Al-Aqsa University Journal (Natural Sciences Series),Vol.15, No.1, Pages 1-17, Jan. 2011
ISSN 2070-3155

Constacyclic codes of even length over $F_2 + uF_2 + u^2F_2$

د. محمد الأشقر*

أ. محمد حمودة *

الملخص

قمنا في هذا البحث بدراسة بنية وتركيب التراميز الدورية الثابتة ذات الطول الزوجي (n) على الحلقة $F_2 + uF_2 + u^2F_2$ حيث أن $u^3 = 0 \bmod 2$.

وقد أوجدنا مجموعة المولدات لكل $(1-u^2)$ترميز دوري و كذلك تراميز الازدواج الزوجي لها ، كما درسنا تراميز الازدواج الزوجي وأوجدنا المجموعات المولدة الدنيا لها.

لقد أثبتنا أن صورة الاقتران "جراي" للـ $(1-u^2)$ ترميز دوري يكون ترميز دوري ثنائي له الطول $(4n)$.

في هذا العمل عممنا النتائج الأساسية للمرجع (2) إلى الحلقة $F_2 + uF_2 + u^2F_2$ حيث أن $u^3 = 0 \bmod 2$

وكذلك دراسة أمثلة لتراميز دورية $(1-u^2)$ ذات الطول الزوجي n .

ABSTRACT

In this paper, we study the structure of constacyclic codes of even length n over the ring $F_2 + uF_2 + u^2F_2$, with $u^3 = 0 \bmod 2$. We find a set of generators for each $(1-u^2)$ -cyclic code and its dual. We study the dual of cyclic codes and find their minimal spanning sets. We prove that the Gray image of a $(1-u^2)$ –cyclic code is a binary cyclic code of length $4n$. In this work, we generalize the main results of [2] to the ring $F_2 + uF_2 + u^2F_2$, with $u^3 = 0 \bmod 2$.

Examples of $(1-u^2)$ -cyclic codes of even lengths are also studied.

AMS: Subject Classification 2000: 94B15

Keywords: $(1-u^2)$ -cyclic codes, Codes over rings, Gray map.

* قسم الرياضيات – الجامعة الإسلامية– غزة - فلسطين.

1 Introduction

Codes over finite rings have been studied in the early 1970. A great deal of attention has been given to codes over finite rings from 1990, because of their new role in algebraic coding theory and their successful application. The structure of cyclic codes over rings of odd length n has been discussed in Bonnecaze and Udaya [4], Conway and Sloen [5], and Grasst[6]. Wolmann[10], and other papers [8], [9] presented a complete structure of cyclic codes over Z_4 of odd length. A calderbank paper [7] has shown that certain nonlinear binary codes with excellent error-correcting capabilities can be identified as images of linear codes over Z_4 under the Gray map. Meanwhile, codes over finite rings can be used to design error-correcting coding schemes for wireless communication systems. Let S be the ring $F_2 + uF_2 + u^2F_2 = \{0,1,u,1+u,u^2,1+u+u^2,u+u^2\}$ where $u^3 = 0$ mod 2.

Notation:(1) We write a for $a(x)$ and $(a)_2$ represents a binary cyclic codes in $F_2[x]$ with generator a.

(2) By a $(1-u^2)$ −cyclic code of length n over the ring S, we mean constacyclic code of length n over the ring S.

In [1], Abualrub and Siap studied cyclic codes of an arbitrary length n over the ring $F_2 + uF_2 = \{0,1,u,u+1\}$ where $u^2 = 0$ mod 2 and over $F_2 + uF_2 + u^2F_2 = \{0,1,u,1+u,u^2,1+u+u^2,u+u^2\}$ where $u^3 = 0$ mod 2.

Furthermore, In [2] they studied constacyclic codes of even length over $F_2 + uF_2$. They showed that the Gray image of a $(1+u)$-cyclic code is a binary cyclic code of length *2n*. In this paper we study $(1-u^2)$-cyclic codes of even length n over S. We give a unique set of generators for these codes and their duals as ideals in the ring $S_n = S[x]/\langle x^n - (1-u^2)\rangle$, where $1-u^2$ is a unit in S. Also we study the rank of these codes and give a minimal generating set for them. We further show that the Gray map of a $(1-u^2)$ −cyclic code of length n is a binary cyclic code of length $4n$.

The remaining part of this paper is organized as follows:

In section 2, we give some basic definitions and results that are used in the sequel of this paper. In section 3, we study $(1-u^2)$ –cyclic codes of even length n over S. We find a unique set of generators for these codes. In section 4, we study the dual of these codes. We also find minimal spanning sets for these codes.
In section 5, we study the Gray map of a linear $(1-u^2)$ –cyclic code. We show that the Gray image of constacyclic codes of even length n over S is a binary cyclic code of length $4n$. In section 6, we include some examples of constacyclic codes over S and their Gray image binary codes.

2 Preliminaries

Consider the ring $S = F_2 + uF_2 + u^2F_2 = \{0,1,u,1+u,u^2,1+u+u^2,u+u^2\}$ where $u^3 = 0$ mod 2.

A linear code C of length n over S is defined to be an additive submodule of the S-module S^n.

A free module C is a module with a basis (a linearly independent spanning set for C). A

linear code of length n over S is cyclic if it is invariant under the automorphism σ which is

$\sigma(c_0, c_1, \ldots, c_{n-1}) = (c_{n-1}, c_0 \ \ldots, c_{n-2})$.

A linear code of length *n* is a $(1-u^2)$ –cyclic if it is invariant under the automorphism v which is given by

$v(c_0, c_1, \ldots, c_{n-1}) = \big((1-u^2)c_{n-1}, c_0 \ \ldots, c_{n-2}\big)$,

where $1-u^2$ is a unit in S. A subset C of S^n is a linear cyclic code if its polynomial

representation is an ideal in $T_n = S[x]/\langle x^n - 1\rangle$.

A subset *C* of S^n is a linear $(1-u^2)$ –cyclic code if its polynomial representation

is an ideal in $S_n = S[x]/\langle x^n - (1-u^2)\rangle$.

The Hamming weight of a codeword c is defined by $\omega_H(c) = |\{i : c_i \neq 0\}|$, i.e the number of the nonzero entries of c. The minimum Hamming weight $d_H(C)$ of a linear code C is given by

$d_H(C) = min\{\omega_H(c) : c \in C \text{ and } c \neq 0\}$.

Let $c = (c_0, \ldots, c_{n-1})$ and $u = (u_0, \ldots, u_{n-1})$ be any two vectors over a ring. We define their inner product by

$c.u = c_0u_0 + \ldots + c_{n-1}u_{n-1}$.

If $c.u = 0$, then c and u are said to be orthogonal. We define the dual of a cyclic code C to be the set

$C^{\perp} = \{c \in S : c.u = 0 \text{ for all } u \in C\}$.

It is clear that $C^{\perp}$ is also a cyclic code. For a linear code C over S, we have $|C||C^{\perp}| = 8^n$.

Definition 2.1. [2] Let I be an ideal in S_n. We define

$A(I) = \{g(x) : f(x)g(x) = 0 \text{ for all } f(x) \in I\}$.

The set $A(I)$ is called the annihilators of I in S_n.

Definition 2.2. [2] If $f(x) = a_0 + a_1x + \ldots + a_rx^r$ is a polynomial of degree r then the reciprocal of $f(x)$ is the polynomial $f^*(x) = a_r + a_{r-1}x + \ldots + a_0x^r$ is. Symbolically, $f^*(x)$ can be expressed by $f^*(x) = x^r f\left(\frac{1}{x}\right)$.

It is obvious that if C is a cyclic code with associated ideal I then the associated ideal *of* $C^{\perp}$ *is* $A(I)^* = \{f^*(x) : f(x) \in A(I)\}$.

Definition 2.3. [3] Let $S = F_2 + uF_2 + u^2F_2 = \{0,1,u,1+u,u^2,1+u+u^2,u+u^2\}$where $u^3 = 0 \mod 2$. We define the Generalized Lee weight of any non zero element t in S by

$$wt_{GL}(t) = \begin{cases} 2, & \text{if } t = u^2 \\ 1, & \text{if } t \neq u^2 \end{cases}$$

and the Generalized Lee weight of 0 is 0.

Further the Generalized Lee weight of any non zero $n-$tuple in S^n is the sum of Generalized Lee weights of its components.

Example 2.1. *Let* $n = 8, x = (1,0,u^2,1+u,1,u+u^2,u^2,0) \in S^8$.

$\Rightarrow wt_{GL}(x) = 16$.

Definition 2.4. [3] The Generalized Lee distance between x and $y \in R^n$ is defined by $d_{GL}(x,y) = wt_{GL}(x-y)$.

Example 2.2. *Let* $x = (0,u,1+u,u^2)$ *and* $y = (0,1,u,0)$ *be two vectors in* $S^4 \Rightarrow d_{GL}(x,y) = wt_{GL}(x-y) = wt_{GL}(0,1+u,1,u^2) = 8$.

Following Abualrub and Siap [1, p.p. 274], the parameters of an $S-$ code C with $8^{k1}4^{k2}2^{k3}$ code words, where k_1 refers to the free part and k_2, k_3 refere to non free part (u and u^2 multiple generators of C), and minimum distance d is denoted by $(n, 8^{k1}4^{k2}2^{k3}, d)$. Such codes are often referred to as a code of type $\{k_1, k_2, k_3\}$.

We define the rank of a code C over S of type $\{k_1, k_2, k_3\}$, denoted by rank (C), by the minimum number of generators of C, and define the free rank of C, denoted by f-rank(C), by the maximum of the ranks of S- free submodules of C. A code C of type $\{k_1, k_2, k_3\}$ has a rank $(k_1 + k_2 + k_3)$and a f-rank k_1.

3 Classification of $(1-u^2)$ –cyclic codes

Following the results in [1], let $R = F_2 + uF_2 = \{0,1,u,1+u\}$ with $u^2 = 0$ mod 2, and $S = F_2 + uF_2 + u^2F_2$with $u^3 = 0$ mod 2. Let C be a constacyclic code in $S_n = S[x]/\langle x^n - (1-u^2)\rangle$. Define $\Psi_1 : S \to R$ by $\Psi_1(a) = a$, Ψ_1 is a ring homomorphism that can be extended to a homomorphism $\Phi : C \to R_n = R[x]/\langle x^n - (1+u)\rangle$ defined by

$\Phi(c_0 + c_1x + \ldots + c_{n-1}x^{n-1}) -$

$\Psi_1(C_0) + \Psi_1(C_1)x + \ldots + \Psi_1(C_{n-1})x^{n-1}$

Ker$\Phi = \{u^2r(x) : r(x) \in Z_2[x]\}$. Let

$J = \{r(x) : u^2r(x) \in \ker \Phi\} \Rightarrow J$ is an ideal in $Z_2[x]/\langle x^n - 1\rangle$ and hence a cyclic code in $Z_2[x]/\langle x^n - 1\rangle$. So $J = \langle a_2(x)\rangle$ and $\ker \Phi = \langle u^2a_2(x)\rangle$ with $a_2(x) | (x^n - 1)$ mod 2. In order to determine the generators of a cyclic code in S_n, we need to know the image Φ which is a constacyclic code in R_n. Let D be a constacyclic code in R_n as above, we define $\Psi_2: R \to Z_2$ by $\Psi_2(a) = a^2 mod 2$. Ψ_2 is a ring homomorphism because $(a+b)^2 = a^2 + b^2$ in R and in $Z_2 = \{0,1\}$. Extend Ψ_2 to a homomorphism $\varphi : D \to Z_2[x]/\langle x^n - 1\rangle$ defined by

$\varphi(c_0 + c_1x + \ldots + c_{n-1}x^{n-1}) =$
$\Psi_2(c_0) + \Psi_2(c_1)\,x + \ldots + \Psi_2(c_{n-1})\,x^{n-1} = c_0^2 + c_1^2x + \ldots + c_{n-1}^2x^{n-1}$ mod 2. Ker $\varphi = \{ur(x) : r(x)\ is\ a\ binary\ polynomial\ in\ Z_2[x]/\langle x^n - 1\rangle\} = \langle ua_1(x)\rangle$
with $a_1(x) | (x^n - 1)$ mod 2.

The image of φ is also an ideal and hence a binary cyclic code generated by $g(x)$ with $g(x) | (x^n - 1)$. So, $C = \langle g(x) + up(x), ua_1(x)\rangle$ for some binary polynomial $p(x)$. Note that $a_1 | \left(p\frac{x^n-1}{g}\right)$ because $\varphi\left(\frac{x^n-1}{g}[g + up]\right) = \varphi\left(up\frac{x^n-1}{g}\right) = 0$ which implies $\left(up\frac{x^n-1}{g}\right) \in ker\varphi = \langle ua_1\rangle$. Also $ug \in ker\varphi$ implies $a_1(x) | g(x)$. Now the image of Φ is an ideal in R_n, then $Im(\Phi) = \langle g(x) + up_1(x), ua_1(x)\rangle$ with $a_1(x) | g(x) | (x^n - 1)$ and $a_1(x) | p_1(x)\left(\frac{x^n-1}{g}\right)$.

Also $ker\Phi = \langle u^2a_2(x)\rangle$ with $a_2(x) | (x^n - 1)$ mod 2. Since $u^2a_1 \in ker\Phi = \langle u^2a_2\rangle$, then we get the following lemma.

Lemma3.1.
$[1] If\ C = \langle g(x) + up(x), ua(x)\rangle\ is\ a\ linear - cyclic\ code\ in\ R_n\ and\ g(x) = a(x)\ with \deg(g(x)) = r, then\ C = \langle g(x) + up(x)\rangle\ and\ (g + up) | (x^n - 1)\ in\ R.$

Lemma3.2.
$[1] If\ C = \langle g + up_1 + u^2p_2, ua_1 + u^2q_1, u^2a_2\rangle\ is\ a\ linear - cyclic\ code\ in\ S_n\ and\ if\ a_2 = g, then\ C = \langle g + up_1 + u^2p_2\rangle\ and\ (g + up_1 + u^2p_2) | (x^n - 1)\ in\ S.$

Lemma3.3. Let
$C\ be\ a\ a\ linear - constacyclic\ code\ in\ S_n = S[x]/\langle x^n - (1 - u^2)\rangle, then\ C\ can\ be\ written\ uniquely\ as\ C = \langle g(x) + up_1(x) + u^2p_2(x), ua_1(x) + u^2q_1(x), u^2a_2(x)\rangle\ where\ a_1(x), a_2(x), p_1(x), p_2(x), q_1(x),$

and $g(x)$ *are binary polynomials with* $a_2|a_1|g|(x^n - 1) mod\ 2, a_1(x)|p_1(x)\left(\frac{x^n-1}{g(x)}\right)$ *and* a_2 *divides* $q_1(x)\left(\frac{x^n-1}{a_1(x)}\right)$, *and* $p_2(x)\left(\frac{x^n-1}{g(x)}\right)\left(\frac{x^n-1}{a_1(x)}\right)$. *Moreover* $\deg p_2 < \deg a_2$, *and* $\deg q_1 < \deg a_2, \deg p_1 < \deg a_1$.

Proof. Assume that $C = \langle g(x) + up_1(x) + u^2p_2(x), ua_1(x) + u^2q_1(x), u^2a_2(x)\rangle =$ $\langle h(x) + um_1(x) + u^2m_2(x), ub_1(x) + u^2l_1(x), u^2b_2(x)\rangle$. *Since* $\ker\Phi = \langle u^2a_2(x)\rangle = \langle u^2b_2(x)\rangle$, *then* $a_2(x) = b_2(x)$ *and similarly* $\ker\varphi = \langle ua_1(x)\rangle = \langle ub_1(x)\rangle$ *implis* $a_1(x) = b_1(x)$.

Also

$\varphi(\Phi(C)) = \langle g(x)\rangle = \langle h(x)\rangle$, *and hence* $g(x) = h(x)$. *Since* $g + up_1 + u^2p_2 \in C = \langle g + um_1 + u^2m_2, ua_1 + u^2l_1, u^2a_2\rangle$, *then* $g + up_1 + u^2p_2 = g + um_1 + u^2m_2 + (ua_2 + u^2l_2)\alpha_1 + u^2a_2\alpha_2 \ldots\ldots\ldots\ldots\ldots\ldots (1)$.

Multiplying by u we get $u^2(p_1 - m_1) = u^2a_1\alpha_1$. *Since* $\deg(p_1 - m_1) < \deg(p_1)$, *then* $p_1 = m_1$. *So equation* (1) *becomes* $u^2p_2 = u^2m_2 + (ua_1 + u^2l_1)\alpha_1 + u^2a_2\alpha_2$ *and* $u^2(p_2 - m_2) = (ua_1 + u^2l_1)a_1 + u^2a_2\alpha_2$. *So* $u^2(p_2 - m_2) \in C$ *and hence* $\in \ker\Phi = \langle u^2a_2(x)\rangle$.

But again $\deg(p_2 - m_2) < \deg(a_2(x))$. Thus $p_2 = m_2$. Similarly, we can show that $q_1 = l_1$ and hence we are done.

Remark 3.1. The above generators $a_1(x), a_2(x)$ and $g(x)$ of C are divisors of $(x^n - 1)\ mod\ 2$ and they are not divisors of $(x^n - (1 - u^2))$, so for this fact makes the study of $(1 - u^2) - cyclic\ code\ easter\ to\ understand$.

Lemma 3.4. $(x + (1 - u^2))^{2L} = (x + 1)^{2L}$ *for any integer* L.

Proof. $(x + (1 - u^2))^{2L} = \left[(x + (1 - u^2))^2\right]^L$
$= [x^2 + (1 - u^2)^2 + 2x(1 - u^2)]^L$

$$= (x^2 + 1 + u^4 - 2u^2)^L$$
$$= (x^2 + 1 + uu^3)^L$$
$$= (x^2 + 1)^L = [(x+1)^2]^L = (x+1)^{2L}.$$

Lemma3.5.

Let $n = 2^e m$ *where* $\gcd(2,m) = 1$. *Then* u^2 *belongs to both ideals* $((x^m + 1))$ *and* $((x+1)^{2^e})$ *in* S_n.

Proof. In the ring S_n, *we have* $u^2 = x^n + 1 = x^{2^e m} + 1 = (x^m + 1)^{2^e} = ((x+1) f(x))^{2^e} = (x+1)^{2^e} f(x)^{2^e} = (x^{2^e} + 1) f(x)^{2^e}$.

Therefore, $u^2 \in ((x+1)^{2^e})$ *and* $u^2 \in ((x^m + 1))$.

Lemma3.6.

If $n = 2^e$, *then* $(1 + (x+1)^i p)$ *is a unit in* S_n *for any polynomial* p *and* $e \geq 0$.

Proof. The same as the proof of lemma (5) in [2].

Theorem3.7.

Let $C = \langle g(x) + up_1(x) + u^2 p_2(x), u^2 a_2(x) \rangle$ *be* $a(1-u^2)$ − *cyclic code in* S_n *for* $n = 2^e$. *Then* $C = \langle d(x+1)^i \rangle$ *where* $d = 1$ *or* u^2 *and* $i < \frac{n}{2}$

.

Proof. *If* $g(x) + up_1(x) + u^2 p_1(x) + u^2 p_2(x) = 0$, *then* $C = \langle u^2 a_2(x) \rangle$ *with* $a(x) \mid (x^n - 1)$.

Hence

$a_2(x) = (x-1)^i, i < n$ *and* $C = \langle u^2 (x+1)^i \rangle$. *If* $g(x) + up_1(x) + u^2 p_2(x) \neq 0$, *then* $g(x) + up_1(x) + u^2 p_2(x) = (x+1)^i + (x+1)^{\frac{n}{2}} p(x) + (x+1)^n p_2(x)$

$$= (x+1)^i \left[1 + (x+1)^{\frac{n}{2}-i} p_1(x) + (x+1)^{n-i} p_2(x)\right]$$
$$= (x+1)^i \left[1 + (x+1)^{\frac{n}{2}-i} \left(p_1(x) + (x+1)^{\frac{n}{2}} p_2(x)\right)\right]$$
$$= (x-1)v \text{ for some unit } v.$$

Hence we may assume that $C = \langle (x+1)^i, u^2(x+1)^j \rangle$. *Since* $u^2 = (x+1)^n$, *then* $u^2(x+1)^j \in \langle (x+1)^i \rangle$. *Therefor* $C = \langle (x+1)^i \rangle$.

Theorem3.8.
Let $C = \langle g(x) + up_1(x) + u^2 p_2(x), u^2 a_2(x) \rangle$ *be a* $(1 - u^2)$*cyclic code in* S_n *for* $n = 2^e m$ *and* $\gcd(2,m) = 1$.
If $p_1(x) = p_2(x) = 0$, *then* $C = \langle g(x) \rangle$ *or* $\langle u^2 g(x) \rangle$.

Proof. Let $C = \langle g(x) + up_1(x) + u^2 p_2(x), u^2 a_2(x) \rangle$ *be a* $(1 - u^2) -$ *cyclic code in* S_n. *Assume that* $p_1(x) = p_2(x) = 0$, *then* $C = \langle g(x), u^2 a_2(x) \rangle$, where $u^2 a_2(x) = (x^n - 1) a_2(x)$. *Since* $g(x) \mid (x^n - 1)$, *then* $u^2 a_2(x) \in \langle g(x) \rangle$. *Hence* $C = \langle g(x) \rangle$ *or* $\langle u^2 g(x) \rangle$.

Theorem 3.9. Suppose that $C = \langle f^k \rangle$ *is a* $(1 - u^2) -$ *cyclic code in* S_n *for* $n = 2^e m$, $\gcd(2,m) = 1$ *and* $f \mid (x^m - 1)$.
Then we assume that $k \leq 2^{e+1}$.

Proof. Sine $\left(\frac{x^n - 1}{f^{2^e}}, f^{2^e}\right) = 1$, *then* $s_1(x^n - 1) f^{2^e} + s_2 f^{2^e} = 1$, $s_1(x^n - 1) + s_2 f^{2^{e+1}} = f^{2^e}$, $s_1 u^2 + s_2 f^{2^{e+1}} = f^{2^e}$. (squaring both sides), $s_2^2 f^{2^{e+2}} = f^{2^{e+1}}$.

This implies $\langle f^{2^{e+2}} \rangle = (f^{2^{e+1}})$ and hence $\langle f^{2^{e+1}} \rangle = (f^k)$ *if* $2^{e+2} \leq k \leq 2^{e+1}$.

If $k = 2^{e+2} + t$, then $\langle f^k \rangle = \langle f^{2^{e+2}+t} \rangle = \langle f^{2^{e+1}+t} \rangle = \langle f^{2^{e+1}} \rangle$.

Lemma 3.10. Suppose $C = \langle f^i, u^2 g^k \rangle$ *is a* $(1 - u^2) -$ *cyclic code in* S_n *for* $n = 2^e m$, *where* $e > 0$, f *and* g *divides* $(x^m + 1)$ *and* $\gcd(2,m) = 1$, *then* $C = \langle h \rangle$ *where* $h = \gcd(f^i (x^n + 1) g^k)$.

Proof. First, note that $u^2 = x^n + 1$ in S_n. Also note that f^i and $(x^n + 1) g^k$ are polynomials in $Z_2[x]$ and hence $h = \gcd(f^i, (x^n + 1) g^k)$ exists.

Second, let $h = \gcd(f^i, (x^n+1)g^k)$ which implies $h \mid f^i$ and $h \mid (x^n+1)g^k$, then f^i and $(x^n+1)g^k \in \langle h \rangle$. Hence $C \subseteq \langle h \rangle$.
On the other hand $h = \alpha f^i + \beta(x^n+1)g^k$ (properties of gcd) for some $\alpha, \beta \in S[x] \Rightarrow h \in C \Rightarrow \langle h \rangle \subseteq C$.
Therefor, $C = \langle h \rangle$.

Remark3.2. Note that by lemma3.9, $\langle u^2\ g^k \rangle = \langle f_1^{i_1} f_2^{i_2} \ldots f_r^{i_r} \rangle$ *wher* $2^k \leq i_1, i_2, \ldots, i_r \leq 2^{s+1}$.
If $C = \langle f^i, u^2\ g^k \rangle$ and $i \leq 2^k$, *then* $h = gcd(f^i, (x^n+1)g^k) = f^i$. If $i \geq i_s$ where $f_s = f$, then $h = gcd(f^i, u^2\ g^k) = f_s^{i_s}$.

Theorem3.11. Let $C = \langle g(x) + up_1(x) + u^2 p_2(x) + u^2 a_2(x) \rangle$ *be a* $(1-u^2)-$ *cyclic code in* S_n *for* $n = 2^s m$ *and* $gcd(2, m) = 1$.
Suppose $p_1(x)$ *and* $p_2(x) \neq 0$, *then* $C = \langle f_1^{i_1} f_2^{i_2} \ldots f_r^{i_r} \rangle$, *where* $f_1, f_2, \ldots, f_r$ *are the monic binary divisors of* $(x^m - 1) mod\ 2$, *and* $i_1, i_2, \ldots, i_r \leq 2^{s+1}$.

Proof. Suppose $p_1(x), p_2(x) \neq 0$. Concider

$$\Phi\left[\left(\frac{x^n-1}{g(x)}\right)(g(x) + up_1(x) + u^2 p_2(x))\right] = \Phi\left[x^n - 1 + u\frac{x^n-1}{g(x)}p_1(x) + u^2\frac{x^n-1}{g(x)}p_2(x)\right]$$

=

$$\Phi\left[u^2 + u\frac{x^n-1}{g(x)}p_1(x) + u^2\frac{x^n-1}{g(x)}p_2(x)\right] = \Phi\left[u\left(u + \frac{x^n-1}{g(x)}p_1(x) + u\frac{x^n-1}{g(x)}p_2(x)\right)\right] = 0$$

Hence $u\left(u + \frac{x^n-1}{g(x)}p_1(x) + u\frac{x^n-1}{g(x)}p_2(x)\right) \in ker\Phi = \langle u^2 a_2(x) \rangle$

So $u + \frac{x^n-1}{g(x)}p_1(x) + u\frac{x^n-1}{g(x)}p_2(x) = a_2(x)k(x)$,

$ug(x) + (x^n-1)p_1(x) + u(x^n-1)p_2(x) = g(x)a_2(x)k(x)$.

$\Rightarrow ug(x) + u^2 p_2(x)$
$= g(x)a_2(x)k(x) \quad (Since\ u^2 = x^n - 1 \Rightarrow u(x^n - 1)$
$= 0)$.

Hence $C = \langle g(x)a_2(x)k(x), u^2 a_2(x)\rangle$.

But $u + \frac{x^n-1}{g(x)}p_1(x) + u\frac{x^n-1}{g(x)}p_2(x) = a_2(x)k(x)$.

$$\Rightarrow u = \frac{x^n-1}{g(x)}p_1(x) + u\frac{x^n-1}{g(x)}p_2(x) + a_2(x)k(x).$$

$$\Rightarrow ug(x)a_2(x) = u^2 a_2(x)p_1(x) + g(x)a_2(x)^2 k(x).$$

This implies that $g(x)a_2(x) \in C$ *and* $C = \langle g(x)a_2(x), u^2 a_2(x)\rangle$.

So we may assume that $C = \langle g_1^{l_1}(x)g_2^{l_2}(x) \ldots g_r^{l_r}(x), u^2 a_2(x)\rangle$, where $g_i(x) \mid (x^n - 1)$. Since $(x^n - 1) = (x^m - 1)^{2^s}$, then each $g_i(x) = f_i^{l_i}(x)$, where f_i is a monic divisor of $x^n + 1$ mod 2 and $l_i \leq 2^s$.

So $C = \langle f_1^{m_1} f_2^{m_2} \ldots f_r^{m_r}, u^2 f_t^{m_t}\rangle$, where $\{f_i\}$ are monic divisor of $(x^m + 1)$ mod 2. By lemma 3.10, we get that $C = \langle f_i^{i_1} f_i^{i_2} \ldots f_i^{i_r}\rangle$, where $f_s \mid (x^m - 1)$ mod 2 and $i_1, i_2, \ldots, i_r \leq 2^{s+1}$.

4 The dual and the minimal spanning set of $(1 - u^2) - cyclic\ code$

Lemma 4.1. *Let* $C = \langle g\rangle$ be a $(1 - u^2) - cyclic\ code$ *of length* $n = 2^s m$ *and* $\gcd(2, m) = 1$ in S_n, *where* $g \mid (x^n - 1) mod\ 2$ *and* $\gcd g = r$. *Then* C *has a minimal spanning set over* S *given by* $\beta = \{g, xg, \ldots, x^{n-r-1}g, u, xu, \ldots, x^{r-1}u, u^2 xu^2, \ldots x^{r-1}u^2\}$, *and* $|C| = 8^{n-r}\, 4^r 2^r$.

Proof. Since $u^2 = x^n - 1$ in S_n, and $g \mid (x^n - 1)$ in S_n, then $u^2 \in C$.

Let

$g(x) = 1 \mid g_1(x) \mid \ldots \mid \mid x^r$ *and* $gc_0 \mid xgc_1 \mid \ldots \mid x^{n-r-1}gc_{n-r-1} = 0 \Rightarrow c_i = 0$

for every $i = 0, 1, \ldots, n - r - 1$.

Now, we show that β spans

$\gamma = \{g, xg, \ldots, x^{n-r-1}g, u, xu, \ldots, x^{r-1}u, u^2 xu^2, \ldots x^{r-1}u^2\}$.

So we only show that $u^i x^r \in span\ (\gamma), for\ i = 1, 2$.

$u^i x^r = u^i g(x) + u^i m(x)$ where $m(x)$ is a polynomial in C of degree less than r, since any polynomial in C must have degree greater or equal to zero, then $0 \leq \deg m(x) < r$.

Hence $u^i m(x) = a_0 u^i + a_1 x u^i + \ldots + a_{r-1} x^{r-1} u^i$. Hence β is generating set.

By comparing coefficient as above, we have that non of the elements in β is a linear

combination of the others. Therefore β is a minimal generating set for C and $|C| = 8^{n-r} 4^r 2^r$.

Lemma 4.2. Let $C = \langle ug \rangle$ *be a* $(1-u^2)$ $-$ *cyclic code of length* $n = 2^s m$ *and* $\gcd(2, m) =$ 1 *in* S_n, *where* $g \mid (x^n - 1) \bmod 2$ *and* $\gcd g = r$. *then* C *has a minimal spanning set over* S *giveng by* $\beta = \{ug, uxg, \ldots, ux^{n-r-1}g, u^2 g, u^2 xg, \ldots, u^2 x^{r-1} g\}$, *and* $|C| = 4^{n-r} 2^r$.

Proof. Since the binary code generated by $g(x)$ has basis $\{g, xg, \ldots, x^{n-r-1}g, ug, uxg, \ldots, ux^{r-1}g, \}$, then the code $C = \langle ug \rangle$ has a minimal spanning set $\beta = \{ug, uxg, \ldots, ux^{n-r-1}g, u^2 g, u^2 xg, \ldots, u^2 x^{r-1} g\}$, *and hence* $|C| = 4^{n-r} 2^r$.

Lemma 4.3. Let $|C| = \langle u^2 g \rangle$ *be a* $(1-u^2)$ $-$ *cyclic code of length* $n = 2^s m$ *and* $\gcd(2, m)$ $= 1$ *in* S_n, *where* $g \mid (x^n - 1) \bmod 2$ *and* $\deg g$ $= r$. *Then* C *has a minimal spanning set over* S *given by* $\beta = \{u^2 g, u^2 xg, \ldots, u^2 x^{n-r-1} g\}$, *and* $|C| = 2^{n-r}$.

Proof. Since the binary code generated by $g(x)$ has basis $\{g, xg, \ldots, x^{n-r-1}g\}$, *then the code* $C =$ $\langle u^2 g \rangle$ *has minimal spanning set* $\beta = \{u^2 g, u^2 xg, \ldots, u^2 x^{n-r-1} g\}$.

Lemma 4.4. Let $C = \langle f_i^{i_1} f_i^{i_2} \ldots f_i^{i_r} \rangle$ *be*

$a\ (1-u^2)\ -cyclic\ code\ of\ length\ n=2^s m\ and\ \gcd(2,m)=1\ in\ S_n.$ *suppose for some* i_j *we have* $2^s \le i_j \le 2^{s+1}$. *Let* $C=\langle fg\rangle$ *where* g *is a polynomial of largest degree such that* $\deg g=r, \deg f=t$ *and* $f|g|(x^n-1)\ mod\ 2.$

Then C has a minimal spanning set over S spanned by

$$\beta=\{fg, xfg, \ldots, x^{n-r-1}fg, uf, xuf, \ldots, x^{r-t-1}uf, u^2f, xu^2f, \ldots, x^{r-t-1}u^2f\}.\ and\ |C|=8^{n-r}4^{r-t}2^{r-t}.$$

Proof. Since $C=\langle fg\rangle\ and\ f|g|(x^n-1)$ mod 2, then the lowest degree polynomial in C is u^2f. Let $c(x)\in C$, then $c(x)=fgh$, for some polynomial $h\in S_n$. Applying the division algorithm, we get $h=\frac{x^n-1}{g}q+d$, where $\deg q \le r-1,\ and\ d=0\ or \deg d < n-r-1.$

This implies that $fgh=fg\left(\frac{x^n-1}{g}q+d\right)=fu^2q+fgd.$

Note that $fgd\in span(\beta)$. If $\deg q \le r-t-1, then\ fu^2q\in span\ (\beta)$ and hence $c(x)=fgh\ \in span\ (\beta).\ If \deg q > r-t, then\ r < \deg(fu^2q) \le r+t-1 < n+t-1=\deg(x^{n-r-1}fg).$

Hence $fu^2q\in span\ (\beta)$. Therefore β spans C. From the construction of C, we have β is a minimal spanning set.

Theorem 4.5. Let $C\ be\ a\ (1-u^2)-cyclic\ code\ S_n where\ n=2^s m,$ gcd(2,m)=1.

$$(1)If\ C=(g(x)), then\ A(C)=\left(u^2\frac{x^n-1}{g}\right) and C^{\perp}=\left(u^2\left(\frac{x^n-1}{g}\right)^*\right).$$

$$(2)If\ C=(g(x)), then\ A(C)=\left(u\frac{x^n-1}{g}\right) and C^{\perp}=\left(u\left(\frac{x^n-1}{g}\right)^*\right).$$

$$(3)If\ C=(u^2g(x)), then\ A(C)=\left(\frac{x^n-1}{g}\right) and C^{\perp}=\left(\left(\frac{x^n-1}{g}\right)^*\right).$$

$(4)If\ C=\langle f_i^{i_1}f_i^{i_2}\ldots f_i^{i_r}\rangle$ *where for some* i_j *and* $2^s < i_j \le 2^{s+1}$, *then*

$$A(C)=\left(f_1^{2^{s+1}-i_1}f_2^{2^{s+1}-i_2}\ldots f_r^{2^{s+1}-i_r}\right) and$$

$$C^{\perp}=\left(\left(f_1^{2^{s+1}-i_1}\right)^*,\left(f_2^{2^{s+1}-i_2}\right)^*,\ \ldots\ ,\left(f_r^{2^{s+1}-i_r}\right)^*\right).$$

Proof.

(1) *Since* $C = \langle g(x) \rangle$, *then from lemma* 4.1 $\left(u^2 \frac{x^n-1}{g}\right) \subseteq A(C)$ *and* $\left|\left(u^2 \frac{x^n-1}{g}\right)\right| = 8^{n-deg\left(u^2\frac{x^n-1}{g}\right)}$, *but* $|C||C^{\perp}| = 8^n$, *hence* $C^{\perp} = \left(u^2\left(\frac{x^n-1}{g}\right)^*\right)$.

(2) *Since* $C = \langle ug(x) \rangle$, *then from lemma* 4.2 $\left(u\frac{x^n-1}{g}\right) \subset A(C)$ *and* $|C| = 4^{n-r}2^r$ *but* $|C||C^{\perp}| = 8^n$, *hence* $C^{\perp} = \left(u\left(\frac{x^n-1}{g}\right)^*\right)$.

(3) Similarly it follows directly from Lemma 4.3.

(4) Similarly it follows directly from Lemma 4.4.

5 The Gray map and $(1-u^2)$ - cyclic codes

An element $z \in S$ can expressed uniquely as

$$z = a + ur + u^2 q, \text{ where } a, r, q \in Z_2.$$

Following [3]; The Generalized Gray map ψ: $S^n \to Z_2^{4n}$ is defined by

$\psi(z_1, z_2, \ldots, z_n) = (q_1, q_2, \ldots, q_n, q_1 \oplus a_1, q_2 \oplus a_2, \ldots, q_n \oplus a_n, q_1 \oplus r_1, q_2 \oplus r_2, \ldots, q_n \oplus r_n, q_1 \oplus r_1 \oplus a_1, q_2 \oplus r_2 \oplus a_2, \ldots, q_n \oplus r_n \oplus a_n)$

where $\oplus$ is componentwise addition in Z_2 and $z_i = a_i + ur_i + u^2 q_i, 1 \le i \le n$.

ψ is an isometry from (S^n, Generalized Leedistance) to (Z_2^{4n}, Hamming distance). The polynomial representation of the Generalized Gray map was given in the following way: Every polynomial $z(x) \in S[x]$ of degree less than n can be expressed as $z(x) = b(x) + ut(x) + u^2 m(x)$,where $b(x), t(x)$, and $m(x) \in Z_2[x]$ are polynomials of degree less than n. Recall that $S_n = S[x]/\langle x^n - (1-u^2) \rangle$.

Define the map $\psi_p : S_n \to Z_2[x]/\langle x^{4n} + 1 \rangle$ by

$$\psi_p(z(x)) = b(x)x^n + t(x)(x^n + 1) + m(x)(x^{2n} + 1).$$

ψ_p is the polynomial representation of ψ where ψ: $S \to Z_2^4$ defined by

$\psi\ (a + ur + u^2q) = (q, q \oplus a, q \oplus r, q \oplus a \oplus r).$

Lemma 5.1. let $C = \langle g \rangle$ *be a* $(1 - u^2) -$ *cyclic code in* S_n *where* $g|\ (x^n - 1)$ mod 2.

Then $\psi_p\ (c) = \langle g \rangle_2$ *is a cyclic code of* $Z_2^{4n}\ [x]$.

Proof. Let $C = \langle g \rangle$ *be any* $(1 - u^2) -$ cyclic code in S_n where $g|\ (x^n - 1)$ mod 2. From the definition of ψ_p we have

$\psi_p\ (\langle g \rangle) = gx^n \in \langle g \rangle_2$

Hence $\psi_p\ (C) \subseteq \langle g \rangle_2$. We have $\psi_p\ (gx^n) = gx^{4n} = g$. Hence $\langle g \rangle_2 \subseteq \psi_p\ (C)$ and $\psi_p\ (C) = \langle g \rangle_2$.

Lemma 5.2. let $C = \langle ug \rangle$ *be a* $(1 - u^2) -$ *cyclic code in* S_n *where* $g|\ (x^n - 1)$ mod 2.

Then $\psi_p\ (C) = \langle g(x^n + 1) \rangle_2$ *is a cyclic code of* $Z_2^{4n}\ [x]$.

Proof. Similar to the proof of lemma 5.1.

Lemma 5.3. *Let* $C = \langle u^2 g \rangle$ *be a* $(1 - u^2) -$ *cyclic code in* S_n *where* $g|\ (x^n - 1)$ mod 2.

Then $\psi_p\ (C) = \langle g\ (x^{2n} + 1) \rangle_2$ *is a cyclic code of* $Z_2^{4n}\ [x]$.

Proof. Similar to the proof of lemma 5.1.

Lemma 5.4. *Let* $C = \langle f_1^{i_1} f_2^{i_2} \ldots f_r^{i_r} \rangle$ *be a* $(1 - u^2) -$ *cyclic code of length* $n = 2^e m$ *and* $\gcd(2, m) = 1$ *in* S_n. *Suppose for some* i_j, *we have* $2^e \leq i_j \leq 2^{e+1}$. *Then* $\psi_p(C)$ *is a binary cyclic code of length* $4n$ *with generator* $\langle f_1^{i_1} f_2^{i_2} \ldots f_r^{i_r} \rangle_2$

Proof. Similar to the proof of Theorem 5.1.

6 Examples

Example 6.1. $x^{10} - 1 = (x + 1)^2 (x^4 + x^3 + x^2 + x + 1)^2$

$= f_1^2\ (x)\ f_2^2\ (x)$

According to lemma 4.4, let $f\ (x) = x + 1 = f_1\ (x)$ *and* $g\ (x)$

$= (x + 1)^2\ (x^4 + x^3 + x^2 + x + 1) = f_1^2\ (x)\ f_2\ (x).$

$\Rightarrow \deg(g(x)) = 6, \deg(f(x)) = 1 \Rightarrow r = 6, t = 1, n - r - 1 = 3,$

$r - t - 1 = 4$

Since $(x+1)|(x+1)^2(x^4+x^3+x^2+x+1)|(x^{10}-1)$
$\Rightarrow f|g|(x^{10}-1) \bmod 2 \Rightarrow C = \langle fg \rangle$
$= \langle f_1^3 f_2 \rangle$. *Thus the generating set of code words of C over S is given by*:
$\beta =$
$\{fg, xfg, x^2fg, x^3fg, uf, xuf, x^2uf, x^3uf, x^4uf,$
$u^2f, xu^2f, x^2u^2f, x^3u^2f, x^4u^2f\}$. *Thus* $|C| = 8^4.4^5.2^5$.

Example 6.2. $x^8 - 1 = (x-1)^8$ *in S*.

Now, since $u^2 = x^n - 1 \Rightarrow u^2 = x^8 - 1$. *Let* $g(x) = (x-1)^4 \Rightarrow$
$g(x)|(x^8-1) \bmod 2 \Rightarrow u^2 g = (x^8-1)(x-1)^4 = x^{12} - 1 = x^4 - 1 \pmod{x^8-1} \Rightarrow C = (x^4-1) = (g(x))$.

According to lemma 4.1, deg $g = 4 \Rightarrow r = 4, n-r-1 = 3, r-1 = 3$.

Thus C has a minimal spanning set over S given by:
$\beta = \{x, xg, x^2g, x^3g, u, xu, x^2u, x^3u, u^2, xu^2, x^2u^2, x^3u^2\}$.
Thus $|C| = 8^4.4^4.2^4$.

7 Conclusion

In this paper, we studied constacyclic codes of even length over the ring $F_2 + u F_2 + u^2 F_2$. The dual and Gray images of this family of codes of codes are studies as well.

Open problems include the study of constacyclic codes of even length over the ring $F_p + u F_p + u^2 F_p + \ldots + u^k F_p$, where k is positive, $u^{k+1} = 0 \bmod p$, and p is a prime interger. Also it will be interesting to construct a decoding algorithm for these codes that works for any length n.

References:

[1] Abualrub T. and Saip I. 2007 : Cyclic Codes over the Rings $Z_2 + uZ_2$ and $Z_2 + uZ_2 + u^2Z_2$, Designs, Codes and Creptography, vol.42, no.03, pp.273-287.

[2] Abualrub T. and Saip I. 2009 : Constacyclic Codes over $F_2 + uF_2$, Journal of the Franklin Institute, vol.346, no.02, pp.520-529.

[3] Al-Ashker M. 2005 : Simplex Codes over the Ring $\sum_{n=0}^{s} u^n F_2$, Turk .J.Math, vol.29,pp.221-233.

[4] Bonnecaze A. and Udaya P. 1999 : Cyclic Codes and Self-dual Codes over $F_2 + uF_2$, IEEE Trans.Inform.Theory, vol.45, no.04, pp. 1250-1255.

[5] Conway J.H. and Sloan N.J.A. 1993 : Self-dual Codes over the Integers modulo 4, Journal of Combinatorial Theory Series A 62, pp.30-45.
[6] Grasst M.: Linear Codes Bounds, IAKS, Fakultat Fur Informatik, Universitat Karl-surhe (TH), Availiable Online at http://www.codetables.de/(grassl@ira.uka.de).
[7] Hammons A.R. and others, 1994 : The Z_4-Linearity of Kerdock, Preparata, Goethals, and Related Codes, IEEE Transactions on Information Theory, vol.40, no.02, pp.301-319.
[8] Pless V. and Qian Z. 1996 : Cyclic Codes and Quadratic Residue Codes over Z_4, IEEE Transactions on Information Theorey, vol.42, no.05, pp.1594-1600.
[9] Qian J.F. and others, 2006 : *(1 + u)* Constacyclic and Cyclic codes over $F_2 + uF_2$, Applied Mathematics Letters Volume 19, Issue 8, pp.820-823.
[10] Wolmann J. 2001 : Binary Images of Cyclic Codes over *Z4*, Transactions on Information Theory, vol.47, no.05, pp. 1773-1779.