We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,900
Open access books available

185,000
International authors and editors

200M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com

Chapter

$Z_2Z_2[u]$-Linear and $Z_2Z_2[u]$-Cyclic Codes

Ismail Aydogdu

Abstract

Additive codes were first introduced by Delsarte in 1973 as subgroups of the underlying abelian group in a translation association scheme. In the case where the association scheme is the Hamming scheme, that is, when the underlying abelian group is of order 2^n, the additive codes are of the form $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ with $\alpha + 2\beta = n$. In 2010, Borges et al. introduced $\mathbb{Z}_2\mathbb{Z}_4$-additive codes which they defined them as the subgroups of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$. In this chapter we introduce $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear and $\mathbb{Z}_2\mathbb{Z}_2[u]$-cyclic codes where $\mathbb{Z}_2 = \{0, 1\}$ is the binary field and $\mathbb{Z}_2[u] = \{0, 1, u, 1 + u\}$ is the ring with four elements and $u^2 = 0$. We give the standard forms of the generator and parity-check matrices of $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear codes. Further, we determine the generator polynomials for $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear cyclic codes. We also present some examples of $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear and $\mathbb{Z}_2\mathbb{Z}_2[u]$-cyclic codes.

Keywords: $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear codes, cyclic codes, generator matrix, duality, parity-check matrix, minimal spanning set

1. Introduction

In coding theory, the most important class of error-correcting codes is the family of linear codes, because the encoding and decoding procedures for a linear code are faster and simpler than those for arbitrary nonlinear codes. Many practically important linear codes have also an efficient decoding. Specifically, a linear code $\mathcal{C}$ of length n is a vector subspace of $\mathbb{F}_q^n$, where $\mathbb{F}_q$ is a finite field with q elements. Among all the codes over finite fields, binary linear codes (linear codes over $\mathbb{F}_2$) have a very special and important place because of their easy implementations and applications. In the beginning, researchers were mainly studying on linear codes over fields, especially binary fields. However, in 1994, a remarkable paper written by Hammons et al. [1] brought a new direction to studies on coding theory. In this paper, they showed that some well-known nonlinear codes, the Nordstrom-Robinson code, Kerdock codes, and Delsarte-Goethals code, are actually binary images of some linear codes over the ring of integers modulo, 4, i.e., $\mathbb{Z}_4$. Such connections motivate the researchers to study on codes over different rings even over other structural algebras such as groups or modules. Even though the structure of binary linear codes and quaternary linear codes (codes over $\mathbb{F}_4$ or $\mathbb{Z}_4$) have been studied in details for the last 50 years, recently, in 2010, a new class of error-correcting codes over the ring $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ called additive codes that generalizes the class of binary linear codes and the class of quaternary linear codes have been introduced by Borges et al. in [2]. A $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ is defined as a subgroup of

$\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, where α and β are positive integers and $\alpha + 2\beta = n$. Despite the fact that $\mathbb{Z}_2\mathbb{Z}_4$-additive codes are a new type of codes, they have shown to have some applications in fields such as the field of steganography. Another important ring of four elements which is not isomorphic to $\mathbb{Z}_4$ is the ring $\mathbb{Z}_2 + u\mathbb{Z}_2 = \{0, 1, u, 1+u\}$ $= \mathcal{R} = \mathbb{Z}_2[u]$ where $u^2 = 0$. Working with the ring $\mathcal{R}$ has some advantages compared to the ring $\mathbb{Z}_4$. For example, the Gray images of linear codes over $\mathcal{R}$ are always binary linear codes which is not always the case for $\mathbb{Z}_4$. Further, since the finite field $\mathbb{F}_2$ is a subring of the ring $\mathcal{R}$, the factorization of polynomials over $\mathcal{R}$ is the same with the factorization of polynomials over $\mathbb{F}_2$, so we do not need Hensel's lift for factorization. Moreover, decoding algorithm of cyclic codes over $\mathcal{R}$ is easier than that over $\mathbb{Z}_4$. In this chapter of the book, we introduce $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear and $\mathbb{Z}_2\mathbb{Z}_2[u]$-cyclic codes. The original study about linear and cyclic codes over $\mathbb{Z}_2\mathbb{Z}_2[u]$ was done by Aydogdu et al. in [3, 4]. So, this chapter is a survey on $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear and $\mathbb{Z}_2\mathbb{Z}_2[u]$-cyclic codes which were introduced in [3, 4].

2. $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear codes

Let $\mathbb{Z}_2 = \{0, 1\}$ be the finite field and $\mathcal{R} = \mathbb{Z}_2 + u\mathbb{Z}_2 = \{0, 1, u, 1+u\}$, $u^2 = 0$ be the finite ring of four elements. Since $\mathbb{Z}_2$ is a subring of $\mathcal{R}$, we define the following set:

$$\mathbb{Z}_2\mathcal{R} = \{(c_1, c_2) | c_1 \in \mathbb{Z}_2 \text{ and } c_2 \in \mathcal{R}\}$$

This set is not well defined with respect to the usual multiplication by $u \in \mathcal{R}$. So it is not an $\mathcal{R}$-module. Hence the set $\mathbb{Z}_2\mathcal{R}$ cannot be endowed with an algebraic structure directly. Therefore we introduce a new multiplication to make it well defined and enriched with an algebraic structure.

Let $d \in \mathcal{R}$; then d can be expressed in the form $d = r + uq$ with $r, q \in \mathbb{Z}_2$. We define the following map:

$$\begin{aligned} \eta &: \mathcal{R} \to \mathbb{Z}_2 \\ \eta(d) &= r = \overline{d} \end{aligned}$$

as $\eta(0) = 0$, $\eta(1) = 1$, $\eta(u) = 0$ and $\eta(1+u) = 1$. It is easy to see that the mapping η is a ring homomorphism. Now, using this map we define the following $\mathcal{R}$-scalar multiplication on $\mathbb{Z}_2\mathcal{R}$. For any element $d \in \mathcal{R}$:

$$d(c_1, c_2) = (\eta(d)c_1, dc_2) = (\overline{d}c_1, dc_2)$$

This new multiplication is well defined and also can be extended over $\mathbb{Z}_2^\alpha \times \mathcal{R}^\beta$ as follows. Let $d \in \mathcal{R}$ and $v = (a_0, a_1, \ldots, a_{\alpha-1}, b_0, b_1, \ldots, b^{\beta-1}) \in \mathbb{Z}_2^\alpha \times \mathcal{R}^\beta$; then define

$$\begin{aligned} dv &= (\eta(d)a_0, \eta(d)a_1, \ldots, \eta(d)a_{\alpha-1}, db_0, db_1, \ldots, db_{\beta-1}) \\ &= (\overline{d}a_0, \overline{d}a_1, \ldots, \overline{d}a_{\alpha-1}, db_0, db_1, \ldots, db_{\beta-1}). \end{aligned}$$

Lemma 2.1. $\mathbb{Z}_2^\alpha \times \mathcal{R}^\beta$ is an $\mathcal{R}$-module with respect to the multiplication defined above.

Definition 2.2. Let $\mathcal{C}$ be a non-empty subset of $\mathbb{Z}_2^\alpha \times \mathcal{R}^\beta$. $\mathcal{C}$ is called a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code if it is an $\mathcal{R}$-submodule of $\mathbb{Z}_2^\alpha \times \mathcal{R}^\beta$.

Note that the ring $\mathcal{R}$ is isomorphic to $\mathbb{Z}_2^2$ as an additive group. Therefore, any $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code $\mathcal{C}$ is isomorphic to a group of the form $\mathbb{Z}_2^{k_0+k_2} \times \mathbb{Z}_2^{2k_1}$, for some $k_0, k_1, k_2 \in \mathbb{Z}^+$. Now let us consider the following sets:

$$\mathcal{C}_\beta^F = \langle \{(a,b) \in \mathbb{Z}_2^\alpha \times \mathcal{R}^\beta | b \text{ is free over } \mathcal{R}^\beta\} \rangle$$

where if $\langle b \rangle = \mathcal{R}^\beta$, then b is called free over $\mathcal{R}^\beta$:

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

Now, denote the dimension of $\mathcal{C}_0$, $\mathcal{C}_1$, and $\mathcal{C}_\beta^F$ as k_0, k_2, and k_1, respectively. Hence, if $\mathcal{C} \subseteq \mathbb{Z}_2^\alpha \times \mathcal{R}^\beta$ is a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code group isomorphic to $\mathbb{Z}_2^{k_0+k_2} \times \mathbb{Z}_2^{2k_1}$, then we say $\mathcal{C}$ is of type $(\alpha, \beta; k_0, k_1, k_2)$. We can consider any $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code $\mathcal{C}$ as a binary code under the special Gray map.

Definition 2.3. Let $(a_0, a_1, \ldots, a_{\alpha-1}, b_0, b_1, \ldots, b_{\beta-1}) \in \mathbb{Z}_2^\alpha \times \mathcal{R}^\beta$ with $b_i = p_i + uq_i$. We define the Gray map as follows:

$$\Psi : \mathbb{Z}_2^\alpha \times \mathcal{R}^\beta \to \mathbb{Z}_2^n$$
$$\Psi\left(a_0, a_1, \ldots, a_{\alpha-1}, p_0 + uq_0, p_1 + uq_1, \ldots, p_{\beta-1} + uq_{\beta-1}\right)$$
$$= \left(a_0, a_1, \ldots, a_{\alpha-1}, q_0, q_1, \ldots, q_{\beta-1}, p_0 + q_0, p_1 + q_1, \ldots, p_{\beta-1} + q_{\beta-1}\right)$$

where $n = \alpha + 2\beta$. The Gray map Ψ is an isometry which transforms the Lee distance in $\mathbb{Z}_2^\alpha \times \mathcal{R}^\beta$ to the Hamming distance in $\mathbb{Z}_2^n$. 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 a codeword is defined as the number of its non-zero entries, and the Lee weights of the elements of $\mathcal{R}$ are defined as $wt_L(0) = 0, wt_L(1) = 1, wt_L(u) = 2, wt_L(1+u) = 1$. It is worth mentioning that the Gray map Ψ is linear, i.e., for a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code $\mathcal{C}$, we have $\Psi(\mathcal{C})$ as a binary linear code which is not the case for $\mathbb{Z}_2\mathbb{Z}_4$-additive codes in general. We can extend the definition of the Lee weight of a codeword in $\mathcal{R}$ to the Lee weight of a codeword $v = (v_1, v_2) \in \mathbb{Z}_2^\alpha \times \mathcal{R}^\beta$ as follows:

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

where $wt_H(v_1)$ is the Hamming weight of v_1 and $wt_L(v_2)$ is the Lee weight of v_2. Further, the minimum distance of the $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code $\mathcal{C}$, denoted by $d(\mathcal{C})$, is naturally defined as

$$d(\mathcal{C}) = \min\{d(c_1, c_2) | c_1, c_2 \in \mathcal{C} \text{ such that } c_1 \neq c_2\}$$

where $d(c_1, c_2) = wt(c_1 - c_2)$. 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 Gray image $\Psi(\mathcal{C})$ 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.

2.1 Generator matrices of $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear codes

A generator matrix for a linear code $\mathcal{C}$ is the matrix G with rows that are formed by a minimal spanning set of $\mathcal{C}$. All linear combinations of the rows of the generator

matrix G constitute the linear code $\mathcal{C}$. We can produce an equivalent code to the $\mathcal{C}$ by applying elementary row and column operations on the generator matrix G. For given two linear codes, if one can be obtained from the other by permutation of their coordinates or (if necessary) changing the coordinates by their unit multiples, then these codes are said to be permutation equivalent code or only equivalent code. Furthermore, the standard form of the matrix G is a special form which is obtained by applying elementary row operations to G. Having the standard form of the generator matrix is very useful that we can easily determine the type of the code and then calculate its size directly. Note that the generator matrices in the standard form of linear codes over a ring contain the minimum number of rows. The theorem below determines the standard form of the generator matrix of a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code $\mathcal{C}$.

Theorem 2.1.1. [3] 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 $\mathcal{C}$ is a permutation equivalent to a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code with the following generator matrix of the standard form:

$$G_s = \begin{bmatrix} I_{k_0} & A_1 & 0 & 0 & uT \\ 0 & S & I_{k_1} & A & B_1 + uB_2 \\ 0 & 0 & 0 & uI_{k_2} & uD \end{bmatrix} \tag{1}$$

where A, A_1, B_1, B_2, T, and D are matrices with all entries from $\mathbb{Z}_2$ and I_{k_0}, I_{k_1}, and I_{k_2} are identity matrices with given sizes. Further $\mathcal{C}$ has $2^{k_0+2k_1+k_2}$ codewords.

Proof. It is well known that any linear code of length β over the ring $\mathcal{R} = \mathbb{Z}_2 + u\mathbb{Z}_2$ has the generator matrix of the form $\begin{bmatrix} I_{k_1} & A' & B_1' + uB_2' \\ 0 & uI_{k_2}' & uD' \end{bmatrix}$. Moreover, any binary linear code of length α can be generated by the matrix $\begin{bmatrix} I_{k_0}' & A_1' \end{bmatrix}$. Since $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code of length $\alpha + \beta$, then $\mathcal{C}$ can be generated by the following matrix:

$$\left[\underbrace{\begin{matrix} I_{k_0}' & A_1' \\ S_{01} & S_{02} \\ S_{11} & S_{12} \end{matrix}}_{\alpha} \;\middle|\; \underbrace{\begin{matrix} T_{01} & T_{02} & T_{03} \\ I_{k_1} & A' & B_1' + uB_2' \\ 0 & uI_{k_2}' & uD' \end{matrix}}_{\beta}\right]$$

with all binary entries. By applying the necessary row operations to the above matrix, we have the desired form.

Example 2.1.2. Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code with the generator matrix $\left[\begin{matrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{matrix} \middle| \begin{matrix} 1+u & 1+u \\ 1 & 1+u \end{matrix}\right]$. First, adding the second row to the first row, we have

$$\left[\begin{matrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{matrix} \middle| \begin{matrix} u & 0 \\ 1 & 1+u \end{matrix}\right].$$

Then multiplying the second row by u and adding it to first row, we have the following standard form of the generator matrix:

$$\left[\begin{array}{cc|cc} \boxed{1} & \boxed{0\quad 1} & \boxed{0} & \boxed{u} \\ \boxed{0} & \boxed{1\quad 1} & \boxed{1} & \boxed{1+u} \end{array}\right] = \left[\begin{array}{cc|cc} I_{k_0} & A_1 & 0 & uT \\ 0 & S & I_{k_1} & B_1+uB_2 \end{array}\right] \quad (2)$$

Therefore,

- $\mathcal{C}$ is of type $(3,2;1,1,0)$.
- $\mathcal{C}$ has $2^{1+2\cdot 1}=8$ codewords:

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

Moreover, the Gray image $\Psi(\mathcal{C})$ of $\mathcal{C}$ is a simplex code of length 7 with parameters [7, 3, 4] which is the dual of the well-known [7, 4, 3] Hamming code.

2.2 Duality on $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear codes and parity-check matrices

In the literature, there is a very well-known concept for the duals of the codes over finite fields and rings. If $\mathcal{C}$ is a linear code over $\mathbb{F}_q^n$, the dual code $\mathcal{C}^\perp$ of $\mathcal{C}$ in $\mathbb{F}_q^n$ is the set of all codewords that are orthogonal to every codeword of $\mathcal{C}$. A generator matrix for $\mathcal{C}^\perp$ is called a parity-check matrix of $\mathcal{C}$. In this part, we determine the standard form of the parity-check matrix of a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code $\mathcal{C}$. Let us begin with the definition of an inner product over $\mathbb{Z}_2^\alpha \times \mathcal{R}^\beta$.

Definition 2.2.1 Let v and w be the two elements in $\mathbb{Z}_2^\alpha \times \mathcal{R}^\beta$. The inner product of v and w is defined by

$$\langle v,w\rangle = u\left(\sum_{i=1}^{\alpha} v_i w_i\right) + \sum_{j=\alpha+1}^{\alpha+\beta} v_j w_j \in \mathcal{R}.$$

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

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

Hence, 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. It is worth mentioning that any two codewords of a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code may be orthogonal to each other, but the binary parts of the codewords may not be orthogonal. For example, $(1,1|\,1+u,u)$, $(0,1|\,u,u) \in \mathbb{Z}_2^2 \times \mathcal{R}^2$ are orthogonal to each other, whereas the binary or $\mathcal{R}$-components are not orthogonal. Moreover, the Gray map Ψ preserves the orthogonality.

We give the standard form of the parity-check matrices of $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear codes with the following theorem.

Theorem 2.2.2. [3] 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 the standard form generator matrix (1). Then the parity-check matrix of $\mathcal{C}$ (the generator matrix of the dual code $\mathcal{C}^\perp$) is given by

$$H_s = \begin{bmatrix} -A_1^t & I_{\alpha-k_0} & -uS^t & 0 & 0 \\ -T^t & 0 & -(B_1+uB_2)^t + D^tA^t & -D^t & I_{\beta-k_1-k_2} \\ 0 & 0 & -uA^t & uI_{k_2} & 0 \end{bmatrix}.$$

Furthermore, $|\mathcal{C}^{\perp}| = 2^{\alpha-k_0}2^{2(\beta-k_1-k_2)}2^{k_2}$.

Proof. It can be easily checked that $G_s \cdot H_s^t = 0$. Therefore every row of H_s is orthogonal to the rows of G_s. Further, since the generator matrices in the standard form of linear codes contain the minimum number of rows, $\mathcal{C}^{\perp}$ has $2^{\alpha-k_0}2^{2(\beta-k_1-k_2)}2^{k_2}$ codewords. Hence, $|\mathcal{C}\,|\,\mathcal{C}^{\perp}| = 2^{k_0}2^{2k_1}2^{k_2}2^{\alpha-k_0}2^{2(\beta-k_1-k_2)}2^{k_2} = 2^{\alpha+2\beta}$. So, the rows of the matrix H_s are not only orthogonal to $\mathcal{C}$, but also they generate all dual space.

Example 2.2.3. Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code of type $(3,2;1,1,0)$ with the standard form of the generator matrix in (2). Then the parity-check matrix of $\mathcal{C}$ is

$$\left[\begin{array}{cc|cc} -A_1^t & I_{3-1} & -uS^t & 0 \\ -T^t & 0 & -(B_1+uB_2)^t + D^tA^t & I_{2-1-0} \end{array}\right] = \left[\begin{array}{c|c|c|c} \begin{matrix}0\\1\end{matrix} & \begin{matrix}1 & 0\\0 & 1\end{matrix} & \begin{matrix}u\\u\end{matrix} & \begin{matrix}0\\0\end{matrix} \\ \boxed{1} & \boxed{\begin{matrix}0 & 0\end{matrix}} & \boxed{1+u} & \boxed{1} \end{array}\right].$$

Therefore, $\mathcal{C}^{\perp}$ is of type $(3,2;2,1,0)$ and has $2^2 2^{2\cdot 1}2^0 = 16$ codewords. The Gray image $\Psi(\mathcal{C}^{\perp})$ is a well-known Hamming code with parameters $[7,4,3]$.

Corollary 2.2.4. 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 $\mathcal{C}^{\perp}$ is of type $(\alpha,\beta;\alpha-k_0,\beta-k_1-k_2,k_2)$.

3. $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear cyclic codes

Cyclic codes form a very small but highly structured and important subset of the set of linear codes. In general, these codes are much easier to implement, and hence they have a very rich algebraic structure that allows them to be encoded and decoded in a relatively easier way. Since cyclic codes can be identified as ideals in a certain ring, they are also of considerable interest from an algebraic point of view. Cyclic codes over finite fields were first introduced by E. Prange in 1957 and 1959 with two Air Force Cambridge Research Laboratory reports. In this section we study the structure of $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear cyclic codes for a positive odd integer β. We give the generator polynomials and the spanning sets for a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear cyclic code $\mathcal{C}$.

Definition 3.1. An $\mathcal{R}$-submodule $\mathcal{C}$ of $\mathbb{Z}_2^{\alpha} \times \mathcal{R}^{\beta}$ is called a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear cyclic code if for any codeword $v = (a_0, a_1, \ldots, a_{\alpha-1}, b_0, b_1, \ldots, b_{\beta-1}) \in \mathcal{C}$, its cyclic shift $T(v) = (a_{\alpha-1}, a_0, \ldots, a_{\alpha-2}, b_{\beta-1}, b_0, \ldots, b_{\beta-2})$ is also in $\mathcal{C}$.

Lemma 3.2. If $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear cyclic code, then the dual code $\mathcal{C}^{\perp}$ is also a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear cyclic code.

Proof. Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear cyclic code and $w = (d_0, d_1, \ldots, d_{\alpha-1}, e_0, e_1, \ldots, e_{\beta-1}) \in \mathcal{C}^{\perp}$. We will show that $T(w) \in \mathcal{C}^{\perp}$. Since $w \in \mathcal{C}^{\perp}$, for $v = (a_0, a_1, \ldots, a_{\alpha-1}, b_0, b_1, \ldots, b_{\beta-1}) \in \mathcal{C}$, we have

$$\langle v, w\rangle = u(a_0d_0 + a_1d_1 + \cdots + a_{\alpha-1}d_{\alpha-1}) + (b_0e_0 + b_1e_1 + \cdots + b_{\beta-1}e_{\beta-1}) = 0.$$

Now, let $\theta = \mathrm{lcm}(\alpha,\beta)$. Since $\mathcal{C}$ is cyclic, then $T^{\theta}(v) = v$, and $T^{\theta-1}(v) = (a_1, a_2, \ldots, a_0, b_1, b_2, \ldots, b_0) = z \in \mathcal{C}$. Therefore,

$$\begin{aligned} 0 = \langle z, w\rangle &= u(a_1d_0 + a_2d_1 + \cdots + a_0d_{\alpha-1}) + \left(b_1e_0 + b_2e_1 + \cdots + b_0e_{\beta-1}\right) \\ &= u(a_0d_{\alpha-1} + a_1d_0 + \cdots + a_{\alpha-1}d_{\alpha-2}) + \left(b_0e_{\beta-1} + b_1e_0 + \cdots + b_{\beta-1}e_{\beta-2}\right) \\ &= \langle v, T(w)\rangle. \end{aligned}$$

Hence, $T(w) \in \mathcal{C}^{\perp}$ and so $\mathcal{C}^{\perp}$ is also cyclic.

Let $\mathcal{C} \subseteq \mathbb{Z}_2^{\alpha} \times \mathcal{R}^{\beta}$ and $v = \left(a_0, a_1, \ldots, a_{\alpha-1}, b_0, b_1, \ldots, b_{\beta-1}\right) \in \mathcal{C}$. $v \in \mathcal{C}$ can be identified with a module element consisting of two polynomials each from different rings in $\mathcal{R}_{\alpha,\beta} = \mathbb{Z}_2[x]/\langle x^{\alpha} - 1\rangle \times \mathcal{R}[x]/\langle x^{\beta} - 1\rangle$ such that

$$\begin{aligned} v(x) &= \left(a_0 + a_1x + \cdots + a_{\alpha-1}x^{\alpha-1}, b_0 + b_1x + \cdots + b_{\beta-1}x^{\beta-1}\right) \\ &= (a(x), b(x)). \end{aligned}$$

This identification gives a one-to-one correspondence between elements in $\mathbb{Z}_2^{\alpha} \times \mathcal{R}^{\beta}$ and elements in $\mathcal{R}_{\alpha,\beta}$.

Definition 3.3. Let $d(x) \in \mathcal{R}[x]$ and $(v(x), w(x)) \in \mathcal{R}_{a,\beta}$. We define the following scalar multiplication:

$$d(x) * (v(x), w(x)) = (d(x)v(x) \bmod u, d(x)w(x))$$

This multiplication is well defined, and moreover, $\mathcal{R}_{\alpha,\beta}$ is a $\mathcal{R}[x]$-module with respect to this multiplication.

The codewords of $\mathcal{C}$ may be represented as polynomials in $\mathcal{R}_{\alpha,\beta}$ by using the above identification. Thus, if $\mathcal{C} \subseteq \mathbb{Z}_2^{\alpha} \times \mathcal{R}^{\beta}$ is a cyclic code, then the element $v = \left(a_0, a_1, \ldots, a_{\alpha-1}, b_0, b_1, \ldots, b_{\beta-1}\right) \in \mathcal{C}$ can be viewed as

$$v(x) = \left(a_0 + a_1x + \cdots + a_{\alpha-1}x^{\alpha-1}, b_0 + b_1x + \cdots + b_{\beta-1}x^{\beta-1}\right) \in \mathcal{R}_{\alpha,\beta}.$$

Further, the property $T(v) = \left(a_{\alpha-1}, a_0, \ldots, a_{\alpha-2}, b_{\beta-1}, b_0, \ldots, b_{\beta-2}\right) \in \mathcal{C}$ translates to

$$x * v(x) = \left(a_{\alpha-1} + a_0x + \cdots + a_{\alpha-2}x^{\alpha-1}, b_{\beta-1} + b_0x + \cdots + b_{\beta-2}x^{\beta-1}\right) \in \mathcal{R}_{\alpha,\beta}.$$

Hence we give the following theorem.

Theorem 3.4. A code $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear cyclic code if and only if $\mathcal{C}$ is an $\mathcal{R}[x]$-submodule of $\mathcal{R}_{\alpha,\beta}$.

3.1 The generators and the spanning sets of $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear cyclic codes

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code. We know that both $\mathcal{C}$ and $\mathcal{R}[x]/\langle x^{\beta} - 1\rangle$ are $\mathcal{R}[x]$-modules. Then we define the following map:

$$\begin{aligned} &\Phi : \mathcal{C} \to \mathcal{R}[x]/\langle x^{\beta} - 1\rangle \\ &\Phi\left(f_1(x), f_2(x)\right) = f_2(x). \end{aligned}$$

It is clear that Φ is a module homomorphism where the $\mathrm{Im}(\Phi)$ is an $\mathcal{R}[x]$-submodule of $\mathcal{R}[x]/\langle x^{\beta} - 1\rangle$ and $\ker(\Phi)$ is a submodule of $\mathcal{C}$. Since $\Phi(\mathcal{C})$ is an ideal of the ring $\mathcal{R}[x]/\langle x^{\beta} - 1\rangle$, we have

$\Phi(\mathcal{C}) = \langle g(x) + ua(x)\rangle$ with $a(x) | g(x) | x^{\beta} - 1 \bmod 2$.

Further the kernel of Φ is

$$\ker(\Phi) = \{(f(x), 0) \in \mathcal{C} | f(x) \in \mathbb{Z}_2^{\alpha} \times \mathcal{R}^{\beta}\}.$$

Now, define the set

$$I = \{f(x) \in \mathbb{Z}_2[x]/\langle x^{\alpha} - 1\rangle | \ (f(x), 0) \in \ker(\Phi)\}.$$

It is clear that I is an ideal and hence a cyclic code in the ring $\mathbb{Z}_2[x]/\langle x^{\alpha} - 1\rangle$. So, by the well-known results about the generators of binary cyclic codes, I is generated by $f(x)$, i.e., $I = \langle f(x)\rangle$.

Now, let $(m(x), 0) \in \ker\Phi$. So, we have $m(x) \in I = \langle f(x)\rangle$, and hence $m(x) = k(x)f(x)$ for some polynomial $k(x) \in \mathbb{Z}_2[x]/\langle x^{\alpha} - 1\rangle$. Therefore $(m(x), 0) = k(x) * (f(x), 0)$, and this implies that $\ker\Phi$ is a submodule of $\mathcal{C}$ generated by one element of the form $(f(x), 0)$ with $f(x) | \ (x^{\alpha} - 1) \bmod 2$. Then by the First Isomorphism Theorem, we have

$$\mathcal{C}/\ker\Phi \cong \langle g(x) + ua(x)\rangle.$$

Let $(l(x), g(x) + ua(x)) \in \mathcal{C}$ such that $\Phi(l(x), g(x) + ua(x)) = \langle g(x) + ua(x)\rangle$. This discussion shows that any $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear cyclic code $\mathcal{C}$ can be generated as a $\mathcal{R}[x]$-submodule of $\mathcal{R}_{\alpha,\beta}$ by two elements of the form $(f(x), 0)$ and $(l(x), g(x) + ua(x))$ such that

$$d_1(x) * (f(x), 0) + d_2(x)(l(x), g(x) + ua(x))$$

where $d_1(x), d_2(x) \in \mathcal{R}[x]$. Since the polynomial $d_1(x)$ can be restricted to a polynomial in $\mathbb{Z}_2[x]$, we can write

$$\mathcal{C} = \langle (f(x), 0), (l(x), g(x) + ua(x))\rangle$$

with binary polynomials $f(x)$ and $l(x)$ where $f(x) | \ (x^{\alpha} - 1) \bmod 2$ and $a(x) | g(x) | \ (x^{\beta} - 1) \bmod 2$.

Theorem 3.1.1. [4] Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear cyclic code in $\mathcal{R}_{\alpha,\beta}$. Then $\mathcal{C}$ can be identified uniquely as $\mathcal{C} = \langle (f(x), 0), (l(x), g(x) + ua(x))\rangle$ where $f(x) | \ (x^{\alpha} - 1) \bmod 2$, $a(x) | g(x) | \ (x^{\beta} - 1) \bmod 2$, and $l(x)$ is a binary polynomial satisfying $\deg(l(x)) < \deg(f(x))$ and $f(x) | \left(\frac{x^{\beta}-1}{a(x)}\right) l(x) \bmod u$.

Proof. We can easily see from the above discussion and Theorem 11 in [5] that $\mathcal{C} = \langle (f(x), 0), (l(x), g(x) + ua(x))\rangle$ with the polynomials $f(x)$, $l(x)$, $g(x)$ and $a(x)$ are as stated in the theorem. So, we need to only show the uniqueness of the generator polynomials. Since $\langle f(x)\rangle$ and $\langle g(x) + ua(x)\rangle$ are cyclic codes over $\mathbb{Z}_2$ and over $\mathcal{R}$, respectively, this implies the uniqueness of the polynomials $f(x)$, $g(x)$ and $a(x)$. Now suppose that $\deg(l(x)) > \deg(f(x))$ with $\deg(l(x)) - \deg(f(x)) = t$. Let

$$\mathcal{D} = \langle (f(x), 0), (l(x) + x^t f(x), g(x) + ua(x))\rangle = \langle (f(x), 0), (l(x), g(x) + ua(x))\rangle + x^t * \langle (f(x), 0)\rangle.$$

Therefore $\mathcal{D} \subseteq \mathcal{C}$. On the other hand,

$$\langle l(x), g(x) + ua(x)\rangle = \langle l(x) + x^t f(x), g(x) + ua(x)\rangle - x^t * \langle (f(x), 0)\rangle.$$

So, $\mathcal{C} \subseteq \mathcal{D}$ and hence $\mathcal{D} = \mathcal{C}$.

Definition 3.1.2. Let $\mathcal{N}$ be an $\mathcal{R}$-module. A linearly independent subset $\mathcal{P}$ of $\mathcal{N}$ that spans $\mathcal{N}$ is called a basis of $\mathcal{N}$. If an $\mathcal{R}$-module has a basis, then it is called a free $\mathcal{R}$-module.

Note that for a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear cyclic code $\mathcal{C} = \langle (f(x), 0), (l(x), g(x) + ua(x)) \rangle$, if $g(x) \neq 0$, then $\mathcal{C}$ is a free $\mathcal{R}$-module. However, if $g(x) = 0$ and $a(x) \neq 0$, then it is not a free $\mathcal{R}$-module. But we can still present $\mathcal{C}$ with the minimal spanning sets. The following theorem determines the minimal spanning sets for a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear cyclic code $\mathcal{C}$.

Theorem 3.1.3. [4] Let $\mathcal{C} = \langle (f(x), 0), (l(x), g(x) + ua(x)) \rangle$ be a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear cyclic code in $\mathcal{R}_{\alpha,\beta}$ with $f(x), l(x), g(x),$ and $a(x)$ in Theorem 3.1.1. Let

$$S_1 = \bigcup_{i=0}^{\deg(h_f(x))-1} \{x^i (f(x), 0)\},$$
$$S_2 = \bigcup_{i=0}^{\deg(h_g(x))-1} \{x^i (l(x), g(x) + ua(x))\},$$
$$S_3 = \bigcup_{i=0}^{\deg(b(x))-1} \{x^i (h_g(x)l(x), uh_g(x)a(x))\}$$

where $f(x)h_f(x) = x^\alpha - 1, g(x)h_g(x) = x^\beta - 1$ and $g(x) = a(x)b(x)$. Then $S = S_1 \cup S_2 \cup S_3$ forms a minimal spanning set for $\mathcal{C}$ as an $\mathcal{R}$-module. Furthermore, $\mathcal{C}$ has $2^{\deg(h_f(x))} 4^{\deg(h_g(x))} 2^{\deg(b(x))}$ codewords.

Proof. Please see the proof of the Theorem 4 in [4].

Example 3.1.4. Let $\mathcal{C} = \langle (f(x), 0), (l(x), g(x) + ua(x)) \rangle$ be a $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear cyclic code in $\mathbb{Z}_2[x]/\langle x^7 - 1 \rangle \times \mathcal{R}[x]/\langle x^7 - 1 \rangle$ with the following generator polynomials:

$$f(x) = x^7 - 1, l(x) = 1 + x^2 + x^3$$
$$g(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6, a(x) = 1 + x^2 + x^3.$$

Therefore, we have $g(x) = a(x)b(x) \Rightarrow b(x) = 1 + x + x^3$ and $g(x)h_g(x) = x^7 - 1 \Rightarrow h_g(x) = 1 + x$. Hence by using the minimal spanning sets in Theorem 3.1.3, we can write the generator matrix for the $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear cyclic code $\mathcal{C}$ as follows:

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1+u & 1 & 1+u & 1+u & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & u & u & u & 0 & u & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & u & u & u & 0 & u & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & u & u & u & 0 & u \end{bmatrix}.$$

It is worth mentioning that the Gray image $\Phi(\mathcal{C})$ of $\mathcal{C}$ is a linear binary code with the parameters [21, 5, 10], which are optimal. If the code $\mathcal{C}$ has the best minimum distance compared to the existing bounds for fixed length and the size, then $\mathcal{C}$ is called optimal or good parameter code.

Example 3.1.5. Let us consider the cyclic code $\mathcal{C} = \langle (f(x), 0), (l(x), g(x) + ua(x)) \rangle$ in $\mathbb{Z}_2[x]/\langle x^7 - 1 \rangle \times \mathcal{R}[x]/\langle x^9 - 1 \rangle$ with generators:

$$f(x) = 1 + x^2 + x^3 + x^4, l(x) = 1 + x + x^3,$$
$$g(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8, a(x) = 1 + x + x^2.$$

Again by using the minimal spanning sets in the above theorem, we have the following generator matrix for $\mathcal{C}$:

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1+u & 1+u & 1+u & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & u & 0 & 0 & u & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & u & 0 & 0 & u & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & u & 0 & 0 & u & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & u & 0 & 0 & u & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & u & 0 & 0 & u & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & u & 0 & 0 & u \end{bmatrix}.$$

The Gray image $\Phi(\mathcal{C})$ of $\mathcal{C}$ is a $[25, 11, 4]$ linear binary code. Moreover we can write the standard form of this generator matrix as

$$G_s = \left[\begin{array}{cccc|cccc}
\overbrace{\begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix}}^{I_{k_0}} & \overbrace{\begin{matrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{matrix}}^{A_1} & \overbrace{\begin{matrix} 0 \\ 0 \\ 0 \end{matrix}}^{0} & \overbrace{\begin{matrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{matrix}}^{0} & \overbrace{\begin{matrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{matrix}}^{uT} \\
\underbrace{\begin{matrix} 0 & 0 & 0 \end{matrix}}_{0} & \underbrace{\begin{matrix} 1 & 1 & 0 & 1 \end{matrix}}_{S} & \underbrace{\begin{matrix} 1 \end{matrix}}_{I_{k_1}} & \underbrace{\begin{matrix} 1 & 1 & 1 & 1 & 1 & 1 \end{matrix}}_{A} & \underbrace{\begin{matrix} 1 & 1 \end{matrix}}_{B_1+uB_2} \\
\hline
\underbrace{\begin{matrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{matrix}}_{0} & \underbrace{\begin{matrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{matrix}}_{0} & \underbrace{\begin{matrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{matrix}}_{0} & \underbrace{\begin{matrix} u & 0 & 0 & 0 & 0 & 0 \\ 0 & u & 0 & 0 & 0 & 0 \\ 0 & 0 & u & 0 & 0 & 0 \\ 0 & 0 & 0 & u & 0 & 0 \\ 0 & 0 & 0 & 0 & u & 0 \\ 0 & 0 & 0 & 0 & 0 & u \end{matrix}}_{uI_{k_2}} & \underbrace{\begin{matrix} u & 0 \\ 0 & u \\ u & u \\ u & 0 \\ 0 & u \\ u & u \end{matrix}}_{uD}
\end{array}\right]$$

Hence $\mathcal{C}$ is of type $(7, 9; 3, 1, 6)$ and has $2^{11} = 2048$ codewords.

4. Conclusion

In this chapter we introduced $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear and $\mathbb{Z}_2\mathbb{Z}_2[u]$-cyclic codes. We determined the standard forms of the generator and parity-check matrices of $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear codes. We further gave the generator polynomials and minimal

spanning sets for $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear cyclic codes. We also presented some illustrative examples of both $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear codes and $\mathbb{Z}_2\mathbb{Z}_2[u]$-cyclic codes.

Acknowledgements

The author would like to thank professors Irfan Siap and Taher Abualrub for their valuable comments and suggestions to improve the quality of the chapter.

Author details

Ismail Aydogdu
Yildiz Technical University, Istanbul, Turkey

*Address all correspondence to: iaydogdu@yildiz.edu.tr

IntechOpen

© 2019 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

References

[1] Hammons AR, Kumar V, Calderbank AR, Sloane NJA, Solé P. The Z4-linearity of Kerdock, Preparata, Goethals, and related codes. IEEE Transactions on Information Theory. 1994;**40**:301-319

[2] Borges J, Fernández-Córdoba C, Pujol J, Rifà J, Villanueva M. Z2Z4-linear codes: Generator matrices and duality. Designs, Codes and Cryptography. 2010;**54**(2):167-179

[3] Aydogdu I, Abualrub T, Siap I. On Z2Z2[u]−additive codes. International Journal of Computer Mathematics. 2015; **92**(9):1806-1814

[4] Aydogdu I, Abualrub T, Siap I. Z2Z2[u]-cyclic and constacyclic codes. IEEE Transactions on Information Theory. 2017;**63**(8):4883-4893

[5] Abualrub T, Siap I, Aydin N. Z2Z4-additive cyclic codes. IEEE Transactions on Information Theory. 2014;**60**(3): 1508-1514