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

Ismail Aydogdu
Department of Mathematics

$\mathbb{Z}_2\mathbb{Z}_4$-additive 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 $\alpha + 2\beta = n$.

$\mathbb{Z}_2\mathbb{Z}_4$-additive 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 $\alpha + 2\beta = n$.
If $\beta = 0$ then $\mathbb{Z}_2\mathbb{Z}_4$- additive codes are just binary linear codes, and if $\alpha = 0$, then $\mathbb{Z}_2\mathbb{Z}_4$- additive codes are the quaternary linear codes over $\mathbb{Z}_4$.

The ring $\mathbb{Z}_2 + u\mathbb{Z}_2$

Another important ring of four elements is the ring $\mathbb{Z}_2 + u\mathbb{Z}_2 = R = \{0, 1, u, u+1\}$ where $u^2 = 0$.

The ring $\mathbb{Z}_2 + u\mathbb{Z}_2$

Another important ring of four elements is the ring $\mathbb{Z}_2 + u\mathbb{Z}_2 = R = \{0, 1, u, u+1\}$ where $u^2 = 0$.
It has been shown that linear and cyclic codes over this ring have advantages compared to the ring $\mathbb{Z}_4$.

The ring $\mathbb{Z}_2 + u\mathbb{Z}_2$

Another important ring of four elements is the ring $\mathbb{Z}_2 + u\mathbb{Z}_2 = R = \{0, 1, u, u+1\}$ where $u^2 = 0$.
It has been shown that linear and cyclic codes over this ring have advantages compared to the ring $\mathbb{Z}_4$.
Some of theses advantages are:

- The finite field $GF(2)$ is a subring of the ring R. So factorization over $GF(2)$ is still valid over the ring R.

- The finite field $GF(2)$ is a subring of the ring R. So factorization over $GF(2)$ is still valid over the ring R.
- The Gray image of any linear codes over R is always a binary linear codes (That is not always the case for $\mathbb{Z}_4$).

- The finite field $GF(2)$ is a subring of the ring R. So factorization over $GF(2)$ is still valid over the ring R.
- The Gray image of any linear codes over R is always a binary linear codes (That is not always the case for $\mathbb{Z}_4$).
- Decoding algorithm of cyclic codes over R is easier than over $\mathbb{Z}_4$).

What Did We Do?

- In this work, we are interested in studying linear codes over $\mathbb{Z}_2\left(\mathbb{Z}_2 + u\mathbb{Z}_2\right)$ which are R-submodules of $\mathbb{Z}_2^{\alpha}R^{\beta}$.

What Did We Do?

- In this work, we are interested in studying linear codes over $\mathbb{Z}_2\left(\mathbb{Z}_2 + u\mathbb{Z}_2\right)$ which are R-submodules of $\mathbb{Z}_2^{\alpha}R^{\beta}$.
- We also investigate structure of self-dual codes over these submodules.

- The structure of such a submodule is a little bit different than the structure of $\mathbb{Z}_2\mathbb{Z}_4$ in the sense that for any element $a \in \mathbb{Z}_4$ the standard multiplication $a\mathbb{Z}_2$ is well defined to be an element in $\mathbb{Z}_2$.

- The structure of such a submodule is a little bit different than the structure of $\mathbb{Z}_2\mathbb{Z}_4$ in the sense that for any element $a \in \mathbb{Z}_4$ the standard multiplication $a\mathbb{Z}_2$ is well defined to be an element in $\mathbb{Z}_2$.
- But for $\mathbb{Z}_2\left(\mathbb{Z}_2 + u\mathbb{Z}_2\right)$ that is not the case. For example if $u \in \mathbb{Z}_2 + u\mathbb{Z}_2$, the standard multiplication $u \cdot 1 = u \notin \mathbb{Z}_2$.

- The structure of such a submodule is a little bit different than the structure of $\mathbb{Z}_2\mathbb{Z}_4$ in the sense that for any element $a \in \mathbb{Z}_4$ the standard multiplication $a\mathbb{Z}_2$ is well defined to be an element in $\mathbb{Z}_2$.
- But for $\mathbb{Z}_2\left(\mathbb{Z}_2 + u\mathbb{Z}_2\right)$ that is not the case. For example if $u \in \mathbb{Z}_2 + u\mathbb{Z}_2$, the standard multiplication $u \cdot 1 = u \notin \mathbb{Z}_2$.
- Hence, in studying linear codes over $\mathbb{Z}_2\left(\mathbb{Z}_2 + u\mathbb{Z}_2\right)$ our first step was to introduce a well-defined multiplication of $u\mathbb{Z}_2 \in \mathbb{Z}_2$. Then based on this multiplication, we will define linear codes over $\mathbb{Z}_2\left(\mathbb{Z}_2 + u\mathbb{Z}_2\right)$.

Well-defined Multiplication Over $\mathbb{Z}_2 R$

Let $n = \alpha + 2\beta$ where $\alpha,\ \beta$ are positive integers. Consider the finite field $\mathbb{Z}_2 = \{0, 1\}$ and the finite ring $R = \{0, 1, u, u+1\}$ where $u^2 = 0$.
It is known that the ring $\mathbb{Z}_2$ is a subring of the ring R. We define the set

Well-defined Multiplication Over $\mathbb{Z}_2 R$

Let $n = \alpha + 2\beta$ where $\alpha,\ \beta$ are positive integers. Consider the finite field $\mathbb{Z}_2 = \{0, 1\}$ and the finite ring $R = \{0, 1, u, u+1\}$ where $u^2 = 0$.
It is known that the ring $\mathbb{Z}_2$ is a subring of the ring R. We define the set

$$\mathbb{Z}_2 R = \{(e_1, e_2) \mid e_1 \in \mathbb{Z}_2 \text{ and } e_2 \in R\}.$$

Further define the mapping

$$\eta : R \to \mathbb{Z}_2$$
$$\eta\left(r + uq\right) = r.$$

i.e., $\eta(0) = 0,\ \eta(1) = 1,\ \eta(u) = 0$ and $\eta(u+1) = 1.$

Further define the mapping

$$\eta : R \to \mathbb{Z}_2$$
$$\eta\left(r + uq\right) = r.$$

i.e., $\eta(0) = 0$, $\eta(1) = 1$, $\eta(u) = 0$ and $\eta(u+1) = 1$.
It is clear that the mapping η is a ring homomorphism. Now for any element $d \in R$, define the following R-scalar multiplication on $\mathbb{Z}_2 R$ as

Further define the mapping

$$\eta : R \to \mathbb{Z}_2$$
$$\eta\left(r + uq\right) = r.$$

i.e., $\eta(0) = 0,\ \eta(1) = 1,\ \eta(u) = 0$ and $\eta(u+1) = 1.$
It is clear that the mapping η is a ring homomorphism. Now for any element $d \in R$, define the following R-scalar multiplication on $\mathbb{Z}_2 R$ as

$$d\left(e_1, e_2\right) = \left(\eta(d)e_1, de_2\right).$$

Definition

This is a well-defined scalar multiplication. In fact this multiplication can be extended over $\mathbb{Z}_2^\alpha \times R^\beta$ in the following way: for any $d \in R$ and $v = (a_0, a_1, ..., a_{\alpha-1,} b_0, b_1, ..., b_{\beta-1}) \in \mathbb{Z}_2^\alpha \times R^\beta$

Definition

This is a well-defined scalar multiplication. In fact this multiplication can be extended over $\mathbb{Z}_2^\alpha \times R^\beta$ in the following way: for any $d \in R$ and $v = (a_0, a_1, ..., a_{\alpha-1,} b_0, b_1, ..., b_{\beta-1}) \in \mathbb{Z}_2^\alpha \times R^\beta$

$$dv = \left(\eta(d)a_0, \eta(d)a_1, ..., \eta(d)a_{\alpha-1,} db_0, db_1, ..., db_{\beta-1}\right).$$

Lemma

$\mathbb{Z}_2^\alpha \times R^\beta$ is an $R-$module under the above definition.

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

Definition (Aydogdu et. al.)

A non-empty subset $\mathcal{C}$ of $\mathbb{Z}_2^\alpha \times R^\beta$ is called a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code if $\mathcal{C}$ is an R-submodule of $\mathbb{Z}_2^\alpha \times R^\beta$.

Differences Between $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear Codes and $\mathbb{Z}_2\mathbb{Z}_4$-additive Codes

- In the case of $\mathbb{Z}_2\mathbb{Z}_4-$additive codes, subgroups of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ are the same as $\mathbb{Z}_4$-submodules of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ and hence a non-empty subset $\mathcal{C}$ of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is called a $\mathbb{Z}_2\mathbb{Z}_4$-additive code if $\mathcal{C}$ is a subgroup (or $\mathbb{Z}_4-$submodule) of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$.

Differences Between $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear Codes and $\mathbb{Z}_2\mathbb{Z}_4$-additive Codes

- In the case of $\mathbb{Z}_2\mathbb{Z}_4-$additive codes, subgroups of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ are the same as $\mathbb{Z}_4$-submodules of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ and hence a non-empty subset $\mathcal{C}$ of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is called a $\mathbb{Z}_2\mathbb{Z}_4$-additive code if $\mathcal{C}$ is a subgroup (or $\mathbb{Z}_4-$submodule) of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$.
- On the other hand, subgroups of $\mathbb{Z}_2^\alpha \times R^\beta$ are different than $R-$submodules of $\mathbb{Z}_2^\alpha \times R^\beta$. The subgroups of $\mathbb{Z}_2^\alpha \times R^\beta$ are closed only under binary operation while submodules are subgroups of $\mathbb{Z}_2^\alpha \times R^\beta$ that are also closed under multiplications by elements in the ring R.

Differences Between $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear Codes and $\mathbb{Z}_2\mathbb{Z}_4$-additive Codes

- In the case of $\mathbb{Z}_2\mathbb{Z}_4-$additive codes, subgroups of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ are the same as $\mathbb{Z}_4$-submodules of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ and hence a non-empty subset $\mathcal{C}$ of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is called a $\mathbb{Z}_2\mathbb{Z}_4$-additive code if $\mathcal{C}$ is a subgroup (or $\mathbb{Z}_4-$submodule) of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$.
- On the other hand, subgroups of $\mathbb{Z}_2^\alpha \times R^\beta$ are different than $R-$submodules of $\mathbb{Z}_2^\alpha \times R^\beta$. The subgroups of $\mathbb{Z}_2^\alpha \times R^\beta$ are closed only under binary operation while submodules are subgroups of $\mathbb{Z}_2^\alpha \times R^\beta$ that are also closed under multiplications by elements in the ring R.
- This is the reason for referring to them as $\mathbb{Z}_2\mathbb{Z}_2[u]-$linear codes and not additive codes as the case of $\mathbb{Z}_2\mathbb{Z}_4$.

- For $a \in R$, there exists unique $r_1, q_1 \in \mathbb{Z}_2$ such that $a = r_1 + uq_1$.
- We note that the ring R is isomorphic $\mathbb{Z}_2^2$ as an additive group.
- Hence, if $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_2[u]-$linear code then it is isomorphic to a group of the form $\mathbb{Z}_2^{k_0} \times \mathbb{Z}_2^{2k_1} \times \mathbb{Z}_2^{k_2}$ for some positive integers k_0 and k_1.

Let $\mathcal{C}_\beta^F$ be the submodule,

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

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

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

Now, denote the dimension of $\mathcal{C}_0$ as a k_0 and denote the dimension of $\mathcal{C}_1$ as a k_2.
Based on this discussion we have the following definition.

Type of $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear Codes

Definition

If $\mathcal{C} \subseteq \mathbb{Z}_2^{\alpha} \times R^{\beta}$ is a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code, group isomorphic to $\mathbb{Z}_2^{k_0} \times \mathbb{Z}_2^{2k_1} \times \mathbb{Z}_2^{k_2}$, then $\mathcal{C}$ is called a $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive(linear) code of type $(\alpha, \beta, k_0, k_1, k_2)$ where k_0, k_1, and k_2 are defined above.

The Gray Map

Definition

For $r_1 + uq_1 = a \in R$, $r_1, q_1 \in \mathbb{Z}_2$. Define the Gray map

$$\Phi : \mathbb{Z}_2^\alpha \times R^\beta \to \mathbb{Z}_2^n$$

$$\begin{aligned} &\Phi\left(x_0, \ldots x_{\alpha-1}, r_0 + uq_0, \ldots r_{\beta-1} + uq_{\beta-1}\right) \\ &\qquad = \left(x_0, \ldots x_{\alpha-1}, q_0, \ldots, q_{\beta-1}, r_0 \oplus q_0, \ldots, r_{\beta-1} \oplus q_{\beta-1}\right) \end{aligned}$$

where $r_i \oplus q_i = r_i + q_i \mod 2$ and $n = \alpha + 2\beta$.

- The map Φ is an isometry which transforms the Lee distance in $\mathbb{Z}_2^\alpha \times R^\beta$ to the Hamming distance in $\mathbb{Z}_2^n$.
- Moreover, for any $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code $\mathcal{C}$, we have that $\Phi(\mathcal{C})$ is a binary linear code as well.
- This property is not valid for the $\mathbb{Z}_2\mathbb{Z}_4-$additive codes. We always have

$$wt(v) = wt_H(v_1) + wt_L(v_2)$$

where $wt_H(v_1)$ is the Hamming of weight of v_1 and $wt_L(v_2)$ is the Lee weight of v_2.

Definition

The binary image $C = \Phi(\mathcal{C})$ of a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code $\mathcal{C}$ of type $(\alpha, \beta, k_0, k_1, k_2)$ is a binary linear code of length $n = \alpha + 2\beta$ and size 2^n. It is also called a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code.

The Standard Form of Generator Matrices

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

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

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

The Standard Form of Parity-check Matrices

Theorem

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

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

Inner Product

For any elements

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

define the inner product

$$\langle v, w \rangle = \left(u \sum_{i=0}^{\alpha-1} a_i d_i + \sum_{j=0}^{\beta-1} b_j e_j \right) \in \mathbb{Z}_2 + u\mathbb{Z}_2.$$

The Dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear Code $\mathcal{C}^\perp$

Definition

Let $\mathcal{C}$ be any $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code. Define the dual of $\mathcal{C}$ to be the code

$$\mathcal{C}^\perp = \left\{ w \in \mathbb{Z}_2^\alpha \times R^\beta \middle| \ \langle v, w \rangle = 0 \ \forall v \in \mathcal{C} \right\}.$$

The Dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear Code $\mathcal{C}^\perp$

Definition

Let $\mathcal{C}$ be any $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code. Define the dual of $\mathcal{C}$ to be the code

$$\mathcal{C}^\perp = \left\{ w \in \mathbb{Z}_2^\alpha \times R^\beta \middle| \ \langle v, w \rangle = 0 \ \forall v \in \mathcal{C} \right\}.$$

Corollary

If $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code of type $(\alpha, \beta; k_0; k_1, k_2)$ then dual code $\mathcal{C}^\perp$ is of type $(\alpha, \beta; \alpha - k_0; \beta - k_1 - k_2, k_2)$.

Weight Enumerators

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code of type$(\alpha, \beta; k_0; k_1, k_2)$ with $n = \alpha + 2\beta$. Then 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

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:

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

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

Lemma

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

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

Lemma

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,

$$(\alpha, \beta; k_0; k_1, k_2) = (\alpha, \beta; \alpha - k_0; \beta - k_1 - k_2, k_2)$$

and we have $\alpha = 2k_0$ and $\beta = 2k_1 + k_2$. $\square$

Corollary

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

Corollary

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

Corollary

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

Lemma

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

Lemma

Let $\mathcal{C}$ be a self-dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code. Let $\mathcal{C}_\alpha$ be the punctured code of $\mathcal{C}$ by deleting the coordinates outside α. Denote the binary subcode of $\mathcal{C}$ by $(\mathcal{C}_b)$ which actually contains all order two codewords and denote the dimension of $(\mathcal{C}_b)_\alpha$ by k_0. Then $(\mathcal{C}_b)_\alpha$ 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, $(\mathcal{C}_b)_\alpha$ has dimension k_0 and is of length $2k_0$. Hence we have $(\mathcal{C}_b)_\alpha$ is self-dual. □

Separable $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear Codes

Definition

Let $\mathcal{C}$ be $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code. Let $\mathcal{C}_\alpha$(respectively $\mathcal{C}_\beta$) be the punctured code of $\mathcal{C}$ by deleting the coordinates outside α (respectively β). If $\mathcal{C} = \mathcal{C}_\alpha \times \mathcal{C}_\beta$ then $\mathcal{C}$ is called separable.

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

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

Theorem

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.

Theorem

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.

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

Theorem

If $\mathcal{C}$ is a binary self-dual code of length α and $\mathcal{D}$ is a self-dual code over R of length β. Then $\mathcal{C} \times \mathcal{D}$ is a self-dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code of length $\alpha + \beta$.

Theorem

If $\mathcal{C}$ is a binary self-dual code of length α and $\mathcal{D}$ is a self-dual code over R of length β. Then $\mathcal{C} \times \mathcal{D}$ is a self-dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code of length $\alpha + \beta$.

Proof.

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

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

Therefore, $\mathcal{C} \times \mathcal{D}$ is self-orthogonal. $\square$

Lemma

Let $\mathcal{C}$ and $\mathcal{D}$ are self-dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear codes of type $(\alpha, \beta; k_0; k_1, k_2)$ and $(\alpha', \beta'; k_0'; k_1', k_2')$ respectively. Then $\mathcal{C} \times \mathcal{D}$ is a self-dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code of type $(\alpha + \alpha', \beta + \beta'; k_0 + k_0'; k_1 + k_1', k_2 + k_2')$.

Lemma

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

Corollary

There exists self-dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear codes of type $(\alpha, \beta; k_0; k_1, k_2)$ for all even α and all β.

Type 0, Type I and Type II $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear Codes

Definition

Let $\mathcal{C}$ be a self-dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code.

Type 0, Type I and Type II $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear Codes

Definition

Let $\mathcal{C}$ be a self-dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code.

- If codewords of $\mathcal{C}$ have an odd weights then $\mathcal{C}$ is called Type 0.
- If $\mathcal{C}$ has only even weights then it is said to be Type I.
- If all codewords of $\mathcal{C}$ have the doubly-even weight then it is said to be Type II.

Definition

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 $(1^\alpha, u^\beta) \in \mathcal{C}$.

Theorem

Let $\mathcal{C} \subseteq \mathbb{Z}_2^\alpha \times R^\beta$ 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 $(1^\alpha, u^\beta) \in \mathcal{C}$ and also it is obvious that $(0^\alpha, u^\beta) \in \mathcal{C}$. Therefore we have, $\mathcal{C}$ is antipodal if and only if $(1^\alpha, 0^\beta) \in \mathcal{C}$. This means that all codewords of $\mathcal{C}_\alpha$ have even weight. □

Theorem

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.

Theorem

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 $\mathcal{C} = \mathcal{C}_\alpha \times \mathcal{C}_\beta$ is separable where $\mathcal{C}_\alpha$ and $\mathcal{C}_\beta$ are self-dual codes over $\mathbb{Z}_2^\alpha$ and R^β respectively. Hence $\mathcal{C}_\alpha$ contains all-1 vector and $\mathcal{C}_\beta$ contains all-u vector then $(1^\alpha, u^\beta) \in \mathcal{C}$. □

Theorem

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 $\mathcal{C} = \mathcal{C}_\alpha \times \mathcal{C}_\beta$ is separable where $\mathcal{C}_\alpha$ and $\mathcal{C}_\beta$ are self-dual codes over $\mathbb{Z}_2^\alpha$ and R^β respectively. Hence $\mathcal{C}_\alpha$ contains all-1 vector and $\mathcal{C}_\beta$ contains all-u vector then $(1^\alpha, u^\beta) \in \mathcal{C}$. □

Corollary

If $\mathcal{C}$ is a self-dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code of Type 0, then $\mathcal{C}$ is non-separable and non-antipodal.

Type 0

Example

Let

$$\mathcal{C}_0 = \{(0,0,0,0),(1,1,0,u),(0,1,1,1),(1,0,1,1+u),(0,0,u,u),\\ (1,1,u,0),(0,1,1+u,1+u),(1,0,1+u,1)\}$$

be a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code of type $(2,2;1;1,0)$. Then $\mathcal{C}_0$ is self-dual Type 0 code.

Separable Type I

Example

Let $\mathcal{C}_1$ be a 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 $[8,3,2]$-binary code.

Non-separable Type I

Example

A $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code $\mathcal{D}_1$ of type $(4,5;2;2,1)$ with the generator matrix,

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

is a self-dual non-separable Type I code.

Separable Type II

Example

Let $\mathcal{C}_2 \subseteq \mathbb{Z}_2^8 \times R^4$ be a self-dual code with generator matrix G_2.

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

Therefore, $\mathcal{C}_2$ is a separable Type II code. Note that, in the above generator matrix, $\mathcal{C}_\alpha$ is the binary extended Hamming code of length 8.

Non-separable Type II

Example

$\mathcal{D}_2$ is a non-separable Type II self-dual $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code with below generator matrix.

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

- I. Aydogdu, T. Abualrub and I. Siap *On $\mathbb{Z}_2\mathbb{Z}_2[u]-$additive codes*, International Journal of Computer Mathematics, doi:10.1080/00207160.2013.859854, (2014).
- S. T. Dougherty, J. Borges and Cristina Fernandez-Cordoba, *Self-Dual codes over $\mathbb{Z}_2 \times \mathbb{Z}_4$*, AMC, Vol. **6**, Number 4, 287-303, (2012).
- S. T. Dougherty, P. Gaborit, M. Harada, and P. Sole, *Type II codes over $F_2 + uF_2$*, IEEE Trans. Inform. Theory 45(1999), no.1, 32-45.
- T. Abualrub and I. Siap, *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).

- Abualrub, T., Siap, I. and Aydin, N.,"$\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes", IEEE Trans. Info. Theory, vol. 60, No. 3, pp. 1508-1514, Mar. 2014.
- 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(AMIS),7, (6), 2271-2278 2013.
- 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).
- 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.