MATHEMATICAL SCIENCES AND APPLICATIONS E-NOTES
5 (2) 69-75 (2017) ©MSAEN

On Self-Dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear Codes

Ismail Aydogdu* and Abidin Kaya

(Communicated by Tamer KOŞAN)

Abstract
The family of self-dual codes particularly the ones over the binary alphabet is studied often. Recently, $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear codes have been defined as R-submodules of $\mathbb{Z}_2^r \times R^s$ in [4] where $R = \mathbb{Z}_2 + u\mathbb{Z}_2 = \{0, 1, u, u+1\}$ is the ring with four elements, $u^2 = 0$ and r, s are positive integers. In this work, we study self-dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear codes. We introduce two types of self-dual codes. Some examples of self-dual separable and non-separable $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear codes for each type are given. Binary self-dual codes are obtained as the Gray images of self-dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-codes.

Keywords: *Self-dual codes; type I codes; type II codes; $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear codes.*

AMS Subject Classification (2010): *Primary: 94B05; Secondary: 94B99.*

****Corresponding author***

1. Introduction

Self-dual codes over the binary field have been an attractive research area in the last decades. The structure of binary and quaternary linear codes have been studied in details for the last sixty years. An upper bound on the minimum distance of a self-dual binary code is given in [7]. Since then, the construction and classification of extremal binary self-dual codes has generated interest. For instance, some new extremal binary self-dual codes of length 68 obtained by codes over the alphabet $\mathbb{Z}_2[x]/\langle x^3 - 1\rangle$ with eight elements in [10].

Another recent research area is additive codes. Finite rings of different characteristics have been used by researchers. Codes over alphabets such as $\mathbb{Z}_2\mathbb{Z}_4$ have been studied. For some of the works done in this direction we refer the reader to [1, 3, 6]. In [6], Borges et al. defined a new class of error correcting codes called $\mathbb{Z}_2 \times \mathbb{Z}_4$-additive codes, which generalize the class of binary linear codes and the class of quaternary linear codes. A $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ is defined to be a subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ where $\alpha + 2\beta = n$. Binary linear codes and codes over $\mathbb{Z}_4$ can be considered as subfamilies of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes. The ring $R = \mathbb{Z}_2[x]/\langle x^2\rangle$ is an important ring with four elements where $R = \mathbb{Z}_2[u] = \{0, 1, u, u+1\}$ and $u^2 = 0$. Cyclic, constacyclic and self-dual codes over the ring R have been studied by many researchers, for some of them we refer to [2, 5, 8, 11]. $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes have been investigated in [4].

In this work, we consider self-dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear codes, determine the conditions on self-dual codes. Via a duality preserving linear Gray map we obtain self-dual binary codes.

The rest of the work is organized as follows: some of the basic definitions about $\mathbb{Z}_2\mathbb{Z}_2[u]$, Gray map to the binary space and their properties are given in Section 2, in Section 3 we study the structure of separable, non-separable, antipodal, Type I and Type II self-dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear codes. Some examples of self-dual codes of each type are given in Section 4.

Received : *17–October–2016,* ***Accepted :*** *02–October–2017*

2. Preliminaries

Let $R=\mathbb{Z}_2+u\mathbb{Z}_2=\{0,1,u,u+1\}$ be the finite ring with four elements where $u^2=0$. It is clear that the ring $\mathbb{Z}_2$ is a subring of the ring R. Therefore we define the set

$$\mathbb{Z}_2\mathbb{Z}_2[u]=\{(a,b)\mid a\in\mathbb{Z}_2 \text{ and } b\in R\}.$$

Here, the set $\mathbb{Z}_2\mathbb{Z}_2[u]$ is not well-defined with respect to the usual multiplication by $u\in R$. So, we must define a new way of multiplication on $\mathbb{Z}_2\mathbb{Z}_2[u]$ to make this set an R-module. Now define the mapping

$$\begin{aligned}\eta &: R\to\mathbb{Z}_2\\ \eta(p+uq) &= p.\end{aligned}$$

i.e., $\eta(0)=0,\ \eta(1)=1,\ \eta(u)=0$ and $\eta(u+1)=1$. It is easy to show that η is a ring homomorphism. And also, for any element $d\in R$, we can define an R-scalar multiplication on $\mathbb{Z}_2\mathbb{Z}_2[u]$ as

$$d(a,b)=(\eta(d)a,db).$$

Furthermore, this multiplication can be extended to $\mathbb{Z}_2^r\times R^s$ as follows. Let $d\in R$ and
$v=(a_0,a_1,...,a_{r-1},b_0,b_1,...,b_{s-1})\in\mathbb{Z}_2^r\times R^s$ define

$$dv=(\eta(d)a_0,\eta(d)a_1,...,\eta(d)a_{r-1},db_0,db_1,...,db_{s-1}).$$

Definition 2.1. Let $\mathcal{C}$ be a non-empty subset of $\mathbb{Z}_2^r\times R^s$. Then $\mathcal{C}$ is called a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code if it is an R-submodule of $\mathbb{Z}_2^r\times R^s$.

Let $a\in R$, then there exists unique $p_1,q_1\in\mathbb{Z}_2$ such that $a=p_1+uq_1$. And also, as an additive group, the ring R is isomorphic to $\mathbb{Z}_2^2$. Therefore, if $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_2[u]-$linear code then it is isomorphic to an abelian group of the form $\mathbb{Z}_2^{k_0}\times\mathbb{Z}_2^{2k_1}$, where k_0 and k_1 are positive integers. Now consider the following sets.

$$\mathcal{C}_s^F=\{(a,b)\in\mathbb{Z}_2^r\times R^s\mid b \text{ free over } R^s\} \text{ and } dim(\mathcal{C}_s^F)=k_1.$$

Let $D=\mathcal{C}\backslash\mathcal{C}_s^F=\mathcal{C}_0\oplus\mathcal{C}_1$ such that

$$\begin{aligned}\mathcal{C}_0 &= \langle\{(a,ub)\in\mathbb{Z}_2^r\times R^s\mid a\neq 0\}\rangle\subseteq\mathcal{C}\backslash\mathcal{C}_s^F\\ \mathcal{C}_1 &= \langle\{(a,ub)\in\mathbb{Z}_2^r\times R^s\mid a=0\}\rangle\subseteq\mathcal{C}\backslash\mathcal{C}_s^F.\end{aligned}$$

Hence, denote the dimension of $\mathcal{C}_0$ and $\mathcal{C}_1$ as k_0 and k_2 respectively. Considering all these parameters we say such a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code $\mathcal{C}$ is of type $(r,s;k_0,k_1,k_2)$.

We can look at $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear codes as binary codes under a special map. For $(x,y)\in\mathbb{Z}_2^r\times R^s$, where $x=(x_0,x_1,\ldots,x_{r-1},y_0,y_1,\ldots,y_{s-1})$ and $y_i=p_i+uq_i$ define the Gray map

$$\begin{aligned}&\Phi:\mathbb{Z}_2^r\times R^s\to\mathbb{Z}_2^n\\ &\Phi(x_0,\ldots x_{r-1},p_0+uq_0,\ldots p_{s-1}+uq_{s-1})\\ &\qquad=(x_0,\ldots x_{r-1},q_0,\ldots,q_{s-1},p_0\oplus q_0,\ldots,p_{s-1}\oplus q_{s-1})\end{aligned}$$

where $p_i\oplus q_i=p_i+q_i \mod 2$ and $n=r+2s$. The Gray map is a distance preserving map which transforms the Lee distance in $\mathbb{Z}_2^r\times R^s$ to the Hamming distance in $\mathbb{Z}_2^n$, where the Hamming and the Lee distance between two codewords is the Hamming weight and the Lee weight of their differences, respectively. The Hamming weight of an any codeword is the number of its nonzero entries, and the Lee weight of an elements of R are, $wt_L(0)=0,\ wt_L(1)=wt_L(1+u)=1,\ wt_L(u)=2$. Furthermore, Φ is a linear map, so the binary image $\Phi(\mathcal{C})$ of an any $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code $\mathcal{C}$, is also a linear code. If $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code of type (r,s,k_0,k_1,k_2) then the binary image $C=\Phi(\mathcal{C})$ is a binary linear code of length $n=r+2s$ and size 2^n.

Next, for any elements

$$v=(a_0,\ldots,a_{r-1},b_0,\ldots,b_{s-1}),w=(d_0,\ldots,d_{r-1},e_0,\ldots,e_{s-1})\in\mathbb{Z}_2^r\times R^s,$$

define the inner product as

$$\langle v,w\rangle=\left(u\sum_{i=0}^{r-1}a_id_i+\sum_{j=0}^{s-1}b_je_j\right)\in\mathbb{Z}_2+u\mathbb{Z}_2.$$

According to this inner product, the dual linear code $\mathcal{C}^{\perp}$ of an any $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code $\mathcal{C}$ is defined in a usual way,

$$\mathcal{C}^{\perp} = \{w \in \mathbb{Z}_2^r \times R^s |\ \langle v, w\rangle = 0 \text{ for all } v \in \mathcal{C}\}.$$

Therefore, if $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code, then $\mathcal{C}^{\perp}$ is also a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code.

Two codewords c_1 and c_2 of a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code may be orthogonal to each other but the binary parts of the vectors may not be orthogonal. For example, $(1|1+u)$ and $(1|u)$ are orthogonal in $\mathbb{Z}_2 \times R$ whereas the binary or R-components are not orthogonal. The Gray map φ from R^s into $\mathbb{Z}_2^{2s}$ defined as $\varphi\left(\overline{a}+u\overline{b}\right) = \left(\overline{b}, \overline{a}+\overline{b}\right)$ preserves orthogonality. But, that is not enough to conclude that Φ preserves orthogonality. Hence, we need to verify that Φ preserves orthogonality.

Theorem 2.1. *Let $\mathcal{C}$ be a self-dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code then $\Phi(\mathcal{C})$ is a binary self-dual code.*

Proof. It is enough to show that the Gray images of codewords are orthogonal whenever the codewords are. Let $\mathcal{C}$ be a self-dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code and $v = \left(\overline{a}, \overline{b}+u\overline{c}\right)$, $w = \left(\overline{d}, \overline{e}+u\overline{f}\right) \in \mathbb{Z}_2^r \times R^s$ be codewords in $\mathcal{C}$ where $\overline{a}$, $\overline{d} \in \mathbb{Z}_2^r$ and $\overline{b}$, $\overline{c}$, $\overline{e}$ and $\overline{f} \in \mathbb{Z}_2^s$. Then $\langle v, w\rangle = u\left\langle \overline{a}, \overline{d}\right\rangle + \left\langle \overline{b}+u\overline{c}, \overline{e}+u\overline{f}\right\rangle = 0$ in R. For ease of notation denote the standard inner product of two binary vectors $\left\langle \overline{a}, \overline{d}\right\rangle$ as $\overline{a}\overline{d}$. So we have $u\left(\overline{ad}+\overline{bf}+\overline{ce}\right)+\overline{be} = 0$ in R which implies $\overline{ad}+\overline{bf}+\overline{ce} = 0 = \overline{be}$ in $\mathbb{Z}_2$. On the other hand, $\Phi(v) = \left(\overline{a}, \overline{c}, \overline{b}+\overline{c}\right)$, $\Phi(w) = \left(\overline{d}, \overline{f}, \overline{e}+\overline{f}\right)$ and $\langle \Phi(v), \Phi(w)\rangle = \overline{ad}+\overline{cf}+\overline{be}+\overline{bf}+\overline{ce}+\overline{cf} = \left(\overline{ad}+\overline{bf}+\overline{ce}\right)+\overline{be} = 0$. Hence the binary image of a self-dual code is self-dual. $\square$

The standard forms of generator and parity-check matrices of a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code $\mathcal{C}$ were given as follows.

Theorem 2.2. *[4] Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code of type $(r, s; k_0, k_1, k_2)$. Then the generator and the parity-check matrices of $\mathcal{C}$ are given in the following standard forms.*

$$G = \left(\begin{array}{cc|ccc} I_{k_0} & A_1 & 0 & 0 & uT \\ \hline 0 & S & I_{k_1} & A & B_1+uB_2 \\ 0 & 0 & 0 & uI_{k_2} & uD \end{array}\right)$$

$$H = \left(\begin{array}{cc|ccc} -A_1^t & I_{r-k_0} & -uS^t & 0 & 0 \\ -T^t & 0 & -(B_1+uB_2)^t+D^tA^t & -D^t & I_{s-k_1-k_2} \\ 0 & 0 & -uA^t & uI_{k_2} & 0 \end{array}\right)$$

where A, A_1, B_1, B_2, D, S and T are matrices over $\mathbb{Z}_2$.

Corollary 2.1. *[4] If $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code of type $(r, s; k_0, k_1, k_2)$ then $\mathcal{C}^{\perp}$ is of type $(r, s; r-k_0, s-k_1-k_2, k_2)$.*

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code of type $(r, s; k_0, k_1, k_2)$ with $n = r+2s$. Then the weight enumerator of $\mathcal{C}$ is defined as

$$W_{\mathcal{C}}(x, y) = \sum_{c\in\mathcal{C}} x^{n-w(c)}y^{w(c)}.$$

Theorem 2.3. *[4] Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_2[u]-$linear code. The relation between the weight enumerators of $\mathcal{C}$ and its dual is,*

$$W_{\mathcal{C}^{\perp}}(x, y) = \frac{1}{|\mathcal{C}|}W_{\mathcal{C}}(x+y, x-y).$$

3. The Structure of Self-Dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear Codes

In this section of the paper we investigate the structure of self-dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear codes.

Lemma 3.1. *If $\mathcal{C}$ is a self-dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code then $\mathcal{C}$ is of type $(2k_0, 2k_1+k_2; k_0, k_1, k_2)$.*

Proof. Since $\mathcal{C}$ is a self-dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code, $\mathcal{C} = \mathcal{C}^{\perp}$. So, types of the $\mathcal{C}$ and its dual have to be equal. Hence,

$$(r, s; k_0, k_1, k_2) = (r, s; r-k_0, s-k_1-k_2, k_2)$$

and we have $r = 2k_0$ and $s = 2k_1+k_2$. $\square$

Corollary 3.1. *If $\mathcal{C}$ is a self-dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code of type $(r, s; k_0, k_1, k_2)$ and length n, then both r and n are even.*

Lemma 3.2. *Let $\mathcal{C} \subseteq \mathbb{Z}_2^r \times R^s$ be a self-dual code. Let $(x, y) \in \mathcal{C}$ and let us denote the number of unit coordinates(coordinates 1 or $1+u$) of any vector $y \in R^s$ by $N_u(y)$. Therefore, we have both $w_H(x)$ and $N_u(y)$ are even.*

Proof. Take $c = (x_0, x_1, \ldots, x_{r-1}, y_0, y_1, \ldots, y_{s-1})$ in $\mathcal{C}$. We know that $\mathcal{C}$ is self-dual so it is self-orthogonal. Hence,

$$\langle c, c\rangle = u\left(x_0^2 + x_1^2 + \ldots + x_{r-1}^2\right) + y_0^2 + y_1^2 + \ldots + y_{s-1}^2 = uw_H(x) + N_u(y) = 0.$$

Therefore, in order to hold to above statement, both of $w_H(x)$ and $N_u(y)$ must be even. □

Corollary 3.2. *Let k^t denote the tuple $(k, k, \ldots, k)$ of length t. If $\mathcal{C}$ is self-dual then $(0^r, u^s)$ is clearly a codeword in $\mathcal{C}$.*

Lemma 3.3. *Let $\mathcal{C}$ be a self-dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code. Let $\mathcal{C}_r$ be the punctured code of $\mathcal{C}$ by deleting the coordinates outside r. Denote the binary subcode of $\mathcal{C}$ by $(\mathcal{C}_b)$ which actually contains all order two codewords and denote the dimension of $(\mathcal{C}_b)_r$ by k_0. Then $(\mathcal{C}_b)_r$ is a binary self-dual code.*

Proof. Since $\mathcal{C}$ is self-dual then is of type $(2k_0, 2k_1 + k_2; k_0, k_1, k_2)$. For any pair of codewords $(x, y), (x', y') \in \mathcal{C}_b$ we have y and y' are orthogonal vectors. So, x and x' are also orthogonal to each other. Moreover, $(\mathcal{C}_b)_r$ has dimension k_0 and is of length $2k_0$. Hence we have $(\mathcal{C}_b)_r$ self-dual. □

Definition 3.1. Let $\mathcal{C}$ be $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code. Let $\mathcal{C}_r$ (respectively $\mathcal{C}_s$) be the punctured code of $\mathcal{C}$ by deleting the coordinates outside r (respectively s). If $\mathcal{C} = \mathcal{C}_r \times \mathcal{C}_s$ then $\mathcal{C}$ is called separable.

If $\mathcal{C}$ is a separable $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code of type $(r, s; k_0, k_1, k_2)$ then it has the following generator matrix in the following form,

$$G = \left(\begin{array}{cc|ccc} I_{k_0} & A_1 & 0 & 0 & 0 \\ \hline 0 & 0 & I_{k_1} & A & B_1 + uB_2 \\ 0 & 0 & 0 & uI_{k_2} & uD \end{array}\right)$$

where $A_1,\ A,\ B_1,\ B_2$ and D are binary matrices.

Theorem 3.1. *Let $\mathcal{C}$ be a self-dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code of type $(2k_0, 2k_1 + k_2; k_0, k_1, k_2)$. Then the following statements are equivalent.*

- *$\mathcal{C}_r$ is a binary self-dual code.*
- *$\mathcal{C}_s$ is a self-dual code over R.*
- *$|\mathcal{C}_r| = 2^{k_0}$ and $|\mathcal{C}_s| = 2^{2k_1+k_2}$.*
- *$\mathcal{C}$ is separable.*

Proof. The proof comes from the natural consequence of Definition 3.1. □

Theorem 3.2. *If $\mathcal{C}$ is a binary self-dual code of length r and $\mathcal{D}$ is a self-dual code over R of length s. Then $\mathcal{C} \times \mathcal{D}$ is a self-dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code of length $r + s$.*

Proof. Let $v = (v_0, v_1, \ldots, v_{r-1}), v' = (v'_0, v'_1, \ldots, v'_{r-1}) \in \mathcal{C}$ and $w = (w_0, w_1, \ldots, w_{s-1})$, $w' = (w'_0, w'_1, \ldots, w'_{r-1}) \in \mathcal{D}$. Since both of $\mathcal{C}$ and $\mathcal{D}$ are self-dual,

$$\langle (v, w), (v', w')\rangle = u\sum_{i=0}^{r-1} v_i v'_i + \sum_{i=0}^{s-1} w_i w'_i \equiv 0\ (mod\ 2).$$

Therefore, $\mathcal{C} \times \mathcal{D}$ is self-orthogonal. It follows that it is self-dual due to the size of the code. □

Lemma 3.4. *Let $\mathcal{C}$ and $\mathcal{D}$ are self-dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear codes of type $(r, s; k_0, k_1, k_2)$ and $(r', s'; k'_0, k'_1, k'_2)$ respectively. Then $\mathcal{C} \times \mathcal{D}$ is a self-dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code of type $(r + r', s + s'; k_0 + k'_0, k_1 + k'_1, k_2 + k'_2)$.*

Proof. Let the generator matrix of $\mathcal{C}$ be $(G_r \mid G_s)$ and the generator matrix of $\mathcal{D}$ be $(G'_r \mid G'_s)$. Then $\mathcal{C} \times \mathcal{D}$ has the following generator matrix of the form.

$$\left(\begin{array}{cc|cc} G_r & 0 & G_s & 0 \\ \hline 0 & G'_r & 0 & G'_s \end{array}\right)$$

It is clear that the rows of the above matrix is orthogonal to each other. Since $\mathcal{C}$ and $\mathcal{D}$ are self-dual, the parameters of the new self-dual code $\mathcal{C} \times \mathcal{D}$ are $(r + r', s + s'; k_0 + k'_0, k_1 + k'_1, k_2 + k'_2)$.

□

Corollary 3.3. *There exists self-dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear codes of type $(r, s; k_0, k_1, k_2)$ for all even r and all s.*

Definition 3.2. Let $\mathcal{C}$ be a self-dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code. If $\mathcal{C}$ has a codeword of odd weight then it is called Type 0. If all codewords of $\mathcal{C}$ have weights divisible by 4 then it is said to be Type II and Type I otherwise.

We easily observe that Type 0 self-dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear codes do not exist. Since the binary image is a binary self-dual code and there is no Type 0 binary self-dual code.

Definition 3.3. Let C be a binary code and $c \in C$. C is called antipodal if $c + 1 \in C$. In the case, where $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code, we say $\mathcal{C}$ is antipodal if $\Phi(\mathcal{C})$ is antipodal.

It is clear that a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code $\mathcal{C}$ is antipodal if and only if $(1^r, u^s) \in \mathcal{C}$.

Proposition 3.1. *Let $\mathcal{C} \subseteq \mathbb{Z}_2^r \times R^s$ be a self-dual code. $\mathcal{C}$ is antipodal if and only if $\mathcal{C}$ is of Type I or Type II.*

Proof. We know that $\mathcal{C}$ is antipodal if and only if $(1^r, u^s) \in \mathcal{C}$ and also it is obvious that $(0^r, u^s) \in \mathcal{C}$. Therefore we have, $\mathcal{C}$ is antipodal if and only if $(1^r, 0^s) \in \mathcal{C}$. This means that all codewords of $\mathcal{C}_r$ have even weight. □

Proposition 3.2. *Let $\mathcal{C}$ be a self-dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code. If $\mathcal{C}$ is separable then $\mathcal{C}$ is antipodal.*

Proof. Assume that $\mathcal{C} = \mathcal{C}_r \times \mathcal{C}_s$ is separable where $\mathcal{C}_r$ and $\mathcal{C}_s$ are self-dual codes over $\mathbb{Z}_2^r$ and R^s respectively. Hence $\mathcal{C}_r$ contains all-1 vector and $\mathcal{C}_s$ contains all-u vector then $(1^r, u^s) \in \mathcal{C}$. □

4. Examples of Self-Dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear Codes

In this section some examples of separable and non-separable self-dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear codes are given. Self-dual binary codes obtained as Gray images of these and some of them are optimal binary codes. If the minimum distance of an any code $\mathcal{C}$ get the possible maximum value according to its length and dimension, then $\mathcal{C}$ is called optimal code. We use the table of optimal linear codes in the website http://www.codetables.de/ [9]. Further, an upper bound for the minimum distance d of a binary self-dual code of length n is given in [7] as $d \leq 4\lfloor \frac{n}{24} \rfloor + 4$ if $n \not\equiv 22 \pmod{24}$. A self-dual binary code of length n where $n \not\equiv 22 \pmod{24}$ is called *extremal* if it meets the bound. The following examples illustrate extremal self-dual binary codes of lengths $8,\ 10,\ 14,\ 16$ and 20.

Example 4.1. (Separable Type I) Let $\mathcal{C}_1$ be self-dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code of type $(2, 3; 1, 1, 1)$ with the generator matrix of the following form.

$$G_1 = \left(\begin{array}{cc|ccc} 1 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & u & 0 \end{array}\right).$$

Therefore, $\mathcal{C}_1$ is a Type I separable code and its image $\Phi(\mathcal{C}_1)$ is the self-dual $[8, 4, 2]_2$ code.

Example 4.2. (Separable Type I) Let $\mathcal{C}_2$ be $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code of type $(8, 1; 4, 0, 1)$ with the generator matrix,

$$G_2 = \left(\begin{array}{cccccccc|c} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & u \end{array}\right).$$

$\mathcal{C}_2$ is a separable Type I code and $\Phi(\mathcal{C}_2)$ is a self-dual $[10, 5, 2]_2$ code with weight enumerator $1 + z^2 + 14z^4 + 14z^6 + z^8 + z^{10}$. Moreover, if we add $(0\ \ 0\ \ 0\ \ 0\ \ u)$ as a last column to G_2, then we have separable Type II, $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code of type $(8, 2; 4, 0, 1)$ and the parameters of the binary image of this new self-dual code is $[12, 5, 4]$, which is optimal.

Example 4.3. (Separable Type I) Let $\mathcal{C}_3$ be $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code of type $(8, 6; 4, 3, 0)$ with the generator matrix,

$$G_3 = \left(\begin{array}{cccccccc|cccccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & u & u & 1+u \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1+u & u & u \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & u & 1+u & u \end{array}\right).$$

Then $\mathcal{C}_3$ is a separable Type I code and $\Phi(\mathcal{C}_3)$ is a self-dual Type I $[20,10,4]_2$ code with weight enumerator

$$1+29z^4+32z^6+226z^{10}+448z^{12}+226z^{14}+32z^{16}+29z^{18}+z^{20}.$$

The automorphism group of the code is of order $2^{15}\times 3^3\times 5\times 7$.

Example 4.4. (Non-separable Type I) Let $\mathcal{C}_4$ be $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code of type $(4,5;2,2,1)$ with the generator matrix,

$$G_4=\left(\begin{array}{cccc|ccccc} 1 & 0 & 1 & 0 & 0 & 0 & u & u & u\\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & u & u\\ \hline 0 & 0 & 1 & 1 & 1 & 0 & 0 & u & 1+u\\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1+u & u\\ 1 & 1 & 1 & 1 & 0 & 0 & u & 0 & 0 \end{array}\right).$$

Then $\mathcal{C}_4$ is a self-dual non-separable Type I code. The binary image is the unique self-dual Type I $[14,7,4]_2$ optimal code with weight enumerator $1+10z^4+21z^6+21z^8+10z^{10}+z^{14}$ with an automorphism group of order $2^8\times 3^2\times 5$.

Example 4.5. (Separable Type II) Let $\mathcal{C}_5\subseteq\mathbb{Z}_2^8\times R^4$ be a self-dual code with generator matrix G_5.

$$G_5=\left(\begin{array}{cccccccc|cccc} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0\\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & u & 0 & u\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & u & u \end{array}\right).$$

Therefore, $\mathcal{C}_5$ is a separable Type II code. Then $\Phi(\mathcal{C}_5)$ is a self-dual Type II $[16,8,4]_2$ code with weight enumerator $1+28z^4+198z^8+28z^{12}+z^{16}$. The code has an automorphism group of order $2^{13}\times 3^2\times 7^2$. Note that, $\mathcal{C}_r$ is the extended binary Hamming code of length 8.

Example 4.6. (Non-separable Type II) Let $\mathcal{C}_6$ be the $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code with the generator matrix:

$$G_6=\left(\begin{array}{cccccccc|cccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & u\\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & u\\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & u\\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & u\\ \hline 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1+u\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & u & 0 & u\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & u & u \end{array}\right).$$

Then $\mathcal{C}_6$ is a non-separable self-dual Type II code. The binary image of $\mathcal{C}_6$ is a self-dual Type II code of parameters $[16,8,4]_2$. The code has the same weight enumerator with $\mathcal{C}_5$ in the previous example. $\Phi(\mathcal{C}_6)$ has an automorphism group of order $2^{14}\times 3^2\times 5\times 7$. Therefore it is not equivalent to $\Phi(\mathcal{C}_5)$.

References

[1] Abualrub, T., Siap, I. and Aydin, N.,$\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, *IEEE Trans. Inform. Theory*, Vol. 60, No. 3, pp. 1508-1514, Mar. 2014.

[2] Abualrub, T. and Siap, I., Cyclic codes over the rings $\mathbb{Z}_2+u\mathbb{Z}_2$ and $\mathbb{Z}_2+u\mathbb{Z}_2+u^2\mathbb{Z}_2$, *Designs Codes and Cryptography*. Vol.42, No.3, 273-287(2007).

[3] Aydogdu, I. and Siap, I., The Structure of $\mathbb{Z}_2\mathbb{Z}_{2^s}-$Additive Codes: Bounds on the minimum distance, *Applied Mathematics and Information Sciences*,7, (6), 2271-2278, 2013.

[4] Aydogdu, I., Abualrub, T. and Siap, I., On $\mathbb{Z}_2\mathbb{Z}_2[u]-$additive codes, International Journal of Computer Mathematics, vol.92, no. 9, pp. 1806-1814, 2015.

[5] Bonnecaze, A. and Udaya, P., Cyclic codes and self-dual codes over $\mathbb{F}_2+u\mathbb{F}_2$, *IEEE Trans. Inform. Theory*. Vol.45, No.4, 1250-1255, 1999.

[6] Borges, J., Fernández-Córdoba, C., Pujol, J., Rifà, J. and Villanueva, M., $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: Generator Matrices and Duality, *Designs, Codes and Cryptography*, 54, (2), 167-179, 2010.

[7] J. H. Conway, and N. J. A. Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE Trans. Inform. Theory*, Vol. 36, No. 6, pp. 1319–1333, 1990.

[8] S.T. Dougherty, P. Gaborit, M. Harada and P. Solé, Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$, *IEEE Trans. Inform. Theory*, Vol. 45, pp.32-45, 1999.

[9] Grassl, M., Code tables: Bounds on the parameters of various types of codes, Online database. Available at http://www.codetables.de/

[10] Kaya, A. Yildiz, B., New extremal binary self-dual codes of length 68, *J. Algebra Comb. Discrete Appl.*, Vol. 1, No. 1, 29-39, 2014.

[11] Qian, J.F., Zhang, L.N. and Zhu, S.X., $(1+u)$-constacyclic and cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$, *Applied Math. Letters* 19 (2006) 820-823.

Affiliations

Ismail Aydogdu
Address: Yildiz Technical University, Dept. of Mathematics, 34210, Istanbul-Turkey.
e-mail: iaydogdu@yildiz.edu.tr

Abidin Kaya
Address: Sampoerna Academy, L'Avenue Campus, 12780, Jakarta, Indonesia.
e-mail: abidinkaya@mail.com