Journal of Algebra and Related Topics
Vol. 14, No. 2, 2026, pp. 79-95. Research Article

Good asymptotic behavior of additive cyclic codes on $\mathbb{F}_q[u]/\langle u^2\rangle \times \mathbb{F}_q[u]/\langle u^3\rangle$

Ali Isapour-Khasadan[†,‡], Shahram Mehry[†*], Saadun Mahmoudi[§]

[†] *Faculty of Mathematical Sciences and Statistics, Malayer University, Malayer, Iran*
[‡] *Department, Faculty of Basic Sciences, Khatam-ol-Anbia(PBU) University, Tehran, Iran*
[§] *Department of Mathematics, Bu Ali Sina University, Hamedan, Iran*
Emails: ali.esapour@stu.malayeru.ac.ir, shmehry@malayeru.ac.ir, mahmoudi.math89@yahoo.com

Abstract. In this paper, we study additive cyclic codes over the direct product of two finite commutative chain rings. Let $S = \mathbb{F}_q[u]/\langle u^2\rangle = \mathbb{F}_q + u\mathbb{F}_q$ and $R = \mathbb{F}_q[u]/\langle u^3\rangle = \mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ are two finite chain rings, where $u^2 = 0 = u^3$ and q is a power of a prime number. We construct a class of SR-additive cyclic codes generated by pairs of polynomials, where S is a R-algebra and SR-additive cyclic code is a R-submodule of $S^\alpha \times R^\beta$. Based on probabilistic arguments, we study the asymptotic behavior of the rates and relative minimum distances of a certain class of the codes. We show that there exists an asymptotically good infinite sequence of SR-additive cyclic codes with the relative minimum distance of the code is convergent to δ, and the rat is convergent to $\frac{2}{q+q^2}$ for $0 < \delta < \frac{1}{1+q}$, and q is a power of a prime number.

Keywords: $\mathbb{F}_q[u]/\langle u^2\rangle \times \mathbb{F}_q[u]/\langle u^3\rangle$-Additive cyclic codes, Random codes, Asymptotically good, Cumulative weight enumerator.
AMS Subject Classification 2020: 94B05, 94B15.

1 Introduction

A sequence of codes $C_1, C_2, \ldots$ with length n_i of C_i approaching infinity is said to be asymptotically good, if both the rate $R(C_i)$ and the relative distance $\Delta(C_i)$ are positively bounded from below. In other words, if $C(n)$ is a family of codes of parameters $[n, k_n, d_n]$, the rate R and relative distance Δ are defined as

$$R = \limsup_{n\longrightarrow\infty} \frac{k_n}{n}$$

*Corresponding author
Received: 13 March 2025/ Revised: 26 June 2025/ Accepted: 28 June 2025
DOI: 10.22124/JART.2025.30109.1780

© 2026 University of Guilan

and

$$\Delta = \liminf_{n \longrightarrow \infty} \frac{d_n}{n}.$$

Then a family of codes is said to be asymptotically good if $R\Delta > 0$.
By Varshamov's probabilistic methods [17], linear codes over a finite field are asymptotically good. Also Shi, et al. proved that there are asymptotically good additive cyclic codes [13], and the construction of different kinds of codes satisfying the modified Gilbert-Varshamov bound was presented in [15,16]. Among other examples, we can see that quasi-cyclic codes are asymptotically good [4].

Recently, additive codes over products of two rings have attracted extensive attention by many researchers. $\mathbb{Z}_2\mathbb{Z}_4$, $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$, $\mathbb{Z}_2\mathbb{Z}_2[u]$ and $\frac{\mathbb{Z}_p[u]}{\langle u^r\rangle} \times \frac{\mathbb{Z}_p[u]}{\langle u^s\rangle}$-additive codes are some examples of these codes which we can see a complete study of these codes in [2,12].
In [8,9], the authors studied the asymptotic behaviour of $\mathbb{Z}_4$-double cyclic codes and $\mathbb{Z}_p\mathbb{Z}_p[v]$-additive cyclic codes and proved that these classes of codes are asymptotically good. Fan et al. proved that $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes are asymptotically good [6]. By using a probabilistic method, Yao et al showed that there exist numerous asymptotically good $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes [18]. Also in [19], it was proved that $\mathbb{Z}_p\mathbb{Z}_p[u]/\langle u^t\rangle$-additive cyclic codes are asymptotically good.
In [1], Abualrub and Siap studied cyclic codes over the rings $S = \mathbb{Z}_2 + u\mathbb{Z}_2$ where $u^2 = 0$ Mod 2 and $R = \mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$ where $u^3 = 0$ Mod 3. In this paper we show that additive cyclic codes over $\mathbb{F}_q[u]/\langle u^2\rangle \times \mathbb{F}_q[u]/\langle u^3\rangle = \mathbb{F}_q[u^2, u^3]$ are asymptotically good. In fact, we study asymptotic properties of the relative distance and the rate of $\mathbb{F}_q[u^2, u^3]$- additive cyclic codes with cyclic length m. Using a probabilistic method, we show that there exists a series of asymptotically good SR-additive cyclic codes.
The paper is organized as follows. In Section 2, some definitions and results on $\mathbb{F}_q[u^2, u^3]$-additive cyclic codes. In Section 3, we construct a class of $\mathbb{F}_q[u^2, u^3]$ - additive cyclic codes generated by pairs of polynomials. In Section 4, based on the probabilistic method, we present the main results of asymptotic properties of the rates and relative distances of this class of codes. In the last section, we conclude the paper.

2 Preliminaries

Let $S = \mathbb{F}_q[u]/\langle u^2\rangle = \mathbb{F}_q + u\mathbb{F}_q$ and $R = \mathbb{F}_q[u]/\langle u^3\rangle = \mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ be the finite commutative chain rings with $u^2 = 0 = u^3$ and q is a power of a prime number. In this section, we present some definitions and results about SR - additive cyclic codes, which are applied throughout this paper.
let R be a finite commutative ring and S be an R-algebra with a ring homomorphism $\mu : R \longrightarrow S$, $a_0 + ua_1 + u^2a_2 \longrightarrow a_0 + ua_1$ where $a_0, a_1, a_2 \in \mathbb{F}_q$. Let α and β be positive integers. For $d \in R$, consider the following scalar multiplication over $S^\alpha \times R^\beta$

$$d \cdot (a \mid b) = (\mu(d)a_0, \mu(d)a_1, \ldots, \mu(d)a_{\alpha-1} \mid db_0, db_1, \ldots, db_{\beta-1}).$$

The set $S^\alpha \times R^\beta$, with this scalar multiplication is an R-module.

Definition 1. *Let α and β be positive integers. A non-empty subset C of $S^\alpha \times R^\beta$ is called an SR-additive code, if C is an R-submodule.*

By Theorem 2.1 in [2], we have the following generator matrix for an SR-additive code C

$$G = \begin{bmatrix} I_{k_0} & R_{01} & R_{02} & 0 & 0 & uA_{01} & uA_{02} \\ 0 & uI_{k_1} & uR_{12} & 0 & 0 & 0 & u^2A_{12} \\ 0 & B_{01} & B_{02} & I_{l_0} & S_{01} & S_{02} & S_{03} \\ 0 & 0 & uB_{12} & 0 & uI_{l_1} & uS_{12} & uS_{13} \\ 0 & 0 & 0 & 0 & 0 & u^2I_{l_2} & u^2S_{23} \end{bmatrix}$$

where R_{ij}, B_{tj} are matrices over S and A_{ij}, S_{pq} are matrices over R. In this case, C is of type $(\alpha, \beta; k_0, k_1; l_0, l_1, l_2)$ and hence

$$| C |= q^{2k_0}q^{k_1}q^{3l_0}q^{2l_1}q^{l_2}.$$

Let $v = (v_0, v_1, \ldots, v_{\alpha-1}, v'_0, v'_1, \ldots, v'_{\beta-1})$ and $w = (w_0, w_1, \ldots, w_{\alpha-1}, w'_0, w'_1, \ldots, w'_{\beta-1}) \in S^\alpha \times R^\beta$, then the inner product of v and w is defined as

$$\langle v, w\rangle = u(\sum_{i=0}^{\alpha-1} v_i w_i) + \sum_{j=0}^{\beta-1} v'_j w'_j \in R.$$

Let C be a SR-additive code. We can define the dual code $C^\perp$ of SR-additive code C in the following standard way,

$$C^\perp = \{w \in S^\alpha \times R^\beta | \langle v, w\rangle = 0, \text{ for all } v \in C\}.$$

It is also clear that $C^\perp$ is an R-submodule of $S^\alpha \times R^\beta$. So, $C^\perp$ is also SR-additive code. Similar to the homogeneous metric introduced in [5], for $x \in S$ and $y \in R$, the homogeneous weights of x and y are defined as follows,

$$wt_{hom}(x) = \begin{cases} 0 & \text{if x} = 0 \\ q & \text{if x} \in \langle \text{u} \rangle \setminus \{0\} \\ q-1 & \text{if x} \in \text{S} \setminus \langle \text{u} \rangle, \end{cases}$$

and

$$wt_{hom}(y) = \begin{cases} 0 & \text{if y} = 0 \\ q^2 & \text{if y} \in \langle \text{u}^2 \rangle \setminus \{0\} \\ (q-1)q & \text{if y} \in \text{R} \setminus \langle \text{u}^2 \rangle, \end{cases}$$

where $\langle u \rangle$ and $\langle u^2 \rangle$ are the principal ideal by the element u and u^2 of S and R respectively. Elements $s \in S$ and $r \in R$ can be written uniquely as $s = a_0 + ua_1$ and $r = a_0 + ua_1 + u^2a_2$ where $a_0, a_1, a_2 \in \mathbb{F}_q$. According to [5], we have Gray maps

$$\begin{array}{rcl} \varphi_1 : S & \to & \mathbb{F}_q^q \\ a_0 + ua_1 & \to & (b_0, b_1, \ldots, b_{q-1}), \end{array}$$

and

$$\varphi_2 : R \to \mathbb{F}_q^{q^2}$$

$$a_0 + ua_1 + u^2a_2 \quad \to \quad (b_0, b_1, \ldots, b_{q^2-1}).$$

These maps φ_1 and φ_2 are linear maps and can be extended form $S^n \times R^n$ to $\mathbb{F}_q^{qn} \times \mathbb{F}_q^{q^2n}$. The homogeneous weight $wt_{hom}(x, y)$ of $S^n \times R^n$ is defined with

$$wt_{hom}(x, y) = \sum_{i=0}^{n-1} wt_{hom}(x_i, y_i),$$

if $(x, y) = (x_0, x_1, \ldots, x_{n-1}, y_0, y_1, \ldots, y_{n-1}) \in S^n \times R^n$. For any two elements (x_1, y_1) and $(x_2, y_2) \in S^n \times R^n$, the homogeneous distance between (x_1, y_1) and (x_2, y_2) is defined as

$$d_{hom} = wt_{hom}((x_1, y_1) - (x_2, y_2)) = wt_{hom}(x_1 - x_2, y_1 - y_2).$$

From [14], the Gray maps φ_1 and φ_2 are a distance preserving isometry from $(S^n \times R^n, d_{hom})$ to $(\mathbb{F}_q^{qn} \times \mathbb{F}_q^{q^2n}, d_H)$, where d_{hom} and d_H are denoted as homogeneous distance and Hamming distance, respectively.
We generalize the maps φ_1 and φ_2 to the map

$$\varphi : S^\alpha \times R^\beta \to \mathbb{F}_q^{q\alpha} \times \mathbb{F}_q^{q^2\beta},$$

such that

$$\varphi(x, y) = (\varphi_1(x), \varphi_2(y)) = (\varphi_1(x_1), \ldots, \varphi_1(x_{\alpha-1}), \varphi_2(y_1), \ldots, \varphi_2(y_{\beta-1})),$$

where $x = (x_1, x_2, \ldots, x_{\alpha-1}) \in S^\alpha$ and $y = (y_1, y_2, \ldots, y_{\beta-1}) \in R^\beta$. The image $\varphi(C)$ of SR-linear code C is a linear code of length $N = q^{s-1}\alpha + q^{r-1}\beta$. Then the map φ is a distance-preserving map from $S^\alpha \times R^\beta$ to the Hamming distance in $\mathbb{F}_q^{q\alpha} \times \mathbb{F}_q^{q^2\beta}$

Let $v = (x, y) \in S^\alpha \times R^\beta$, the weight of code C is defined by

$$\begin{aligned} wt_{hom}(v) &= wt_{hom}(x, y) = w_H(\varphi(x, y)) = w_H(\varphi_1(x), \varphi_2(y)) \\ &= w_H(\varphi_1(x)) + w_H(\varphi_2(y)), \end{aligned} \tag{1}$$

Let C be a SR-additive code, the minimum weight of code C is defined $wt(C) = min\{wt(c)|c \in C \setminus \{0\}\}$. The relative minimum distance and the rate of C is defined by $\triangle(C) = \dfrac{wt(C)}{N}$ and $R(C) = \dfrac{K}{N}$, where $K = \sum_{i=1}^{2}(3-i)k_i + \sum_{j=1}^{3}(4-j)l_j$ and $N = q\alpha + q^2\beta$.

Definition 2. *Anon-empty subset C of $S^\alpha \times R^\beta$ is called a SR-additive cyclic code if (i) C is an additive code, and (ii) for any codeword $c = (a_0, a_1, \ldots, a_{\alpha-1}, b_0, b_1, \ldots, b_{\beta-1}) \in C$, its cyclic shift $\rho(c) = (a_{\alpha-1}, a_0, a_1, \ldots, a_{\alpha-2}, b_{\beta-1}, b_0, b_1, \ldots, b_{\beta-2})$ is still in C.*

Let $R_{\alpha,\beta} = S[x]/\langle x^\alpha - 1\rangle \times R[x]/\langle x^\beta - 1\rangle$, for any element

$$c = (a_0, a_1, \ldots, a_{\alpha-1}, b_0, b_1, \ldots, b_{\beta-1}) \in S^\alpha \times R^\beta,$$

there is a one-one correspondence between the element C of $S^\alpha \times R^\beta$ and $C(x) = (a(x), b(x))$ of $R_{\alpha,\beta}$, where

$$a(x) = a_0 + a_1x + \cdots + a_{\alpha-1}x^{\alpha-1} \in S[x]/\langle x^\alpha - 1\rangle = S_\alpha,$$

and

$$b(x) = b_0 + b_1x + \cdots + b_{\alpha-1}x^{\beta-1} \in R[x]/\langle x^\beta - 1\rangle = R_\alpha.$$

3 A class of SR-additive cyclic codes

Throughout the paper, we assume that $\alpha = \beta = m$, and $\gcd(m, q) = 1$. Also, by the correspondence μ in the previous section, we consider SR-additive cyclic codes as $R[x]$-submodules of $S_m \times R_m$ where

$$S_m = S[x]/\langle x^m - 1\rangle,\ R_m = R[x]/\langle x^m - 1\rangle.$$

In this section, we construct a class of $R[x]$-submodules of $S_m \times R_m$ and we study the properties of this class.
Define $\chi : S \to R$ by $\chi(a) = ua$ for every $a \in S$. Then χ is an additive group homomorphism and the image of this homomorphism is

$$uR = uS = \{0, u, 2u, \ldots, (q-1)u\} \subset R = \mathbb{F}_q[u]/\langle u^3\rangle.$$

Now consider the following $R[x]$-submodule of R_m

$$uR_m = \{r(x) = \sum_{i=0}^{m-1} r_i x^i \in R_m :\ r_i = ua_i, a_i \in \mathbb{F}_q\}.$$

By the group homomorphism χ, we have the following $R[x]$-module isomorphism

$$\chi' : S_m \to uR_m,\ \sum_{i=0}^{m-1} s_i x^i \to \sum_{i=0}^{m-1} us_i x^i.$$

So $S_m \times uR_m$ is an $R[x]$-submodule of $S_m \times R_m$.
Any element of $S_m \times uR_m$ can be uniquely expressed as $(a(x), ub(x))$, where $a(x) = \sum_{i=0}^{m-1} a_i x^i$ and $b(x) = \sum_{i=0}^{m-1} b_i x^i$ are elements of S_m. For $(a(x), b(x)) \in S_m \times S_m$, define

$$C_{a,b} = \{(f(x)a(x), uf(x)b(x)) \in S_m \times uR_m \mid f(x) \in S_m\},$$

which is an S_m-submodule of $S_m \times uR_m$. Since S is an R-algebra, $C_{a,b}$ is also an $R[x]$-submodule of $S_m \times R_m$ and hence is an SR-additive cyclic code generated by $(a(x), b(x))$.

Note that $C_{a,b}$ is an S-module and S is a $\mathbb{F}_q$-vector space. So $C_{a,b}$ is also a $\mathbb{F}_q$-vector space. We denote the dimension of $C_{a,b}$ over S and $\mathbb{F}_q$ by $\dim_S C_{a,b}$ and $\dim_{\mathbb{F}_q} C_{a,b}$, respectively.

Now consider the SR-additive cyclic code $C_{a,b}$ generated by $(a(x), b(x))$. Let $a(x) = a_0 + a_1x + \cdots + a_{m-1}x^{m-1}$ and $b(x) = b_0 + b_1x + \cdots + b_{m-1}x^{m-1}$. Define two circulant $m \times m$ matrices as follows,

$$A = \begin{bmatrix} a_0 & a_1 & \ldots & a_{m-1} \\ a_{m-1} & a_0 & \ldots & a_{m-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \ldots & a_0 \end{bmatrix},$$

and

$$B = \begin{bmatrix} b_0 & b_1 & \ldots & b_{m-1} \\ b_{m-1} & b_0 & \ldots & b_{m-2} \\ \vdots & \vdots & \ddots & \vdots \\ b_1 & b_2 & \ldots & b_0 \end{bmatrix}.$$

Now let $D = \begin{bmatrix} A & uB \end{bmatrix}$. Then

$$C_{a,b} = \{(y_0, y_1, \ldots, y_{m-1})D \in S^m \times R^m \mid (y_0, y_1, \ldots, y_{m-1}) \in S^m\}.$$

The following theorem gives the structure of $C_{a,b}$, where $\gcd(\cdot,\cdot)$ denotes the greatest common divisor and $\deg f(x)$ is the degree of the polynomial.

Theorem 1. *Let* $(a(x), b(x)) \in S_m \times S_m$, $g_{a,b}(x) = \gcd(a(x), b(x), x^m - 1)$ *and* $h_{a,b}(x) = \dfrac{x^m - 1}{g_{a,b}(x)}$. *Then* $(a(x), b(x))$ *induces an* S_m*-module homomorphism*

$$\begin{array}{rcl} \psi_{a,b} : S_m & \to & S_m \times uR_m \\ f(x) & \to & (f(x)a(x), uf(x)b(x)), \end{array}$$

and the following hold.

i) *The image* $\mathrm{Im}(\psi_{a,b}) = C_{a,b}$.

ii) *The kernel* $\ker(\psi_{a,b}) = \langle h_{a,b}(x)\rangle_{S_m}$, *and* $\dim_S C_{a,b} = \deg(h_{a,b}(x))$.

iii) $\psi_{a,b}$ *induces an isomorphism* $\langle g_{a,b}(x)\rangle_{S_m} \cong C_{a,b}$, *in particular,*

$$C_{a,b} = \{(f(x)a(x), uf(x)b(x)) \in S_m \times uR_m \mid f(x) \in \langle g_{a,b}(x)\rangle_{S_m}\}. \tag{2}$$

Proof. i) It is obvious that $\psi_{a,b}$ is an R_m-module homomorphism and $\mathrm{Im}(\psi_{a,b}) = C_{a,b}$.

ii) For $f(x) \in S_m$, $f(x) \in \ker(\psi_{a,b})$ if and only if

$$\begin{array}{l} f(x)a(x) \equiv 0 \ (\mathrm{Mod}\ x^m - 1), \\ f(x)b(x) \equiv 0 \ (\mathrm{Mod}\ x^m - 1), \end{array}$$

which implies that $f(x)\gcd(a(x), b(x)) \equiv 0 \ (\mathrm{Mod}\ x^m - 1)$ in $S[x]$. Hence

$$f(x) \equiv 0 \ (\mathrm{Mod}\ \frac{x^m - 1}{\gcd(a(x), b(x), x^m - 1)}).$$

Then $f(x) \in \langle h_{a,b}(x)\rangle_{S_m}$, where $h_{a,b}(x) = \dfrac{x^m - 1}{g_{a,b}(x)}$ and $\dim_S C_{a,b} = \dim_S S_m - \dim_S \ker(\psi_{a,b}) = m - \deg(g_{a,b}(x)) = \deg(h_{a,b}(x))$.

iii) Since $\gcd(m, q) = 1$, S_m is semisimple, we have $S_m = \langle g_{a,b}(x)\rangle_{S_m} \oplus \langle h_{a,b}(x)\rangle_{S_m}$. Then the above S_m-module homomorphism $\psi_{a,b}$ induces the following S_m-module isomorphism

$$\bar{\psi}_{a,b} : \langle g_{a,b}(x)\rangle_{S_m} \to C_{a,b} \quad ; \quad c(x) \to (c(x)a(x), uc(x)b(x)).$$

Therefore, (2) is proved.

□

Corollary 1. *Let* $C_{a,b}$, $h_{a,b}(x)$ *be as presented in Theorem 1 and* $r = deg(h_{a,b}(x))$. *Let* $D = \begin{bmatrix} A & uB \end{bmatrix}$. *Then the matrix consisting of the first* r *rows of* D *is a generator matrix of* $C_{a,b}$.

Proof. From the above theorem, we see that the rank of D is equal to r. By [7], the first r rows of D are linearly independent. □

Example 1. Let $q = 2$ and $S = \mathbb{F}_2[u]/\langle u^2\rangle = \mathbb{F}_2 + u\mathbb{F}_2$, $R = \mathbb{F}_2[u]/\langle u^3\rangle = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$. Also, let $m = 3$, $a(x) = 1 + x$ and $b(x) = 1 + x + x^2$. By Theorem 1,

$$g_{a,b}(x) = \gcd(a(x), b(x), x^3 - 1) = 1$$

$$h_{a,b}(x) = \frac{x^3 - 1}{g_{a,b}(x)} = x^3 - 1.$$

Therefore, $\dim C_{a,b} = 3$. Using the notations in Corollary 1,

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \quad , \quad B = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \quad , \quad D = \begin{bmatrix} 1 & 1 & 0 & u & u & u \\ 0 & 1 & 1 & u & u & u \\ 1 & 0 & 1 & u & u & u \end{bmatrix}.$$

Thus the three rows of D are linearly independent and

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

is a generator matrix of $C_{a,b}$.

Since $\gcd(m, q) = 1$, $x^m - 1$ has the factorization into distinct monic irreducible polynomials over S. Let $x^m - 1 = f_0(x)f_1(x)\cdots f_t(x)$ be an irreducible decomposition of $x^m - 1$ in $S[X]$. By the Chinese Remainder Theorem,

$$\frac{S[x]}{x^m - 1} = \frac{S[x]}{\bigcap_{i=0}^{t}\langle f_i\rangle(x)} \cong \bigoplus_{i=0}^{t} \frac{S[x]}{\langle f_i(x)\rangle} \cong \bigoplus_{i=0}^{t} G_i.$$

Let $\deg(f_i(x)) = d_i$, then $\dim_S G_i = \deg(f_i(x)) = d_i$. If $f_0(x) = x - 1$, then $d_0 = 1$.

Clearly $x^m - 1 = (x - 1)(x^{m-1} + \cdots + x + 1)$ in $S[x]$. Hence,

$$S_m = \frac{S[x]}{\langle x^m - 1\rangle} = \langle x^{m-1} + \cdots + x + 1\rangle_{S_m} \oplus \langle x - 1\rangle_{S_m}.$$

Let $J_m = \langle x-1\rangle_{S_m}$ be the ideal of S_m generated by $x-1$. Similarly $J'_m = \langle x-1\rangle_{R_m}$ be the ideal of R_m generated by $x - 1$. We have that $uJ'_m = \langle u(x - 1)\rangle_{R_m}$. The $R[x]$-module isomorphism $\chi' : S_m \to uR_m$ induces the following R_m-module isomorphism

$$\begin{array}{rcl} J_m \times J_m & \to & J_m \times u\acute{J}_m \\ (a(x), b(x)) & \to & (a(x), ub(x)). \end{array}$$

Now, let $a(x), b(x) \in J_m$. Since J_m is an ideal, the SR-additive cyclic code $C_{a,b}$ can be expressed as follows

$$C_{a,b} = \{(c(x)a(x), uc(x)b(x)) \in S_m \times uR_m \mid c(x) \in J_m\}.$$

Assume that $\frac{x^m-1}{x-1} = f_1(x)f_2(x)\cdots f_t(x)$ is a basic irreducible decomposition of $\frac{x^m-1}{x-1}$ in $S[x]$.

Lemma 1. *With the above notations, let* $(a(x), b(x)) \in J_m \times J_m$. *Then* $\dim_S C_{a,b} \leq m-1$. *Moreover,* $\dim_S C_{a,b} < m-1$ *if and only if there is an irreducible factor* $p(x)$ *of* $\frac{x^m-1}{x-1}$ *in* S_m *such that* $p(x) \mid a(x)$ *and* $p(x) \mid b(x)$.

Proof. Assume that $g_{a,b}(x) = \gcd(a(x), b(x), x^m - 1)$. We have that $(x-1) \mid g_{a,b}(x)$ and hence $\langle g_{a,b}(x)\rangle_{S_m} \subseteq \langle x-1\rangle_{S_m} = J_m$. By Theorem 3.1, $\dim_S C_{a,b} = \dim_S \langle g_{a,b}(x)\rangle_{S_m} \leq \dim_S J_m = m-1$. Thus, $\dim_S C_{a,b} = m-1$ if and only if $g_{a,b}(x) = \gcd(a(x), b(x), x^m-1) = x-1$. It follows that there is no irreducible factor $p(x)$ of $\frac{x^m-1}{x-1}$ such that $p(x) \mid a(x)$ and $p(x) \mid b(x)$. □

Lemma 2. *Let* $l_m = \min\{deg(f_1(x)), \deg(f_2(x)), \ldots, \deg(f_t(x))\}$ *in* $S[x]$,*and* d *be an integer with* $l_m \leq d \leq m-1$. *Then any non-zero ideal of* S_m *contained in* J_m *is of dimension at least* l_m, *and the number of the ideals with dimension* d *contained in* J_m *is at most* $m^{\frac{d}{l_m}}$.

Proof. The proof of this lemma is the same as [18, Lemma 3.3]. We repeat this by our notations. Every irreducible ideal contained in J_m corresponds exactly to one irreducible divisor $f_i(x)$ $(1 \leq i \leq t)$ of $\frac{x^m-1}{x-1}$, which implies that the dimension of the ideal is equal to $\deg(f_i(x))$. Therefore, the minimal dimension of the ideal contained in J_m is l_m. Any d-dimension ideal contained in J_m is a sum of at most d/l_m irreducible ideals. So the number of the d-dimensional ideals contained in J_m is at most the partial sum of binomial coefficients $\sum_{i=1}^{\lfloor d/l_m \rfloor} \binom{h}{i}$, where h is the number of irreducible ideals contained in J_m and $\lfloor d/l_m \rfloor$ denotes the largest integer which is not larger than d/l_m. It is easy to check that

$$\sum_{i=1}^{\lfloor d/l_m \rfloor} \binom{h}{i} \leq \sum_{i=1}^{\lfloor d/l_m \rfloor} \binom{m}{i} \leq \frac{d}{l_m} \times \frac{m(m-1)\cdots(m-\frac{d}{l_m}+1)}{1 \times 2 \times \cdots \times \frac{d}{l_m}} \leq m^{\frac{d}{l_m}}.$$

□

4 Random SR-additive cyclic codes

In this section, we view the sets $J_m \times J_m$ and $J_m \times u\acute{J}_m$ as probability spaces of $S_m \times S_m$ and $S_m \times uR_m$, respectively, whose samples are obtained with equal probability. By probabilistic method, we determine the asymptotic rates and relative distance of the class of SR-additive cyclic codes.

Recall that, for any prime power q, the function

$$\alpha_q(x) = 1 - h_q(x) = 1 - x\log_q(q-1) + x\log_q x - (1-x)\log_q(1-x),$$

is called the q-ary asymptotic *Gilbert*-Varshamov bound, or GV-bound in short for $0 < x \leq \frac{q-1}{q}$ where $h_q(x)$ is called the q-ary entropy with $0\log_q 0 = 0$ conventionally.

Then $\alpha_q(x)$ is a strictly decreasing convex function in the interval $[0, \frac{q-1}{q}]$ with $\alpha_q(0) = 1$ and $\alpha_q(\frac{q-1}{q}) = 0$, [10, sec.2.10.6]. In the following, we always assume that δ is a positive real number and $q = p^s$ such that $0 < \delta < \frac{2}{1+q} \cdot h_q^{-1}(1/2) < \frac{1}{1+q}$ for $h_q^{-1}(1/2) < 1/2$ and $\alpha_q(\frac{1+q}{2}\delta) = 1 - h_q(\frac{1+q}{2}\delta) > \frac{1}{2}$.

For each sample $(a(x), ub(x)) \in J_m \times uJ'_m$ with $(a(x), b(x)) \in J_m \times J_m$, we have an SR-additive cyclic code with cyclic length m as follows

$$C_{a,b} = \{(c(x)a(x), uc(x)b(x)) \in S_m \times uR_m \mid c(x) \in J_m\},$$

which is viewed as a random code over the probability space $J_m \times uJ'_m$. Hence the the relative distances $\Delta(C_{a,b})$ of $C_{a,b}$ and $\dim_S C_{a,b}$ of $C_{a,b}$ are random variables over the probability space. We will study the asymptotic behaviour of the probabilities $Pr(\dim_S C_{a,b} = m-1)$ and $Pr(\Delta(C_{a,b}) > \delta)$.
Let $N_{C_{a,b}}(\delta)$ be the number of non-zero codewords of $C_{a,b}$ with relative weight at most δ, i.e

$$N_{C_{a,b}}(\delta) = |\{c(x) \in J_m | 1 \leq wt(c(x)a(x), uc(x)b(x)) \leq q(1+q)m\delta\}|.$$

Then, $N_{C_{a,b}}$ is a non-negative integral random variable defined over the probability space $J_m \times uJ'_m$. According to [9], we call $N_{C_{a,b}}$ the cumulative weight enumerator of the random code $C_{a,b}$. For any $c(x) \in J_m$, and samples $(a(x), ub(x)) \in J_m \times uJ'_m$, we have the following indicator random variable

$$Y_c = \begin{cases} 1, & 1 \leq \mathrm{wt(c(x)a(x), uc(x)b(x))} \leq \mathrm{q(1+q)m}\delta \\ 0, & \text{otherwise.} \end{cases},$$

Let $I_c = \{c(x)a(x) \in S_m | a(x) \in J_m\}$ be the ideal of S_m generated by $c(x)$, where $c(x) \in J_m$, and denote its dimension over $\mathbb{F}_q$ by d_c, that is

$$I_c = \langle c(x) \rangle_{S_m} \subseteq J_m, \quad \dim_{\mathbb{F}_q} I_c = d_c.$$

Similarly, $I'_c = \langle uc(x) \rangle_{R_m} \subseteq uJ'_m$. By the S_m-module isomorphism from J_m to uJ'_m, we have that $\dim_{\mathbb{F}_q} I'_c = d_c$.

Lemma 3. *With the above notations, let*

$$(I_c \times I_c)^{\leq q(1+q)m\delta} = \{(f(x), g(x)) \in I_c \times I_c : \ wt(f(x), g(x)) \leq q(1+q)m\delta\}.$$

Then

$$|(I_c \times I_c)^{\leq q(1+q)m\delta}| \leq q^{2d_c h_q(\frac{1+q}{2}\delta)}.$$

Proof. Consider the Gray map $\varphi_1 : S \to \mathbb{F}_q^q$. So $\phi(I_c \times I_c) = \varphi_1(I_c) \times \varphi_1(I_c)$ is a linear code of length $2qm$. Since $0 < \delta < \frac{1}{1+q}$, the relative weight of $\phi((I_c \times I_c)^{\leq q(1+q)m\delta})$ is at most

$$\begin{aligned} \frac{q(1+q)m\delta}{2qm} &= \frac{(1+q)\delta}{2} \\ &< \frac{1+q}{2} \times \frac{1}{1+q} \\ &= \frac{1}{2} \leq 1 - \frac{1}{q}. \end{aligned}$$

Also the dimension of $I_c \times I_c$ over $\mathbb{F}_q$ is $2d_c$. Now by Corollary 2 of [7], we have the following inequality which completes the proof

$$|(I_c \times I_c)^{\leq q(1+q)m\delta}| = |\phi((I_c \times I_c)^{\leq q(1+q)m\delta})|$$

$$< \quad q^{2d_c h_q(\frac{1+q}{2}\delta)}.$$

□

Lemma 4. $E(Y_c) \leq q^{-2d_c(1-h_q(\frac{(1+q)}{2}\delta))}$.

Proof. Since $uJ'_m \subseteq R_m$, we have the following ideal

$$I'_c = \langle uc(x)\rangle_{R_m} = \{uc(x)b(x) \in R_m : \ b(x) \in J_m\} \subseteq uJ'_m.$$

For $I_c \times I'_c \subseteq S_m \times uR_m$, let $(I_c \times I'_c)^{\leq q(1+q)m\delta} = \{(f(x), ug(x)) \in I_c \times I'_c : \ wt(f(x), ug(x)) \leq q(1+q)m\delta\}$. Then

$$E(Y_c) = Pr(Y_c = 1) = \frac{|(I_c \times I'_c)^{\leq q(1+q)m\delta}| - 1}{|I_c \times I'_c|}.$$

For $f(x), g(x) \in S_m$, from the homogeneous weights on S and R, we have that

$$wt_{hom}(ug(x)) = qwt_{hom}(g(x)),$$

where $wt_{hom}(ug(x))$ and $wt_{hom}(g(x))$ are computed in R and S, respectively. Therefore,

$$wt(f(x), ug(x)) \geq wt(f(x), g(x)).$$

Hence,

$$|(I_c \times I'_c)^{\leq q(1+q)m\delta}| \leq |(I_c \times I_c)^{\leq q(1+q)m\delta}|.$$

Now, by Lemma 3 and $\dim_{\mathbb{F}_q} I'_c = \dim_{\mathbb{F}_q} I_c = d_c$, we obtain

$$\begin{aligned} E(Y_c) &= \frac{|(I_c \times I'_c)^{\leq q(1+q)m\delta}| - 1}{|I_c \times I'_c|} \\ &\leq \frac{|(I_c \times I_c)^{\leq q(1+q)m\delta}|}{|I_c \times I_c|} \\ &\leq \frac{q^{2d_c h_q(\frac{(1+q^{r-s})}{2}\delta)}}{q^{2d_c}} \\ &= q^{-2d_c(1-h_q(\frac{(1+q)}{2}\delta))}. \end{aligned}$$

□

Lemma 5. *Let* $0 < \delta < \frac{1}{1+q}$ *and* l_m *be as defined in Lemma 2. Then*

$$Pr(\Delta(C_{a,b}) \leq \delta) \leq \sum_{j=l_m}^{m-1} q^{-2sj(\frac{1}{2}-h_q(\frac{(1+q)}{2}\delta)-\frac{\log_q m}{2l_m})}.$$

Proof. Let $Y = \sum_{c(x)\in J_m} Y_c$. Then $Y_0 = 0$ and $N_{C_{a,b}}(\delta) = \sum_{c(x)\in J_m} Y_c = Y$. Now $Y = 0$ if and only if $Y_c = 0$ for any $c(x) \in J_m$, if and only if $wt(c(x)a(x), uc(x)b(x)) > q(1+q)m\delta$ for all $c(x) \in J_m \setminus \{0\}$. But we have this if and only if $\Delta(C_{a,b}) > \frac{q(1+q)m\delta}{(q+q^2)m} = \delta$. Hence $Pr(\Delta(C_{a,b}) \leq$

$\delta) = Pr(Y > 0)$. By Markov's inequality in [17, Theorem 3.1], we have $Pr(Y > 0) \leq E(Y)$. Now we obtain the expectation $E(Y) = \sum_{c(x)\in J_m} E(Y_c)$.
For any ideal I of J_m, we denote $I^* = \{c(x) \in I \mid I_c = I\}$ and $\dim_{\mathbb{F}_q} I = \dim_{\mathbb{F}_p} I_c$. Then

$$J_m = \bigcup_{0\neq I\leq J_m} I^*,$$

where the subscript $0 \neq I \leq J_m$ means that I runs over the non-zero ideals contained in J_m. Also, by Lemma 2, $l_m \leq \dim_S(I) \leq m-1$. Hence,

$$E(Y) = E(\sum_{c(x)\in J_m} Y_c) = \sum_{0\neq I\leq J_m} \sum_{c(x)\in I^*} E(Y_c) = \sum_{j=l_m}^{m-1} \sum_{I\leq J_m, \dim_S(I)=j} \sum_{c(x)\in I^*} E(Y_c).$$

For $I \leq J_m$ with $\dim_S I = j$, $|I^*| \leq |I| = q^{2j}$. By Lemma 4, we have

$$\begin{aligned} \sum_{c(x)\in I^*} E(Y_c) &\leq \sum_{c(x)\in I^*} q^{-4j(1-h_q(\frac{1+q}{2}\delta))} \\ &\leq q^{2j} \cdot q^{-4j(1-h_q(\frac{1+q}{2}\delta))} = q^{-2j+4jh_q(\frac{1+q}{2}\delta))}. \end{aligned}$$

By Lemma 2, $|\{I \leq J_m : \dim_S(I) = j\}| = m^{\frac{j}{l_m}} \leq m^{\frac{2j}{l_m}}$. Also $\log_q m \leq \frac{2j\log_q m}{l_m}$. Now we have the result by the following

$$\begin{aligned} E(Y) &\leq \sum_{j=l_m}^{m-1} m^{\frac{sj}{l_m}} \cdot q^{-2j+4jh_q(\frac{1+q}{2}\delta))} \\ &= \sum_{j=l_m}^{m-1} q^{-2j+4jh_q(\frac{1+q}{2}\delta)+\frac{2j}{l_m}\log_q m} \\ &= \sum_{j=l_m}^{m-1} q^{-4j(\frac{1}{2}-h_q(\frac{1+q}{2}\delta)-\frac{\log_q m}{2l_m})}. \end{aligned}$$

□

Example 2. Let $S = \mathbb{F}_2[u]/\langle u^2\rangle = \mathbb{F}_2 + u\mathbb{F}_2$ and $R = \mathbb{F}_2[u]/\langle u^3\rangle = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$. Consider random SR-additive cyclic codes over $S_3 \times R_3$. So we have the probability space $J_3 \times J_3$ and hence we have $|J_3 \times J_3| = 2^8$ random codes for $m = 3$. For a random code C, $\triangle(C) = \frac{wt(C)}{(q+q^2)m} = \frac{wt(C)}{18}$. If $\delta = \frac{1}{24}$, then $\triangle(C) \leq \delta$ if and only if $\frac{wt(C)}{18} \leq \frac{1}{24}$, and we have this equality if and only if $wt(C) \leq \frac{18}{24} = \frac{3}{4}$. But $C = \{\mathbf{0}\}$ is the only code with $wt(C) \leq \frac{3}{4}$. So $Pr(\Delta(C_{a,b}) \leq \delta) = \frac{1}{|J_3\times J_3|} = \frac{1}{2^8} = 0.00390625$.
On other hand, we have that $x^3 - 1 = (x+1)(x^2+x+1)$ over $\mathbb{F}_2$ which shows that $l_3 = 2$. Hence,

$$\sum_{j=l_m}^{m-1} q^{-4j(\frac{1}{2}-h_q(\frac{(1+q)}{2}\delta)-\frac{\log_q m}{2l_m})} = 2^{-8(\frac{1}{2}-h_q(\frac{(1+q)}{2}\delta)-\frac{\log_q m}{2l_m})}$$

$$\begin{aligned} &= 2^{-8(\frac{1}{2}-h_q(\frac{1}{16})-\frac{\log_2 3}{4})} \\ &= 2^{-8(-0.2335306918)} \\ &= 2^{1.8682455344} \\ &= 3.650883250516. \end{aligned}$$

Therefore, the following inequality holds for random codes when $m = 3$ and $\delta = \frac{1}{24}$

$$Pr(\Delta(C_{a,b}) \leq \delta) \leq \sum_{j=l_m}^{m-1} q^{-4j(\frac{1}{2}-h_q(\frac{(1+q)}{2}\delta)-\frac{\log_q m}{2l_m})}.$$

By Lemma 2.6 of [3], there exist positive integers $m_1, m_2, \ldots$ satisfying that

$$m_i \to \infty, \text{and } \lim_{i\to\infty} \frac{\log_q m_i}{l_{m_i}} = 0, \tag{3}$$

where l_{m_i} is the minimal degree of the irreducible divisors of $\frac{x^{m_i}-1}{x-1}$ as defined in Lemma 2.

Example 3. Let p be a prime number and $\frac{x^p-1}{x-1} = f_1 f_2 \cdots f_t$ be a monic basic irreducible decomposition of $\frac{x^p-1}{x-1}$ in $S[x]$. Also, let l_p be the minimal degree of the irreducible divisors of $\frac{x^p-1}{x-1}$. If $\mu : S[x] \longrightarrow \mathbb{F}_q[x]$ is the natural projection of $S[x]$ on to $\mathbb{F}_q[x]$, then $\mu(f_1)\mu(f_2)\cdots\mu(f_t) = \frac{x^p-1}{x-1} \in \mathbb{F}_q[x]$ is an irreducible decomposition of $\frac{x^p-1}{x-1}$ in $\mathbb{F}_q[x]$. By Theorem 2.47 in [11], we have that $l_p = \min\{d : \ q^d - 1 = kp \text{ for some } \ k\}$.

Define $P_q = \{p : \quad p \text{ is a prime}, \quad q^d - 1 \neq kp \text{ for all } \ 0 < d < \log_q(p)\log_q\log_q(p)\}$. By the proof of Lemma 2.6 in [3], P_q is an infinite set of prime numbers. Now, suppose that $m_i \in P_q$, then

$$\lim_{i\to\infty} \frac{\log_q m_i}{l_{m_i}} \leq \lim_{i\to\infty} \frac{\log_q m_i}{\log_q(m_i)\log_q\log_q(m_i)} = 0.$$

So P_q introduce positive integers $m_1, m_2, \ldots$ satisfying (3). It is easy to see that

$$P_2 = \{3, 5, 11, 13, 19, 23, 29, 37, ...\}$$

which contains almost all prime numbers.

For each m_i, let

$$C_{a,b}^{(i)} = \{(c(x)a(x), uc(x)b(x)) \in S_{m_i} \times uR_{m_i} \mid c(x) \in J_{m_i}\}$$

be the random SR-additive cyclic code with cyclic m_i over the probability space $J_{m_i} \times uJ'_{m_i}$.

Theorem 2. *If* $\alpha_q(\frac{1+q}{2}\delta) \geq \frac{1}{2}$ *for* $0 < \delta < \frac{1}{1+q}$, *then*

$$\lim_{i\to\infty} Pr(\Delta(C_{a,b}^{(i)}) > \delta) = 1.$$

Proof. If $1-h_q(\frac{1+q}{2}\delta)=\alpha_q(\frac{1+q}{2}\delta)>\frac{1}{2}$, then $\frac{1}{2}-h_q(\frac{1+q}{2}\delta)>0$. By Eq(3), there exists a positive real number β and an integer n such that

$$s(\frac{1}{2}-h_q(\frac{1+q}{2}\delta)-\frac{\log_q m_i}{2l_{m_i}})\geq\beta, \text{for all } i>n.$$

By Lemma 5,

$$\begin{aligned}\lim_{i\to\infty} Pr(\Delta(C^{(i)}_{a,b}) &\leq \delta) \leq \lim_{i\to\infty}\sum_{j=l_{m_i}}^{m_i-1} q^{-2j\beta}\\ &\leq \lim_{i\to\infty}\sum_{j=l_{m_i}}^{m_i-1} q^{-2l_{m_i}\beta}\\ &\leq \lim_{i\to\infty} m_i q^{-2l_{m_i}\beta}=\lim_{i\to\infty} q^{-2l_{m_i}(\beta-\frac{\log_q m_i}{2l_{m_i}})}.\end{aligned}$$

Since $\lim_{i\to\infty}\frac{\log_q m_i}{2l_{m_i}}=0$ (which implies that $\lim_{i\to\infty} l_{m_i}=\infty$), we have that

$$\lim_{i\to\infty} Pr(\Delta(C^{(i)}_{a,b})\leq\delta)=0.$$

Therefore,

$$\lim_{i\to\infty} Pr(\Delta(C^{(i)}_{a,b})>\delta)=1-\lim_{i\to\infty} Pr(\Delta(C^{(i)}_{a,b})\leq\delta)=1.$$

□

Theorem 3. *let $m_1, m_2, \ldots$ be positive integers satisfying Eq(3), and $C^{(i)}_{a,b}$ be as defined above. Then*

$$\lim_{i\to\infty} Pr(\dim_S C^{(i)}_{a,b}=m_i-1)=1.$$

Proof. Let $\frac{x^{m_i}-1}{x-1}=f_{i1}(x)f_{i2}(x)\cdots f_{it}(x)$ be an irreducible decomposition in $S[X]$. Then

$$J_{m_i}=\langle x-1\rangle_{S_{m_i}}\cong S[X]/\langle f_{i1}(x)\rangle\times\cdots\times S[X]/\langle f_{it}(x)\rangle,$$

which implies that there exists a surjective homomorphism

$$\begin{aligned}\varphi^{(j)}_{m_i}: J_{m_i} &\to S[X]/\langle f_{ij}(x)\rangle\\ c(x) &\to c(x)\ (\mathrm{mod} f_{ij}(x))\end{aligned}$$

for $j=1,2,\ldots,t_i$. By the Chinese Remainder Theorem, we have the following isomorphism:

$$\begin{aligned}\varphi_{m_i}: J_{m_i} &\to S[X]/\langle f_{i1}(x)\rangle\times\cdots\times S[X]/\langle f_{it}(x)\rangle\\ c(x) &\to (\varphi^{(1)}_{m_i}(c(x)),\ldots,\varphi^{(t)}_{m_i}(c(x))).\end{aligned}$$

By Lemma 1, $\dim_S C^{(i)}_{a,b}=m_i-1$ if and only if

$$(\varphi^{(j)}_{m_i}(a(x)),\varphi^{(j)}_{m_i}(b(x)))\neq(0,0)$$

in $S[X]/\langle f_{ij}(x)\rangle \times S[X]/\langle f_{ij}(x)\rangle$ for $1 \leq j \leq t_i$. Let $\deg f_{ij}(x) = d_{ij}$ and $q = p^s$. Then $\mid S[X]/\langle f_{ij}(x)\rangle \mid = q^{d_{ij}}$. Therefore, the probability of $(\varphi_{m_i}^{(j)}(a(x)), \varphi_{m_i}^{(j)}(b(x))) \neq (0,0)$ is $\frac{q^{2d_{ij}}-1}{q^{2d_{ij}}} = 1 - q^{-2d_{ij}}$. Hence,

$$Pr(\dim C_{a,b}^{(i)} = m_i - 1) = \prod_{j=1}^{t}(1 - q^{-2d_{ij}}).$$

Since $d_{ij} \geq l_{m_i}$ for $j = 1, 2, \ldots, t_i$, we have that $t \leq \frac{m_i-1}{l_{m_i}} \leq \frac{m_i}{l_{m_i}}$. Thus,

$$\begin{aligned} Pr(\dim_S C_{a,b}^{(i)} = m_i - 1) &\geq (1 - q^{-2l_{m_i}})^{\frac{m_i}{l_{m_i}}} \\ &= (1 - q^{-2l_{m_i}})^{q^{2l_{m_i}} \cdot \frac{m_i}{l_{m_i} q^{2l_{m_i}}}}. \end{aligned}$$

But

$$(1 - q^{-2l_{m_i}})^{q^{2l_{m_i}}} > \frac{1}{4},$$

and

$$\lim_{i\to\infty} \frac{m_i}{l_{m_i} q^{2l_{m_i}}} = \lim_{i\to\infty} q^{-l_{m_i}(2 - \frac{\log_q m_i}{l_{m_i}} + \frac{\log_q l_{m_i}}{l_{m_i}})} = 0.$$

Hence,

$$\lim_{i\to\infty} Pr(\dim_S C_{a,b}^{(i)} = m_i - 1) \geq \lim_{i\to\infty} (\frac{1}{4})^{\frac{m_i}{l_{m_i} q^{2l_{m_i}}}} = 1.$$

□

Example 4. Let $S = \mathbb{F}_2[u]/\langle u^2\rangle = \mathbb{F}_2 + u\mathbb{F}_2$ and $R = \mathbb{F}_2[u]/\langle u^3\rangle = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$. Let $\mu : S[x] \longrightarrow \mathbb{F}_2[x]$ be the natural projection of $S[x]$ on to $\mathbb{F}_2[x]$. If $\frac{x^{m_i}-1}{x-1} = f_{i1} f_{i2} \cdots f_{it}$ be a monic basic irreducible decomposition of $\frac{x^{m_i}-1}{x-1}$ in $S[x]$ with $\deg(f_{ij}) = d_{ij}$, then $Pr(\dim_S C_{a,b}^{(i)} = m_i - 1) = \prod_{j=1}^{t}(1 - 4^{-2d_{ij}})$. But $\mu(f_{i1})\mu(f_{i2}) \cdots \mu(f_{it}) = \frac{x^{m_i}-1}{x-1}$ is the irreducible decomposition of $\frac{x^{m_i}-1}{x-1}$ in $\mathbb{F}_2[x]$ where $\deg(f_{ij}) = \deg \mu(f_{it})$. So for calculate $Pr(\dim_S C_{a,b}^{(i)} = m_i - 1)$ it suffices to have irreducible decomposition of $\frac{x^{m_i}-1}{x-1}$ in $\mathbb{F}_2[x]$.

Now consider random SR-additive cyclic codes of length m_i where

$$m_i \in P_2 = \{3, 5, 11, 13, 19, 23, 29, \ldots\}.$$

Then we have the following factorizations for $x^{m_i} - 1$ in $\mathbb{F}_2[x]$.

$$\begin{aligned} x^3 - 1 &= (x+1)(x^2 + x + 1) \\ x^5 - 1 &= (x+1)(x^4 + x^3 + x^2 + x + 1) \\ x^{11} - 1 &= (x+1)(x^{10} + x^9 + \cdots + x^2 + x + 1) \\ x^{13} - 1 &= (x+1)(x^{12} + x^{11} + \cdots + x^2 + x + 1) \\ x^{19} - 1 &= (x+1)(x^{18} + x^{17} + \cdots + x^2 + x + 1) \\ x^{23} - 1 &= (x+1)(x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1)(x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1) \\ x^{29} - 1 &= (x+1)(x^{28} + x^{27} + \cdots + x^2 + x + 1) \end{aligned}$$

$$\vdots \;=\; \vdots$$

Therefore, we have the following sequence for $Pr(\dim_S C^{(i)}_{a,b} = m_i - 1)$ with respect to m_i : $3, 5, 11, 13, \ldots \in P_2$

$$Pr(\dim_S C^{(i)}_{a,b} = m_i - 1) : \; 0.99609375,\; 0.9999847412109,\; 0.9999999999991, \ldots.$$

It can be seen that $\lim_{i\to\infty} Pr(\dim C^{(i)}_{a,b} = m_i - 1) = 1$.

By Theorems 2 and 3. we have the following result.

Corollary 2. *Let δ be a real number with $\alpha_q(\frac{1+q}{2}\delta) > \frac{1}{2}$ for $0 < \delta < \frac{1}{1+q}$. Then there is a sequence of $SR-$additive cyclic codes $C_1, C_2, \ldots$ with cyclic length $m_i \to \infty$ such that*

i) $\lim_{i\to\infty} R(C_i) = \frac{2}{q+q^2}$,

ii) $\Delta(C_i) \geq \delta$ *for all* $i = 1, 2, \ldots$.

Proof. i) Assume that $C_i = C^{(i)}_{a,b}$. By the definition of the rate of C_i,

$$R(C_i) = \frac{\dim_{\mathbb{F}_q} C_i}{(q+q^2)m_i} = \frac{2(m_i - 1)}{(q+q^2)m_i}.$$

Then

$$\lim_{i\to\infty} R(C_i) = \lim_{i\to\infty} \frac{s(m_i - 1)}{(q+q^2)m_i} = \frac{2}{q+q^2}.$$

ii) From Theorem 2, there exists an SR-additive cyclic code C_i with cyclic length m_i such that $\Delta(C_i) > \delta$ for $i > n$. Delete the first n codes and renumber the remaining codes, the proof is completed.

□

5 Conclusion

In this paper, we construct a class of $\mathbb{F}_q[u]/\langle u^2\rangle \times \mathbb{F}_q[u]/\langle u^3\rangle$-additive cyclic codes, which are generated by pairs of polynomials.We presented new Gray maps and obtained a new weight function. By using a probabilistic method, we studied the asymptotic properties of the rates and relative distances of this class of codes and present some examples. Consequently, we proved that $\mathbb{F}_q[u]/\langle u^2\rangle \times \mathbb{F}_q[u]/\langle u^3\rangle$-additive cyclic codes are asymptotically good with $\alpha_q(\frac{1+q}{2}\delta) > \frac{1}{2}$, $0 < \delta < \frac{1}{1+q}$.

Acknowledgments

The authors would like to thank referees for providing us helpful and constructive comments and suggestions.

References

[1] T. Abualrub and I. Siap, *cyclic codes over the rings* $\mathbb{Z}_2 + u\mathbb{Z}_2$ *and* $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$, Designs, Codes and Cryptography, **42**, (2007), 273–287.

[2] I. Aydogdu, *Codes over* $\frac{\mathbb{Z}_p[u]}{\langle u^r\rangle} \times \frac{\mathbb{Z}_p[u]}{\langle u^s\rangle}$, J. Algebra Comb. Discrete Appl., **32** (2019), 39–51.

[3] L. M. J. Bazzi and S. K. Mitter, *Some randomized code constructions from group actions*, IEEE Trans. Inform. Theory, **52** (2006), 3210-3219.

[4] V. V. Chepyzhov, *New lower bounds for minimum distance of linear quasi-cyclic and almost linear cyclic codes*, Problemy Peredachi Inform., **28** (1992), 39-51.

[5] I. Constantinescu and W. Heise, A metric for codes over residue class rings, Probl. Peredachi Inform, **33** (1997), 22-28.

[6] Y. Fan and H. liu, $\mathbb{Z}_2\mathbb{Z}_4$*-additive cyclic codes are asymptotically good*, (2019), arxiv:1911.09350.

[7] Y. Fan and H. Liu, *Double circulantmatrices*, Linear and Multil. Algebra, **66**, (2018), 2119-2137.

[8] J. Gao and X. Hou, $\mathbb{Z}_4$*-double cyclic codes are asymptotically good*, IEEE Communications Letters, **24** (2020), 1593-1597.

[9] X. Hou and J. Gao, $\mathbb{Z}_p\mathbb{Z}_p[v]$*-additive cyclic codes are asymptotically good*, J.Appl. Math.comput., **66** (2021), 871-884.

[10] W. C. Huffman and V. Pless, *Fundamentals of Error Correcting Codes*, Cambridge University Press, (2003).

[11] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, 1997.

[12] S. Mahmoudi and K. Samei, *SR-additive codes*, Bulletin of the Korean Mathematical Society, **56** (2019), 1235–1255.

[13] M. Shi, R. Wu and P. Sol, *Asymptotically good additive cyclic codes exist*, IEEE Commun. Lett., **22** (2018), 1980-1983.

[14] M. Shi, R. Wu, L. Qian, L. Sok and P. Sole, *New classes of* $p-$*ary few weight codes*, Bull. Malays. Math. Sci. Soc., **42** (2019), 1393-1412.

[15] M. J. Shi, D. T. Huang, L. Sok, et al, *Double circulant LCD codes over* $\mathbb{Z}_4$, Finite Fields Appl., **58** (2019), 133-144.

[16] M. J. Shi, L. Q. Qian and P. Sole, *On self-dual negacirculant codes of index two and four*, Desings, Codes and Cryptography, **86** (2018), 2485-2494.

[17] R. R. Varshamov, *Estimate of the number of signals in error-correcting codes*, (in Russian), Dokl. Acad. Nauk, **117** (1957), 739-741.

[18] T. Yao, S. Zhu and X. Kai, *Asymptotically good $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes*, Finite Fields Appl., **63** (2020), 101633, 15 pp.

[19] T. Yao, H. Xu, Y. Tang and S. Zhu, *Asymptotically good $\mathbb{Z}_p\mathbb{Z}_p[u]/\langle u^t\rangle$-additive cyclic codes*, Advances in Mathematics of Communications., **17** (2023), 1290–1301.