)x^4$	$[20,18,2]^*$
$1+u+u^2x+(1+u+u^3)x^3+(u+u^2+u^3)x^4$	$[20,19,2]^*$

Table 6: Some cyclic codes of length 6 and the binary images

$g(x)$	$\phi_L(\langle g(x)\rangle)$
$u^3 + u^3x + u^2x^2 + u^2x^3 + u^2x^4$	$[24, 8, 6]$
$1+u^3+(1+u+u^2)x+u^2x^2+(1+u+u^2)x^3+(1+u^2+u^3)x^4+ux^5$	$[24, 14, 4]$
$u^3+(1+u^2+u^3)x+x^2+(u^2+u^3)x^3+(1+u+u^2)x^4+(1+u+u^2)x^5$	$[24, 15, 4]$*
$1 + u + u^3 + (1 + u^2 + u^3)x + (1 + u + u^2 + u^3)x^2 + (1 + u^2 + u^3)x^3 + x^4 + (1 + u^2 + u^3)x^5$	$[24, 16, 4]$*
$1 + u + u^3 + (1 + u + u^3)x + ux^2 + (u + u^2)x^4 + (1 + u^2)x^5$	$[24, 20, 2]$*

Table 7: Some cyclic codes of length 7 and the binary images

$g(x)$	$\phi_L(\langle g(x)\rangle)$
$u+u^2+(u+u^3)x+u^2x^2+(u^2+u^3)x^3+(u+u^2)x^4+u^3x^5+u^2x^6$	$[28, 12, 8]$*
$1+u+u^3+u^2x+(1+u+u^2)x^3+(1+u)x^4+(1+u+u^3)x^5+(u^2+u^3)x^6$	$[28, 15, 4]$
$1 + u^3 + (1 + u + u^3)x + (1 + u + u^2)x^2 + (1 + u^2 + u^3)x^3 + (1 + u^2 + u^3)x^4 + x^5 + (1 + u + u^2 + u^3)x^6$	$[28, 16, 4]$
$1+u+ux+(1+u^3)x^2+(u+u^2+u^3)x^3+(1+u^3)x^5+(1+u+u^2+u^3)x^6$	$[28, 18, 4]$
$1 + u^2 + (1 + u + u^3)x + u^3x^2 + (u^2 + u^3)x^3 + (1 + u)x^4 + ux^5 + (1 + u + u^3)x^6$	$[28, 21, 4]$*
$u^2 + u^3 + (1 + u + u^2)x + (1 + u + u^3)x^2 + (1 + u)x^3 + (u + u^2 + u^3)x^5 + (1 + u^2)x^6$	$[28, 22, 2]$
$u^2 + (u + u^2)x + (1 + u + u^2 + u^3)x^2 + x^3 + (1 + u + u^2 + u^3)x^4 + (1 + u + u^3)x^5 + u^3x^6$	$[28, 24, 2]$*
$1 + u^3 + (1 + u^2 + u^3)x + u^2x^2 + (u + u^2)x^3 + (u + u^2)x^4 + (1 + u^2 + u^3)x^5 + (u^2 + u^3)x^6$	$[28, 25, 2]$*
$(1 + u^3)x + u^3x^2 + (u + u^3)x^4 + (1 + u^2)x^5 + (u + u^3)x^6$	$[28, 26, 2]$*
$u^2 + u^3x + (u^2 + u^3)x^2 + x^3 + u^3x^4 + (u^2 + u^3)x^5 + (1 + u)x^6$	$[28, 27, 2]$*

Remark 4.5. *The ^{b} in Table 8 indicates that the code with those parameters is the best known.*

Remark 4.6. *Because ϕ_L takes $\mathcal{S}_4$ to $\mathbb{F}_2^4$, it is easy to show that the binary images of cyclic codes over $\mathcal{S}_4$ are 4-quasicyclic binary codes. Thus all the binary codes found in the above tables are 4-quasicyclic.*

5. $(1 + u^2)$-Constacyclic Codes Over $\mathcal{S}_4$ of odd length

Constacyclic codes are a generalization of cyclic codes. The following is a standard definition of a constacyclic code over any ring R:

Definition 5.1. *Let γ be a unit in the ring R. Then a linear code C over R is said to be a γ-constacylic code if and only if for any $(c_0, c_1, \ldots, c_{n-1}) \in C$, we have $(\gamma c_{n-1}, c_0, \ldots, c_{n-1}) \in C$.*

Table 8: Some cyclic codes of length 8 and the binary images

$g(x)$	$\phi_L(\langle g(x)\rangle)$
$1 + u^3 + (1 + u^2 + u^3)x + u^3x^3 + (1 + u^2)x^4 + x^5$	$[32, 14, 8]^b$
$u + ux + (1 + u^2 + u^3)x^2 + (u + u^2)x^3 + u^2x^4 + (u^2 + u^3)x^5 + (1 + u + u^2)x^6 + u^2x^7$	$[32, 16, 8]$*
$1 + u + (1 + u + u^3)x + (1 + u^2)x^2 + (u + u^2)x^3 + (u + u^3)x^4 + (u + u^2)x^6 + (1 + u + u^3)x^7$	$[32, 24, 4]$*
$1 + u + u^2 + (u + u^3)x + u^2x^2 + (1 + u)x^4 + (u + u^3)x^5 + (1 + u^2 + u^3)x^6 + (1 + u^2)x^7$	$[32, 28, 2]$*

When $\gamma = 1$, we get the ordinary cyclic codes. In the same way as for cyclic codes, when we identify codewords $(c_0, c_1, \ldots, c_{n-1})$ with polynomials $c_0 + c_1x + \cdots + c_{n-1}x^{n-1} \in R[x]$, the γ-constacyclic shift corresponds to multiplying the polynomial by x in the quotient ring $R[x]/(x^n - \gamma)$. Thus in our case we see that

Lemma 5.2. *Let $\gamma \in \mathcal{S}_4$ be a unit. Then a linear code C of length n over $\mathcal{S}_4$ is γ-constacylic if and only if the corresponding polynomial set is an ideal in $\mathcal{S}_4[x]/(x^n - \gamma)$.*

In [1], constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$ were studied in a general setting while in [13] $(1+u)$-constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$ were considered. [16], [9], [12] and [4] are some other examples of works on constacyclic codes over different rings. In this section we will focus on $(1+u^2)$-constacyclic codes over $\mathcal{S}_4$ of odd length. There are a few reasons for our choice of $1+u^2$. First of all $(1+u^2)^k$ is 1 if k is even and it is $1+u^2$ if k is odd. Also

$$\phi_L((1+u^2)(a+bu+cu^2+du^3)) = (c+d, a+b+c+d, d, b+d),$$

which is permutation equivalent to $\phi_L(a+bu+cu^2+du^3)$. This means that multiplying any coordinate of a codeword by $(1+u^2)$ does not affect the weight. Another important reason will be the following isomorphism which will reduce studying $(1+u^2)$-constacyclic codes over $\mathcal{S}_4$ to studying cyclic codes:

Theorem 5.3. *Let $\psi : \mathcal{S}_4[x]/(x^n-1) \to \mathcal{S}_4[x]/(x^n-(1+u^2))$ be defined as $\psi(c(x)) = c((1+u^2)x)$. If n is odd, then ψ is a ring isomorphism from $\mathcal{S}_4[x]/(x^n-1)$ to $\mathcal{S}_4[x]/(x^n-(1+u^2))$.*

Proof. Clearly ψ is a ring homomorphism. To complete the proof, we need to show that ψ is bijective. We just saw above that $(1+u^2)^k$ is $(1+u^2)$ if k is odd and 1 otherwise. Thus, since n is odd, we see that $(1+u^2)^n = 1+u^2$. Now, suppose $a(x) \equiv b(x) \pmod{x^n-1}$, i.e., $a(x)-b(x) = (x^n-1)q(x)$ for some $q(x) \in \mathcal{S}_4[x]$. Then $a((1+u^2)x) - b((1+u^2)x) = ((1+u^2)^n x^n - 1)q((1+u^2)x) = ((1+u^2)x^n - (1+u^2)^2)q((1+u^2)x) = (1+u^2)(x^n-(1+u^2))q((1+u^2)x)$, which means if $a(x) = b(x) \pmod{x^n-1}$, then $a((1+u^2)x) = b((1+u^2)x) \pmod{x^n-(1+u^2)}$. But the converse can easily be shown as well which means $a(x) = b(x) \pmod{x^n-1} \Leftrightarrow a((1+u^2)x) = b((1+u^2)x) \pmod{x^n-(1+u^2)}$. Note that the $\Rightarrow$ of the above equivalence shows that ψ is well defined and the $\Leftarrow$ shows that it is injective. But since the rings are finite this proves that ψ is an isomorphism. □

The following are natural consequences of the previous theorem:

Corollary 5.4. *I is an ideal of $\mathcal{S}_4[x]/(x^n-1)$ if and only $\psi(I)$ is an ideal of $\mathcal{S}_4[x]/(x^n-(1+u^2))$ when n is odd.*

Corollary 5.5. *Let $\overline{\psi}$ be the map that acts on $\mathcal{S}_4^n$ with odd length n as follows:*

$$\overline{\psi}(c_0, c_1, \cdots, c_{n-1}) = (c_0, (1+u^2)c_1, (1+u^2)^2c_2, \cdots, (1+u^2)^{n-1}c_{n-1})$$

Then C is a linear cyclic code over $\mathcal{S}_4$ of odd length n if and only if $\overline{\psi}(C)$ is a linear $(1+u^2)$-constacylic code of length n over $\mathcal{S}_4$.

Corollary 5.6. *C is a cyclic code over $\mathcal{S}_4$ of parameters $[n, 2^k, d]$ if and only if $\overline{\psi}(C)$ is a $(1+u^2)$-constacyclic code over $\mathcal{S}_4$ of parameters $[n, 2^k, d]$, where n is odd.*

So now, in the light of above corollaries, we refer to the results obtained in the previous section about cyclic codes and by modifying the generators by ψ in the way described above, we get the following tables for $(1+u^2)$-constacyclic codes of odd lengths over $\mathcal{S}_4$. Again, the ones marked by * denote the optimal ones by [8]:

Table 9: Some $(1+u^2)$-constacyclic codes of length 3 and the binary images

$g(x)$	$\phi_L(\langle g(x)\rangle)$
$u^3+u^3x+u^3x^2$	$[12,1,12]^*$
u^3+u^3x	$[12,2,8]^*$
$u+(u+u^3)x+ux^2$	$[12,3,6]^*$
$u^3+u^2x+u^2x^2$	$[12,5,4]^*$
$u+(u+u^3)x$	$[12,6,4]^*$
$u^3+(u+u^3)x+ux^2$	$[12,7,4]^*$
$1+u+u^2+x+(u+u^2)x^2$	$[12,9,2]^*$
$1+u+u^2+u^3+(u+u^3)x+(1+u+u^2)x^2$	$[12,11,2]^*$

Table 10: Some $(1+u^2)$-constacyclic codes of length 5 and the binary images

$g(x)$	$\phi_L(\langle g(x)\rangle)$
$u^3+u^3x+u^3x^2+u^3x^3+u^3x^4$	$[20,1,20]^*$
$u^2+u^3+u^3x+(u+u^2+u^3)x^2+(u+u^2+u^3)x^3+(u^2+u^3)x^2$	$[20,12,4]^*$
$u^3+ux+(u+u^2+u^3)x^2+u^3x^3+(u^2+u^3)x^4$	$[20,13,4]^*$
$u^3+(1+u+u^2+u^3)x+(u+u^2+u^3)x^2+u^3x^3+(1+u^2)x^4$	$[20,17,2]^*$
$1+ux+(u^2+u^3)x^2+(1+u+u^3)x^4$	$[20,18,2]^*$
$1+u+u^2x+(1+u+u^2)x^3+(u+u^2+u^3)x^4$	$[20,19,2]^*$

Table 11: Some $(1+u^2)$-constacyclic codes of length 7 and the binary images

$g(x)$	$\phi_L(\langle g(x)\rangle)$
$u+u^2+ux+u^2x^2+(u^2+u^3)x^3+(u+u^2)x^4+u^3x^5+u^2x^6$	$[28,12,8]^*$
$1+u+u^3+u^2x+(1+u+u^3)x^3+(1+u)x^4+(1+u+u^2)x^5+(u^2+u^3)x^6$	$[28,15,4]$
$1+u^3+(1+u+u^2)x+(1+u+u^2)x^2+(1+u^3)x^3+(1+u^2+u^3)x^4+(1+u^2)x^5+(1+u+u^2+u^3)x^6$	$[28,16,4]$
$1+u+(u+u^3)x+(1+u^3)x^2+(u+u^3)x^3+(1+u^2+u^3)x^5+(1+u+u^2+u^3)x^6$	$[28,18,4]$
$1+u^2+(1+u+u^2)x+u^3x^2+(u^2+u^3)x^3+(1+u)x^4+(u+u^3)x^5+(1+u+u^3)x^6$	$[28,21,4]^*$
$u^2+u^3+(1+u+u^3)x+(1+u+u^3)x^2+(1+u+u^2+u^3)x^3+(u+u^2+u^3)x^5+(1+u^2)x^6$	$[28,22,2]$
$u^2+(u+u^2+u^3)x+(1+u+u^2+u^3)x^2+(1+u^2)x^3+(1+u+u^2+u^3)x^4+(1+u+u^2)x^5+u^3x^6$	$[28,24,2]^*$
$1+u^3+(1+u^3)x+u^2x^2+(u+u^2+u^3)x^3+(u+u^2)x^4+(1+u^3)x^5+(u^2+u^3)x^6$	$[28,25,2]^*$
$(1+u^2+u^3)x+u^3x^2+(u+u^3)x^4+x^5+(u+u^3)x^6$	$[28,26,2]^*$
$u^2+u^3x+(u^2+u^3)x^2+(1+u^2)x^3+u^3x^4+(u^2+u^3)x^5+(1+u)x^6$	$[28,27,2]^*$

References

[1] T. Abualrub, İ. Şiap, Constacylic codes over $\mathbb{F}_2 + u\mathbb{F}_2$, J. Frank. Inst. 346 (2009) 520–529.
[2] T. Abualrub, İ. Şiap, Cyclic codes over the rings $\mathbb{Z}_2 + u\mathbb{Z}_2$ and $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$, Des. Codes Crypt. 42 (2007) 273–287.
[3] A. Bonnecaze, P. Udaya, Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inform. Theory 45 (1999) 1250–1255.
[4] H. Q. Dinh, Constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, J. Algebra 324 (2010) 940–950.
[5] H. Q. Dinh, S. Lopez-Permóuth, Cyclic and negacyclic codes over finite chain rings, IEEE Trans. Inform. Theory 50 (2004) 1728–1744.
[6] S. T. Dougherty, P. Gaborit, M. Harada, P. Solé, Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inform. Theory, 45 (1999) 32–45.
[7] S. T. Dougherty, S. Karadeniz, B. Yıldız, Cyclic codes over R_k, Des. Codes and Crypt. 63 (2012) 113–126.
[8] M. Grassl, Bounds on the minimum distance of linear codes and quantum codes, online available at **www.codetables.de**.
[9] X. Kai, S. Zhu, P. Li,$(1 + \lambda u)$ -constacyclic codes over $\mathbb{F}_p [u] / (u^m)$, J. Frank. Inst. 347 7 (2010) 51–762.
[10] P. Konmar, S. K. Lopez-Permouth, Cyclic codes over integers modulo p^m, Finite Fields and Applications 3 (2007) 334–352.
[11] G. H. Norton, A. Sălăgean, On the structure of linear and cyclic codes over a finite chain ring, Appl. Alg. Engrg. Comm. & Comput. 10 (2000) 489–506.
[12] J. Qian, L. Zhang, S. X. Zhu, Constacyclic and cyclic odes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$, IEICE Transactions on Fundamental of Electronics and Computer Sciences Archive. E89-A (2006) 1863–1885.
[13] J. F. Qian, L. N. Zhang, S. X. Zhu, $(1 + u)$-constacyclic and cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$, Applied Math. Letters 19 (2006) 820–823.
[14] J. Wolfmann, Negacyclic and cyclic codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory 45 (1999) 2527–2532.
[15] J. Wood, Duality for modules over finite rings and applications to coding theory, Amer. J. Math. 121 (1999) 555–575.
[16] B. Yıldız, S. Karadeniz, $(1 + v)$-constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, J. Frank. Inst. 347 (2010) 1888–1894.
[17] B. Yıldız, S. Karadeniz, Cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, Des. Codes Crypt. 58 (2011) 221–234.
[18] B. Yıldız, İ. Şiap, Cyclic codes over $\mathbb{F}_2 [u] / (u^4 - 1)$ and applications to DNA codes, Comput. Math Appl. 63 (2012) 1169–1176.