EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
Vol. 10, No. 2, 2017, 392-409
ISSN 1307-5543 – www.ejpam.com
Published by New York Business Global

$\mathbb{Z}_2$-Triple cyclic codes and their duals

Srinivasulu B[1], Maheshanand Bhaintwal[2]

[1,2] *Department of Mathematics, Indian Institute of Technology Roorkee, Roorkee, India.*

Abstract. A $\mathbb{Z}_2$-triple cyclic code of block length (r, s, t) is a binary code of length $r + s + t$ such that the code is partitioned into three parts of lengths r, s and t such that each part is invariant under the cyclic shifts of the coordinates. Such a code can be viewed as $\mathbb{Z}_2[x]$-submodules of $\frac{\mathbb{Z}_2[x]}{\langle x^r-1\rangle} \times \frac{\mathbb{Z}_2[x]}{\langle x^s-1\rangle} \times \frac{\mathbb{Z}_2[x]}{\langle x^t-1\rangle}$, in polynomial representation. In this paper, we determine the structure of these codes. We have obtained the form of the generators for such codes. Further, a minimal generating set for such codes is obtained. Also, we study the structure of the duals of these codes via the generators of the codes.

2010 Mathematics Subject Classifications: 94B05, 94B60

Key Words and Phrases: Triple cyclic codes, minimal spanning sets, dual codes

1. Introduction

Codes over rings were introduced in early 1970s. Among them, cyclic codes are an important class of linear codes because of their richness in algebraic structure and practical use. Cyclic codes over finite fields are well studied [15] and they have been extended to various finite rings [11]. The search for new codes with good parameters encourages researchers to introduce various families of linear codes.

In 1973, Delsarte and Levenshtein [10] defined additive codes in terms of association schemes as the subgroups of the underlying abelian group. Under binary Hamming scheme, the underlying group of order 2^k is isomorphic to $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta}$, where α and β are non-negative integers. The subgroups of underlying group are called $\mathbb{Z}_2\mathbb{Z}_4$-additive codes. Borges et al. [5] have studied $\mathbb{Z}_2\mathbb{Z}_4$-additive codes by deriving their generator matrices and parity check matrices. In [1], $\mathbb{Z}_2\mathbb{Z}_4$-cyclic codes of block length $(r,\ t)$ for odd t have been defined as $\mathbb{Z}_4$-submodules of $\mathbb{Z}_2^r \times \mathbb{Z}_4^t$, and a minimal spanning set for these codes has been determined. Extending this work, Borges et al. [6] gave duals of $\mathbb{Z}_2\mathbb{Z}_4$-cyclic codes of block length $(r,\ t)$ for odd t. Recently Aydogdu et al. [3] have studied a new class of codes over the structure $\mathbb{Z}_2\mathbb{Z}_2[u]$, where $\mathbb{Z}_2[u] = \mathbb{Z}_2 + u\mathbb{Z}_2$, $u^2 = 0$. They have defined $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes as $\mathbb{Z}_2[u]$-submodules of $\mathbb{Z}_2^s \times \mathbb{Z}_2[u]^t$, and obtained their generator and parity check matrices. They have also defined the type of these codes and have shown that some optimal binary codes are Gray images of $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes.

Email addresses: bslu1981@gmail.com (Srinivasulu B), mahesfma@iitr.ac.in (M. Bhaintwal)

Extending the concepts given in [6], recently Aydogdu and Siap have studied [2] the algebraic structure of $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes. They have determined the generator and parity check matrices for these codes. Borges et al. [4] have derived the structure of $\mathbb{Z}_2$-double cyclic codes. They have determined generating polynomials for these codes and derived the relationship between the codes and their duals. Similarly structure of double cyclic codes over the rings $\mathbb{Z}_4$ and $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2,\ u^3 = 0$ have been studied in [14][17]. In [14], Gao et al. have obtained some optimal or suboptimal non-linear binary codes. A double cyclic code is in fact a generalized quasi-cyclic (GQC) code of index two. Siap and Kulhan[16] introduced GQC codes over finite fields and the study has been extended to various finite rings by many authors [7, 8, 9, 12, 13]. Most of these studies focused on exploring 1-generator GQC codes where they have succeeded in finding their duals and obtained a good number of optimal codes.

In this paper, extending the concepts of [4] and [17] we introduce $\mathbb{Z}_2$-triple cyclic codes and study their algebraic structure. We give a minimal spanning set for these codes. Further we present the structure of duals of these codes via their generators. The paper is organized as follows. In Section 2, we introduce some basic notations and definitions of $\mathbb{Z}_2$-triple cyclic codes and derive the form of their generators. In this section, we also determine a minimal spanning set for $\mathbb{Z}_2$-triple cyclic codes. In Section 3, we study the duals of $\mathbb{Z}_2$-triple cyclic codes.

2. $\mathbb{Z}_2$-triple cyclic codes

Let $r,\ s$ and t be three positive integers and $n = r + s + t$. Let C be a binary linear code of length n. The n coordinates of each codeword of C can be partitioned into three sets of size $r,\ s$ and t. Therefore C is a $\mathbb{Z}_2$-submodule of $\mathbb{Z}_2^r \times \mathbb{Z}_2^s \times \mathbb{Z}_2^t$.

Definition 1. *For any three positive integers r, s and t, a $\mathbb{Z}_2$-triple cyclic code* C *of block length (r, s, t) is a binary linear code of length $n = r + s + t$ such that* $\sigma(c) = (c_{1,r-1}, c_{1,0}, \cdots, c_{1,r-2} \mid c_{2,s-1}, c_{2,0}, \cdots, c_{2,s-2} \mid c_{3,t-1}, c_{3,0}, \cdots, c_{3,t-2}) \in \mathrm{C}$, *whenever* $c = (c_{1,0}, c_{1,1}, \cdots, c_{1,r-1} \mid c_{2,0}, c_{2,1}, \cdots, c_{2,s-1} \mid c_{3,0}, c_{3,1}, \cdots, c_{3,t-1}) \in \mathrm{C}$.

Let C be a $\mathbb{Z}_2$-triple cyclic code of block length (r, s, t). Let C_r be the canonical projection of C on the first r coordinates, C_s be the projection of C on next s coordinates and C_t be the projection of C on the last t coordinates. It is easy to see that these projections C_r, C_s and C_t are binary cyclic codes of lengths r, s and t, respectively. C is called separable if $\mathrm{C} = \mathrm{C}_r \times \mathrm{C}_s \times \mathrm{C}_t$.

The dual $\mathrm{C}^\perp$ of a $\mathbb{Z}_2$-triple cyclic code C of block length (r, s, t) is defined as

$$\mathrm{C}^\perp = \{v' \in \mathbb{Z}_2^r \times \mathbb{Z}_2^s \times \mathbb{Z}_2^t \mid v \cdot v' = 0 \text{ for all } v \in \mathrm{C}\},$$

where $v \cdot v'$ is the usual inner product over $\mathbb{Z}_2$.

Let $m = \mathrm{lcm}(r, s, t)$. The following result shows that the dual of a $\mathbb{Z}_2$-triple cyclic code of block length (r, s, t) is also a $\mathbb{Z}_2$-triple cyclic code of same block length.

Theorem 1. *If* C *is a $\mathbb{Z}_2$-triple cyclic code of block length (r, s, t), then $\mathrm{C}^\perp$ is also $\mathbb{Z}_2$-triple cyclic code of block length (r, s, t).*

Proof. Let $u \in \mathrm{C}^{\perp}$ and $v \in \mathrm{C}$. Since C is invariant under σ, $\sigma^{m-1}(v) \in \mathrm{C}$. Therefore

$$\begin{aligned} 0 = u \cdot \sigma^{m-1}(v) &= (u_{1,0}v_{1,1} + \cdots + u_{1,r-2}v_{1,r-1} + u_{1,r-1}v_{1,0}) + (u_{2,0}v_{2,1} + \cdots + \\ &\qquad u_{2,s-1}v_{2,0}) + (u_{3,0}v_{3,1} + \cdots + u_{3,t-1}v_{3,0}) \\ &= (u_{1,r-1}v_{1,0} + u_{1,0}v_{1,1} + \cdots + u_{1,r-2}v_{1,r-1}) + (u_{2,s-1}v_{2,0} + \cdots + \\ &\qquad u_{2,s-2}v_{2,s-1}) + (u_{3,t-1}v_{3,0} + \cdots + u_{3,t-2}v_{3,t-1}) \\ &= \sigma(u) \cdot v. \end{aligned}$$

As u is an arbitrary element of $\mathrm{C}^{\perp}$, the result follows.

Now we determine the generators for a $\mathbb{Z}_2$-triple cyclic code C of block length (r, s, t). For this, we first consider the algebraic structure of C in $\frac{\mathbb{Z}_2[x]}{\langle x^r-1\rangle} \times \frac{\mathbb{Z}_2[x]}{\langle x^s-1\rangle} \times \frac{\mathbb{Z}_2[x]}{\langle x^t-1\rangle}$.

Let $\mathrm{R}_{r,s,t}[x] = \frac{\mathbb{Z}_2[x]}{\langle x^r-1\rangle} \times \frac{\mathbb{Z}_2[x]}{\langle x^s-1\rangle} \times \frac{\mathbb{Z}_2[x]}{\langle x^t-1\rangle}$, $\mathbb{Z}_{2,r}[x] = \frac{\mathbb{Z}_2[x]}{\langle x^r-1\rangle}$, $\mathbb{Z}_{2,s}[x] = \frac{\mathbb{Z}_2[x]}{\langle x^s-1\rangle}$ and $\mathbb{Z}_{2,t}[x] = \frac{\mathbb{Z}_2[x]}{\langle x^t-1\rangle}$. By identifying each $c = (c_1 \mid c_2 \mid c_3) \in \mathbb{Z}_2^r \times \mathbb{Z}_2^s \times \mathbb{Z}_2^t$ with a triplet of polynomials $(c_1(x) \mid c_2(x) \mid c_3(x)) \in \mathrm{R}_{r,s,t}[x]$, where $c_1(x) = \sum_{j=0}^{r-1} c_{1,j}x^j$, $c_2(x) = \sum_{j=0}^{s-1} c_{2,j}x^j$ and $c_3(x) = \sum_{k=0}^{t-1} c_{3,j}x^j$, we get a $\mathbb{Z}_2$-module isomorphism between $\mathbb{Z}_2^r \times \mathbb{Z}_2^s \times \mathbb{Z}_2^t$ and $\mathrm{R}_{r,s,t}[x]$. Also for any $f(x) \in \mathbb{Z}_2[x]$ and $c = (c_1(x) \mid c_2(x) \mid c_3(x)) \in \mathrm{R}_{r,s,t}[x]$, we define the product $f(x) * (c_1(x) \mid c_2(x) \mid c_3(x)) = (f(x)c_1(x) \mid f(x)c_2(x) \mid f(x)c_3(x)) \in \mathrm{R}_{r,s,t}[x]$, where $f(x)c_i(x)$ is determined in the corresponding residue ring. Clearly this product is well defined. Therefore $\mathrm{R}_{r,s,t}[x]$ is a $\mathbb{Z}_2[x]$-module with respect to this product. We note that, in polynomial representation, $x(c_1(x) \mid c_2(x) \mid c_3(x)) = (xc_1(x) \mid xc_2(x) \mid xc_3(x))$ represents $\sigma(c)$ for the corresponding element $c = (c_1 \mid c_2 \mid c_3) \in \mathbb{Z}_2^r \times \mathbb{Z}_2^s \times \mathbb{Z}_2^t$. The codes in the present setting are in fact the extensions of both binary cyclic codes and $\mathbb{Z}_2$-double cyclic codes that defined in [4].

We denote $f * g$ simply by fg. The following result follows immediately from the previous discussion.

Theorem 2. *Let* C *be a binary linear code of length* $r+s+t$*. Then* C *is a* $\mathbb{Z}_2$*-triple cyclic code in* $\mathbb{Z}_2^r \times \mathbb{Z}_2^s \times \mathbb{Z}_2^t$ *if and only if* C *is a* $\mathbb{Z}_2[x]$*-submodule of* $\mathrm{R}_{r,s,t}[x]$.

Since both the modules $\mathbb{Z}_2^r \times \mathbb{Z}_2^s$ and $\mathbb{Z}_2^t$ can be obtained by projecting $\mathbb{Z}_2^r \times \mathbb{Z}_2^s \times \mathbb{Z}_2^t$ on first $r + s$ coordinates and last t coordinates, respectively, we make use of the cyclic structures of both binary codes and $\mathbb{Z}_2$-double cyclic codes as given in [4] to find the generator polynomials for a $\mathbb{Z}_2$-triple cyclic code C of block length (r, s, t) in $\mathrm{R}_{r,s,t}[x]$. The following theorem gives the generators for a $\mathbb{Z}_2$-double cyclic code of block length (r, s), which is useful for the rest of our study.

Theorem 3. *[4, Theorem 3.1] The* $\mathbb{Z}_2[x]$*-module* $\mathrm{R}_{r,s} = \frac{\mathbb{Z}_2[x]}{\langle x^r-1\rangle} \times \frac{\mathbb{Z}_2[x]}{\langle x^s-1\rangle}$ *is a noetherian module, and every submodule* C *of* $\mathrm{R}_{r,s}$ *can be written as*

$$\mathrm{C} = \langle (b(x) \mid 0), (l(x) \mid a(x) \rangle,$$

where $b(x)$, $l(x) \in \mathbb{Z}_2[x]/\langle x^r - 1\rangle$ *with* $b(x) \mid (x^r - 1)$ *and* $a(x) \in \mathbb{Z}_2[x]/\langle x^s - 1\rangle$ *with* $a(x) \mid (x^s - 1)$.

Theorem 4. *[4, Proposition 3.2.] Let* C *be a* $\mathbb{Z}_2$*-double cyclic code of block length* (r,s)*, such that* $\mathrm{C} = \langle (b(x) \mid 0), (l(x) \mid a(x))\rangle$*, where* $b(x)|x^r - 1$*,* $a(x)|x^s - 1$ *over* $\mathbb{Z}_2$*. If* $deg(b(x)) = t_1$ *and* $deg(a(x)) = t_2$*, then a minimal spanning set for* C *is* $S' = S'_1 \cup S'_2$*, where*

$$S'_1 = \bigcup_{i=0}^{r-t_1-1} x^i * (b(x) \mid 0) \qquad\qquad S'_2 = \bigcup_{i=0}^{s-t_2-1} x^i * (l(x) \mid a(x)).$$

In the following theorem, we determine the generator polynomials for $\mathbb{Z}_2$-triple cyclic codes of block length (r,s,t).

Theorem 5. *Let* C *be a* $\mathbb{Z}_2$*-triple cyclic code of block length* (r,s,t)*. Then* $\mathrm{C} = \langle (b(x) \mid 0 \mid 0), (l(x) \mid a(x) \mid 0), (g_1(x) \mid g_2(x) \mid g_3(x))\rangle$*, where* $b(x), l(x), g_1(x) \in \mathbb{Z}_{2,r}[x]$ *with* $b(x)|x^r - 1$ *and* $a(x), g_2(x) \in \mathbb{Z}_{2,s}[x]$ *with* $a(x)|x^s - 1$ *and* $g_3(x) \in \mathbb{Z}_{2,t}[x]$ *with* $g_3(x)|x^t - 1$*.*

Proof. Consider the canonical projection $\pi_t : \mathrm{C} \to \mathbb{Z}_{2,t}[x]$ such that $(c_1 \mid c_2 \mid c_3) \mapsto c_3$. It is easy to see that π_t is a $\mathbb{Z}_2[x]$-module homomorphism with kernel $ker_{\mathrm{C}}(\pi_t) = \{(c_1 \mid c_2 \mid 0) \in \mathrm{C}\}$, and therefore the set $K = \{(c_1 \mid c_2) \in \mathrm{C} : (c_1 \mid c_2 \mid 0) \in \mathrm{C}\}$ is a $\mathbb{Z}_2$-double cyclic code of block length (r,s) in $\mathrm{R}_{r,s}[x]$. From Theorem 3, there exist $b, l \in \mathbb{Z}_{2,r}[x]$ and $a \in \mathbb{Z}_{2,s}[x]$ such that $K = \langle (b \mid 0), (l \mid a)\rangle$, with $b|x^r - 1$ and $a|x^s - 1$. This implies that $ker_{\mathrm{C}}(\pi_t) = \langle (b \mid 0 \mid 0), (l \mid a \mid 0)\rangle$. On the other hand the image of C under π_t is an ideal of $\mathbb{Z}_{2,t}[x]$ and as $\mathbb{Z}_{2,t}[x]$ is a PID, there exists $g_3 \in \mathbb{Z}_{2,t}[x]$ such that $\pi_t(\mathrm{C}) = \langle g_3\rangle$. Therefore we have $\frac{\mathrm{C}}{Ker_{\mathrm{C}}(\pi_t)} \cong \pi_t(\mathrm{C})$, and hence $\mathrm{C} = \langle (b \mid 0 \mid 0), (l \mid a \mid 0), (g_1 \mid g_2 \mid g_3)\rangle$ for some $g_1 \in \mathbb{Z}_{2,r}[x]$ and $g_2 \in \mathbb{Z}_{2,s}[x]$. Hence the theorem. □

Let $(c_1 \mid 0 \mid 0) \in \mathrm{C}$. Then $(c_1 \mid 0) \in K = \{(c_1 \mid c_2) \in \mathrm{C} : (c_1 \mid c_2 \mid 0) \in \mathrm{C}\}$. Also, from Theorem 5, we have $K = \langle (b \mid 0), (l \mid a)\rangle$. Therefore $c_1 \in \langle b\rangle$. Hence $(c_1 \mid 0 \mid 0) \in \mathrm{C}$ implies that $c_1 \in \langle b\rangle$. The following results are useful to understand the structure of $\mathbb{Z}_2$-triple cyclic code and to determine their minimal spanning sets. The minimal spanning set of a $\mathbb{Z}_2$-triple cyclic code can be used to determine its cardinality and the generator matrix. In the rest of the paper we consider the $\mathbb{Z}_2$-triple cyclic code as defined in Theorem 5.

Lemma 1. *Let* $\mathrm{C} = \langle (b \mid 0 \mid 0), (l \mid a \mid 0), (g_1 \mid g_2 \mid g_3)\rangle$ *be a* $\mathbb{Z}_2$*-triple cyclic code of block length* (r,s,t)*. Then* $deg(l) < deg(b)$ *and* $deg(g_1) < deg(b)$*.*

Proof. Assume $\deg(l) \geq \deg(b)$. By applying division algorithm, there exist polynomials q and r in $\mathbb{Z}_2[x]$ such that $l = bq + r$, where $r = 0$ or $\deg(r) < \deg(b)$.
Then

$$\begin{aligned}\langle (b \mid 0 \mid 0), (l \mid a \mid 0)\rangle &= \langle (b \mid 0 \mid 0), (bq + r \mid a \mid 0)\rangle \\ &= \langle (b \mid 0 \mid 0), (r \mid a \mid 0)\rangle.\end{aligned}$$

Hence, we may assume that $\deg(l) < \deg(b)$. Similarly, we can show $\deg(g_1) < \deg(b)$. □

Lemma 2. *Let* $\mathrm{C} = \langle (b \mid 0 \mid 0), (l \mid a \mid 0), (g_1 \mid g_2 \mid g_3)\rangle$ *be a* $\mathbb{Z}_2$*-triple cyclic code of block length* (r,s,t)*. Then* *(i)* $b|\frac{x^s-1}{a}l$;

(ii) $a|\frac{x^t-1}{g_3}g_2$ *and if* $g_2 = 0$, *then* $b|\frac{x^t-1}{g_3}g_1$;

(iii) b divides $\frac{x^t-1}{g_3 a}lg_2 + \frac{x^t-1}{g_3}g_1$.

Proof. We have $\frac{x^s-1}{a}(l \mid a \mid 0) = \left(\frac{x^s-1}{a}l \mid 0 \mid 0\right) \in \mathrm{C}$. This implies that $\frac{x^s-1}{a}l \in \langle b\rangle$ and hence $b|\frac{x^s-1}{a}l$. Similarly, we can prove the second result. For result (3), as $a|\frac{x^t-1}{g_3}g_2$, we have $\frac{x^t-1}{g_3}g_2 = ka$ for some $k \in \mathbb{Z}_2[x]$. Also as $(kl \mid ka \mid 0), (\frac{x^t-1}{g_3}g_1 \mid \frac{x^t-1}{g_3}g_2 \mid 0) \in \mathrm{C}$, implies that $(kl \mid ka \mid 0) + (\frac{x^t-1}{g_3}g_1 \mid \frac{x^t-1}{g_3}g_2 \mid 0) = (kl + \frac{x^t-1}{g_3}g_1 \mid 0 \mid 0) \in \mathrm{C}$. The result follows as $kl + \frac{x^t-1}{g_3}g_1 \in \langle b\rangle$. □

In the following theorem we determine a minimal spanning set for a $\mathbb{Z}_2$-triple cyclic code.

Theorem 6. *Let* $\mathrm{C} = \langle (b \mid 0 \mid\ 0), (l \mid a \mid 0), (g_1 \mid g_2 \mid g_3)\rangle$ *be a* $\mathbb{Z}_2$*-triple cyclic code of block length* (r, s, t) *such that* $b, l, g_1 \in \mathbb{Z}_{2,r}[x]$, $a, g_2 \in \mathbb{Z}_{2,s}[x]$, $g_3 \in \mathbb{Z}_{2,t}[x]$ *with* $b|x^r - 1$, $a|x^s - 1$ *and* $g_3|x^t - 1$. *Let* $h_1 = \frac{x^r-1}{b}$, $h_2 = \frac{x^s-1}{a}$ *and* $h_3 = \frac{x^t-1}{g_3}$. *If deg*$(b) = t_1$, *deg*$(a) = t_2$ *and deg*$(g_3) = t_3$, *then a minimal spanning set for* C *is* $S = S_1 \cup S_2 \cup S_3$, *where*

$$S_1 = \bigcup_{i=0}^{r-t_1-1} x^i * (b \mid 0 \mid 0) \quad S_2 = \bigcup_{i=0}^{s-t_2-1} x^i * (l \mid a \mid 0) \quad S_3 = \bigcup_{i=0}^{t-t_3-1} x^i * (g_1 \mid g_2 \mid g_3).$$

Moreover, $\mid \mathrm{C} \mid = 2^{r+s+t-deg(b)-deg(a)-deg(g_3)}$.

Proof. Let c be a codeword in C. Then there exist d_1, d_2, $d_3 \in \mathbb{Z}_2[x]$ such that

$$\begin{aligned} c &= d_1 * (b \mid 0 \mid 0) \ + \ d_2 * (l \mid a \mid 0) \ + \ d_3 * (g_1 \mid g_2 \mid g_3) \\ &= (d_1 b \mid 0 \mid 0) \ + \ (d_2 l \mid d_2 a \mid 0) \ + \ (d_3 g_1 \mid d_3 g_2 \mid d_3 g_3) \end{aligned} \tag{1}$$

We first show that $d_1 * (b \mid 0 \mid 0) \in span(S_1)$. If $\deg(d_1) < r - t_1$, then obviously $d_1 * (b \mid 0 \mid 0) \in span(S_1)$. Let $\deg(d_1) \geq r - t_1$. By division algorithm, there exist Q_1,$R_1$$\in \mathbb{Z}_2[x]$ such that $d_1 = Q_1\frac{x^r-1}{b} + R_1$ with $R_1 = 0$ or $\deg(R_1) < r - t_1$. Then

$$\begin{aligned} (d_1 b \mid 0 \mid 0) &= \left(\left(Q_1\frac{x^r-1}{b} + R_1\right) b \mid 0 \mid 0\right) \\ &= (Q_1(x^r - 1) + R_1 b \mid 0 \mid 0) \\ &= Q_1(x^r - 1 \mid 0 \mid 0) + R_1(b \mid 0 \mid 0) \\ &= R_1(b \mid 0 \mid 0) \in span(S_1). \end{aligned}$$

Next we show that $d_2 * (l \mid a \mid 0) \in \ span(S_1 \cup S_2)$. We have by division algorithm $d_2 = Q_2 h_2 + R_2$ with $R_2 = 0$ or $\deg(R_2) < s - t_2$, $Q_2, R_2 \in \mathbb{Z}_2[x]$. Therefore

$$d_2 * (l \mid a \mid 0) = (Q_2 h_2 + R_2)(l \mid a \mid 0)$$

$$= Q_2(lh_2 \mid 0 \mid 0) + R_2(l \mid a \mid 0). \tag{2}$$

Since $0 \leq \deg(R_2) \leq s - t_2 - 1$, we have $R_2(l \mid a \mid 0) \in span(S_2)$. Also from Lemma 2, we have $b \mid h_2 l$, which implies that $Q_2(lh_2 \mid 0 \mid 0) \in span(S_1)$. Therefore from (2) we get $d_2 * (l \mid a \mid 0) \in span(S_1 \cup S_2)$.

Finally we show that $d_3 * (g_1 \mid g_2 \mid g_3)$ belongs to $span(S_1 \cup S_2 \cup S_3)$. Again by the division algorithm, we have $d_3 = Q_3 h_3 + R_3$ with $R_3 = 0$ or $\deg(R_3) < t - t_3$, where Q_3 and $R_3 \in \mathbb{Z}_2[x]$. Then

$$\begin{aligned} d_3 * (g_1 \mid g_2 \mid g_3) &= (Q_3 h_3 + R_3)\,(g_1 \mid g_2 \mid g_3) \\ &= Q_3 h_3 (g_1 \mid g_2 \mid 0) + R_3 (g_1 \mid g_2 \mid g_3). \end{aligned} \tag{3}$$

It easy to see that $Q_3 h_3 (g_1 \mid g_2 \mid 0) \in \mathrm{C}$ and hence $Q_3 h_3 (g_1 \mid g_2) \in K = \{(c_1 \mid c_2) : (c_1 \mid c_2 \mid 0) \in \ker_{\mathrm{C}}(\pi_t)\}$. From Theorem 4, we have $Q_3 h_3 (g_1 \mid g_2) \in span(S_1' \cup S_2')$. This implies that, $Q_3 h_3 (g_1 \mid g_2 \mid 0) \in span(S_1 \cup S_2)$. Also, $R_3 (g_1 \mid g_2 \mid g_3) \in span(S_3)$, as $\deg(R_3) < t - t_3$. Therefore, from (3), $d_3 * (g_1 \mid g_2 \mid g_3) \in span(S_1 \cup S_2 \cup S_3)$. Hence $\mathrm{C} \in span(S_1 \cup S_2 \cup S_3)$. The second result follows as S is linearly independent. □

The following example illustrates this.

Example 1. *Let* $r = s = t = 7$. *We have* $x^7 - 1 = (x+1)(x^3+x+1)(x^3+x^2+1)$ *over* $\mathbb{Z}_2$. *Let* $\mathrm{C} = \langle (b \mid 0 \mid 0), (l \mid a \mid 0), (g_1 \mid g_2 \mid g_3) \rangle$, *where* $b = (x+1)(x^3+x^2+1)$, $l = (x+1)^2$, $a = (x+1)(x^3+x+1)$, $g_1 = x+1$, $g_2 = x^2+x$ *and* $g_3 = (x+1)(x^3+x^2+1)$. *Then,* C *satisfies all the conditions of Lemma 1 and Lemma 2. Therefore,* C *is a* $\mathbb{Z}_2$*-triple cyclic code of block length* $(7,7,7)$. *Also,* $S = S_1 \cup S_2 \cup S_3$ *forms a generating set for* C, *where* $S_1 = \cup_{i=0}^{2} x^i (x^4+x^2+x+1 \mid 0 \mid 0)$, $S_2 = \cup_{i=0}^{2} x^i (x^2+1 \mid x^4+x^3+x^2+1 \mid 0)$ *and* $S_3 = \cup_{i=0}^{2} x^i (x+1 \mid x+x^2 \mid x^4+x^2+x+1)$. *The cardinality of* C *is* 2^9. *Also,* C *is generated by the generator matrix* G, *where*

$$G = \begin{pmatrix} 1\,1\,1\,0\,1\,0\,0 & 0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0 \\ 0\,1\,1\,1\,0\,1\,0 & 0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,1\,1\,1\,0\,1 & 0\,0\,0\,0\,0\,0\,0 & 0\,0\,0\,0\,0\,0\,0 \\ 1\,0\,1\,0\,0\,0\,0 & 1\,0\,1\,1\,1\,0\,0 & 0\,0\,0\,0\,0\,0\,0 \\ 0\,1\,0\,1\,0\,0\,0 & 0\,1\,0\,1\,1\,1\,0 & 0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,1\,0\,1\,0\,0 & 0\,0\,1\,0\,1\,1\,1 & 0\,0\,0\,0\,0\,0\,0 \\ 1\,1\,0\,0\,0\,0\,0 & 0\,1\,1\,0\,0\,0\,0 & 1\,1\,1\,0\,1\,0\,0 \\ 0\,1\,1\,0\,0\,0\,0 & 0\,0\,1\,1\,0\,0\,0 & 0\,1\,1\,1\,0\,1\,0 \\ 0\,0\,1\,1\,0\,0\,0 & 0\,0\,0\,1\,1\,0\,0 & 0\,0\,1\,1\,1\,0\,1 \end{pmatrix}.$$

Further, the minimum Hamming distance of C *is* 4 *and therefore,* C *is a* $[21, 9, 4]$ *binary linear code with the Hamming weight distribution given by* $[< 0, 1 >, < 4, 7 >, < 6, 21 >, < 8, 98 >, < 10, 154 >, < 12, 175 >, < 14, 49 >, < 16, 7 >]$.

3. Duals of $\mathbb{Z}_2$-triple cyclic codes

In this section, we determine the duals of $\mathbb{Z}_2$-triple cyclic codes of block length (r, s, t). In Theorem 1, it is shown that the dual $\mathrm{C}^{\perp}$ of a $\mathbb{Z}_2$-triple cyclic code C is also a $\mathbb{Z}_2$-triple cyclic code. Therefore, we may let $\mathrm{C}^{\perp} = \langle (\hat{b} \mid 0 \mid 0), (\hat{l} \mid \hat{a} \mid 0), (\hat{g}_1 \mid \hat{g}_2 \mid \hat{g}_3) \rangle$ with $\hat{b} | x^r - 1$, $\hat{a} | x^s - 1$ and $\hat{g}_3 | x^t - 1$ over $\mathbb{Z}_2$. Further, let $m = lcm(r, s, t)$ and denote the polynomial $\sum_{i=0}^{m-1} x^i$ by $\theta_m(x)$. Then by [4, Preposition 4.2], we have the following result.

Proposition 1. *Let $r, s, t \in \mathbb{N}$ and $m = lcm(r, s, t)$. Then, $x^m - 1 = \theta_{\frac{m}{r}}(x^r)(x^r - 1) = \theta_{\frac{m}{s}}(x^s)(x^s - 1) = \theta_{\frac{m}{t}}(x^t)(x^t - 1)$.*

For any polynomials $f, g \in \mathbb{Z}_2[x]$, we denote the g.c.d. of f and g by (f, g), and we extend this notation for three or more polynomials. For any polynomial f of degree n the reciprocal of f is defined as $f^* = x^n f(\frac{1}{x})$. The following result is usefull for our study.

Theorem 7. *Let f and g be two binary polynomials, such that $\deg(f) \geq \deg(g)$. Then*

(i) $\deg(f) \geq \deg(f^*)$, *and equality holds if* $x \nmid f$;

(ii) $(fg)^* = f^* g^*$;

(iii) $(f + g)^* = f^* + x^{\deg(f) - \deg(g)} g^*$;

(iv) $g \mid f \Rightarrow g^* \mid f^*$ *and*

(v) $(f^*, g^*) = (f, g)^*$.

Proof. The proofs of 1, 2 and 3 are straight forward. For 4, let $g \mid f$, so that $f = kg$ for some $k \in \mathbb{Z}_2[x]$. Then $f^* = k^* g^*$. Therefore $g^* \mid f^*$. From the definition of g.c.d., there exist $m_1, m_2 \in \mathbb{Z}_2[x]$ such that $(f, g) = m_1 f + m_2 g$. Assuming $\deg(m_1 f) \geq \deg(m_2 g)$, we get

$$(f, g)^* = m_1^* f^* + x^{\deg(m_1 f) - \deg(m_2 g)} m_2^* g^*.$$

Again as $(f^*, g^*) \mid f^*$ and $(f^*, g^*) \mid g^*$, so $(f^*, g^*) \mid (f, g)^*$. On the other hand, $(f, g) \mid f$ implies that $(f, g)^* \mid f^*$. Similarly $(f, g)^* \mid g^*$. Hence

$$(f, g)^* \mid (f^*, g^*).$$

The result follows. □

Remark 1. *If $x \nmid f$ or $x \nmid g$, then it is easy to prove that $\deg(f^*, g^*) = \deg(f, g)^* = \deg(f, g)$.*

Now we define a mapping $\psi : \mathrm{R}_{r,s,t}[x] \times \mathrm{R}_{r,s,t}[x] \rightarrow \frac{\mathbb{Z}_2[x]}{\langle x^m - 1 \rangle}$ such that

$$\psi(u, v) = u_1 \theta_{\frac{m}{r}}(x^r) x^{m - \deg(v_1) - 1} v_1^* + u_2 \theta_{\frac{m}{s}}(x^s) x^{m - \deg(v_2) - 1} v_2^* + u_3 \theta_{\frac{m}{r}}(x^r) x^{m - \deg(v_3) - 1} v_3^*, \tag{4}$$

where $u = (u_1 \mid u_2 \mid u_3)$, $v = (v_1 \mid v_2 \mid v_3) \in \mathrm{R}_{r,s,t}[x]$. The map ψ is a bilinear map between the two $\mathbb{Z}_2[x]$-modules. ψ is a generalization of a similar map defined in [4] for $\mathbb{Z}_2$-double cyclic codes.

Lemma 3. *Let $u = (u_1 \mid u_2 \mid u_3)$, $v = (v_1 \mid v_2 \mid v_3)$ be elements in $\mathbb{Z}_2^r \times \mathbb{Z}_2^s \times \mathbb{Z}_2^t$ with associated polynomials $u(x) = (u_1(x) \mid u_2(x) \mid u_3(x))$ and $v(x) = (v_1(x) \mid v_2(x) \mid v_3(x))$ in $\mathrm{R}_{r,s,t}[x]$. Then u is orthogonal to v and all its cyclic shifts if and only if $\psi(u, v) = 0$.*

Proof. Let $u = (u_{1,0}, u_{1,1}, \cdots, u_{1,r-1} \mid u_{2,0}, u_{2,1}, \cdots, u_{2,s-1} \mid u_{3,0}, u_{3,1}, \cdots, u_{3,t-1})$ and $v = (v_{1,0}, v_{1,1}, \cdots, v_{1,r-1} \mid v_{2,0}, v_{2,1}, \cdots, v_{2,s-1} \mid v_{3,0}, v_{3,1}, \cdots, v_{3,t-1})$ be two elements in $\mathbb{Z}_2^r \times \mathbb{Z}_2^s \times \mathbb{Z}_2^t$. Let $\sigma^{(i)}(v)$ be the i-th shift of v. Then $\sigma^{(i)}(v) = (v_{1,0+i}, v_{1,1+i}, \cdots, v_{1,i-1} \mid v_{2,0+i}, v_{2,1+i}, \cdots, v_{2,i-1} \mid v_{3,0+i}, v_{3,1+i}, \cdots, v_{3,i-1})$ for $1 \leq i \leq m-1$. Under polynomial representation we have

$$\psi(u, \sigma^{(i)}(v)) = \sum_{p=0}^{r-1} \left(\theta_{\frac{m}{r}}(x^r) \sum_{j=0}^{r-1} u_{1,j} v_{1,p+j} x^{m-1-p} \right) + \sum_{q=0}^{s-1} \left(\theta_{\frac{m}{s}}(x^s) \sum_{k=0}^{s-1} u_{2,k} v_{2,q+k} x^{m-1-q} \right) + \sum_{l=0}^{t-1} \left(\theta_{\frac{m}{t}}(x^t) \sum_{w=0}^{t-1} u_{3,w} v_{3,l+w} x^{m-1-l} \right).$$

Rearranging the terms in the summation we get

$$\psi(u, \sigma^{(i)}(v)) = \sum_{i=0}^{m-1} S_i x^{m-1-i} \bmod (x^m - 1),$$

where $S_i = \sum_{j=0}^{r-1} u_{1,j} v_{1,i+j} + \sum_{k=0}^{s-1} u_{2,k} v_{2,i+k} + \sum_{l=0}^{t-1} u_{1,l} v_{2,i+l}$. On the other hand, we have $u \cdot \sigma^{(i)}(v) = \sum_{j=0}^{r-1} u_{1,j} v_{1,i+j} + \sum_{k=0}^{s-1} u_{2,k} v_{2,i+k} + \sum_{l=0}^{t-1} u_{1,l} v_{2,i+l} = S_i$. Thus, $\psi(u, \sigma^{(i)}(v)) = 0$ if and only if $S_i = 0$ for all $1 \leq i \leq m-1$. Hence the result. □

Lemma 4. *Let $u = (u_1 \mid u_2 \mid u_3)$ and $v = (v_1 \mid v_2 \mid v_3)$ in $\mathrm{R}_{r,s,t}[x]$ such that $\psi(u, v) = 0$. Then*

(i) If $u_2 = 0$ or $v_2 = 0$ and $u_3 = 0$ or $v_3 = 0$, then $u_1 v_1^* = 0 \pmod{x^r - 1}$.

(ii) If $u_1 = 0$ or $v_1 = 0$ and $u_3 = 0$ or $v_3 = 0$, then $u_2 v_2^* = 0 \pmod{x^s - 1}$.

(iii) If $u_1 = 0$ or $v_1 = 0$ and $u_2 = 0$ or $v_2 = 0$, then $u_3 v_3^* = 0 \pmod{x^t - 1}$.

Proof. Let $u_2 = 0$ or $v_2 = 0$ and $u_3 = 0$ or $v_3 = 0$. Then from the definition of ψ, we have $\psi(u, v) = u_1 \theta_{\frac{m}{r}}(x^r) x^{m-\deg(v_1)-1} v_1^* = 0 \pmod{x^m - 1}$. This implies that $u_1 \theta_{\frac{m}{r}}(x^r) x^{m-\deg(v_1)-1} v_1^* = (x^m - 1) g$ for some $g \in \mathbb{Z}_2[x]$. Taking $f = x^{\deg(v_1)+1} g$, we get $u_1 \theta_{\frac{m}{r}}(x^r) x^m v_1^* = f(x^m - 1)$ and therefore $u_1 (x^m - 1) x^m v_1^* = (x^m - 1)(x^r - 1) f$. Since x and $x^r - 1$ are relatively prime, we have $u_1 v_1^* = 0 \pmod{x^r - 1}$. Other results can be proved similarly. □

Now we determine the form of generator matrix of a $\mathbb{Z}_2$-triple cyclic code. The generator matrix of a $\mathbb{Z}_2$-triple cyclic code C determines the cardinalities of the projections C_r, C_s and C_t and their duals, and these are further be used to obtain the duals of a $\mathbb{Z}_2$-triple cyclic codes.

Let $\mathrm{C} = \langle (b \mid 0 \mid 0), (l \mid a \mid 0), (g_1 \mid g_2 \mid g_3) \rangle$ be a $\mathbb{Z}_2$-triple cyclic code of block length (r, s, t) and $\mathrm{C}^\perp$ be its dual. Then from Theorem 6, C is spanned by $S = S_1 \cup S_2 \cup S_3$ and therefore C is generated by the matrix whose rows are the elements of the set S. Let C_1, C_2 and C_3 be the subcodes of C generated by S_1, S_2 and S_3, respectively, and let $\mathbf{G}_1$, $\mathbf{G}_2$ and $\mathbf{G}_3$ be their generator matrices, where $\mathbf{G}_1 = (I_{r-\deg(b)} \quad A \mid 0 \mid 0), \mathbf{G}_2 = (B \mid C \quad I_{r-\deg(a)} \mid 0), \mathbf{G}_3 = (D \mid E \mid F \quad I_{t-\deg(g_3)})$. Then, the matrix $\mathbf{G} = \begin{pmatrix} \mathbf{G}_1 \\ \mathbf{G}_2 \\ \mathbf{G}_3 \end{pmatrix}$ forms a generator matrix for C.

We obtain an equivalent form of the matrix $\mathbf{G}$ by adjusting its rows, so that we can make use of this equivalent form to find the cardinalities of the respective projections C_r, C_s and C_t. It is easy to see that C_r is generated by (b, l, g_1), and this implies that the dimension of C_r is $r - \deg(b, l, g_1)$, which is greater than or equal to $r - \deg(b)$. Therefore, the matrices B and D must have submatrices, say B_{ϵ_1} and D_{ϵ_2} of full ranks ϵ_1 and ϵ_2, respectively, such that $\epsilon_1 + \epsilon_2 = \deg(b) - \deg(b, l, g_1)$. Add the corresponding rows of $\mathbf{G}_2$ and $\mathbf{G}_3$ that contain B_{ϵ_1} and D_{ϵ_2}, to $\mathbf{G}_1$. As a result, $\mathbf{G}_2$ and $\mathbf{G}_3$ are now reduced to the matrices of the form $\mathbf{G}_2' = (0 \mid C_1 \quad I_{r-\deg(a)-\epsilon_1} \mid 0)$ and $\mathbf{G}_3' = (0 \mid E_1 \mid F_1 \quad I_{t-\deg(g_3)-\epsilon_2})$. Similarly the dimension of C_s is $s - \deg(a, g_2)$, as C_s is generated by (a, g_2). Therefore, the matrix E_1 must have a submatrix, say E_{k_1}, of full rank $k_1 = \deg(a) - \epsilon_2 - \deg(a, g_2)$. Again, adding the rows that contain the matrix E_{k_1}, to $\mathbf{G}_2'$, we get the remaining part of the generating matrix $\mathbf{G}$ of C as $(0 \mid 0 \mid F_1' \quad I_{t-\deg(g_3)-\epsilon_2-k_1})$. Let $k_2 = \deg(g_3) + \epsilon_2 + k_1 = \deg(a) + \deg(g_3) - \deg(a, g_2)$. Therefore, the generator matrix $\mathbf{G}$ of C is permutation equivalent to the matrix $\mathbf{G}'$, where

$$\mathbf{G}' = \left(\begin{array}{cccc|ccccc|cccc}
I_{r-\deg(b)} & A_1 & A_2 & A_3 & & & & & & & & & \\
 & B_{\epsilon_1} & B_1 & B_2 & C_{11} & I_{\epsilon_1} & & & & & & & \\
 & & 0 & 0 & C_{21} & R_1 & I_{s-\deg(a)-\epsilon_1} & 0 & 0 & & & & \\
 & & D_{\epsilon_2} & D_{11} & E_{11} & E_{12} & & E_{\epsilon_2} & E_{14} & F_{11} & I_{\epsilon_2} & & \\
 & & & & E_{21} & E_{22} & & E_{k_1} & E_{24} & F_{21} & R_2 & I_{k_1} & \\
 & & & & & & & & & F_{31} & F_{32} & R_3 & I_{t-k_2}
\end{array}\right).$$

The cardinalities of C_r, C_s and C_t and their duals follow from $\mathbf{G}'$. The cardinalities of $(\mathrm{C}^\perp)_r$, $(\mathrm{C}^\perp)_s$ and $(\mathrm{C}^\perp)_t$ can be obtained by projecting the parity check matrix of C on first r coordinates, next s coordinates and remaining last t coordinates, respectively. The results are summarized in the following theorem.

Theorem 8. *Let* $\mathrm{C} = \langle (b \mid 0 \mid 0), (l \mid a \mid \ 0), (g_1 \mid g_2 \mid g_3) \rangle$ *be a* $\mathbb{Z}_2$*-triple cyclic code of block length* (r, s, t)*. Then,*

$$\begin{array}{lll}
\mid \mathrm{C}_r \mid = 2^{r-deg(b)+\epsilon} & \mid (\mathrm{C}_r)^\perp \mid = 2^{deg(b,l,g_1)} & \mid (\mathrm{C}^\perp)_r \mid = 2^{deg(b)}, \\
\mid \mathrm{C}_s \mid = 2^{r-deg(a,g_2)} & \mid (\mathrm{C}_s)^\perp \mid = 2^{deg(a,g_2)} & \mid (\mathrm{C}^\perp)_s \mid = 2^{deg(a)+\epsilon_1} \text{ and} \\
\mid \mathrm{C}_t \mid = 2^{r-deg(g_3)} & \mid (\mathrm{C}_t)^\perp \mid = 2^{deg(g_3)} & \mid (\mathrm{C}^\perp)_t \mid = 2^{k_2},
\end{array}$$

where $\epsilon = deg(b) - deg(b, l, g_1)$ *and* $k_2 = deg(a) + deg(g_3) - deg(a, g_2)$*.*

Theorem 9. *Let* $\mathrm{C} = \langle (b \mid 0 \mid 0), (l \mid a \mid 0), (g_1 \mid g_2 \mid g_3)\rangle$ *be a* $\mathbb{Z}_2$*-triple cyclic code of block length* (r, s, t) *and* $\mathrm{C}^{\perp} = \langle (\hat{b} \mid 0 \mid 0), (\hat{l} \mid \hat{a} \mid 0), (\hat{g}_1 \mid \hat{g}_2 \mid \hat{g}_3)\rangle$ *be the dual of* C*. Then*

$$\hat{b} = \frac{x^r - 1}{(b, l, g_1)^*}.$$

Proof. First we determine the degree of $\hat{b}$. From the definition of $\mathrm{C}^{\perp}$, it is easy to show that $(\mathrm{C}_r)^{\perp} = \langle \hat{b} \rangle$. This implies that $\mid (\mathrm{C}_r)^{\perp} \mid = 2^{r-\deg(\hat{b})}$. From Theorem 8, we have $\mid (\mathrm{C}_r)^{\perp} \mid = 2^{\deg(b,l,g_1)}$. Therefore

$$\deg(\hat{b}) = r - \deg(b, l, g_1). \tag{5}$$

Now, as $(\hat{b} \mid 0 \mid 0) \in \mathrm{C}^{\perp}$, from the definition of ψ, we have

$$\psi\Big((\hat{b} \mid 0 \mid 0), (b \mid 0 \mid 0)\Big) = \psi\Big((\hat{b} \mid 0 \mid 0), (l \mid a \mid 0)\Big) = \psi\Big((\hat{b} \mid 0 \mid 0), (g_1 \mid g_2 \mid g_3)\Big) = 0,$$

all modulo $(x^m - 1)$. This implies that $\hat{b}\ b^* = \hat{b}\ l^* = \hat{b}\ g_1^* = 0 \pmod{x^r - 1}$. Therefore, $\hat{b}\ \gcd(b^*, l^*, g_1^*) = 0 \pmod{x^r - 1}$. Since $(b^*, l^*, g_1^*) = (b, l, g_1)^*$, we have $\hat{b}\ \gcd(b, l, g_1)^* = 0 \pmod{x^r - 1}$. Then there exists $\lambda \in \mathbb{Z}_2[x]$ such that,

$$\hat{b}\ (b, l, g_1)^* = \lambda(x^r - 1) \tag{6}$$

From equations (5) and (6), we get $\lambda = 1$ and hence $\hat{b}\ (b, l, g_1)^* = (x^r - 1)$. □

Lemma 5. *Let* $\mathrm{C} = \langle (b \mid 0 \mid 0), (l \mid a \mid 0), (g_1 \mid g_2 \mid g_3)\rangle$ *be a* $\mathbb{Z}_2$*-triple cyclic code of block length* (r, s, t)*. Then* $\left(0 \mid 0 \mid \frac{abg_3}{(a,g_2)}\right) \in \mathrm{C}$.

Proof. Since $(b \mid 0 \mid 0), (l \mid a \mid 0) \in \mathrm{C}$, so $l(b \mid 0 \mid 0) + b(l \mid a \mid 0) = (0 \mid ab \mid 0) \in \mathrm{C}$. Similarly $(b \mid 0 \mid 0), (g_1 \mid g_2 \mid g_3) \in \mathrm{C}$ implies that $(0 \mid bg_2 \mid bg_3) \in \mathrm{C}$. Therefore, as $(0 \mid ab \mid 0), (0 \mid bg_2 \mid bg_3) \in \mathrm{C}$, we have $\frac{g_2}{(a,g_2)}(0 \mid ab \mid 0) + \frac{a}{(a,g_2)}(0 \mid bg_2 \mid bg_3) = \left(0 \mid 0 \mid \frac{abg_3}{(a,g_2)}\right) \in \mathrm{C}$. □

Theorem 10. *Let* $\mathrm{C} = \langle (b \mid 0 \mid 0), (l \mid a \mid 0), (g_1 \mid g_2 \mid g_3)\rangle$ *be a* $\mathbb{Z}_2$*-triple cyclic code of block length* (r, s, t) *and* $\mathrm{C}^{\perp} = \langle (\hat{b} \mid 0 \mid 0), (\hat{l} \mid \hat{a} \mid 0), (\hat{g}_1 \mid \hat{g}_2 \mid \hat{g}_3)\rangle$ *be the dual of* C*. Then*

$$\hat{g}_3 = \frac{(x^t - 1)(a, g_2)^*}{a^* g_3^*}.$$

Proof. Again, first we determine the degree of $\hat{g}_3$. From the definition of $\mathrm{C}^{\perp}$, it is easy to show that $(\mathrm{C}^{\perp})_s = \langle \hat{g}_3 \rangle$ and this implies that $\mid (\mathrm{C}^{\perp})_s \mid = 2^{t-\deg(\hat{g}_3)}$. Also from Theorem 8, we have $\mid (\mathrm{C}^{\perp})_s \mid = 2^{k_2}$. Therefore

$$\deg(\hat{g}_3) = t - \deg(g_3) - \deg(a) + \deg(a, g_2). \tag{7}$$

Now from Lemma 5, we have $\left(0 \mid 0 \mid \frac{abg_3}{(a,g_2)}\right) \in \mathrm{C}$ and also, as $(\hat{g}_1 \mid \hat{g}_2 \mid \hat{g}_3) \in \mathrm{C}^\perp$, we have $\psi\left(\left(0 \mid 0 \mid \frac{abg_3}{(a,g_2)}\right), (\hat{g}_1 \mid \hat{g}_2 \mid \hat{g}_3)\right) = 0 \pmod{x^m - 1}$. This implies that $\hat{g}_3 \frac{a^* b^* g_3^*}{(a,g_2)^*} = 0 \pmod{x^t - 1}$, and therefore $\hat{g}_3 \frac{a^* g_3^*}{(a,g_2)^*} = 0 \pmod{x^t - 1}$. Hence $\hat{g}_3 \frac{a^* g_3^*}{(a,g_2)^*} = \lambda'(x^t - 1)$ for some $\lambda' \in \mathbb{Z}_2[x]$. From the degree consideration of $\hat{g}_3$ i.e. from (7), we get $\lambda' = 1$. The result follows. □

Theorem 11. *Let* $\mathrm{C} = \langle (b \mid 0 \mid 0), (l \mid a \mid 0), (g_1 \mid g_2 \mid g_3) \rangle$ *be a* $\mathbb{Z}_2$*-triple cyclic code of block length* (r, s, t) *and* $\mathrm{C}^\perp = \langle (\hat{b} \mid 0 \mid 0), (\hat{l} \mid \hat{a} \mid 0), (\hat{g}_1 \mid \hat{g}_2 \mid \hat{g}_3) \rangle$ *be the dual of* C. *Then, for some* $\lambda_1,\ \lambda_2 \in \mathbb{Z}_2[x]$, *we have*

$$\hat{g}_1\ b^* = \lambda_1(x^r - 1) \qquad \text{and} \qquad \hat{g}_2\ a^* b^* = \lambda_2(x^s - 1)(b, l, g_1)^*.$$

Proof. From the definitions of C and $\mathrm{C}^\perp$, we have $\psi((\hat{g}_1 \mid \hat{g}_2 \mid \hat{g}_3), (b \mid 0 \mid 0)) = 0 \pmod{x^m - 1}$. This implies that $\hat{g}_1\ b^* = \lambda_1(x^r - 1)$ for some $\lambda_1 \in \mathbb{Z}_2[x]$.

On the other hand, it is easy to show that $\left(0 \mid \frac{ab}{(b,l,g_1)} \mid 0\right) \in \mathrm{C}$. Therefore, $\psi\left(\left(0 \mid \frac{ab}{(b,l,g_1)} \mid 0\right), (\hat{g}_1 \mid \hat{g}_2 \mid \hat{g}_3)\right) = 0 \pmod{x^m - 1}$. This implies that $\hat{g}_2\ a^* b^* = \lambda_2(x^s - 1)(b, l, g_1)^*$ for some $\lambda_2 \in \mathbb{Z}_2[x]$. □

In the following theorem, we obtain the explicit forms for λ_1 and λ_2 that are given in Theorem 11.

Theorem 12. *Let* $\mathrm{C} = \langle (b \mid 0 \mid 0), (l \mid a \mid 0), (g_1 \mid g_2 \mid g_3) \rangle$ *be a* $\mathbb{Z}_2$*-triple cyclic code of block length* (r, s, t) *and* $\mathrm{C}^\perp = \langle (\hat{b} \mid 0 \mid 0), (\hat{l} \mid \hat{a} \mid 0), (\hat{g}_1 \mid \hat{g}_2 \mid \hat{g}_3) \rangle$ *be the dual code of* C. *Let* $\rho_1 = \frac{l^*}{(b,l,g_1)^*}$ *and* $\rho_2 = \frac{g_2^*}{(a,g_2)^*}$. *Then* $\hat{g}_1 b^* = \lambda_1(x^r - 1)$ *and* $\hat{g}_2\ a^* b^* = \lambda_2(x^s - 1)(b, l, g_1)^*$, *where*

$$\lambda_1 = (\rho_1)^{-1} (\rho_2)^{-1} \frac{b^*}{(b, l, g_1)^*} x^{2m + deg(l) - deg(a) + deg(g_2) - deg(g_3)} \left(\bmod \left(\frac{(b, g_1)^*}{(b, l, g_1)^*}, \frac{a^*}{(a, g_2)^*}\right)\right)$$

and

$$\lambda_2 = \left(\frac{g_2^*}{(a, g_2)^*}\right)^{-1} \frac{b^*}{(b, l, g_1)^*}\ x^{2m + deg(g_2) - deg(g_3)} \qquad \left(\bmod \frac{a^*}{(a, g_2)^*}\right).$$

Proof. Since $(l \mid a \mid 0), (g_1 \mid g_2 \mid g_3) \in \mathrm{C}$ and $(\hat{g}_1 \mid \hat{g}_2 \mid \hat{g}_3) \in \mathrm{C}^\perp$, we have $\psi((\hat{g}_1 \mid \hat{g}_2 \mid \hat{g}_3), (l \mid a \mid 0)) = \psi(\hat{g}_1 \mid \hat{g}_2 \mid \hat{g}_3), (g_1 \mid g_2 \mid g_3)) = 0 \pmod{x^m - 1}$. This implies that

$$\hat{g}_1 \theta_{\frac{m}{r}}(x^r) x^{m-1-\deg(l)} l^* + \hat{g}_2 \theta_{\frac{m}{s}}(x^s) x^{m-1-\deg(a)} a^* = 0 \pmod{x^m - 1} \tag{8}$$

and

$$\begin{aligned} \hat{g}_1 \theta_{\frac{m}{r}}(x^r) x^{m-1-\deg(g_1)} g_1^* + \hat{g}_2 \theta_{\frac{m}{s}}(x^s) x^{m-1-\deg(g_2)} g_2^* \\ + \hat{g}_3 \theta_{\frac{m}{t}}(x^t) x^{m-1-\deg(g_3)} g_3^* = 0 \pmod{x^m - 1} \end{aligned} \tag{9}$$

Substituting $\hat{g}_1$ and $\hat{g}_2$ from Theorem 11, in (8) and (9), and rearranging the terms, we get

$$(x^m-1)\frac{l^*}{b^*}\ x^{m-1-\deg(l)}\lambda_1+(x^m-1)\frac{(b,l,g_1)^*}{b^*}\ x^{m-1-\deg(a)}\lambda_2=0 \pmod{x^m-1} \quad (10)$$

and

$$(x^m-1)\frac{g_1^*}{b^*}\ x^{m-1-\deg(g_1)}\lambda_1+(x^m-1)\frac{(b,l,g_1)^*g_2^*}{a^*b^*}\ x^{m-1-\deg(g_2)}\lambda_2$$
$$+(x^m-1)\frac{(a,g_2)^*}{a^*}\ x^{m-1-\deg(g_3)}=0 \pmod{x^m-1} \quad (11)$$

From (10) and (11), we get

$$(x^m-1)\frac{(b,l,g_1)^*g_1^*}{b^*}\ x^{2m-2-\deg(a)-\deg(g_1)}\lambda_2+(x^m-1)\frac{(b,l,g_1)^*}{a^*b^*}g_2^*l^*\ x^{2m-2-\deg(l)-\deg(g_2)}\lambda_2$$
$$+(x^m-1)\frac{(a,g_2)^*}{a^*}l^*\ x^{2m-2-\deg(l)-\deg(g_3)}=0 \pmod{x^m-1}. \quad (12)$$

Equation (12) can be rewritten as

$$(x^m-1)\frac{(b,l,g_1)^*}{b^*}\frac{(a,g_2)^*}{a^*}\left[\frac{g_1^*a^*}{(a,g_2)^*}\ x^{2m-2-\deg(a)-\deg(g_1)}\lambda_2+\frac{g_2^*}{(a,g_2)^*}l^*\ x^{2m-2-\deg(l)-\deg(g_2)}\lambda_2\right.$$
$$\left.+\frac{b^*}{(b,l,g_1)^*}l^*\ x^{2m-2-\deg(l)-\deg(g_3)}\right]=0 \pmod{x^m-1}. \quad (13)$$

This implies that

$$\left[\frac{g_1^*a^*}{(a,g_2)^*}\ x^{2m-2-\deg(a)-\deg(g_1)}\lambda_2+\frac{g_2^*}{(a,g_2)^*}l^*\ x^{2m-2-\deg(l)-\deg(g_2)}\lambda_2+\frac{b^*}{(b,l,g_1)^*}l^*\right.$$
$$\left.x^{2m-2-\deg(l)-\deg(g_3)}\right]=0 \pmod{x^m-1}.$$

Since $\frac{a^*}{(a,g_2)^*}$ divides x^m-1, we get

$$\frac{g_2^*}{(a,g_2)^*}\ x^{2m-2-\deg(l)-\deg(g_2)}\lambda_2+\frac{b^*}{(b,l,g_1)^*}\ x^{2m-2-\deg(l)-\deg(g_3)}=0 \bmod \left(\frac{a^*}{(a,g_2)^*}\right). \quad (14)$$

Since $\frac{a^*}{(a,g_2)^*}$ and $\frac{g_2^*}{(a,g_2)^*}$ are relatively prime, we get from (14)

$$\lambda_2=\left(\frac{g_2^*}{(a,g_2)^*}\right)^{-1}\frac{b^*}{(b,l,g_1)^*}x^{2m+\deg(g_2)-\deg(g_3)}\ \left(\bmod\ \frac{a^*}{(a,g_2)^*}\right).$$

.
Using the similar arguments that are given in finding λ_1, we therefore get

$$\lambda_1 = (\rho_1)^{-1}(\rho_2)^{-1}\frac{b^*}{(b,l,g_1)^*}x^{2m-\deg(g_3)-\deg(a)+\deg(g_2)+\deg(l)}\left(\text{mod}\ \left(\frac{(b,g_1)^*}{(b,l,g_1)^*},\frac{a^*}{(a,g_2)^*}\right)\right),$$

where $\rho_1 = \frac{l^*}{(b,l,g_1)^*}$ and $\rho_2 = \frac{g_2^*}{(a,g_2)^*}$. Hence the result. □

Theorem 13. *Let* $\mathrm{C} = \langle (b \mid 0 \mid 0), (l \mid a \mid 0), (g_1 \mid g_2 \mid g_3)\rangle$ *be a* $\mathbb{Z}_2$*-triple cyclic code of block length* (r,s,t) *and* $\mathrm{C}^\perp = \langle (\hat{b} \mid 0 \mid 0), (\hat{l} \mid \hat{a} \mid 0), (\hat{g}_1 \mid \hat{g}_2 \mid \hat{g}_3)\rangle$ *be the dual code of* C. *Then*

$$\hat{a}\ b^*(a,g_2)^* = (x^s-1)(b,l,g_1)^*.$$

Proof. First we determine the degree of $\hat{a}$. We note that $\dim(\mathrm{C}^\perp) = (r+s+t) - (\deg(\hat{b}) + \deg(\hat{a}) + \deg(\hat{g_3}))$. Also, since $\dim(\mathrm{C}) = (r+s+t) - (\deg(b) + \deg(a) + \deg(g_3))$ implies that $\dim(\mathrm{C}^\perp) = \deg(b)+\deg(a)+\deg(g_3)$. Therefore from Theorem 9 and Theorem 10, we get

$$\deg(\hat{a}) = s - b - (a,g_2) + (b,l,g_1). \tag{15}$$

Now since $\left(0 \mid \frac{ab}{(b,l,g_1)} \mid 0\right)$ and $\left(0 \mid \frac{bg_2}{(b,l,g_1)} \mid \frac{bg_3}{(b,l,g_1)}\right)$ are in C, and $(\hat{l} \mid \hat{a} \mid 0) \in \mathrm{C}^\perp$, we have
$\psi\left((\hat{l} \mid \hat{a} \mid 0),\ \left(0 \mid \frac{ab}{(b,l,g_1)} \mid 0\right)\right) = \psi\left((\hat{l} \mid \hat{a} \mid 0),\ \left(0 \mid \frac{bg_2}{(b,l,g_1)} \mid \frac{bg_3}{(b,l,g_1)}\right)\right) = 0$. This implies that $\hat{a}\frac{a^*b^*}{(b,l,g_1)^*} = \hat{a}\frac{g_2^*b^*}{(b,l,g_1)^*} = 0 \pmod{(x^s-1)}$ and hence $\hat{a}\frac{(a,g_2)^*b^*}{(b,l,g_1)^*} = 0 \pmod{(x^s-1)}$. Therefore, for some $\gamma \in \mathbb{Z}_2[x]$, we have

$$\hat{a}\frac{(a,g_2)^*b^*}{(b,l,g_1)^*} = \gamma(x^s-1)\ . \tag{16}$$

From equation (15) and equation (16), we get $\gamma = 1$ and hence $\hat{a}\ b^*(a,g_2)^* = (x^s - 1)(b,l,g_1)^*$. □

Theorem 14. *Let* $\mathrm{C} = \langle (b \mid 0 \mid 0), (l \mid a \mid 0), (g_1 \mid g_2 \mid g_3)\rangle$ *be a* $\mathbb{Z}_2$*-triple cyclic code of block length* (r,s,t) *and* $\mathrm{C}^\perp = \langle (\hat{b} \mid 0 \mid 0), (\hat{l} \mid \hat{a} \mid 0), (\hat{g}_1 \mid \hat{g}_2 \mid \hat{g}_3)\rangle$ *be the dual code of* C. *Then*

$$\hat{l}\ b^* = \beta(x^r-1),$$

where $\beta = \left(\frac{l^*}{(b,l,g_1)^*}\right)^{-1}\frac{a^*}{(a,g_2)^*}\ x^{m+deg(l)-deg(a)}\ \left(\text{mod}\ \frac{(b,g_1)^*}{(b,l,g_1)^*}\right)$.

Proof. Since $(b \mid 0 \mid 0) \in \mathrm{C}$ and $(\hat{l} \mid \hat{a} \mid 0) \in \mathrm{C}^\perp$, we have $\hat{l}b^* = 0 \pmod{x^r-1}$. Therefore $\hat{l}\ b^* = \beta(x^r-1)$ for some $\beta \in \mathbb{Z}_2[x]$.

Again, as $(\hat{l} \mid \hat{a} \mid 0) \in \mathrm{C}^\perp$ and $(l \mid a \mid 0) \in \mathrm{C}$, so $\psi\left((\hat{l} \mid \hat{a} \mid 0),\ (l \mid a \mid 0)\right) = 0 \pmod{x^m - 1}$. This implies that

$$\hat{l}\theta_{\frac{m}{r}}(x^r)x^{m-1-\deg(l)}l^* + \hat{a}\theta_{\frac{m}{s}}(x^s)x^{m-1-\deg(a)}a^* = 0 \text{ (mod } x^m-1). \tag{17}$$

Substituting $\hat{l}$ and $\hat{a}$ in equation (17), we get

$$(x^m-1)\frac{l^*}{b^*}x^{m-1-\deg(l)}\beta + (x^m-1)\frac{(b,l,g_1)^*}{b^*(a,g_2)^*}a^*x^{m-1-\deg(a)} = 0 \text{ (mod } x^m-1). \tag{18}$$

Rearranging the terms in equation (18), we get

$$(x^m-1)\frac{(b,l,g_1)^*}{b^*}\left[\frac{l^*}{(b,l,g_1)^*}x^{m-1-\deg(l)}\beta + \frac{a^*}{(a,g_2)^*}x^{m-1-\deg(a)}\right] = 0 \text{ (mod } x^m-1). \tag{19}$$

With similar arguments as in Theorem 12, we get

$$\beta = \left(\frac{l^*}{(b,l,g_1)^*}\right)^{-1}\frac{a^*}{(a,g_2)^*}\;x^{m+\deg(l)-\deg(a)}\;\left(\text{mod }\frac{(b,g_1)^*}{(b,l,g_1)^*}\right). \tag{20}$$

Hence the result. □

Summarising the previous results we have the following theorem.

Theorem 15. *Let* $\mathrm{C} = \langle (b \mid 0 \mid 0), (l \mid a \mid 0), (g_1 \mid g_2 \mid g_3)\rangle$ *be a* $\mathbb{Z}_2$*-triple cyclic code of block length* (r,s,t) *and* $\mathrm{C}^\perp = \langle (\hat{b} \mid 0 \mid 0), (\hat{l} \mid \hat{a} \mid 0), (\hat{g}_1 \mid \hat{g}_2 \mid \hat{g}_3)\rangle$ *be the dual code of* C. *Let* $\rho_1 = \frac{l^*}{(b,l,g_1)^*}$ *and* $\rho_2 = \frac{g_2^*}{(a,g_2)^*}$. *Then*

(i) $\hat{b} = \frac{x^r-1}{(b,l,g_1)^*}$;

(ii) $\hat{g}_3 = \frac{(x^t-1)(a,g_2)^*}{a^*g_3^*}$;

(iii) $\hat{a} = \frac{(x^s-1)(b,l,g_1)^*}{(a,g_2)^*b^*}$;

(iv) $\hat{g}_1 = \lambda_1\frac{(x^r-1)}{b^*}$, $\hat{g}_2 = \lambda_2\frac{(x^s-1)(b,l,g_1)^*}{a^*b^*}$, *where*

$$\lambda_1 = (\rho_1)^{-1}(\rho_2)^{-1}\frac{b^*}{(b,l,g_1)^*}\;x^{2m+deg(l)-deg(a)+deg(g_2)-deg(g_3)}\left(\text{mod}\left(\frac{(b,g_1^*)}{(b,l,g_1)^*},\frac{a^*}{(a,g_2)^*}\right)\right)$$

and

$$\lambda_2 = \left(\frac{g_2^*}{(a,g_2)^*}\right)^{-1}\frac{b^*}{(b,l,g_1)^*}x^{2m+deg(g_2)-deg(g_3)}\quad\left(\text{mod }\frac{a^*}{(a,g_2)^*}\right).$$

(v) $\hat{l}\;b^* = \beta(x^r-1)$, *where* $\beta = \left(\frac{l^*}{(b,l,g_1)^*}\right)^{-1}\frac{a^*}{(a,g_2)^*}\;x^{m+deg(l)-deg(a)}\;\left(\text{mod }\frac{(b,g_1)^*}{(b,l,g_1)^*}\right)$.

Example 2. *Let* $r = 10, s = 12$ *and* $t = 15$. *Let* $\mathrm{C} = \langle (b \mid 0 \mid 0), (l \mid a \mid 0), (g_1 \mid g_2 \mid g_3) \rangle$, *where* $b = x^6 + x^5 + x + 1$, $l = x^5 + 1$, $a = x^6 + 1$, $g_1 = x^5 + 1$, $g_2 = x^5 + x^4 + x^2 + x$ *and* $g_3 = x^{12} + x^9 + x^6 + x^5 + x^4 + x^2 + x + 1$. C *satisfies all the conditions given in Lemma 1 and Lemma 2. Therefore,* C *is a* $\mathbb{Z}_2$*-triple cyclic code of block length* $(10, 12, 15)$. *Also,* $S = S_1 \cup S_2 \cup S_3$ *forms a generating set for* C, *where* $S_1 = \cup_{i=0}^{3} x^i (x^6 + x^5 + x + 1 \mid 0 \mid 0)$, $S_2 = \cup_{i=0}^{5} x^i (x^5 + 1 \mid x^6 + 1 \mid 0)$ *and* $S_3 = \cup_{i=0}^{2} x^i (x^5 + 1 \mid x^5 + x^4 + x^2 + x \mid x^{12} + x^9 + x^6 + x^5 + x^4 + x^2 + x + 1)$. *The cardinality of* C *is* 2^{13}. *A generator matrix of* C *is*

$$G = \begin{pmatrix}
1100011000 & 000000000000 & 000000000000000 \\
0110001100 & 000000000000 & 000000000000000 \\
0011000110 & 000000000000 & 000000000000000 \\
0001100011 & 000000000000 & 000000000000000 \\
1000010000 & 100000100000 & 000000000000000 \\
0100001000 & 010000010000 & 000000000000000 \\
0010000100 & 001000001000 & 000000000000000 \\
0001000010 & 000100000100 & 000000000000000 \\
0000100001 & 000010000010 & 000000000000000 \\
1000010000 & 000001000001 & 000000000000000 \\
1000010000 & 011011000000 & 111011100100100 \\
0100001000 & 001101100000 & 011101110010010 \\
0010000100 & 000110110000 & 001110111001001
\end{pmatrix}.$$

Further, the minimum Hamming distance of C *is* 4 *and therefore,* C *is a* $[37, 13, 4]$ *binary linear Code. From Theorem 15, we have the dual code of* C *as* $\mathrm{C}^{\perp} = \langle (\hat{b} \mid 0 \mid 0), (\hat{l} \mid \hat{a} \mid 0), (\hat{g}_1 \mid \hat{g}_2 \mid \hat{g}_3) \rangle$, *where* $\hat{b} = (x + 1)(x^4 + x^3 + x^2 + x + 1)$, $\hat{a} = (x + 1)(x^2 + x + 1)^3$, $\hat{g}_3 = x + 1$, $\hat{g}_1 = \hat{l} = 0$ *and* $\hat{g}_2 = (x + 1)(x^2 + x + 1)^2$.

Let $t = 0$. Then by taking $g_1 = g_2 = g_3 = 0$, we have $(b, l, g_1) = (b, l)$ and $(b, g_1) = b$ and hence from Theorem (15), we see that $\mathbb{Z}_2$-double cyclic codes are special case of the family of codes that we are considering when $t = 0$. Thus we have the following result.

Corollary 1. *Let* $\mathrm{C} = \langle (b \mid 0 \mid 0), (l \mid a \mid 0) \rangle$ *be a* $\mathbb{Z}_2$*-double cyclic code of block length* (r, s) *and* $\mathrm{C}^{\perp} = \langle (\hat{b} \mid 0 \mid 0), (\hat{l} \mid \hat{a} \mid 0) \rangle$ *be the dual code of* C. *Then*

(i) $\hat{b} = \frac{x^r - 1}{(b,l)^*}$;

(ii) $\hat{a}\ a^* b^* = (x^s - 1)(b, l)^*$;

(iii) $\hat{l}\ b^* = \beta (x^r - 1)$, *where* $\beta = \left(\frac{l^*}{(b,l)^*} \right)^{-1} x^{m - deg(a) + deg(l)} \quad \left(\mathrm{mod} \quad \left(\frac{b^*}{(b,l)^*} \right) \right)$.

Let $\mathrm{C} = \langle (b \mid 0 \mid 0), (l \mid a \mid 0), (g_1 \mid g_2 \mid g_3) \rangle$ be a $\mathbb{Z}_2$-triple cyclic code of block length (r, s, t) as in Theorem (3). If $b | l$, $b | g_1$ and $a | g_2$, then $\mathrm{C} = \langle (b \mid 0 \mid 0), (0 \mid a \mid 0), (0 \mid 0 \mid g_3) \rangle$. We note that $\mathrm{C}_r = \langle b \rangle$, $\mathrm{C}_s = \langle a \rangle$ and $\mathrm{C}_t = \langle g_3 \rangle$ and $\mathrm{C} = \mathrm{C}_r \times \mathrm{C}_s \times \mathrm{C}_t$. Hence C is separable. A generator matrix of C is permutation equivalent to the matrix

$$\mathbf{G}=\left(\begin{array}{cc|cc|cc} I_{r-\deg(b)} & A & 0 & 0 & 0 & 0\\ 0 & 0 & I_{s-\deg(a)} & B & 0 & 0\\ 0 & 0 & 0 & 0 & C & I_{t-\deg(g_3)}\end{array}\right).$$

The following theorem shows that the dual of a separable $\mathbb{Z}_2$-triple cyclic code is also separable.

Theorem 16. *Let* $\mathrm{C}=\langle (b \mid 0 \mid 0),(0 \mid a \mid 0),(0 \mid 0 \mid g_3)\rangle$ *be a separable* $\mathbb{Z}_2$*-triple cyclic code of block length* (r,s,t)*. Then*

(i) $\mathrm{C}^{\perp}$ *is also a separable* $\mathbb{Z}_2$*-triple cyclic code of block length* (r,s,t)*,*

(ii) $\mathrm{C}^{\perp}=\left\langle\left(\frac{x^r-1}{b} \mid 0 \mid 0\right),\left(0 \mid \frac{x^s-1}{a} \mid 0\right),\left(0 \mid 0 \mid \frac{x^t-1}{g_3}\right)\right\rangle$*, and*

(iii) $d_{min}(\mathrm{C})=\min\{d_{min}(\mathrm{C}_r),d_{min}(\mathrm{C}_s),d_{min}(\mathrm{C}_t)\}$*.*

Proof. As $l=g_1=g_2=0$, the proof follows from Theorem 15. □

Remark 2. *If* C *is a non-separable* $\mathbb{Z}_2$*-triple cyclic code of block length* (r,s,t)*, then* $d_{min}(\mathrm{C})\geq\min\{d_{min}(\mathrm{C}_r),d_{min}(\mathrm{C}_s),d_{min}(\mathrm{C}_t)\}$*.*

Example 3. *Let* $r=6,s=4$ *and* $t=5$*. Let* $\mathrm{C}=\langle (b \mid 0 \mid 0),(0 \mid a \mid 0),(0 \mid 0 \mid g_3)\rangle$*, where* $b=(x+1)(x^2+x+1)^2$*,* $a=(x+1)^3$ *and* $g_3=x^4+x^3+x^2+x+1$*. Then* C *is a* $\mathbb{Z}_2$*-triple cyclic code of block length* $(6,4,5)$*. The set* $S=\{(x^5+x^4+x^3+x^2+x+1 \mid 0 \mid 0),(0 \mid x^3+x^2+x+1 \mid 0),(0 \mid 0 \mid x^4+x^3+x^2+x+1)\}$ *forms a generating set for* C*. The cardinality of* C *is* 2^3*. Further, the minimum Hamming distance of* C *is* 4 *and therefore* C *is a* $[15,3,4]$ *binary linear code with the Hamming weight distribution* $[<0,\ 1>,<4,\ 1>,<5,\ 1>,<6,\ 1>,<9,\ 1>,<10,\ 1>,<11,\ 1>,<15,\ 1>]$*. The dual of* C *is also a separable* $\mathbb{Z}_2$*-triple cyclic code of block length* $(6,4,5)$ *such that* $\mathrm{C}^{\perp}=\langle (x+1 \mid 0 \mid 0),(0 \mid x+1 \mid 0),(0 \mid 0 \mid x+1)\rangle$ *with minimum Hamming distance* 2 *and therefore it is a* $[15,12,2]$ *binary code.*

4. Conclusion

In this paper we have considered $\mathbb{Z}_2$-triple cyclic codes of block length (r,s,t). We have studied the structure these codes and determined the form of their generators of these codes. We have determined the size of $\mathbb{Z}_2$-triple cyclic codes by giving a minimal spanning set. We also studied the relationship between the generators of $\mathbb{Z}_2$-triple cyclic codes and their duals and determined the generators for dual of a $\mathbb{Z}_2$-triple cyclic code.

References

[1] T. Abualrub, I. Siap and N. Aydin. $\mathbb{Z}_2\mathbb{Z}_4$-Additive cyclic codes. IEEE Trans. Inform. Theory, $60(3) : 1508 - 1514,\ 2014$.

[2] I. Aydogdu and I. Siap. $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes. Linear Multilinear Algebra, $63(10) : 2089 - 2102,\ 2014$.

[3] I. Aydogdu, T. Abualrub and I. Siap. On $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes. Int. J. of Comput. Math., $92(9) : 1806 - 1814,\ 2013$.

[4] J. Borges, C. Fernàndez-Còrdoba and R. Ten-Valls. $\mathbb{Z}_2$-double cyclic codes, $arXiv : 1410.5604v1$.

[5] J. Borges, C. Fernàndez-Còrdoba, J. Pujol, J. Rifà and M. Villanueva. $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: generator matrices and duality, Des. Codes Crypt., $54(2) : 167 - 179,\ 2009$.

[6] J. Borges, C. Fernàndez-Còrdoba and R. Ten-Valls. $\mathbb{Z}_2\mathbb{Z}_4$-Additive cyclic codes, generator polynomials and dual codes. IEEE Trans. Inform. Theory, $62(11) : 6348 - 6354,\ 2016$.

[7] M. Bhaintwal and S. Wasan. On quasi-cyclic codes over $\mathbb{Z}_q$. Appl. Algebra Engrg. Comm. Comput., $20(5) : 459 - 480,\ 2009$.

[8] Y. Cao. Structural properties and enumeration of 1-generator generalized quasi-cyclic codes. Des. Codes Cryptogr., $60(1) : 67 - 79,\ 2011$.

[9] Y. Cao. Generalized quasi-cyclic codes over Galois rings: structural properties and enumeration. Appl. Algebra Eng. Commun. Comput., $22(3) : 219 - 233,\ 2011$.

[10] P. Delsarte and V. I. Levenshtein. Association schemes and coding theory. IEEE Trans. Inform. Theory, $44(6) : 2477 - 2504,\ 1998$.

[11] H. Q. Dinh and S. R. Lopéz-Permouth. Cyclic and negacyclic codes over finite chain rings. IEEE Trans. Inform. Theory., $50(8) : 1728 - 1743,\ 2004$.

[12] M. Esmaeili and S. Yari. Generalized quasi-cyclic codes: structural properties and code construction. Appl. Algebra Eng. Commun. Comput., $20(2) : 159 - 173,\ 2009$.

[13] J. Gao, F-W. Fu, L. Shen and W. Ren. Some results on generalized quasi-cyclic codes over $\mathbb{F}_q + u\mathbb{F}_q$. IEICE Trans. Fund., $97(4) : 1005 - 1011,\ 2014$.

[14] J. Gao, M. Shi, T. Wu and F-W. Fu. On double cyclic codes over $\mathbb{Z}_4$. Finite Fields Appl., $39 : 233 - 250$ 2016.

[15] F. J. MacWilliams and N. J. A. Sloane. The Theory of Error Correcting Codes. North Holland, Amsterdam, 1977.

[16] I. Siap and N. Kulhan. The structure of generalized quasi-cyclic codes. Appl. Math. E-Notes, $5: 24-30,\ 2005$.

[17] T. Yao, M. Shi and P. Solé. Double cyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$. Int. J. Inf. Coding Theory, $3(2): 145-157,\ 2015$.