Z₂(Z₂+uZ₂)(Z₂+uZ₂+u²Z₂)-Additive Cyclic Codes

Zhihui Li
Department of Mathematics, School of Mathematics and Statistics, Shandong University of Technology, Zibo, China

Email address: li_zhihui1@163.com

To cite this article: Zhihui Li. Z₂(Z₂+uZ₂)(Z₂+uZ₂+u²Z₂)-Additive Cyclic Codes. Engineering Mathematics. Vol. 3, No. 2, 2019, pp. 30-39. doi: 10.11648/j.engmath.20190302.11

Received: June 14, 2019; Accepted: October 11, 2019; Published: October 25, 2019

Abstract: In this paper, we introduce the algebraic structure of Z₂(Z₂+uZ₂)(Z₂+uZ₂+u²Z₂)-additive codes and Z₂(Z₂+uZ₂)(Z₂+uZ₂+u²Z₂) -additive cyclic codes. Compared to the Z₂Z₂-linear codes, the Gray image of any Z₂(Z₂+uZ₂)(Z₂+uZ₂+u²Z₂) -linear code will always be a linear binary code. Therefore, we consider the Z₂(Z₂+uZ₂)(Z₂+uZ₂+u²Z₂) -additive cyclic codes as a (Z₂+uZ₂)(Z₂+u²Z₂) -submodule of Z₂(Z₂+uZ₂)(Z₂+u²Z₂). We give the definition of Z₂(Z₂+uZ₂)(Z₂+uZ₂+u²Z₂)-additive codes with generator matrices and parity-check matrices. Furthermore, we give the fundamental result on considering their additive cyclic codes with generator polynomials and spanning sets.

Keywords: Additive Codes, Cyclic Codes, Minimal Generating Set

1. Introduction

Codes over rings were introduced in early 1970s. However, this research topic had been widely and really concerned after a milestone paper written by Hammons et al. in 1994, which shown that some special classes of non-linear binary codes could be obtained as Gray images of linear codes over Z₄ [1]. Since then, several families of codes over finite rings have been studied by many scientists [2-4].

In 1973, Delsarte defined additive codes in terms of association schemes as the subgroups of the underlying abelian group [5]. In 2010, Borges et al. brought a new perspective to additive codes over rings, introducing ZZZ4- additive codes [6]. Under binary Hamming scheme, the underlying group of order 2^k isomorphic to Z₄α×Z₄β, where α and β are nonnegative integers. The subgroups of underlying group are called Z₄-Z₄-additive codes. Therefore, a Z₄-Z₄-additive code C is defined to be a subgroup of Z₄α×Z₄β, where α+2β=n. If α=0, then C are quaternary linear codes over Z₄ and if β=0, C are equivalent to binary linear codes. In 2014, Abualrub et al. studied Z₄-Z₄-additive cyclic codes and Z₂+uZ₂ -linear cyclic codes [7]. In 2015, Aydogdu et al. studied the Z₄-Z₄[u]-additive codes [8]. In 2016, Borges et al. researched the generator polynomials and dual codes of Z₂Z₄ -additive codes [9]. One year later, Aydogdu et al. studied the Z₄Z₄Z₄ₖ-cyclic codes [10], in which they introduced that if α, β and θ are odd integers, Z₄Z₄Z₄ₖ-cyclic codes is a Z₄ₖ-submodule of Z₄/(x₄α-1)×Z₄/(x₄β-1)×Z₄/(x₄θ-1) and give the minimal generating set for Z₄Z₄Z₄ₖ-cyclic code. In 2018, the binary images of Z₄Z₄Z₄ₖ-additive cyclic codes have been done also by Borges et al. [11]. Further, Ismail et al. discussed the structure properties of ZZZ₂₄s-additive cyclic codes [12].

In this paper, we will study some structure of Z₂(Z₂+uZ₂)(Z₂+uZ₂+u²Z₂) -additive cyclic codes, including their generator polynomials and spanning sets. The rest of this paper is organized as follows. In Section 2, some results on Z₂(Z₂+uZ₂)(Z₂+uZ₂+u²Z₂) -additive code are given, and associate these codes with submodules of Z₄α×(Z₂+uZ₂)β×(Z₂+uZ₂+u²Z₂)θ. Moreover, the generator matrices and parity-check matrices of Z₂(Z₂+uZ₂)(Z₂+uZ₂+u²Z₂) -additive codes are given in this section. In Section 3, the definition of Z₂(Z₂+uZ₂)(Z₂+uZ₂+u²Z₂) -additive cyclic codes and their generator polynomials and spanning sets are given.

Some examples are given to illustrate the main results appeared in this paper. Moreover, using the Gray map, some good binary linear codes can be obtained by...
Let $Z_2$ be the finite field of order 2, and let $R$ be the ring $Z_2 + uZ_2 = \{0, 1, u, 1+u\}$, where $u^2 = 0 \mod 2$, and let $S$ be the ring $Z_2 + uZ_2 + u^2Z_2 = \{0, 1, u, 1+u, 1+u^2, 1+u+u^2\}$, where $u^2 = 0 \mod 2$. Construct the following set

$$\mathcal{R} = Z_2^{\theta} \times (Z_2 + uZ_2)^{\theta} \times (Z_2 + uZ_2 + u^2Z_2)^{\theta}$$

$$= \{(m, v, w) | m \in Z_2^\theta, v \in (Z_2 + uZ_2)^\theta, w \in (Z_2 + uZ_2 + u^2Z_2)^\theta\}$$

Clearly, this set is closed under usual addition and it becomes an additive abelian group. Define the following multiplication for $(m, v, w) \in \mathcal{R}$ and $d \in S$, in order to make $\mathcal{R}$ closed under multiplication by elements from $S$,

$$d \cdot (m, v, w) = (dm \mod u, dv \mod u^2, dw) \quad \text{(2)}$$

Since $d \cdot (m, v, w) \in S$, it follows that $\mathcal{R}$ is a $S$-module with respect to this scalar multiplication.

Definition 1 A non-empty subset $C$ of $Z_2^\theta \times R_2^\theta \times S_2^\theta$ is called a $Z_2 RS$-additive code if it is a subgroup of $Z_2^\theta \times R_2^\theta \times S_2^\theta$.

Clearly, $C$ is a binary linear code of length $\alpha$ if $\beta = 0$ and $\theta = 0$, a $Z_2 R$-additive code of length $(\alpha, \beta)$ if $\theta = 0$ and a linear code of length $\theta$ over $S$ if $\alpha = 0$ and $\beta = 0$. The type of a $Z_2 RS$-additive code of block length $(\alpha, \beta, \theta)$ is defined as follows.

$$\Phi(m, v, w) = (m_0, \ldots, m_{\alpha-1}, \phi_1(v_0), \ldots, \phi_\beta(v_{\beta-1}), \phi_\theta(w_0), \ldots, \phi_\theta(w_{\theta-1}))$$

where

$$m = (m_0, m_1, \ldots, m_{\alpha-1}) \in Z_2^\alpha, \quad v = (v_0, v_1, \ldots, v_{\beta-1}) \in (Z_2 + uZ_2)^\beta$$

$$w = (w_0, w_1, \ldots, w_{\theta-1}) \in (Z_2 + uZ_2 + u^2Z_2)^\theta \quad \text{(6)}$$

Definition 2 A $Z_2 RS$-additive code $C$ of length $(\alpha, \beta, \theta)$ is called $Z_2 RS$-additive code of type $(\alpha, \beta, \theta, k_0, k_1, k_2, k_3, k_4, k_5)$, if $C$ is a group isomorphic to the abelian structure

$$Z_2^{k_0} \times R_2^{k_1} \times Z_2^{k_2} \times S_2^{k_3} \times R_2^{k_4} \times Z_2^{k_5} \quad \text{(3)}$$

From [13, 14], define $\phi : Z_2 + uZ_2 \to Z_2^2$ by $\phi(0) = (0, 0)$, $\phi(1) = (0, 1)$, $\phi(u) = (1, 1)$, $\phi(1+u) = (1, 0)$ and $\phi_2 : Z_2 + uZ_2 + u^2Z_2 \to Z_2^3$ by $\phi_2(0) = (0, 0, 0)$, $\phi_2(1) = (0, 1, 0)$, $\phi_2(u) = (1, 0, 0)$, $\phi_2(1+u) = (1, 1, 0)$, $\phi_2(u^2) = (1, 0, 1)$, $\phi_2(1+u+u^2) = (1, 0, 0)$.

By the maps $\phi$ and $\phi_2$, Gray map can be defined by

$$\Phi : Z_2^\theta \times R_2^\theta \times S_2^\theta \to Z_2^2 \quad \text{(4)}$$

where

$$m = (m_0, m_1, \ldots, m_{\alpha-1}) \in Z_2^\alpha, \quad v = (v_0, v_1, \ldots, v_{\beta-1}) \in (Z_2 + uZ_2)^\beta$$

$$w = (w_0, w_1, \ldots, w_{\theta-1}) \in (Z_2 + uZ_2 + u^2Z_2)^\theta \quad \text{(5)}$$

Let $F_q$ be the finite field with $q$ elements, a linear code of length $n$ over $F_q$ is a linear subspace of the vector space $F_q^n$.

The generator matrix of linear codes can be formed by the minimal spanning set of this linear code. Since the minimum spanning set of the linear codes is not unique, then the generator matrix of the linear codes is not unique. In this following, the paper gives the standard form of generator matrix of $Z_2 RS$-additive codes first.

Theorem 1 Let $C$ be a $Z_2 RS$-additive code of type $(\alpha, \beta, \theta, k_0, k_1, k_2, k_3, k_4, k_5)$. Then $C$ is permutation equivalent to a $Z_2 RS$-additive code with the standard form matrix.

$$[C] = 2^{k_0} \cdot 4^{k_1} \cdot 2^{k_2} \cdot 8^{k_3} \cdot 4^{k_4} \cdot 2^{k_5} \quad \text{(8)}$$

Define a inner product for the elements $u, v \in Z_2^\alpha \times R_2^\beta \times S_2^\theta$ as
\[ u \cdot v = u^\tau \left( \sum_{i=1}^{\alpha} u_i v_i \right) + u \left( \sum_{j=\alpha+1}^{\alpha+\beta+\theta} u_j v_j \right) + \sum_{k=\alpha+\beta+\theta+1}^{\alpha+2\beta+2\theta} u_k v_k \]  
(9)

The dual code \( C^\perp \) can be defined in usual way with respect to the inner product.

\[ C^\perp = \left\{ u \in Z_2^n \times R^\beta \times S^\theta \mid u \cdot v = 0 \text{ for all } u \in C \right\} \]  
(10)

It is obviously that \( C^\perp \) is also a \( Z_2R^S \)-additive code.

Corollary 1 Let \( C \) be a \( Z_2R^S \)-additive code of type with standard form generator matrix (7). Then, the code \( C^\perp \) is of type

\[ (\alpha, \beta, \theta; \alpha - k_0, \beta - k_1, k_2; \theta - k_3 - k_4 - k_5, k_6, k_7) \]  
(11)

3. \( Z_2R^S \)-Additive Cyclic Codes

Cyclic codes are a very significant class of linear codes because of their good algebraic structures for coding and decoding [15]. In this section, we study the structural properties of \( Z_2R^S \)-additive cyclic codes, including their generator polynomials and minimal spanning sets.

Let \( \delta \) be a standard shift operator on \( Z_2^n \times R^\beta \) and \( S^\theta \). For any \((m, v, w) \in Z_2^n \times R^\beta \times S^\theta \), let \( \tau \) be a shift operator on

\[ Z_2^n \times R^\beta \times S^\theta \]  
as \( \tau(m, v, w) = (\delta(m), \delta(v), \delta(w)) \)  
(12)

Definition 4 The \( Z_2R^S \)-additive code \( C \) of length \( n = \alpha + \beta + \theta \) over \( \mathbb{R} \) is said to be a \( Z_2R^S \)-additive cyclic code if it is invariant under \( \tau \), i.e. for any codeword,

\[ \mathcal{C} = \left\{ (m_0, m_1, \ldots, m_{\alpha-1}, v_0, v_1, \ldots, v_{\beta-1}, w_0, w_1, \ldots, w_{\theta-1}) \in C \right\} \]  
(13)

its cyclic shift

\[ \tau(c) = (m_{\alpha-1}, m_0, m_1, \ldots, m_{\alpha-2}, v_1, v_0, v_1, \ldots, v_{\beta-1}, w_0, w_1, \ldots, w_{\theta-1}) \in C \]  
(14)

In Section 2, the paper defined the inner product in \( Z_2^n \times R^\beta \times S^\theta \).

Lemma 1 If \( C \) is a \( Z_2R^S \)-additive cyclic code, then \( C^\perp \) is also a \( Z_2R^S \)-additive cyclic code.

Proof Let \( C \) be a \( Z_2R^S \)-additive cyclic code, and

\[ m = (a_0, \ldots, a_{\alpha-1}, h_0, \ldots, h_{\beta-1}, d_0, \ldots, d_{\theta-1}) \in C^\perp \]  
(15)

In the following, it only needs to prove \( \tau(m) \in C^\perp \). Since \( m \in C^\perp \), for

\[ v = (e_0, \ldots, e_{\alpha-1}, g_0, \ldots, g_{\beta-1}, h_0, h_{\beta-1}) \in C \]  
(16)

it have

\[ m \cdot v = u^2(a_0e_0 + \cdots + a_{\alpha-1}e_{\alpha-1}) + u(h_0g_0 + \cdots + h_{\beta-1}g_{\beta-1}) + d_0h_0 + \cdots + d_{\theta-1}h_{\theta-1} \equiv 0 \mod u^3. \]  
(17)

Let

\[ l = \text{lcm}(\alpha, \beta, \theta) \]  
(18)

and

\[ d^{-1}(v) = (e_1, \ldots, e_{\alpha-1}, e_0, g_1, \ldots, g_{\beta-1}, g_0, h_1, \ldots, h_{\beta-1}, h_0) = w \]  
(19)

Then \( \tau'(w) = v \). Since \( C \) is a cyclic code, it follows that \( w \in C \). Therefore,

\[ 0 = w \cdot m \]
\[ = u^2(e_0a_0 + \cdots + e_{\alpha-1}a_{\alpha-1} + e_0a_{\alpha-1}) + u(g_0h_0 + \cdots + g_{\beta-1}h_{\beta-1}) + h_0d_0 + h_0d_{\theta-1} \]
\[ = u^2(e_0a_0 + \cdots + e_{\alpha-1}a_{\alpha-1}) + u(g_0h_0 + h_0d_0 + h_0d_{\theta-1}) \]
\[ = v \cdot \tau(m). \]

Hence, \( \tau(u) \in C \), \( C^\perp \) is also a \( Z_2R^S \)-additive cyclic code.

Definition 5 Define the set

\[ Z_2[x]/(x^{\alpha-1}) \times R[x]/(x^{\beta-1}) \times S[x]/(x^{\theta-1}) \]  
by \( \mathbb{R}_{\alpha, \beta, \theta} \).

For \( C \subseteq Z_2^n \times R^\beta \times S^\theta \) any element:

\[ c = \left( (m_0, m_1, \ldots, m_{\alpha-1}, v_0, v_1, \ldots, v_{\beta-1}, w_0, w_1, \ldots, w_{\theta-1}) \in C \right) \]

its cyclic shift

\[ \tau(c) = (m_{\alpha-1}, m_0, m_1, \ldots, m_{\alpha-2}, v_1, v_0, v_1, \ldots, v_{\beta-1}, w_0, w_1, \ldots, w_{\theta-1}) \in C \]  
(14)

Therefore, it is possible to see that \( \mathbb{R}_{\alpha, \beta, \theta} \equiv Z_2^n \times R^\beta \times S^\theta \).

Define the product \( \ast \), for \( d(x) \in S[x] \) and \( (f(x), g(x), h(x)) \in \mathbb{R}_{\alpha, \beta, \theta} \),

\[ d(x) \ast (f(x), g(x), h(x)) = (d(x)f(x) \mod u, d(x)g(x) \mod u^2, d(x)h(x)) \]  
(22)

This extended multiplication is also well defined and \( Z_2^n \times R^\beta \times S^\theta \) is a \( S[x] \)-module with respect to this multiplication.

Lemma 2 Under the definition of \( \ast \), \( \mathbb{R}_{\alpha, \beta, \theta} \) is an \( S[x] \)-module, and any \( Z_2R^S \)-additive cyclic code \( C \) corresponds to an \( S[x] \)-submodule of \( \mathbb{R}_{\alpha, \beta, \theta} \).

In this part, we study \( S[x] \)-submodules for \( \mathbb{R}_{\alpha, \beta, \theta} \). The generator and a minimal spanning set of these submodules are determined. Assume that \( \alpha, \beta, \theta \) are odd positive integers. Since the \( Z_2R^S \)-additive cyclic code \( C \) is an \( S[x] \)
A map can be defined as follows
\[ \psi : C \to S[x]/(x^\theta - 1) \]
\[ (f(x), g(x), h(x)) \to h(x) \] (23)

Clearly, \( \psi \) is an \( S[x] \)-module homomorphism with kernel
\[ \text{Ker}(\psi) = \{(f(x), g(x), 0) \in C : f(x) \in Z_2[x]/(x^\theta - 1), g(x) \in R[x]/(x^\theta - 1)\} \] (24)

Since the image \( \psi(C) \) of \( C \) is an ideal of \( S[x]/(x^\theta - 1) \).

and \( \theta \) is an odd integer, which implies that
\[ \psi(C) = \{p(x) + ug(x) + u^2r(x)\} \] (25)

where \( r(x) | q(x) | p(x) | (x^\theta - 1) \) mod \( u^3 \).

From the discussion above, which implies that the following theorem is got.

**Theorem 3** Let \( C \) be a \( Z_2 RS \)-additive cyclic code. Then \( C \) can be generated as an \( R[x] \)-submodule of \( \mathcal{R}_{\alpha, \beta, \theta} \) with this form
\[ C = \{ (f(x), 0, 0), (f_1(x), g_1(x) + u\alpha_1(x), 0), (f_2(x), g_2(x), p(x) + ug(x) + u^2r(x)) \} \] (26)

Proof Let \( I \) be a set, and
\[ I = \{(f(x), g(x), 0) \in Z_2[x]/(x^\theta - 1) \times R[x]/(x^\theta - 1) : (f(x), g(x), 0) \in \text{Ker}(\psi)\} \] (27)

Clearly, \( I \) is an \( R[x] \)-submodule of \( Z_2[x]/(x^\theta - 1) \times R[x]/(x^\theta - 1) \). Hence, \( I \) is a \( Z_2 RS \)-additive cyclic code. From [7],
\[ I = \{(f(x), 0), (f_1(x), g_1(x) + u\alpha_1(x)) \} \] (28)

where \( f(x) | x^\theta - 1 \) and \( g_1(x) + u\alpha_1(x) \) is a polynomial over \( R \) with \( \alpha_1(x) | g_1(x) | x^\theta - 1 \) and \( f(x) | \frac{x^\theta - 1}{\alpha_1(x)} f_1(x) \).

Let \( (c_1(x), c_2(x), 0) \in \text{Ker}(\psi) \). Then that have
\[ (c_1(x), c_2(x)) \in I \]
\[ \{ (f(x), 0), (f_1(x), g_1(x) + u\alpha_1(x)) \} \] (29)

Therefore, for polynomials \( m_1 \in Z_2[x]/(x^\theta - 1) \) and \( m_2 \in R[x]/(x^\theta - 1) \), it get
\[ (c_1(x), c_2(x)) = m_1 * (f(x), 0) + m_2 * (f_1(x), g_1(x) + u\alpha_1(x)) \] (30)

So
\[ \text{Ker}(\psi) = \{(f(x), 0, 0), (f_1(x), g_1(x) + u\alpha_1(x), 0) \} \] (31)

is a submodule of \( C \). By the first isomorphism theorem of modules, there are \( C / \text{Ker}(\psi) \cong \{p(x) + ug(x) + u^2r(x)\} \).

Let \( (f_2(x), g_2(x), p(x) + ug(x) + u^2r(x)) \in C \) such that
\[ \psi(f_2(x), g_2(x), p(x) + ug(x) + u^2r(x)) = p(x) + ug(x) + u^2r(x) \] (32)

Then
\[ C = \{(f(x), 0, 0), (f_1(x), g_1(x) + u\alpha_1(x), 0), (f_2(x), g_2(x), p(x) + ug(x) + u^2r(x)) \} \] (33)

**Lemma 3** Let
\[ C = \{(f(x), 0, 0), (f_1(x), g_1(x) + u\alpha_1(x), 0), (f_2(x), g_2(x), p(x) + ug(x) + u^2r(x)) \} \] (34)

be a \( Z_2 RS \)-additive cyclic code. Then
\[ \deg f_1(x) < \deg f(x) \] (35)

and \( \deg f_2(x) < \deg f(x) \) and
\[ \deg g_2(x) < \deg g_1(x) \] (36)

Proof Let \( \deg f_1(x) \geq \deg f(x) \). Since \( f(x) \) is monic, it can apply division algorithm, i.e. there exists polynomials \( q(x) \) and \( r(x) \) over \( Z_2 \) such that
\[ f_1(x) = f(x)q'(x) + r'(x) \] (37)

where \( r'(x) = 0 \) or \( 0 \leq \deg r'(x) < \deg f(x) \), which implies that
\[ \{ (f(x), 0, 0), (f_1(x), g_1(x) + u\alpha_1(x), 0), (f_2(x), g_2(x), p(x) + ug(x) + u^2r(x)) \} \] (38)

\[ = \{(f(x), 0, 0), (f_1(x), g_1(x) + u\alpha_1(x), 0), (f_2(x), g_2(x), p(x) + ug(x) + u^2r(x)) \} \]

\[ \{ (f(x), 0, 0), (r'(x), g_1(x) + u\alpha_1(x), 0), (f_2(x), g_2(x), p(x) + ug(x) + u^2r(x)) \} \]

Hence we may assume that \( \deg f_1(x) < \deg f(x) \) . Similarly the \( \deg f_2(x) < \deg f(x) \) and \( \deg g_2(x) < \deg g_1(x) \) also can be proved.

**Lemma 4** Let
\[ C = \{(f(x), 0, 0), (f_1(x), g_1(x) + u\alpha_1(x), 0), (f_2(x), g_2(x), p(x) + ug(x) + u^2r(x)) \} \] (39)

be a \( Z_2 RS \)-additive cyclic code. Then
Proof It is well known that
\[ \psi(C) = \{ p(x) + uq(x) + u^2 r(x) \} \] (41)

Hence,
\[ \psi\left( \frac{x^\theta - 1}{a_1(x)} \right) f_1(x), \psi\left( \frac{x^\theta - 1}{a_1(x)} \right) g_1(x) + u a_1(x), 0 \}
= 0
\]
(42)

where \( (f_1(x), g_1(x) + u a_1(x), 0) \in C \), which implies that
\[ \psi\left( \frac{x^\theta - 1}{a_1(x)} \right) f_1(x) = \psi\left( \frac{x^\theta - 1}{a_1(x)} \right) g_1(x) + u a_1(x), 0 \} \in \ker(\psi) \] (43)

Therefore,
\[ f(x) \mid \frac{x^\theta - 1}{a_1(x)} f_1(x) \] (44)

Lemma 5 Let
\[ C = \{ (f(x), 0, 0), (f_1(x), g_1(x) + u a_1(x), 0), (f_2(x), g_2(x), p(x) + u q(x) + u^2 r(x)) \} \] (45)

be a \( Z_2 RS \)-additive cyclic code. Then have
\[ (g_1(x) + u a_1(x)) \mid \frac{x^\theta - 1}{r(x)} g_2(x) \mod u^2 \] (46)
\[ f(x) \mid (k(x) f_1(x) + \frac{x^\theta - 1}{r(x)} f_2(x)) \mod u \] (47)

Where
\[ k(x) (g_1(x) + u a_1(x)) = \frac{x^\theta - 1}{r(x)} g_2(x) \mod u^2 \] (48)

Proof (i) Consider
\[ \psi\left( \frac{x^\theta - 1}{r(x)} \right) f_2(x), \psi\left( \frac{x^\theta - 1}{r(x)} \right) g_2(x), p(x) + u q(x) + u^2 r(x) \}
= \psi\left( \frac{x^\theta - 1}{r(x)} \right) f_2(x), \psi\left( \frac{x^\theta - 1}{r(x)} \right) g_2(x), 0 \}
= 0.
\] (49)

Since
\[ \delta\left( \frac{x^\theta - 1}{r(x)} \right) g_2(x) = \frac{x^\theta - 1}{r(x)} g_2(x) \in \ker(\psi) \] (50)

then
\[ (g_1(x) + u a_1(x)) \mid \frac{x^\theta - 1}{r(x)} g_2(x) \mod u^2 \] (51)

(ii) Let
\[ (g_1(x) + u a_1(x)) \mid \frac{x^\theta - 1}{r(x)} g_2(x) \mod u^2 \] (52)

Then there exists \( k(x) \in S \) such that
\[ k(x) (g_1(x) + u a_1(x)) = (k(x) f_1(x)) \] (53)

Having
\[ (k(x) f_1(x) + k(x)(g_1(x) + u a_1(x), 0)) \] (54)

Thereore,
\[ (k(x) f_1(x) + k(x)(g_1(x) + u a_1(x), 0)) \] (55)

Hence,
\[ f(x) \mid (k(x) f_1(x) + \frac{x^\theta - 1}{r(x)} f_2(x)) \mod u \] (56)

From the discussion above, the following theorem can be directly obtained.

Theorem 4 Let \( C \) be a \( Z_2 RS \)-additive cyclic code. Then,
\[ C = \{ (f(x), 0, 0), f(x) \mid (x^\alpha - 1) \mod u^2 \} \] (57)

and
\[ (x^\alpha - 1) \mid \frac{x^\theta - 1}{a_1(x)} f_1(x) \] (58)

or
\[ C = \{ (f(x), g(x) + u a_1(x), 0), a_1(x) \mid g_1(x) \mid (x^\beta - 1) \mod u^2 \} \] (59)

where
\[ r(x) | g(x) | p(x) | (x^\theta - 1) \mod u \]
\[ \deg g_2(x) < \deg g_1(x) \] (60)
and
\[ (g_1(x) + \alpha_0 x) \mid \frac{x^\theta - 1}{q_1(x)} g_2(x) \mod u^2 \]
\[ \deg f_1(x) < \deg f(x), \deg f_2(x) < \deg f(x) \] (62)
\[ f(x) \mid \left( \frac{x^\theta - 1}{q_1(x)} \right) f_1(x) \mod u \]
\[ f(x) \mid \left( k(x)f_1(x) + \frac{x - 1}{r(x)} f_2(x) \right) \mod u \] (64)
where
\[ k(x)(g_1(x) + \alpha_0(x)) = \frac{x^\theta - 1}{r(x)} g_2(x) \mod u^2 \] (66)

In the following, get the main result on the minimum generating sets of \( Z_2 RS \)-additive cyclic codes.

**Theorem 5** Let
\[ C = \{ (f(x), 0, 0), (f_1(x), g_1(x) + \alpha_0(x), 0), (f_2(x), g_2(x), p(x) + \alpha_2(x) + \alpha u r(x)) \} \] (67)

Let,
\[ D_1 = \bigcup_{i=0}^{\deg r(x) - 1} \left\{ i \cdot (r(x), 0, 0) \right\} \]
\[ D_2 = \bigcup_{i=0}^{\deg r(x) - 1} \left\{ i \cdot (f_1(x), g_1(x) + \alpha_0(x), 0) \right\} \]
\[ D_3 = \bigcup_{i=0}^{\deg r(x) - 1} \left\{ i \cdot (f_2(x), g_2(x), p(x) + \alpha_2(x) + \alpha u r(x)) \right\} \]
\[ D_4 = \bigcup_{i=0}^{\deg r(x) - 1} \left\{ i \cdot \left[ p(x) + (f_1(x), g_1(x) + \alpha_0(x), 0) \right] \right\} \]
\[ D_5 = \bigcup_{i=0}^{\deg r(x) - 1} \left\{ i \cdot \left[ f_1(x), g_1(x) + \alpha_0(x), 0 \right] \right\} \]
\[ D_6 = \bigcup_{i=0}^{\deg r(x) - 1} \left\{ i \cdot \left[ f_2(x), g_2(x), p(x) + \alpha_2(x) + \alpha u r(x) \right] \right\} \]

where \( \deg f(x) = t_1, \deg g_1(x) = t_2, \deg p(x) = t_3 \),
\[ a_0(x) = \frac{g_1(x)}{q_1(x)}, \quad q(x) = \frac{p(x)}{r(x)}, \quad r(x) = \frac{q(x)}{r(x)}, \quad f_1(x) f(x) = x^\theta - 1, \]
\[ f_2(x) g_2(x) = x^\theta - 1, \quad f_2(x) p(x) = f_2(x) q(x) = x^\theta - 1. \]
Then
\[ D = D_1 \cup D_2 \cup D_3 \cup D_4 \cup D_5 \cup D_6 \] (69)
is a minimal spanning set for \( C \), and
\[ |C| = 2^{\alpha - n}.4^{\beta - t_1}.8^{\theta - t_2}.2^{\deg q_1(x)}.4^{\deg q_2(x)}2^{\deg r(x)} \] (70)

**Proof** Let \( c(x) \) be any codeword in \( C \). There exist some polynomials \( e_1(x), e_2(x), e_3(x) \in S[x] \), such that \( c(x) \) can be represented by
\[ c(x) = e_1(x) \ast \left( f(x), 0, 0 \right) + e_2(x) \ast \left( f_1(x), g_1(x) + \alpha_0(x), 0 \right) \]
\[ + e_3(x) \ast \left( f_2(x), g_2(x), p(x) + \alpha_2(x) + \alpha u r(x) \right) \] (71)

If
\[ \deg e_1(x) < \deg l_f(x) \]
then
\[ e_1(x) \ast \left( f(x), 0, 0 \right) \in \langle D_1 \rangle \] (72)
Otherwise, have
\[ e_1(x) = l_f(x) q_1(x) + \eta_1(x) \] (73)
where \( \eta_1(x) = 0 \) or \( \deg \eta_1(x) < \deg l_f(x) \). Hence,
\[ e_1(x) \ast \left( f(x), 0, 0 \right) = l_f(x) q_1(x) + \eta_1(x) \ast \left( f(x), 0, 0 \right) \]
\[ = \eta_1(x) \ast \left( f(x), 0, 0 \right) \in \langle D_1 \rangle. \]

If \( \deg e_2(x) < \deg l_f(x) \), then
\[ e_2(x) \ast \left( f_1(x), g_1(x) + \alpha_0(x), 0 \right) \in \langle D_2 \rangle \] (75)
Otherwise, have
\[ e_2(x) = l_{g_1}(x) q_2(x) + r_2(x) \] (76)
where \( r_2(x) = 0 \) or \( \deg r_2(x) = \deg l_{g_1}(x) \). Hence,
\[ e_2(x) \ast \left( f_1(x), g_1(x) + \alpha_0(x), 0 \right) \]
\[ = l_{g_1}(x) q_2(x) + r_2(x) \ast \left( f_1(x), g_1(x) + \alpha_0(x), 0 \right) \]
\[ = l_{g_1}(x) q_2(x) \ast \left( f_1(x), g_1(x) + \alpha_0(x), 0 \right) \]
\[ + r_2(x) \ast \left( f_1(x), g_1(x) + \alpha_0(x), 0 \right) \]
\[ = q_2(x) \ast \left( l_{g_1}(x) f_1(x), l_{g_1}(x) u_0(x), 0 \right) \]
\[ + r_2(x) \ast \left( f_1(x), g_1(x) + \alpha_0(x), 0 \right) \]
\[ = q_2(x) \ast \left( l_{g_1}(x) f_1(x), l_{g_1}(x) u_0(x), 0 \right) \] (77)
where \( r_2(x) \ast \left( f_1(x), g_1(x) + \alpha_0(x), 0 \right) \in \langle D_2 \rangle \).

For
\[ q_2(x) \ast \left( l_{g_1}(x) f_1(x), l_{g_1}(x) u_0(x), 0 \right) \] (78)
if \( \deg q_2(x) < \deg a_0(x) \), then
\[ q_2(x) \ast \left( l_{g_1}(x) f_1(x), u_0(x), 0 \right) \] (79)
Otherwise, have
\[
q_2(x) = q_3(x)a_1'(x) + r_1(x)
\] (80)
where \( r_1(x) = 0 \) or \( \deg r_1(x) < \deg a_1'(x) \). Hence, and since
\[
q_2(x)*\left(l_{g_1}(x)f_1(x),ul_{g_1}(x)a_1(x),0\right) = \left(q_3(x)a_1'(x) + r_1(x)\right)*\left(l_{g_1}(x)f_1(x),ul_{g_1}(x)a_1(x),0\right)
\] (81)
\[
= q_3(x)*\left(l_{g_1}(x)f_1(x),a_1'(x),0,0\right) + r_1(x)*\left(l_{g_1}(x)f_1(x),ul_{g_1}(x)a_1(x),0,0\right)
\]
\[
q_3(x)*\left(l_{g_1}(x)f_1(x)a_1'(x),0,0\right) = q_3(x)*\left(\frac{x^\beta - 1}{a_1(x)} f_1(x),0,0\right) \in \langle D_1 \rangle
\] (82)
Here,
\[
\]
Finally, for \( e_3(x)*\left(f_2(x),g_2(x),p(x)+uq(x)+u^2r(x)\right), \) if \( \deg e_3(x) < \deg l_{r}(x) \), then
\[
e_3(x) = l_{p}(x)q_4(x) + r_4(x)
\] (86)
\[
e_3(x)*\left(f_2(x),g_2(x),p(x)+uq(x)+u^2r(x)\right) \in \langle D_3 \rangle
\] (85)
where \( r_4(x) = 0 \) or \( \deg r_4(x) < \deg l_{r}(x) \). Hence,
\[
\]
Otherwise,
\[
e_3(x)*\left(f_2(x),g_2(x),p(x)+uq(x)+u^2r(x)\right) = l_{p}(x)q_4(x) + r_4(x)*\left(f_2(x),g_2(x),p(x)+uq(x)+u^2r(x)\right)
\]
\[
= q_4(x)*\left(l_{p}(x)f_2(x),l_{p}(x)g_2(x),ul_{p}(x)q(x)+u^2l_{p}(x)r(x)\right)
\]
\[
+ r_4(x)*\left(f_2(x),g_2(x),p(x)+uq(x)+u^2r(x)\right)
\]
Here,
\[
r_4(x)*\left(f_2(x),g_2(x),p(x)+uq(x)+u^2r(x)\right) \in \langle D_3 \rangle
\] (88)
For
\[
q_4(x)*\left(l_{p}(x)f_2(x),l_{p}(x)g_2(x),ul_{p}(x)q(x)+u^2l_{p}(x)r(x)\right)
\] (87)
if \( \deg q_4(x) < \deg q'(x) \), then
\[
q_4(x)*\left(l_{p}(x)f_2(x),l_{p}(x)g_2(x),ul_{p}(x)q(x)+u^2l_{p}(x)r(x)\right) \in \langle D_3 \rangle
\] (89)
Otherwise, have
\[
q_4(x) = q'(x)q_5(x) + r_5(x)
\] (91)
where \( r_5(x) = 0 \) or \( \deg r_5(x) < \deg q'(x) \). Hence,
\[ q_4(x) \cdot \left( l_p(x) f_2(x), l_p(x) g_2(x), u l_p(x) q(x) + u^2 l_p(x) r(x) \right) \]
\[ = q(x) q_5(x) \]
\[ + r_5(x) \cdot \left( l_p(x) f_2(x), l_p(x) g_2(x), u l_p(x) q(x) + u^2 l_p(x) r(x) \right) \]
\[ = q_5(x) \cdot \left( l_p(x) f_2(x), l_p(x) g_2(x), u^2 l_p(x) r(x) \right) \]
\[ + r_5(x) \cdot \left( l_p(x) f_2(x), l_p(x) g_2(x), u l_p(x) q(x) + u^2 l_p(x) r(x) \right) \]

Here,
\[ r_5(x) \cdot \left( l_p(x) f_2(x), l_p(x) g_2(x), u l_p(x) q(x) + u^2 l_p(x) r(x) \right) \in \langle D_5 \rangle. \]
For \( q_5(x) \cdot \left( l_p(x) f_2(x), l_p(x) g_2(x), u l_p(x) q(x) + u^2 l_p(x) r(x) \right) \), if
\[ \deg \left( q_5(x) \right) / \deg \left( r'(x) \right), \]
\[ \deg \left( q_5(x) \right) / \deg \left( r'(x) \right) \]

where \( r_5(x) = 0 \) or \( \deg r_5(x) < \deg r'(x) \).
Hence,
\[ r'(x) q_6(x) + r_6(x) \cdot \left( l_p(x) f_2(x), l_p(x) g_2(x), u^2 l_p(x) r(x) \right) \]
\[ = q_6(x) \cdot \left( \frac{x^\theta - 1}{r(x)} f_2(x), \frac{x^\theta - 1}{r(x)} g_2(x), 0 \right) \]
\[ + r_6(x) \cdot \left( l_p(x) f_2(x), l_p(x) g_2(x), u^2 l_p(x) r(x) \right) \]
Have
\[ r_6(x) \cdot \left( l_p(x) f_2(x), l_p(x) g_2(x), u^2 l_p(x) r(x) \right) \in \langle D_6 \rangle. \]

Example 1 Let \( C \) be a \( Z_2 \) additive cyclic code in generated \( Z_2[x]/(x-1) \times R[x]/(x-1) \times S[x]/(x^5 - 1) \) by
\[ \{ (f(x), 0, 0), (f_2(x), g_2(x), u q(x)), (f_2(x), g_2(x), p(x) + u q(x) + u^2 r(x)) \}, \]
where \( f(x) = 1 + x, f_1(x) = f_2(x) = 1, f_2(x) = f_2(x) = 1, g_2(x) = 1, q(x) = 1, \) \( p(x) = 1 + x, q(x) = 1, r(x) = 1. \) In this following,
Furthermore, the $\Phi(C)$ is a $[18, 6, 3]$ linear binary code. There is a table about some examples. The binary codes with these parameter are not nice codes. But the binary codes which are marked with * are only about 1 less in minimum distance than the corresponding nice codes.

**Table 1. The codes of binary images of C.**

<table>
<thead>
<tr>
<th>Generator</th>
<th>$\alpha, \beta, \theta$</th>
<th>Binary Images</th>
</tr>
</thead>
<tbody>
<tr>
<td>$f(x)=1+x$, $f_1(x)=f_2(x)=1$, $g_1(x)=1+x$, $g_2(x)=1$</td>
<td>$1, 1, 1$</td>
<td>[6, 2, 3]*</td>
</tr>
<tr>
<td>$f_2(x)=1+x+u+u^2$, $q(x)=1+x$, $q_1(x)=1+x$</td>
<td>$1, 3, 1$</td>
<td>[10, 3, 4]*</td>
</tr>
<tr>
<td>$f_3(x)=1+x$, $f_1(x)=f_2(x)=1$, $g_1(x)=1+x$, $g_2(x)=1+x+x^2$, $q(x)=1+x$, $q_2(x)=1+x$</td>
<td>$1, 5, 1$</td>
<td>[14, 2, 8]*</td>
</tr>
<tr>
<td>$f_4(x)=1+x$</td>
<td>$1, 3, 3$</td>
<td>[16, 4, 6]</td>
</tr>
<tr>
<td>$f_5(x)=1+x+u+u^2$, $r(x)=1+x$, $r_1(x)=1+x$</td>
<td>$1, 7, 1$</td>
<td>[18, 5, 6]</td>
</tr>
<tr>
<td>$f_6(x)=1+x$, $f_1(x)=f_2(x)=1$, $g_1(x)=1+x$, $g_2(x)=1+x+x^2+x^3+x^4$, $q(x)=1+x$, $q_1(x)=1+x$</td>
<td>$1, 7, 1$</td>
<td>[18, 2, 10]</td>
</tr>
<tr>
<td>$f_7(x)=1+x+u+u^2$, $r(x)=1+x$, $r_1(x)=1+x$</td>
<td>$1, 7, 1$</td>
<td>[18, 7, 4]</td>
</tr>
</tbody>
</table>

4. Conclusion

In this paper, we have studied additive cyclic codes over the ring $\mathbb{Z}_2\mathcal{R}S$, where $R = \mathbb{Z}_2 + u\mathbb{Z}_2$, $u^2 = 0 \mod 2$, and $S = \mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$, $u^2 = 0 \mod 2$. We have given the definition of $Z_2(Z_2 + u\mathbb{Z}_2)(Z_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2)$-additive codes with generator matrices and parity-check matrices. Furthermore, the fundamental results on the generator polynomials and spanning sets for these additive cyclic codes of block length $(\alpha, \beta, \theta)$, where $\theta$ is odd have been obtained. Finding $\mathbb{Z}_2\mathcal{R}S$-additive cyclic code and its dual of
arbitrary block length $(\alpha, \beta, \theta)$ may be an interesting problem.

References


