Applicable Algebra in Engineering, Communication and Computing (2023) 34:81–97
https://doi.org/10.1007/s00200-020-00474-4

ORIGINAL PAPER

On the number of $\mathbb{Z}_2\mathbb{Z}_4$ and $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive cyclic codes

Eda Yildiz[1] · Taher Abualrub[2] · Ismail Aydogdu[1]

Received: 1 May 2020 / Revised: 28 October 2020 / Accepted: 6 November 2020 /
Published online: 10 January 2021

Abstract
In this paper, we give the exact number of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes of length $n = r + s$, for any positive integer r and any positive odd integer s. We will provide a formula for the the number of separable $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes of length n and then a formula for the number of non-separable $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes of length n. Then, we have generalized our approach to give the exact number of $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive cyclic codes of length $n = r + s$, for any prime p, any positive integer r and any positive integer s where $\gcd(p, s) = 1$. Moreover, we will provide examples of the number of these codes with different lengths $n = r + s$.

Keywords $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes · $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive cyclic codes · counting · separable · non-separable codes

Mathematics Subject Classification 94B05 · 94B60

1 Introduction

In coding theory, the class of linear codes is one of the most studied codes because of their rich algebraic structure and their well-defined mathematical properties. A linear code of length n over a finite field $\mathbb{F}_q$ is a subspace of $\mathbb{F}_q^n$. In the early history of coding theory, researchers mainly studied linear codes over finite fields, especially over $\mathbb{Z}_2$. Later, codes over rings have been considered by many researchers since the early seventies. However, they became a very popular

✉ Ismail Aydogdu
iaydogdu@yildiz.edu.tr

Eda Yildiz
edyildiz@yildiz.edu.tr

Taher Abualrub
abualrub@aus.edu

1 Department of Mathematics, Yildiz Technical University, Istanbul, Turkey

2 Department of Mathematics and Statistics, American University of Sharjah, Sharjah, United Arab Emirates

research area with the work of Hammons et al. [9]. In [9], Hammons and coauthors showed that some well-known non-linear codes such as the Kerdock and Preparata codes, are actually Gray images of linear codes over $\mathbb{Z}_4$. This work has led researchers to study codes over different rings, such as $\mathbb{Z}_{2^k}$, $\mathbb{Z}_{p^k}$ and $\mathbb{F}_q + u\mathbb{F}_q$. The reader may find some of such studies in [6, 8, 10].

In 2010, Borges et. al. introduced a new class of codes over rings, called $\mathbb{Z}_2\mathbb{Z}_4$ -additive codes [3]. They defined $\mathbb{Z}_2\mathbb{Z}_4$-additive codes as subgroups of $\mathbb{Z}_2^r \times \mathbb{Z}_4^s$. In fact, $\mathbb{Z}_2\mathbb{Z}_4$-additive codes are generalization of binary linear codes and quaternary linear codes. If we take $s = 0$, then we have the binary linear codes of length r and if $r = 0$, then $\mathbb{Z}_2\mathbb{Z}_4$-additive codes are quaternary linear codes over $\mathbb{Z}_4$ of length s. Although the class of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes is a very new family of codes, they have some applications in the field of Steganography [11]. In [1], a number of optimal binary linear codes were constructed as images of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes using the Gray map. In [5], Borges et. al. generalized the study of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes to $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes where p is a prime number and, r and s are coprimes with p.

The class of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes is a very huge class. This implies that the number of distinct $\mathbb{Z}_2\mathbb{Z}_4$-additive codes is huge compared to the number of linear codes over $\mathbb{Z}_2$ or the number of linear codes over $\mathbb{Z}_4$. In [7], Steven Dougherty et. al. studied the number of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes. Moreover, Siap and Aydogdu studied counting the number of generator matrices of $\mathbb{Z}_2\mathbb{Z}_8$-additive codes in [12].

In this paper, we are interested in finding the exact number of distinct $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic codes of length $n = r + s$, for any positive integer r and any positive odd integer s. If s is any positive odd integer, then the ring $\mathbb{Z}_4[x]/\langle x^s - 1\rangle$ is a principal ideal ring and hence cyclic codes of length s over $\mathbb{Z}_4$ are principal ideals. We will provide a formula for the number of separable $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes of length n and another formula for the number of non-separable $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes of length n. Then, we have generalized our approach to provide the exact number of $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive cyclic codes of length $n = r + s$, for any prime p, any positive integer r and any positive integer s where $\gcd(p, s) = 1$. The condition that $\gcd(p, s) = 1$ will guarantee that the ring $\mathbb{Z}_{p^2}[x]/\langle x^s - 1\rangle$ is a principal ideal ring and hence cyclic codes of length s over $\mathbb{Z}_{p^2}$ are principal ideals. As an application of our study, we will provide examples of the exact number of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes and $\mathbb{Z}_3\mathbb{Z}_9$-additive cyclic codes of different lengths.

2 $\mathbb{Z}_2\mathbb{Z}_4$-additive and $\mathbb{Z}_2\mathbb{Z}_4$-cyclic codes

In this section, we give the definitions of $\mathbb{Z}_2\mathbb{Z}_4$-additive and $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, and we also give some properties of these codes. A comprehensive study of these codes can be found in [1] and in [3].

Definition 1 A non-empty subset $\mathcal{C}$ of $\mathbb{Z}_2^r \times \mathbb{Z}_4^s$ is called a $\mathbb{Z}_2\mathbb{Z}_4$-additive code if $\mathcal{C}$ is a subgroup of $\mathbb{Z}_2^r \times \mathbb{Z}_4^s$.

If $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive code, then it is isomorphic to an abelian group $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$ with the order of $\mathcal{C}$ given by $|\mathcal{C}| = 2^\gamma 4^\delta$. Also, the number of order two codewords in $\mathcal{C}$ is $2^{\gamma+\delta}$. Let κ be the dimension of the binary linear code obtained by taking the subcode of $\mathcal{C}$ containing all order-two codewords. In this case, the code $\mathcal{C}$ will be referred to as of type $(r, s;\gamma, \delta;\kappa)$.

Let $\varphi : \mathbb{Z}_4 \to \mathbb{Z}_2^2$ be the usual Gray map defined by $\varphi(0) = 00$, $\varphi(1) = 01$, $\varphi(2) = 11$ and $\varphi(3) = 10$. φ can be extended to a map Φ defined by

$$\Phi : \mathbb{Z}_2^r \times \mathbb{Z}_4^s \to \mathbb{Z}_2^n$$
$$\left(u_0, u_1, \dots u_{r-1} | v_0, v_1, \dots v_{s-1}\right) \to \left(u_0, u_1, \dots u_{r-1} | \varphi(v_0), \varphi(v_1), \dots \varphi(v_{s-1})\right)$$

where $n = r + 2s$, $\left(u_0, u_1, \dots u_{r-1} | v_0, v_1, \dots v_{s-1}\right) \in \mathbb{Z}_2^r \times \mathbb{Z}_4^s$. The Gray image $\Phi(\mathcal{C})$ is a binary code (not necessary linear since Φ is not linear).

Example 2 Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code generated by

$$\left(\begin{array}{cc|cccc} 1 & 0 & 0 & 0 & 2 & 2 \\ 1 & 1 & 1 & 1 & 0 & 2 \end{array}\right).$$

Hence, $\mathcal{C} = \{00|0000, 10|0022, 11|1102, 01|1120, 00|2200, 10|2222, 11|3302, 01|3320\}$.

- The order of $\mathcal{C}$ is $2^1 4^1$, so $\gamma = 1$ and $\delta = 1$.
- $r = 2, s = 4$ and $\kappa = 1$.
- Therefore, $\mathcal{C}$ is of type (2, 4; 1, 1; 1).

Definition 3 Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of length $n = r + s$. $\mathcal{C}$ is called a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code if $c = \left(u_0, u_1, \dots u_{r-1} | v_0, v_1, \dots v_{s-1}\right)$ is a codeword in $\mathcal{C}$, then

$$\sigma(c) = \left(u_{r-1}, u_0, \dots u_{r-2} | v_{s-1}, v_0, \dots v_{s-2}\right)$$

is also in $\mathcal{C}$.

Let $\mathcal{R}_{r,s} = \mathbb{Z}_2[x]/\langle x^r - 1\rangle \times \mathbb{Z}_4[x]/\langle x^s - 1\rangle$. Then any element $c = \left(u_0, u_1, \dots u_{r-1} | v_0, v_1, \dots v_{s-1}\right) \in \mathbb{Z}_2^r \times \mathbb{Z}_4^s$ can be identified with an element in $\mathcal{R}_{r,s}$ as follows:

$$\begin{aligned} c(x) &= \left(u_0 + u_1 x + \dots + u_{r-1}x^{r-1}, v_0 + v_1 x + \dots + v_{s-1}x^{s-1}\right) \\ &= (u(x), v(x)) \end{aligned}$$

This is one-one correspondence between the elements of $\mathbb{Z}_2^r \times \mathbb{Z}_4^s$ and the elements of $\mathcal{R}_{r,s}$. Therefore, we can identify $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes with polynomials of $\mathcal{R}_{r,s}$. The following theorem gives the generator polynomials of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes when s is an odd integer. Throughout this paper, we will use the notation f instead of the polynomial $f(x)$.

Theorem 4 ([1]) *Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic code in $\mathcal{R}_{r,s}$ with odd integer s. Then $\mathcal{C}$ can be identified as*

$$\mathcal{C} = \langle (f, 0), (l, g + 2a) \rangle,$$

where $f|(x^r - 1) \, mod \, 2$, $a|g|(x^s - 1) \, mod \, 4$, l is a binary polynomial satisfying $\deg(l) < \deg(f)$, and $f | \frac{x^s - 1}{a} l$.

Lemma 5 *Let $\mathcal{C} = \langle (f, 0), (l, g + 2a) \rangle$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code in $\mathcal{R}_{r,s}$ with odd integer s, where the generators satisfy the conditions in Theorem 4. Then the generators f, l, g* and *a are unique.*

Proof The proof is similar to the proof of Theorem 3 in [2]. □

Example 6 Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code in $\mathbb{Z}_2[x]/\langle x^7 - 1 \rangle \times \mathbb{Z}_4[x]/\langle x^7 - 1 \rangle$ generated by $\langle (f, 0), (l, g + 2a) \rangle$, where

$$\begin{aligned} f &= x^7 - 1, \; l = 1 + x^2 + x^3, \\ a &= 3 + 2x + 3x^2 + x^3, \; g = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6. \end{aligned}$$

The code $\mathcal{C}$ has the following generator matrix

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 & 3 & 1 & 3 & 3 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 2 & 2 & 2 & 0 & 2 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 2 & 2 & 2 & 0 & 2 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 2 & 2 & 2 & 0 & 2 \end{pmatrix}.$$

Furthermore, the binary image of $\mathcal{C}$ under the Gray map that we defined above is an optimal binary linear code with parameters [21, 5, 10].

Definition 7 Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code. $\mathcal{C}$ is called separable if $\mathcal{C} = \mathcal{C}_X \times \mathcal{C}_Y$, where

$$\mathcal{C}_X \times \mathcal{C}_Y = \{(a, b) \mid \text{there are codewords } (a, c_2), (c_1, b) \in \mathcal{C}\}.$$

Corollary 8 ([4]) *Let $\mathcal{C} = \langle (f, 0), (l, g + 2a) \rangle$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code. Then, $\mathcal{C}$ is separable if and only if $l = 0$.*

3 The number of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code in $\mathcal{R}_{r,s}$, where s is an odd integer. Then $\mathcal{C}$ can be uniquely identified as

$$\mathcal{C} = \langle (f, 0), (l, g + 2a) \rangle, \tag{1}$$

where $f|(x^r - 1) \, mod \, 2$, $a|g|(x^s - 1) \, mod \, 4$, l is a binary polynomial satisfying $\deg(l) < \deg(f)$ and $f | \frac{(x^s - 1)}{a} l$. In this section, we are interested to determine a formula for the number of distinct $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes of length $n = r + s$. Before starting our main work, we will give a few remarks which are related to our work.

Remark

1. The generator polynomials in Eq. 1 are unique.
2. The only restrictions on the polynomial l are $\deg(l) < \deg(f)$ and $f | \frac{(x^s - 1)}{a} l$. This makes the number of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code in $\mathcal{R}_{r,s}$ to be huge compared to the number of cyclic codes over $\mathbb{Z}_2$ or over $\mathbb{Z}_4$. Moreover, the existence of the polynomial l as a part of the generators will make the problem of finding a general formula for the number of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code a challenging problem.
3. If r is odd then, $(x^r - 1) = \widetilde{f_1}\widetilde{f_2}\ldots\widetilde{f_t} \mod 2$, is factored as a product of the irreducible factors $\widetilde{f_1}, \widetilde{f_2}, \ldots, \widetilde{f_t}$. Any factor (not equal 1) of $(x^r - 1)$ will be labeled as f_i where $i \in \{1, 2, \ldots, 2^t - 1\}$. The same is applied for $(x^s - 1) \mod 4$.

The number of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes of length $n = r + s$, where r is any integer and s is an odd integer will be given in Corollary 14. But first we will find the number of these codes when r and s are odd positive integers. For the results from Lemma 9 until Theorem 13, we will always assume that r and s are any odd positive integers.

Lemma 9 *Let* $\mathcal{C} = \langle (f, 0), (l, g + 2a) \rangle$ *be a cyclic code in* $\mathbb{Z}_2[x]/\langle x^r - 1\rangle \times \mathbb{Z}_4[x]/\langle x^s - 1\rangle$, *where* $f | (x^r - 1) \bmod 2$, $a | g | (x^s - 1) \bmod 4$, l *is a binary polynomial satisfying* $\deg(l) < \deg(f)$ *and* $f | \frac{(x^s - 1)}{a} l$. *If* $\gcd\left(f, \frac{(x^s - 1)}{a}\right) = 1$, *then* $\mathcal{C}$ *is a separable code.*

Proof By Corollary 12 in [1], the polynomial $l = 0$. Hence, $\mathcal{C}$ is separable. □

Lemma 10 *The number of separable* $\mathbb{Z}_2\mathbb{Z}_4$*-additive cyclic codes in* $\mathcal{R}_{r,s}$ is $2^{w_1}3^{w_2}$ *where* w_1 *is the number of irreducible factors of* $(x^r - 1) \bmod 2$ *and* w_2 *is the number of irreducible factors of* $(x^s - 1) \bmod 4$.

Proof Since $\mathcal{C}$ is separable then $\mathcal{C} = \langle (f, 0), (0, g + 2a) \rangle = \mathcal{C}_1 \times \mathcal{C}_2$, where $\mathcal{C}_1 = \langle f \rangle$ is a binary cyclic code of length r and $\mathcal{C}_2 = \langle g + 2a \rangle$ is a quaternary cyclic code over $\mathbb{Z}_4$ of length s. The result follows from the fact that there are 2^{w_1} binary cyclic codes of length r and 3^{w_2} quaternary cyclic codes over $\mathbb{Z}_4$ of length s. □

In order to count the number of non-separable cyclic codes in $\mathbb{Z}_2[x]/\langle x^r - 1\rangle \times \mathbb{Z}_4[x]/\langle x^s - 1\rangle$, by Lemma 9 we must always have $\gcd\left(f, \frac{(x^s - 1)}{a}\right) > 1$. Hence, when we consider non-separable $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, we will always assume that $\gcd\left(f, \frac{(x^s - 1)}{a}\right) > 1$.

Lemma 11 *Suppose that* $\mathcal{C} = \langle (f,0),(l,g+2a)\rangle$ *is a non-separable* $\mathbb{Z}_2\mathbb{Z}_4$*-additive cyclic code in* $\mathbb{Z}_2[x]/\langle x^r-1\rangle \times \mathbb{Z}_4[x]/\langle x^s-1\rangle$ *with* $\gcd(r,s)=1$. *Then*

$$\mathcal{C} = \langle \big((x-1)Q_1,0\big),\big(Q_1,g+2a\big)\rangle,$$

where $Q_1 | (x^r-1) \, mod \, 2$, $a|g|(x^s-1) \, mod \, 4$ *and* $(x-1)$ *is not a factor of* a.

Proof Let $\mathcal{C} = \langle (f,0),(l,g+2a)\rangle$ be a non-separable cyclic code in $\mathbb{Z}_2[x]/\langle x^r-1\rangle \times \mathbb{Z}_4[x]/\langle x^s-1\rangle$, with $\gcd(r,s)=1$. Since $\gcd(r,s)=1$, then the only common factors of (x^r-1) and (x^s-1) mod 2 are 1 and $(x-1)$. Suppose that $a=(x-1)J$ for some binary polynomial J. Since $f|\frac{(x^s-1)}{a}l$ and $\gcd\left(f,\frac{(x^s-1)}{a}\right)=1$, we get $f|l$, which is a contradiction unless $l=0$, and hence the code is separable. Now, suppose that $(x-1)$ is not a factor of f. Then, $\gcd\left(f,\frac{x^s-1}{a}\right)=1$ and again l must be zero giving that $\mathcal{C}$ is a separable code. Hence, in order for $\mathcal{C}$ to be a non-separable code, we must have $\gcd\left(f,\frac{x^s-1}{a}\right)=x-1$. This implies that $f=(x-1)Q_1$ and $\frac{x^s-1}{a}=(x-1)Q_2$, with $\gcd\big(Q_1,Q_2\big)=1$. Since $f|\frac{(x^s-1)}{a}l$, then $Q_1|Q_2l$ which implies that $Q_1|l$ and $l=Q_1V$. Since $\deg l < \deg f$ and $f=(x-1)Q_1$, then $l=Q_1$. Thus, $\mathcal{C} = \langle \big((x-1)Q_1,0\big),\big(Q_1,g+2a\big)\rangle$, where $(x-1)$ is not a factor of a. □

Theorem 12 *Let* $\mathcal{C} = \langle (f,0),(l,g+2a)\rangle$ *be a non-separable cyclic code in* $\mathbb{Z}_2[x]/\langle x^r-1\rangle \times \mathbb{Z}_4[x]/\langle x^s-1\rangle$ *and let* $x^r-1=\widetilde{f_1}\widetilde{f_2}\dots\widetilde{f_t}$ mod 2 *and* $x^s-1=\widetilde{g_1}\widetilde{g_2}\dots\widetilde{g_w}$ mod 4 *be the factorizations of* x^r-1 *and* x^s-1 *into irreducible polynomials in* $\mathbb{Z}_2[x]$ *and* $\mathbb{Z}_4[x]$, *respectively, with* $\gcd(r,s)=1$. *Then, the number of non-separable* $\mathbb{Z}_2\mathbb{Z}_4$*-additive cyclic codes is given by*

$$2^t 3^{w-1}.$$

Proof By Lemma 11, we know that $\mathcal{C} = \langle \big((x-1)Q_1,0\big),\big(Q_1,g+2a\big)\rangle$, where $Q_1|(x^r-1) \, mod \, 2$, $a|g|(x^s-1) \, mod \, 4$ and $(x-1)$ is not a factor of a. Since $x^r-1=\widetilde{f_1}\widetilde{f_2}\dots\widetilde{f_t}$ mod 2, then (x^r-1) has 2^t different factors and Q_1 has 2^{t-1} choices (because $(x-1)$ cannot be a factor of Q_1). For the polynomials a and g , we must have $a\,|\,g\,|(x^s-1)$ and $(x-1)$ is not a factor of a. Hence, the number of choices for a and g is

$$\begin{aligned}&\binom{w}{0}2^w+\binom{w-1}{1}2^{w-1}+\binom{w-2}{2}2^{w-2}+\ldots+\binom{w-1}{w-1}2^1\\&=2^w+2\left[\binom{w-1}{1}2^{w-2}+\binom{w-2}{2}2^{w-3}+\ldots+\binom{w-1}{w-2}2^1+\binom{w-1}{w-1}2^0\right]\\&=2^w+2\left[\begin{array}{c}\binom{w-1}{0}2^{w-1}+\binom{w-1}{1}2^{w-2}+\binom{w-2}{2}2^{w-3}+\ldots+\binom{w-1}{w-2}2^1\\+\binom{w-1}{w-1}2^0-\binom{w-1}{0}2^{w-1}\end{array}\right]\\&2^w+2\left[3^{w-1}-2^{w-1}\right]\\&=2\times 3^{w-1}.\end{aligned}$$

Therefore, if $\gcd(r,s)=1$, then the number of non-separable cyclic codes is $2^{t-1}\times 2\times 3^{w-1}=2^t3^{w-1}$. □

Our next theorem gives the number of non-separable cyclic codes for any odd integers r and s.

Theorem 13 *Let $\mathcal{C}=\langle (f,0),(l,g+2a)\rangle$ be a non-separable cyclic code in $\mathbb{Z}_2[x]/\langle x^r-1\rangle\times\mathbb{Z}_4[x]/\langle x^s-1\rangle$. Assume that $x^r-1=\widetilde{f_1}\widetilde{f_2}\ldots\widetilde{f_t}$ and $x^s-1=\widetilde{g_1}\widetilde{g_2}\ldots\widetilde{g_w}$ are the factorizations of x^r-1 and x^s-1 into irreducible polynomials in $\mathbb{Z}_2[x]$ and $\mathbb{Z}_4[x]$, respectively. The number of non-separable $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes is given by*

$$\left[\sum_{i=1}^{2^t-1}\left(\sum_{j=0}^{w-1}2^{w-j}\sum_{k}\left(2^{\deg(m_{ijk})}-1\right)\right)\right],\qquad(2)$$

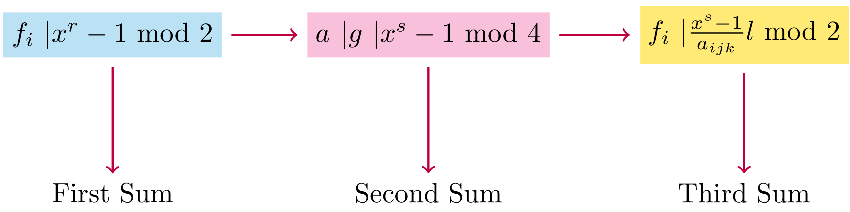
where $m_{ijk}=\gcd\left(f_i,\frac{x^s-1}{a_{ijk}}\right)>1$ and $a=a_{ijk}$ is the collection of all polynomials that satisfy the following conditions:

1. $f_i|\left(\frac{x^s-1}{a_{ijk}}l\right)mod\,2.$
2. *f_i is not a factor of a_{ijk} mod 2.*
3. *a_{ijk} has exactly j factors of x^s-1.*
4. *The sum k runs over all the choices for a satisfying the above conditions.*

Proof Suppose that $\mathcal{C}$ is a non-separable $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code in $\mathcal{R}_{r,s}$ of the form $\mathcal{C}=\langle (f,0),(l,g+2a)\rangle$ where

$$l\neq 0,\ f\mid (x^r-1)mod\,2,\ a\mid g\mid (x^s-1)mod\,4\ \text{and}\, f\mid\left(\frac{x^s-1}{a}l\right)mod\,2\ \text{with}\ \deg(l)<\deg(f).$$

We use the following diagram in order to give a clear picture of the proof. In the above theorem, we get the first sum by considering the condition $f\,|x^r-1$ for a $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic code $\mathcal{C}$ and we have the other sums in a similar approach.



If $f = 1$, then l must be 0 and hence the code is separable. Thus f is a polynomial of degree at least 1 satisfying the condition $f \mid (x^r - 1)$. This will give $\binom{t}{1} + \binom{t}{2} + \cdots + \binom{t}{t-1} + \binom{t}{t} = 2^t - 1$ different choices for f. So f runs over all the factors of $x^r - 1$ except for 1. That is, $f = f_i, i \in \{1, 2, \ldots, 2^t - 1\}$. This explains the first sum in Eq. 2. Now we will consider the polynomials g and a. We choose these polynomials among the ones that satisfy $a \mid g \mid (x^s - 1) mod\, 4$.

Case 1 $a = 1$. Since $f_i \mid \left(\frac{x^s-1}{a} l\right)$, then $f_i \mid (x^s - 1)l$. This will produce $\binom{w}{0} + \binom{w}{1} + \binom{w}{2} + \cdots + \binom{w}{w} = 2^w$ different choices for g with $a \mid g \mid x^s - 1$.

Case 2 $a = \widetilde{g_{i_1}}$, $i \in \{1, 2, ..., w\}$, i.e., a has only one factor of $x^s - 1$. Again, since we know that $a \mid g \mid x^s - 1$, then, we have $\binom{w-1}{0} + \binom{w-1}{1} + \binom{w-1}{2} + \cdots + \binom{w-1}{w-1} = 2^{w-1}$ different choices for g.

Case 3 $a = \widetilde{g_{i_1}} \widetilde{g_{i_2}} \ldots \widetilde{g_{i_j}}$, i.e., a has exactly j irreducible factors of $x^s - 1$, $2 \leq j \leq w - 1$. Similar to the above cases we have 2^{w-j} different choices for g. It is important to emphasize that a cannot be equal to $x^s - 1$ since we must have $f_i \mid \frac{x^s-1}{a} l$ with $\deg(l) < \deg(f_i)$. So, we take $j < w$.

Note that the polynomial l satisfies the condition (1) in the theorem above. Suppose that f_i is a factor of $a_{ijk}\, mod\, 2$. Then $a_{ijk} = f_i T\, mod\, 2$. If $f_i \mid \left(\frac{x^s-1}{f_i T} l\right) \bmod 2$ and since s is odd, then $f_i \mid l$ which contradicts the fact that $\deg l < \deg f_i$. Thus, f_i is not a factor of $a_{ijk}\, mod\, 2$. This implies that the polynomial a must satisfy the conditions in the theorem to be one of the generators.

Finally, we will consider the polynomial l. Let $m_{ijk} = \gcd\left(f_i, \frac{x^s - 1}{a_{ijk}}\right)$. Then, $f_i = q_1 m_{ijk}$ and $\frac{x^s - 1}{a_{ijk}} = q_2 m_{ijk}$ with $\gcd(q_1, q_2) = 1$. Since $f_i \mid \left(\frac{x^s - 1}{a_{ijk}} l\right)$,

$$
\begin{aligned}
\frac{x^s - 1}{a_{ijk}} l &= f_i M \\
q_2 m_{ijk} l &= q_1 m_{ijk} M \\
q_2 l &= q_1 M.
\end{aligned}
$$

Hence, $q_1 \mid q_2 l$. Since $\gcd(q_1, q_2) = 1$, $q_1 \mid l$, and $l = q_1 q_3 = \frac{f_i}{m_{ijk}} q_3$. Since $\deg l < \deg f_i$, q_3 may be any polynomial of degree less than the degree of m_{ijk}. Hence, there are $2^{\deg(m_{ijk})}$ different choices for l. However, if $l = 0$ then we get a separable code. Thus, there are $2^{\deg(m_{ijk})} - 1$ choices for l which produces non-separable codes. Consequently, the number of non-separable $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes is

$$\left[\sum_{i=1}^{2^t-1}\left(\sum_{j=0}^{w-1} 2^{w-j} \sum_{k} \left(2^{\deg(m_{ijk}(x))} - 1\right)\right)\right].$$

□

Our next result gives the number of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes for any integer r and any odd integer s. Let $r = 2^v N$ where N is an odd integer. Then, we know that $(x^r - 1) = \left(x^N - 1\right)^{2^v} = \widetilde{f_1}^{2^v}\widetilde{f_2}^{2^v} \ldots \widetilde{f_t}^{2^v}$ is the factorization of $(x^r - 1)$ into powers of irreducible polynomials. The number of binary cyclic codes of length r is $(2^v + 1)^t$. Based on this fact, our previous results can be applied for any integer r.

Corollary 14 *Suppose that $(x^r - 1) = \left(x^N - 1\right)^{2^v} = \widetilde{f_1}^{2^v}\widetilde{f_2}^{2^v} \ldots \widetilde{f_t}^{2^v}$ is the factorization of $(x^r - 1)$ into powers of irreducible polynomials in $\mathbb{Z}_2[x]$ and $x^s - 1 = \widetilde{g_1}\widetilde{g_2}\ldots\widetilde{g_w}$ be the factorization $x^s - 1$ into irreducible polynomials in $\mathbb{Z}_4[x]$.*

1. *The number of separable $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes is $(2^v + 1)^t 3^w$.*
2. *If $(r, s) = 1$, then the number of non-separable $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes is $(2^v + 1)^t 3^{w-1}$.*
3. *If $(r, s) \neq 1$, then the number of non-separable $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes is*

$$\left[\sum_{i=1}^{(2^v+1)^t-1}\left(\sum_{j=0}^{w-1} 2^{w-j} \sum_{k} \left(2^{\deg(m_{ijk}(x))} - 1\right)\right)\right].$$

Proof The proof follows from Lemma 10, Theorems 12 and 13 □

4 Examples

Example 15 Let $r = 9$ and $s = 7$. Then,

$$x^9 - 1 = x^9 - 1 = (1 + x)(1 + x + x^2)(1 + x^3 + x^6) \text{ in } \mathbb{Z}_2[x] \text{ and}$$
$$x^7 - 1 = (x + 3)(x^3 + 2x^2 + x + 3)(x^3 + 3x^2 + 2x + 3) \text{ in } \mathbb{Z}_4[x].$$

The number of separable $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes is $2^3 3^3 = 216$. Since $\gcd(r, s) = 1$, the number of non-separable $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes is $2^3 3^2 = 72$ by Theorem 12. Hence, the total number of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes of length $n = r + s = 16$ is $216 + 72 = 288$.

Example 16 Let $r = 7 = s$. Then

$$x^7 - 1 = (x-1)(x^3 + x + 1)(x^3 + x^2 + 1) \text{ in } \mathbb{Z}_2[x] \text{ and}$$
$$x^7 - 1 = (x+3)(x^3 + 2x^2 + x + 3)(x^3 + 3x^2 + 2x + 3) \text{ in } \mathbb{Z}_4[x].$$

Label the factors of $\left(x^7 - 1\right) \mod 2$ as: $f_1 = (1+x), f_2 = (1+x+x^3), f_3 = (1+x^2+x^3)$, $f_4 = (1+x)(1+x+x^3)$, $f_5 = (1+x)(1+x^2+x^3)$, $f_6 = (1+x+x^3)(1+x^2+x^3)$, $f_7 = x^7 - 1$. Label the factors of $\left(x^7 - 1\right)$ in $\mathbb{Z}_4[x]$ as

$$\begin{aligned} g_1 =&(3+x), g_2 = (3+x+2x^2+x^3), g_3 = (3+2x+3x^2+x^3),\\ g_4 =&(3+x)(3+x+2x^2+x^3), g_5 = (3+x)(3+2x+3x^2+x^3),\\ g_6 =&(3+x+2x^2+x^3)(3+2x+3x^2+x^3), g_7 = x^7 - 1. \end{aligned}$$

First, let $\mathcal{C}$ be a separable $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code with $\mathcal{C} = \langle (f, 0), (0, g + 2a) \rangle$. By Lemma 10, there are $2^3 3^3 = 216$ separable $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes.

Now, we will find the number of non-separable $\mathbb{Z}_2 \mathbb{Z}_4$-additive cyclic codes. According to Theorem 13, the number of non-separable $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes with $r = s = 7$ is

$$\sum_{i=1}^{7} \left(\sum_{j=0}^{2} 2^{3-j} \sum_{k} \left(2^{\deg(m_{ijk})} - 1\right) \right),$$

where the number of choices for the polynomial f is 7. Let $f = (1+x) = f_1$. Based on Theorem 13, we have the number of codes for this choice of f to be

$$\sum_{j=0}^{2} 2^{3-j} \sum_{k} \left(2^{\deg(m_{1jk})} - 1\right).$$

If $j = 0$, then $a_{1,0,k}$ is the collection of all polynomials that do not contain $f_1 \mod 2$ and have 0 factors of $x^7 - 1$. Hence, there is only one choice for $a = 1$ and in this case $k = 1$ with

$$m_{1,0,1}(x) = \gcd\left(1 + x, x^7 - 1\right) = (1 + x) = f_1(x).$$

If $j = 1$, then $a_{1,1,k}$ is the collection of all polynomials that do not contain $f_1 \mod 2$ and have 1 factor of $\left(x^7 - 1\right) \mod 2$. Hence, there are two choices as g_2, g_3 and in this case $k = 1, 2$ with

$$\begin{aligned} m_{1,1,1} =& \gcd\left(1 + x, \frac{x^7 - 1}{g_2}\right) = (1 + x) = f_1, \text{ and}\\ m_{1,1,2} =& \gcd\left(1 + x, \frac{x^7 - 1}{g_3}\right) = (1 + x) = f_1. \end{aligned}$$

If $j = 2$, then $a_{1,2,k}$ is the collection of all polynomials that do not contain $f_1 \mod 2$ and have 2 factors of $x^7 - 1$. Hence there is only 1 choice as g_6 and in this case $k = 1$ with

$$m_{1,2,1} = \gcd\left(1 + x, \frac{x^7 - 1}{g_6}\right) = (1 + x) = f_1.$$

Thus the number of codes when $f = f_1$ is

$$8\left(2^1 - 1\right) + 4\left[\left(2^1 - 1\right) + \left(2^1 - 1\right)\right] + 2\left(2^1 - 1\right) = 18.$$

If $f = f_2 = (1 + x + x^3)$, then a similar approach as above will give

$$8\left(2^3 - 1\right) + 4\left[\left(2^3 - 1\right) + \left(2^3 - 1\right)\right] + 2\left(2^3 - 1\right) = 126 \text{ codes.}$$

If $f = f_3 = (1 + x^2 + x^3)$, then a similar approach as above will give

$$8\left(2^3 - 1\right) + 4\left[\left(2^3 - 1\right) + \left(2^3 - 1\right)\right] + 2\left(2^3 - 1\right) = 126 \text{ codes.}$$

If $f = (1 + x)(1 + x + x^3) = f_4$ then a similar approach as above will give

$$8\left[2^4 - 1\right] + 4\left[(2^3 - 1) + (2^1 - 1) + (2^4 - 1)\right] + 2\left[(2^3 - 1) + (2^1 - 1)\right] = 228 \text{ codes.}$$

If $f = (1 + x)(1 + x^2 + x^3) = f_5$ then we get the same number of codes as in the case $f = f_4$ above. Hence, there are 228 codes with $f = f_5$.

If $f = f_6 = f = (1 + x + x^3)(1 + x^2 + x^3)$, then we have $j = 0$. In this case there is only one choice for $a = 1$ and $k = 1$ with

$$m_{6,0,1} = \gcd\left(f_6, x^7 - 1\right) = f_6.$$

If $j = 1$, then there are 3 choices for a and $k = 1, 2, 3$ with

$$m_{6,1,1} = \gcd\left(f_6, \frac{x^7 - 1}{g_1}\right) = f_6$$
$$m_{6,1,2} = \gcd\left(f_6, \frac{x^7 - 1}{g_2}\right) = \left(1 + x^2 + x^3\right)$$
$$m_{6,1,3} = \gcd\left(f_6, \frac{x^7 - 1}{g_3}\right) = \left(1 + x + x^3\right).$$

If $j = 2$, then there are 2 choices for a and $k = 1, 2$ with

$$m_{6,2,1} = \gcd\left(f_6, \frac{x^7 - 1}{g_4}\right) = \left(1 + x^2 + x^3\right)$$
$$m_{6,2,2} = \gcd\left(f_6, \frac{x^7 - 1}{g_5}\right) = \left(1 + x + x^3\right).$$

Hence in this case, the number of codes is

$$\sum_{j=0}^{2} 2^{3-j} \sum_{k} \left(2^{\deg(m_{i,j,k})} - 1\right) =8\left[2^6 - 1\right] + 4\left[(2^6 - 1) + (2^3 - 1) + (2^3 - 1)\right] + 2\left[(2^3 - 1) + (2^3 - 1)\right] =504 + 308 + 28 = 840.$$

If $f = f_7 = x^7 - 1$, then we get

$$\sum_{j=0}^{2} 2^{3-j} \sum_{k} \left(2^{\deg(m_{i,j,k})} - 1\right) =2^3\left[2^7 - 1\right] + 2^2\left[\left(2^6 - 1\right) + \left(2^4 - 1\right) + \left(2^4 - 1\right)\right] + 2\left[\left(2^3 - 1\right) + \left(2^3 - 1\right) + \left(2^1 - 1\right)\right] =1016 + 372 + 30 = 1418 \text{ codes}.$$

Therefore, the total number of non-separable $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes when $r = s = 7$ is

$$18 + 126 + 126 + 228 + 228 + 840 + 1418 = 2984.$$

Example 17 Let $r = 9$ and $s = 15$. Then,

$$x^9 - 1 =(1 + x)(1 + x + x^2)(1 + x^3 + x^6) \text{ in } \mathbb{Z}_2[x] \text{ and}$$
$$x^{15} - 1 =(3 + x)(1 + x + x^2)(1 + 3x + 2x^2 + x^4)(1 + 2x^2 + 3x^3 + x^4)(1 + x + x^2 + x^3 + x^4) \text{ in } \mathbb{Z}_4[x].$$

Hence, by Lemma 10, the number of separable $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes for $r = 9$ and $s = 7$ is $2^3 3^5 = 1944$. By Theorem 13, the number of non-separable $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes is

$$\sum_{i=1}^{2^3-1} \left(\sum_{j=0}^{4} 2^{5-j} \sum_{k} \left(2^{\deg(m_{i,j,k})} - 1\right) \right).$$

Let us label the factors of $x^9 - 1$ as

$$f_1 =(1 + x), f_2 = (1 + x + x^2), f_3 = (1 + x^3 + x^6),$$
$$f_4 =(1 + x)(1 + x + x^2), f_5 = (1 + x)(1 + x^3 + x^6),$$
$$f_6 =(1 + x + x^2)(1 + x^3 + x^6), f_7 = x^9 - 1,$$

and label the factors of $x^{15} - 1$ as

$$\begin{aligned}
g_1 &= (3 + x), g_2 = (1 + x + x^2), g_3 = (1 + 3x + 2x^2 + x^4),\\
g_4 &= (1 + 2x^2 + 3x^3 + x^4), g_5 = (1 + x + x^2 + x^3 + x^4),\\
g_6 &= (3 + x)(1 + x + x^2), g_7 = (3 + x)(1 + 3x + 2x^2 + x^4),\\
&\vdots \quad \vdots \quad \vdots\\
g_{30} &= (3 + x)(1 + x + x^2)(1 + 3x + 2x^2 + x^4)(1 + 2x^2 + 3x^3 + x^4),\\
g_{31} &= x^{15} - 1.
\end{aligned}$$

Note that since $\gcd\left(f_3, x^{15}-1\right)=1$, f cannot be chosen as to be f_3. We start calculating the cyclic codes which correspond to $f=f_1=1+x$.

If $j=0$, then $k=1$, $a=1$, and

$$m_{1,0,1}=\gcd\left(1+x, x^{15}-1\right)=1+x.$$

If $j=1$, then, $k\in\{1,2,3,4\}$ and

$$m_{1,1,1}=m_{1,1,2}=m_{1,1,3}=m_{1,1,4}=1+x$$

If $j=2$, then, $k\in\{1,2,3,4,5,6\}$ and

$$m_{1,2,1}=m_{1,2,2}=\cdots=m_{1,2,6}=1+x$$

For $j=3$, then, $k\in\{1,2,3,4\}$ and

$$m_{1,3,1}=m_{1,3,2}=m_{1,3,3}=m_{1,3,4}=1+x$$

Finally, for $j=4$,

$$\begin{aligned} m_{1,4,1} &= \gcd\left(f_1, \frac{x^{15}-1}{a_{1,4,1}(x)}\right)=1+x, \text{ where} \\ a_{1,4,1} &= (1+x+x^2)(1+3x+2x^2+x^4)(1+2x^2+3x^3+x^4)(1+x+x^2+x^3+x^4). \end{aligned}$$

Consequently, we have

$$\begin{aligned} &32\cdot(2^1-1)+16\cdot[\underbrace{(2^1-1)+\cdots+(2^1-1)}_{4\text{ times}}]+8\cdot[\underbrace{(2^1-1)+\cdots+(2^1-1)}_{6\text{ times}}] \\ &\quad+4\cdot[\underbrace{(2^1-1)+\cdots+(2^1-1)}_{4\text{ times}}]+2\cdot(2^1-1)=32+64+48+16+2=162 \end{aligned}$$

$\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes for $f=f_1=1+x$. If we take $f=f_2$, then we have

$$\begin{aligned} &32\cdot(2^2-1)+16\cdot[\underbrace{(2^2-1)+\cdots+(2^2-1)}_{4\text{ times}}]+8\cdot[\underbrace{(2^2-1)+\cdots+(2^2-1)}_{6\text{ times}}] \\ &\quad+4\cdot[\underbrace{(2^2-1)+\cdots+(2^2-1)}_{4\text{ times}}]+2\cdot(2^2-1)=96+192+144+48+6=486\text{ codes.} \end{aligned}$$

For $f=f_4$, by applying Theorem 13, we get

$$32 \cdot (2^3-1) + 16 \cdot [(2^2-1) + (2^1-1) + \underbrace{(2^3-1) + \cdots + (2^3-1)}_{3 \text{ times}}]$$
$$+ 8 \cdot [\underbrace{(2^2-1) + \cdots + (2^2-1)}_{3 \text{ times}} + \underbrace{(2^1-1) + \cdots + (2^1-1)}_{3 \text{ times}} + \underbrace{(2^3-1) + \cdots + (2^3-1)}_{3 \text{ times}}]$$
$$+ 4 \cdot [\underbrace{(2^2-1) + \cdots + (2^2-1)}_{3 \text{ times}} + \underbrace{(2^1-1) + \cdots + (2^1-1)}_{3 \text{ times}} + (2^3-1)]$$
$$+ 2 \cdot [(2^2-1) + (2^1-1)] = 32 \cdot 7 + 16 \cdot 25 + 8 \cdot 33 + 4 \cdot 19 + 2 \cdot 4 = 972$$

$\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes. Furthermore, we calculate the number of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes as

$$\begin{aligned} &\text{for } f_5 \longrightarrow 162, \\ &\text{for } f_6 \longrightarrow 486, \\ &\text{for } f_7 \longrightarrow 972. \end{aligned}$$

Finally the total number of non-separable additive cyclic code $\mathcal{C} \subseteq \mathbb{Z}_2[x]/\langle x^9-1\rangle \times \mathbb{Z}_4[x]/\langle x^{15}-1\rangle$ is

$$162 + 486 + 972 + 162 + 486 + 972 = 3240,$$

and the total number of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes is $1944 + 3240 = 5184$.

5 The number of $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive cyclic codes

Let p be any prime number, r is any positive integer and s is any positive integer relatively prime with p. In this case, the ring $\mathbb{Z}_{p^2}[x]/\langle x^s-1\rangle$ will be a principal ideal ring. In this section, we are interested to generalize our previous results and find formulas for the number of separable and non-separable $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive cyclic codes of length $n = r + s$. In [5], Borges et. al. studied the structure of $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes. Hence, based on this work if $\mathcal{C}$ is an additive cyclic code over $\mathbb{Z}_p\mathbb{Z}_{p^2}$ of length $n = r + s$, then $\mathcal{C}$ is generated by

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

where $f|(x^r-1) \, mod \, p$, $a|g|(x^s-1) \, mod \, p^2$, l is a polynomial over $\mathbb{Z}_p[x]$ satisfying $\deg(l) < \deg(f)$, and $f|\frac{x^s-1}{a}l$. As in the case of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, the above generators are unique. Moreover, the code $\mathcal{C}$ is separable if and only if the polynomial $l = 0$.

Lemma 18 *The number of separable $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive cyclic codes of length $n = r + s$ is $(p^v+1)^{w_1}3^{w_2}$ where $(x^r-1) = \left(x^N-1\right)^{p^v}$, w_1 is the number of irreducible factors of (x^r-1) mod p and w_2 is the number of irreducible factors of (x^s-1)mod p^2.*

Proof The proof is similar to the proof of Lemma 10. □

In fact, as we have showed in the proof of Theorem 13, the number of $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic codes are determined only by the generator polynomials of the code $\mathcal{C}$. Hence, the same proof can easily be applied to give the exact number of $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive cyclic codes of length $n = r + s$.

Corollary 19 *Let $\mathcal{C} = \langle (f, 0), (l, g + pa) \rangle$ be a non-separable cyclic code in $\mathbb{Z}_p[x]/\langle x^r - 1\rangle \times \mathbb{Z}_{p^2}[x]/\langle x^s - 1\rangle$ with $(r, s) \neq 1$. Assume that $x^r - 1 = (\widetilde{f_1}\widetilde{f_2}\ldots\widetilde{f_t})^{p^v}$ and $x^s - 1 = \widetilde{g_1}\widetilde{g_2}\ldots\widetilde{g_w}$ are the factorizations of $x^r - 1$ and $x^s - 1$ into irreducible polynomials in $\mathbb{Z}_p[x]$ and $\mathbb{Z}_{p^2}[x]$, respectively. The number of $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive cyclic codes is given by*

$$\left[\sum_{i=1}^{(p^v+1)^t-1}\left(\sum_{j=0}^{w-1} 2^{w-j}\sum_k \left(p^{\deg(m_{ijk})} - 1\right)\right)\right],$$

where $m_{ijk} = \gcd\left(f_i, \frac{x^s-1}{a_{ijk}}\right) > 1$ and $a = a_{ijk}$ is the collection of all polynomials that satisfy the following conditions:

1. $f_i | \left(\frac{x^s-1}{a_{ijk}} l\right) \bmod p$.
2. *f_i is not a factor of $a_{ijk} \bmod p$.*
3. *a_{ijk} has exactly j factors of $x^s - 1$.*
4. *The sum k runs over all the choices for a satisfying the above conditions.*

Proof The proof of this corollary is very similar to the proof of Theorem 13. So we skip it. □

Example 20 Let $\mathcal{C}$ be a $\mathbb{Z}_3\mathbb{Z}_9$-additive cyclic code in $\mathbb{Z}_3[x]/\langle x^7 - 1\rangle \times \mathbb{Z}_9[x]/\langle x^7 - 1\rangle$. Hence, $p = 3$, $r = 7 = s$. Therefore,

$$\begin{aligned} x^7 - 1 =& (2 + x)(1 + x + x^2 + x^3 + x^4 + x^5 + x^6)\ in\ \mathbb{Z}_3[x] \text{ and} \\ x^7 - 1 =& (8 + x)(1 + x + x^2 + x^3 + x^4 + x^5 + x^6)\ in\ \mathbb{Z}_9[x]. \end{aligned}$$

Label the factors of $\left(x^7 - 1\right)$ mod 3 as: $f_1 = (2 + x)$, $f_2 = (1 + x + x^2 + x^3 + x^4 + x^5 + x^6)$, and $f_3 = \left(x^7 - 1\right)$. Label the factors of $\left(x^7 - 1\right)$ in $\mathbb{Z}_9[x]$ as: $g_1 = (8 + x)$, $g_2 = (1 + x + x^2 + x^3 + x^4 + x^5 + x^6)$, and $g_3 = \left(x^7 - 1\right)$.

First, let $\mathcal{C}$ be a separable $\mathbb{Z}_3\mathbb{Z}_9$-additive cyclic code with $\mathcal{C} = \langle (f, 0), (0, g + 3a)\rangle$. By Lemma 18, there are $2^3 3^3 = 216$ separable $\mathbb{Z}_3\mathbb{Z}_9$-additive cyclic codes.

Based on Corollary 19, the number of non-separable $\mathbb{Z}_3\mathbb{Z}_9$-additive cyclic codes with $r = s = 7$ is

$$\sum_{i=1}^{3}\left(\sum_{j=0}^{1} 2^{2-j}\sum_k \left(3^{\deg(m_{ijk})} - 1\right)\right),$$

where the number of choices for the polynomial f is 3. First, take $f = (2 + x) = f_1$. Hence, the number of codes for this choice of f is

$$\sum_{j=0}^{1} 2^{2-j} \sum_{k} \left(3^{\deg(m_{1jk})} - 1\right).$$

If $j = 0$, then $a_{1,0,k}$ is the collection of all polynomials that do not contain $f_1 \mod 3$ and have 0 factors of $x^7 - 1$. Hence, there is only one choice for $a = 1$ and in this case $k = 1$ with

$$m_{1,0,1}(x) = \gcd\left(2 + x, x^7 - 1\right) = (2 + x) = f_1(x).$$

If $j = 1$, then $a_{1,1,k}$ is the collection of all polynomials that do not contain $f_1 \mod 3$ and have 1 factor of $\left(x^7 - 1\right) \mod 3$. Hence, there is only one choice which is g_2 and in this case $k = 1$ with

$$m_{1,1,1} = \gcd\left(2 + x, \frac{x^7 - 1}{g_2}\right) = (2 + x) = f_1.$$

Thus the number of codes when $f = f_1$ is

$$4\left(3^1 - 1\right) + 2\left(3^1 - 1\right) = 12.$$

Now, if $f = f_2 = (1 + x + x^2 + x^3 + x^4 + x^5 + x^6)$ then similarly we have

$$4\left(3^6 - 1\right) + 2\left(3^6 - 1\right) = 4368 \text{ codes.}$$

If $f = f_3 = x^7 - 1$, then we get

$$\begin{aligned}\sum_{j=0}^{1} 2^{2-j} \sum_{k} \left(3^{\deg(m_{i,j,k})} - 1\right) &= 2^2\left[3^7 - 1\right] + 2\left[\left(3^6 - 1\right) + \left(3^1 - 1\right)\right] \\ &= 8744 + 1460 = 10204 \text{ codes.}\end{aligned}$$

Therefore, the total number of non-separable $\mathbb{Z}_3\mathbb{Z}_9$-additive cyclic codes when $r = s = 7$ is

$$12 + 4368 + 10204 = 14584.$$

Note that the number of non-separable $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes for $r = s = 7$ is 2984.

6 Conclusion

$\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes were studied recently by many researchers [1, 3, 4]. In this paper, we focused on counting the exact number of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes of length $n = r + s$, for any positive integer r and any positive odd integer

s. Moreover, we provided formulas which give the exact number of separable and non-separable $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes. We then generalized our results to find the number of separable and non-separable $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive cyclic codes of length $n = r + s$, for any prime p, any positive integer r and any positive integer s where $\gcd(p, s) = 1$.

Acknowledgements The authors would like to thank the reviewers for their careful reading of the paper and their valuable comments that improved the paper tremendously. In fact, the reviewers comments played a huge impact to create Sect. 5 of the paper that generalizes our results from counting the number of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes to counting the numbers of $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive cyclic codes.

References

1. Abualrub, T., Siap, I., Aydin, N.: $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes. IEEE Trans. Inf. Theory **60**(3), 1508–1514 (2014)
2. Aydogdu, I., Abualrub, T., Siap, I.: $\mathbb{Z}_2\mathbb{Z}_2[u]$-cyclic and constacyclic codes. IEEE Trans. Inf. Theory **63**(8), 4883–4893 (2017)
3. Borges, J., Fernández-Córdoba, C., Pujol, J., Rif à, J., Villanueva, M.: $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: generator matrices and duality. Des. Codes Cryptogr. **54**(2), 167–179 (2010)
4. Borges, J., Fernández-Córdoba, C., Ten-Valls, R.: $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, generator polynomials and dual codes. IEEE Trans. Inf. Theory **62**(11), 6348–6354 (2016)
5. Borges, J., Fernández-Córdoba, C., Ten-Valls, R.: On $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes. Adv. Math. Commun. **12**(1), 169–179 (2018)
6. Carlet, C.: $\mathbb{Z}_{2^k}$-linear codes. IEEE Trans. Inf. Theory **44**, 1543–1547 (1998)
7. Dougherty, S., Salturk, E.: Counting additive $\mathbb{Z}_2\mathbb{Z}_4$ codes. Contemp. Math. **634**, 137–147 (2015)
8. Greferath, M., Schmidt, S.E.: Gray isometries for finite chain rings. IEEE Trans. Inf. Theory **45**(7), 2522–2524 (1999)
9. Hammons, A.R., Kumar, P.V., Calderbank, A.R., Sloane, N.J.A., Solé, P.: The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes. IEEE Trans. Inf. Theory **40**(2), 301–319 (1994)
10. Honold, T., Landjev, I.: Linear codes over finite chain rings. In: In Optimal Codes and Related Topics, Sozopol, Bulgaria, pp. 116–126 (1998)
11. Rifà-Pous, H., Rifà, J., Ronquillo, L.: $\mathbb{Z}_2\mathbb{Z}_4$-additive perfect codes in steganography. Adv. Math. Commun. **5**(3), 425–433 (2011)
12. Siap, I., Aydogdu, I.: Counting the generator matrices of $\mathbb{Z}_2\mathbb{Z}_8$ codes. Math. Sci. Appl. E-Notes **1**(2), 143–149 (2013)