



Article ID 1007-1202(2025)03-0289-13 DOI <https://doi.org/10.1051/wujns/2025303289>

Cite this article: GUO Ye, LIU Xiusheng. Construction of Constant Rank and Orbit Codes over Finite Chain Rings[J]. *Wuhan Univ J of Nat Sci*, 2025, 30(3): 289-301.

Construction of Constant Rank and Orbit Codes over Finite Chain Rings

□ GUO Ye, LIU Xiusheng[†]

Department of Science and Technology, College of Arts and Science of Hubei Normal University, Huangshi 435109, Hubei, China

Abstract: In this paper, we first generalize the constant dimension and orbit codes over finite fields to the constant rank and orbit codes over finite chain rings. Then we provide a relationship between constant rank codes over finite chain rings and constant dimension codes over the residue fields. In particular, we prove that an orbit submodule code over a finite chain ring is a constant rank code. Finally, for special finite chain ring $\mathbb{F}_q + \gamma\mathbb{F}_q$, we define a Gray map Φ from $(\mathbb{F}_q + \gamma\mathbb{F}_q)^n$ to \mathbb{F}_q^{2n} , and by using cyclic codes over $\mathbb{F}_q + \gamma\mathbb{F}_q$, we obtain a method of constructing an optimum distance constant dimension code over \mathbb{F}_q .

Key words: finite chain ring; rank of linear codes; constant rank codes; orbit codes

CLC number: O236.2

0 Introduction

Random linear network coding, first introduced in Ref. [1], is a strong tool for effective data transmission over noisy and lossy networks. It was proved in Ref. [1] that the information rate of a network can be improved by using coding at the nodes of the network, instead of simply routing the received inputs. An algebraic approach to random network coding was provided by Koetter and Kschischang in Ref. [2]. They proposed transmitting information by means of the subspaces of finite fields \mathbb{F}_q^n and defined subspace codes as a class of codes well suited for error correction. In the case that all the codewords in a subspace code have the same dimension, the subspace code is said to be a constant dimension subspace code. The theory of constant

dimension subspace code has received a lot of attention in recent years (see Refs. [3-9]). As we know, the approach of constructing good constant dimension subspace codes is an interesting research field. In Ref. [9], Trautmann *et al* introduced the concept of orbit codes as subspace codes obtained from the action of subgroups of the general linear group $GL(n, q)$ on the set of subspaces of \mathbb{F}_q^n . When the acting group is cyclic, the code is called a cyclic orbit code. Because of the simplicity of their algebraic structure and the existence of efficient encoding/decoding algorithms, this family of codes has attracted great interest. Gluesing-Luerssen and Lehmann^[3] presented a detailed study of cyclic orbit codes based on the stabilizer subfield. Later, Gluesing-Luerssen *et al*^[4] investigated the structure of the distance distribution for cyclic orbit codes, which

Received date: 2024-11-03 © Wuhan University 2025

Foundation item: Supported by Research Funds of Hubei Province (D20144401, Q20174503)

Biography: GUO Ye, male, Master, Lecturer, research direction: algebraic coding. E-mail: 771088974@qq.com

[†] Corresponding author. E-mail: lxs6682@163.com

are subspace codes generated by the action of \mathbb{F}_q^n on an \mathbb{F}_q -subspace \mathcal{U} of \mathbb{F}_q^n . Ref. [10] gave a systematic construction of subspace codes using subspace polynomials. By using Ben-Sasson's idea, Chen *et al*^[6] also provided some constructions of cyclic subspace codes. Roth *et al*^[11] and Zhang *et al*^[12] generalized and improved their result, so that one can obtain larger codes for fixed parameters and increase the density of some possible parameters.

Linear codes over finite rings have played a very important role in the theory of error correcting codes and practice (see Refs. [13-19]). On the one hand, by means of linear codes over finite rings, one can obtain good linear codes over finite fields (see Refs. [20-22]). On the other hand, new quantum codes and entanglement-assisted quantum codes can be obtained from linear codes over finite rings (see Refs. [23-27]).

Inspired by these works, in this paper, we first generalize subspace codes over finite fields to submodule codes over finite chain rings, and generalize constant dimension codes over finite fields to constant rank codes over finite chain rings. Under suitable conditions, we give a characterization of the constant rank codes over finite chain rings. We give a sufficient condition for which an orbit submodule code over a finite chain ring is a constant rank code.

This paper is organized as follows. In Section 1, we recall the necessary background materials of linear codes over finite chain rings. In Section 2, we first generalize the constant dimension codes over finite fields to constant rank codes over finite chain rings. Then, we give a relationship between constant rank codes over finite chain rings and constant dimension codes over the residue fields. By means of this relationship, we obtain a method to construct constant rank codes over finite chain rings. In Section 3, we collect concepts of orbit codes over finite fields, which are generalized to the orbit submodule codes over finite chain rings. Then we study orbit submodule constant rank codes over finite chain rings. We give two new examples of the open problem proposed by Gluesing-Luerssen *et al* in Ref. [4] (see Examples 1 and 2). In Section 4, we define a Gray map Φ from $(\mathbb{F}_q + \gamma\mathbb{F}_q)^n$ to \mathbb{F}_q^{2n} , and we give a method for constructing an optimum distance constant dimension code over \mathbb{F}_q by using cyclic codes over $\mathbb{F}_q + \gamma\mathbb{F}_q$. Finally, a brief summary of this work is described in Section 5.

1 Linear Codes over Chain Rings

Throughout this paper \mathcal{R} will denote a finite chain ring. In this section, we recall some basic concepts and results of linear codes over \mathcal{R} , necessary for the development of this work. For more details, we refer to Refs. [16, 19, 28-30].

It is well known that \mathcal{R} has the unique maximal ideal, denoted by \mathbf{m} . Let γ be a generator of the unique maximal ideal \mathbf{m} , i.e., $\mathbf{m} = \langle \gamma \rangle$. Its chain of ideals is

$$\mathcal{R} = \langle \gamma^0 \rangle \supset \langle \gamma^1 \rangle \supset \dots \supset \langle \gamma^{t-1} \rangle \supset \langle \gamma^t \rangle = \{0\}.$$

The integer t is called the nilpotency index of \mathbf{m} . Let $\mathbb{F}_q = \mathcal{R}/\mathbf{m}$ be the residue field with characteristic p , where $q = p^s$ and p is a prime number. There is a natural homomorphism from \mathcal{R} onto $\mathbb{F}_q = \mathcal{R}/\mathbf{m}$, i.e.,

$$\bar{\cdot} : \mathcal{R} \rightarrow \mathbb{F}_q = \mathcal{R}/\mathbf{m}, r \mapsto r + \mathbf{m} = \bar{r}, \text{ for any } r \in \mathcal{R}.$$

This natural homomorphism from \mathcal{R} onto $\mathbb{F}_q = \mathcal{R}/\mathbf{m}$ can be extended naturally to a homomorphism from \mathcal{R}^n onto \mathbb{F}_q^n . For an element $c \in \mathcal{R}^n$, let \bar{c} be its image under this homomorphism.

Let \mathcal{R}^* denote the group of units of \mathcal{R} . \mathcal{R}^* is just the set of non-nilpotent elements of \mathcal{R} i.e., $\mathcal{R}^* = \mathcal{R} - \mathbf{m}$. The subgroup $1 + \mathbf{m}$ of \mathcal{R}^* is a p -group.

It is well known that the group of units \mathcal{R}^* of \mathcal{R} contains a unique cyclic subgroup T^* of order $q-1$. $T = T^* \cup \{0\}$ is called the Teichmüller set of \mathcal{R} and forms a system of coset representatives of $\mathbb{F}_q = \mathcal{R}/\mathbf{m}$. More precisely, \mathcal{R} contains a unit element ζ with multiplicative order $q-1$ such that $T = \{0, 1, \zeta, \zeta^2, \dots, \zeta^{q-2}\}$. We call ζ the generator of T . Since the set T modulo γ equals \mathbb{F}_q , we do not make distinction between T and \mathbb{F}_q . Every element $r \in \mathcal{R}$ can be written as $r = \sum_{i=0}^{t-1} r_i \gamma^i$, where $r_0, r_1, \dots, r_{t-1} \in T$ (see Refs. [7, 18]).

Lemma 1 Let notations be as above. We have $\mathcal{R}^* = T^* \cdot (1 + \mathbf{m}) \cong T^* \times (1 + \mathbf{m})$.

A nonempty subset $C \subseteq \mathcal{R}^n$ is called a linear code of length n over \mathcal{R} if it is an \mathcal{R} -submodule of \mathcal{R}^n . All codes are assumed to be linear. We say that a linear code C over \mathcal{R} is free if C is isomorphic as a module to \mathcal{R}^μ for some positive Integer μ , denoted by $C \cong \mathcal{R}^\mu$.

For two vectors $\mathbf{a} = (a_1, a_2, \dots, a_n)$ and $\mathbf{b} = (b_1, b_2, \dots, b_n)$ in \mathcal{R}^n , we define the Euclidean inner product as $[\mathbf{a}, \mathbf{b}]$ to be $[\mathbf{a}, \mathbf{b}] = \sum_{i=1}^n a_i b_i$.

Let C be a linear code over \mathcal{R}^n . We define the Euclidean dual code of C as

$$C^\perp = \{ \mathbf{a} \in \mathcal{R}^n \mid [\mathbf{a}, \mathbf{b}] = 0 \text{ for all } \mathbf{b} \in C \}.$$

The following lemma is well-known in Ref. [30].

Lemma 2 Let C be a linear code of length n over \mathcal{R} (or an \mathcal{R} -submodule of \mathcal{R}^n). Then

$$|C| |C^\perp| = |\mathcal{R}|^n.$$

One of the most important tools in coding theory is finding a generator matrix for a code. In general, we want not only a matrix that generates code by rows, but also a matrix that generates code by a minimum number of rows. To describe the generator matrix for a code over \mathcal{R} , we introduce the following two definitions and lemmas which come from Refs. [16, 28].

Definition 1 Let $\mathbf{w}_1, \dots, \mathbf{w}_k$ be nonzero vectors in \mathcal{R}^n . Then $\mathbf{w}_1, \dots, \mathbf{w}_k$ are \mathcal{R} -independent if $\sum_{j=1}^k \delta_j \mathbf{w}_j = \mathbf{0}$ implies that $\delta_j \mathbf{w}_j = \mathbf{0}$ for all j , where $\delta_j \in \mathcal{R}$.

Following Definition 1, we can easily get the following lemma.

Lemma 3 If the nonzero vectors $\mathbf{w}_1, \dots, \mathbf{w}_s$ in \mathcal{R}^n are \mathcal{R} -independent and $\sum_{j=1}^s \delta_j \mathbf{w}_j = \mathbf{0}$, then $\delta_j \in \langle \gamma \rangle$ for all j .

Let $\mathbf{w}_1, \dots, \mathbf{w}_s$ be vectors in \mathcal{R}^n . As usual, we denote the set of all linear combinations of $\mathbf{w}_1, \dots, \mathbf{w}_s$ by $\langle \mathbf{w}_1, \dots, \mathbf{w}_s \rangle$.

Lemma 4 If the nonzero vectors $\mathbf{w}_1, \dots, \mathbf{w}_s$ in \mathcal{R}^n are \mathcal{R} -independent, then none of the vectors $\mathbf{w}_1, \dots, \mathbf{w}_s$ is a linear combination of the other vectors.

With the help of the above definition and two lemmas, we give a definition of a generator matrix for a code over \mathcal{R} .

Definition 2 Let $C \neq \{0\}$ be a linear code over \mathcal{R} (or an \mathcal{R} -submodule of \mathcal{R}^n). The nonzero codewords $\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_k$ are called a basis of C if they are \mathcal{R} -independent and generate C . Let \mathbf{G}_C be a $k \times n$ matrix where $\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_k$ are rows of \mathbf{G}_C . Then \mathbf{G}_C is a generator matrix of C .

Definition 3 A parity-check matrix \mathbf{H}_D for a linear code D over \mathcal{R} is a generator matrix for the dual code D^\perp .

Let $\mathbf{M}_{m \times l}(\mathcal{R})$ be the set of all $m \times l$ matrices over \mathcal{R} . For $\mathbf{A} \in \mathbf{M}_{m \times l}(\mathcal{R})$, \mathbf{A}^T denotes the transpose of the matrix \mathbf{A} . We also let $\mathbf{0}$ denote the zero matrix, where the size will either be obvious from the context or specified whenever necessary. Similarly, we denote the $m \times m$ identity matrix by \mathbf{I}_m , or simply \mathbf{I} if the size is clear from the context.

Let $\mathbf{A} \in \mathbf{M}_{m \times l}(\mathcal{R})$, and let $\mathbf{A}^{\text{row}} \subset \mathcal{R}^l$ and $\mathbf{A}^{\text{col}} \subset \mathcal{R}^m$ be the submodules generated by the rows of \mathbf{A} and the col-

umns of \mathbf{A} , respectively. Now, we introduce the definition of the row-rank (or column-rank) of the matrix from Ref. [31].

Definition 4 The parameter $\log_{|\mathcal{R}|} |\mathbf{A}^{\text{row}}|$ is called the row-rank of the matrix \mathbf{A} and denoted by $\text{rk}_r(\mathbf{A})$, and similarly $\log_{|\mathcal{R}|} |\mathbf{A}^{\text{col}}|$ is called the column-rank of the matrix \mathbf{A} and denoted by $\text{rk}_c(\mathbf{A})$.

Obviously, when \mathcal{R} is a finite field, the above definition coincides with the usual rank of a matrix. We need the following two lemmas which can be found in Ref. [31].

Lemma 5 Let $\mathbf{A} \in \mathbf{M}_{m \times l}(\mathcal{R})$. Then $\text{rk}_r(\mathbf{A}) = \text{rk}_c(\mathbf{A})$.

In \mathcal{R} , we define $\text{rk}_r(\mathbf{A})$ or $\text{rk}_c(\mathbf{A})$ as the rank of the matrix \mathbf{A} , denoted by $\text{rk}(\mathbf{A})$. The following two concepts and a result about matrices over finite chain rings appear in Ref. [32].

Let $\mathbf{A} = (a_{ij}) \in \mathbf{M}_{m \times m}(\mathcal{R})$. If there is an $m \times m$ matrix \mathbf{B} over \mathcal{R} such that $\mathbf{AB} = \mathbf{BA} = \mathbf{I}$, then \mathbf{A} is invertible and \mathbf{B} is an inverse of \mathbf{A} . If the determinant $\det(\mathbf{A})$ is a unit of \mathcal{R} , then \mathbf{A} is non-singular.

Lemma 6 Let \mathbf{A} be an $m \times m$ matrix over \mathcal{R} . The following statements are equivalent: (1) \mathbf{A} is invertible; (2) \mathbf{A} is non-singular; (3) $\text{rk}(\mathbf{A}) = m$.

Lemma 7 Let $\mathbf{A} \in \mathbf{M}_{m \times l}(\mathcal{R})$ and $\mathbf{B} \in \mathbf{M}_{l \times s}(\mathcal{R})$. Then $\text{rk}(\mathbf{AB}) \leq \min \{ \text{rk}(\mathbf{A}), \text{rk}(\mathbf{B}) \}$.

Corollary 1 Let $\mathbf{A} \in \mathbf{M}_{m \times l}(\mathcal{R})$. If $\mathbf{P} \in \mathbf{M}_{m \times m}$ and $\mathbf{Q} \in \mathbf{M}_{l \times l}$ are non-singular, then $\text{rk}(\mathbf{A}) = \text{rk}(\mathbf{PA}) = \text{rk}(\mathbf{AQ}) = \text{rk}(\mathbf{PAQ})$.

Proof Let $\mathbf{B} = \mathbf{PA}$. Then, by Lemma 7, we have $\text{rk}(\mathbf{B}) = \text{rk}(\mathbf{PA}) \leq \text{rk}(\mathbf{A})$. On the other hand, considering the matrix \mathbf{P} is non-singular, we obtain $\mathbf{A} = \mathbf{P}^{-1}\mathbf{B}$. Again by Lemma 7, we have $\text{rk}(\mathbf{A}) = \text{rk}(\mathbf{P}^{-1}\mathbf{B}) \leq \text{rk}(\mathbf{B})$. Therefore, $\text{rk}(\mathbf{A}) = \text{rk}(\mathbf{PA})$.

Similarly, we can show that $\text{rk}(\mathbf{A}) = \text{rk}(\mathbf{AQ}) = \text{rk}(\mathbf{PAQ})$.

Definition 5 Let \mathbf{G} be a generator matrix of a linear code C over \mathcal{R} . Then the rank of the code C , denoted by $\text{rank}_{\mathcal{R}}(C)$, is defined as $\text{rank}_{\mathcal{R}}(C) = \text{rk}(\mathbf{G})$.

Let C be a code of length n over \mathcal{R} . We define $\bar{C} = \{ \bar{\mathbf{c}} \mid \mathbf{c} \in C \}$ and $(C:r) = \{ \mathbf{a} \in \mathcal{R}^n \mid r\mathbf{a} \in C \}$, where r is an element of \mathcal{R} . The following two definitions can be found in Ref. [22].

Definition 6 To any code C over \mathcal{R} , we associate the tower of codes $C = (C:\gamma^0) \subseteq (C:\gamma) \subseteq \dots \subseteq (C:\gamma^{t-1})$ over \mathcal{R} and its projection to \mathbb{F}_q ,

$$\bar{C} = (\bar{C}:\gamma^0) \subseteq (\bar{C}:\gamma) \subseteq \dots \subseteq (\bar{C}:\gamma^{t-1}).$$

Definition 7 Let C be a linear code over \mathcal{R} . A generator matrix \mathbf{G} for C is said to be in standard form if, after a suitable permutation of the coordinates, \mathbf{G} can be written as the following block matrix:

$$\mathbf{G} = \begin{pmatrix} \mathbf{I}_{k_0} & \mathbf{A}_{0,1} & \mathbf{A}_{0,2} & \mathbf{A}_{0,3} & \cdots & \mathbf{A}_{0,t-1} & \mathbf{A}_{0,t} \\ 0 & \gamma \mathbf{I}_{k_1} & \gamma \mathbf{A}_{1,2} & \gamma \mathbf{A}_{1,3} & \cdots & \gamma \mathbf{A}_{1,t-1} & \gamma \mathbf{A}_{1,t} \\ 0 & 0 & \gamma^2 \mathbf{I}_{k_2} & \gamma^2 \mathbf{A}_{2,3} & \cdots & \gamma^2 \mathbf{A}_{2,t-1} & \gamma^2 \mathbf{A}_{2,t} \\ \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \gamma^{t-1} \mathbf{I}_{k_{t-1}} & \gamma^{t-1} \mathbf{A}_{t-1,t} \end{pmatrix} = \begin{pmatrix} \mathbf{A}_0 \\ \gamma \mathbf{A}_1 \\ \vdots \\ \gamma^{t-1} \mathbf{A}_{t-1} \end{pmatrix}. \tag{1}$$

We associate the following matrix with \mathbf{G}

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}_0 \\ \mathbf{A}_1 \\ \vdots \\ \mathbf{A}_{t-1} \end{pmatrix}. \tag{2}$$

For any constant $r \in \mathcal{R}$ and any $\mathbf{c} \in \mathcal{R}^n$, we denote by $r\mathbf{c}$ the usual multiplication of a vector by a scalar. We say that a vector $\mathbf{c} \in \mathcal{R}^n$ is divisible by a constant $r \in \mathcal{R}$, and write as $r\mathbf{c}$, if there exists a vector $\mathbf{a} \in \mathcal{R}^n$ such that $\mathbf{c} = r\mathbf{a}$, i.e., all entries of \mathbf{c} are divisible by r .

Let C be a linear code over \mathcal{R} . For $i = 1, 2, \dots, t-1$, we denote by k_i the number of row vectors of \mathbf{G} that are divisible by γ^i but not by γ^{i+1} . A code with generator matrix of this form is said to have type $\{k_0, k_1, \dots, k_{t-1}\}$. It is immediate that the number of elements in a code C with this generator matrix is

$$|C| = |\mathcal{R}/\mathfrak{m}|^{\sum_{i=0}^{t-1} (t-i)k_i} = |\mathbb{F}_q|^{\sum_{i=0}^{t-1} (t-i)k_i}.$$

Thus, we have $\text{rank}_{\mathcal{R}}(C) = \frac{1}{t} \sum_{i=0}^{t-1} (t-i)k_i$. This means that the rank of a linear code over \mathcal{R} could be a fraction.

2 Constant Rank Codes over Chain Rings

In this section, we first generalize the constant dimension and orbit codes over finite fields to the constant rank and orbit codes over finite chain rings. Then, a method of constructing the constant rank code over \mathcal{R} is given.

In order to give the definition of the rank distance of a submodule code over finite chain rings, we need the following lemma.

Lemma 8 Let C and D be two linear codes of length n over \mathcal{R} . Then we have

$$\text{rank}_{\mathcal{R}}(C+D) = \text{rank}_{\mathcal{R}}(C) + \text{rank}_{\mathcal{R}}(D) - \text{rank}_{\mathcal{R}}(C \cap D).$$

Proof Let $\mathbf{u} \in C+D$. Then there are $\mathbf{a} \in C, \mathbf{b} \in D$ such that $\mathbf{u} = \mathbf{a} + \mathbf{b}$. Obviously, for any $\mathbf{w} \in C \cap D$, we have

$$\mathbf{u} = (\mathbf{a} + \mathbf{w}) + (\mathbf{b} - \mathbf{w}).$$

Thus, there are $|C \cap D|$ such expressions for \mathbf{u} . This means that $|C+D| = \frac{|C| \cdot |D|}{|C \cap D|}$. So,

$$\text{rank}_{\mathcal{R}}(C+D) = \log_{|\mathcal{R}|} |C+D| = \log_{|\mathcal{R}|} |C| + \log_{|\mathcal{R}|} |D| - \log_{|\mathcal{R}|} |C \cap D|,$$

i.e., $\text{rank}_{\mathcal{R}}(C+D) = \text{rank}_{\mathcal{R}}(C) + \text{rank}_{\mathcal{R}}(D) - \text{rank}_{\mathcal{R}}(C \cap D)$.

Definition 8 Let \mathcal{C} be a set of submodules (or linear codes) of length n over \mathcal{R} . Then \mathcal{C} is called a submodule code of length n over \mathcal{R} . The submodule code \mathcal{C} is called a constant rank code if all submodules have the same rank. If every submodule of \mathcal{C} has the same type $\{k_0, k_1, \dots, k_{t-1}\}$, then the submodule code \mathcal{C} is called a constant rank code of type $\{k_0, k_1, \dots, k_{t-1}\}$.

Definition 9 Let \mathcal{U} and \mathcal{V} be two submodules over \mathcal{R} . Then the rank distance is defined as

$$d_M(\mathcal{U}, \mathcal{V}) := \text{rank}_{\mathcal{R}}(\mathcal{U} + \mathcal{V}) - \text{rank}_{\mathcal{R}}(\mathcal{U} \cap \mathcal{V}).$$

The minimum rank distance of a submodule code \mathcal{C} is definite as

$$d_M(\mathcal{C}) := \min \{d_M(\mathcal{U}, \mathcal{V}) \mid \mathcal{U} \neq \mathcal{V}, \mathcal{U}, \mathcal{V} \in \mathcal{C}\}.$$

Remark 1 By Lemma 8, we have

$$d_M(\mathcal{U}, \mathcal{V}) = \text{rank}_{\mathcal{R}}(\mathcal{U}) + \text{rank}_{\mathcal{R}}(\mathcal{V}) - 2\text{rank}_{\mathcal{R}}(\mathcal{U} \cap \mathcal{V}) = 2\text{rank}_{\mathcal{R}}(\mathcal{U} + \mathcal{V}) - (\text{rank}_{\mathcal{R}}(\mathcal{U}) + \text{rank}_{\mathcal{R}}(\mathcal{V})).$$

As a consequence, suppose that \mathcal{C} is a constant rank code of rank k and length n , then its minimum submodule distance is even integer and it is upper bounded by

$$d_M(\mathcal{C}) \leq \begin{cases} 2k & \text{if } 2k \leq n, \\ 2(n-k) & \text{if } 2k \geq n. \end{cases}$$

This bound is attained by submodule code in which the intersection of every two different submodules has rank of $\max\{0, 2k-n\}$.

Remark 2 When $\mathcal{R} = \mathbb{F}_q$, the submodule code \mathcal{C} is a subspace code. In this case, the distance between two subspace is $d_M(\mathcal{U}, \mathcal{V}) = d_S(\mathcal{U}, \mathcal{V}) = \dim_{\mathbb{F}_q}(\mathcal{U}) + \dim_{\mathbb{F}_q}(\mathcal{V}) - 2\dim_{\mathbb{F}_q}(\mathcal{U} \cap \mathcal{V})$. This means that the distance of subspace code over \mathbb{F}_q is a special case of the rank distance of submodule code over \mathcal{R} .

Let \mathcal{C} be a constant rank code of rank k and length n over \mathcal{R} . If it attains bound $d_M(\mathcal{C}) = \min\{2k, 2(n-k)\}$, then \mathcal{C} is called an optimum distance constant rank code.

A code \mathcal{C} is called an $(n, |\mathcal{C}|, d; K)_q$ submodule code over \mathcal{R} if the ranks of the codewords of \mathcal{C} are contained in a set $K \subset \{0, 1, 2, \dots, n\}$. In the case $K = \{k\}$, i.e., \mathcal{C} is a constant rank code, we denote its parameters by $(n, |\mathcal{C}|, d; k)_q$, where q is the number of elements of the residue field \mathbb{F}_q . If all codewords do not have the same rank, then \mathcal{C} is called a mixed rank code. Such submodule code is denoted by $(n, |\mathcal{C}|, d)$. Constant rank codes are the most well-studied submodule codes, being the analogues of classical codes over finite rings.

Remark 3 When $\mathcal{R} = \mathbb{F}_q$, the submodule code \mathcal{C} is a subspace code. In this case, the distance between two subspace is $d_M(\mathcal{U}, \mathcal{V}) = d_S(\mathcal{U}, \mathcal{V})$. This means that the parameters of submodule codes over \mathcal{R} are generalizations of the parameters of subspace codes over \mathbb{F}_q .

In order to connect a constant rank code of rank k and length n over \mathcal{R} with a constant dimension code of dimension k and length n over \mathbb{F}_q , we need the following lemma, which can be found in Ref. [19].

Lemma 9 (Lemma 9 in Ref. [19]) Suppose that C is a linear code of length n over \mathcal{R} with a generator matrix G in standard form (1) and let A be as in (2). Then, for $0 \leq i \leq t-1$, $\overline{(C:\gamma^i)}$ has a generator matrix

$$\overline{G}_i = \begin{pmatrix} \overline{A_0} \\ \vdots \\ \overline{A_i} \end{pmatrix}.$$

In addition, $\dim_{\mathbb{F}} \overline{(C:\gamma^i)} = k_0 + k_1 + \dots + k_i$.

Lemma 10 Let C and D be two linear codes over \mathcal{R} . Then, for $i = 0, 1, \dots, t-1$, we have

$$\overline{(C \cap D:\gamma^i)} \subset \overline{(C:\gamma^i)} \cap \overline{(D:\gamma^i)}. \tag{3}$$

$$\overline{(C:\gamma^i)} + \overline{(D:\gamma^i)} \subset \overline{(C+D:\gamma^i)}. \tag{4}$$

Proof 1) We first prove that

$$\overline{(C \cap D:\gamma^i)} = \overline{(C:\gamma^i)} \cap \overline{(D:\gamma^i)}. \tag{5}$$

In fact, for any $\mathbf{a} \in \overline{(C \cap D:\gamma^i)}$, we have $\gamma^i \mathbf{a} \in C \cap D$. So, $\gamma^i \mathbf{a} \in C$ and $\gamma^i \mathbf{a} \in D$, which implies that $\mathbf{a} \in \overline{(C:\gamma^i)}$ and $\mathbf{a} \in \overline{(D:\gamma^i)}$. Thus, $\mathbf{a} \in \overline{(C:\gamma^i)} \cap \overline{(D:\gamma^i)}$, i. e.,

$$\overline{(C \cap D:\gamma^i)} \subset \overline{(C:\gamma^i)} \cap \overline{(D:\gamma^i)}. \tag{6}$$

On the other hand, let $\mathbf{b} \in \overline{(C:\gamma^i)} \cap \overline{(D:\gamma^i)}$. Then $\gamma^i \mathbf{b} \in C$ and $\gamma^i \mathbf{b} \in D$. This means that $\gamma^i \mathbf{b} \in C \cap D$, i. e., $\mathbf{b} \in \overline{(C \cap D:\gamma^i)}$. Thus,

$$\overline{(C \cap D:\gamma^i)} \supset \overline{(C:\gamma^i)} \cap \overline{(D:\gamma^i)}. \tag{7}$$

Combining Eqs. (6) and (7), we have $\overline{(C \cap D:\gamma^i)} = \overline{(C:\gamma^i)} \cap \overline{(D:\gamma^i)}$. So, the Eq. (5) holds.

Next, let $\overline{\mathbf{u}} \in \overline{(C \cap D:\gamma^i)} = \overline{(C:\gamma^i)} \cap \overline{(D:\gamma^i)}$, where $\mathbf{u} \in \overline{(C:\gamma^i)} \cap \overline{(D:\gamma^i)}$. Then $\mathbf{u} \in \overline{(C:\gamma^i)}$ and $\mathbf{u} \in \overline{(D:\gamma^i)}$. Therefore, $\overline{\mathbf{u}} \in \overline{(C:\gamma^i)}$ and $\overline{\mathbf{u}} \in \overline{(D:\gamma^i)}$, which implies that $\overline{\mathbf{u}} \in \overline{(C:\gamma^i)} \cap \overline{(D:\gamma^i)}$. Thus, we complete the proof of Eq. (3).

2) For any $w \in \overline{(C:\gamma^i)} + \overline{(D:\gamma^i)}$, there are $u \in \overline{(C:\gamma^i)}$ and $v \in \overline{(D:\gamma^i)}$ such that $w = u + v$. Thus, we can find that $a \in (C:\gamma^i)$ and $b \in (D:\gamma^i)$ with $u = \bar{a}$ and $v = \bar{b}$. This means that $\gamma^i a \in C$ and $\gamma^i b \in D$. Therefore, $\gamma^i(a + b) \in C + D$, i.e., $a + b \in (C + D:\gamma^i)$. Hence, $\overline{a + b} \in \overline{(C + D:\gamma^i)}$. Since $\bar{}$ is a homomorphism from \mathcal{R}^n onto \mathbb{F}_q^n , we have $w = u + v = \bar{a} + \bar{b} = \overline{a + b} \in \overline{(C + D:\gamma^i)}$. This prove that $\overline{(C:\gamma^i)} + \overline{(D:\gamma^i)} \subset \overline{(C + D:\gamma^i)}$, i.e., we complete the proof of Eq. (4).

Let \mathcal{C} be submodule code of length n over \mathcal{R} . In the following, we denote by $\overline{(C:\gamma^{t-1})}$ the set $\{\overline{(U:\gamma^{t-1})} | U \in \mathcal{C}\}$.

Combining Lemmas 9 and 10, we give the following theorem.

Theorem 1 Let \mathcal{C} be a submodule code of length n over \mathcal{R} with type $\{k_0, k_1, \dots, k_{t-1}\}$ and the minimum rank distance $d_M(\mathcal{C})$. Then

1) $\overline{(C:\gamma^{t-1})}$ is a constant dimension code over \mathbb{F}_q of dimension $l = k_0 + k_1 + \dots + k_{t-1}$ and length n . In addition, $d_s(\overline{(C:\gamma^{t-1})}) \leq d_M(\mathcal{C})$.

2) In particular, write $k = \frac{1}{t} \sum_{i=0}^{t-1} (t-i)k_i$. If $2k \leq n$ and \mathcal{C} is an optimum distance constant rank code, then $\overline{(C:\gamma^{t-1})}$ is also an optimum distance constant dimension code with the minimum distance $2l$.

Proof 1) By assumptions, for any $U, V \in \mathcal{C}$, we have $\text{rank}_{\mathcal{R}}(U) = \text{rank}_{\mathcal{R}}(V) = \frac{1}{t} \sum_{i=0}^{t-1} (t-i)k_i$.

According to Lemma 9, for any $\overline{(U:\gamma^{t-1})}, \overline{(V:\gamma^{t-1})} \in \overline{(C:\gamma^{t-1})}$, we obtain $\dim_{\mathbb{F}_q} \overline{(U:\gamma^{t-1})} = \dim_{\mathbb{F}_q} \overline{(V:\gamma^{t-1})} = \sum_{i=0}^{t-1} k_i$.

Thus, $\overline{(C:\gamma^{t-1})}$ is a constant dimension code over \mathbb{F}_q of dimension $k_0 + k_1 + \dots + k_{t-1}$ and length n .

On the other hand, by Lemmas 9 and 10, for any $U, V \in \mathcal{C}$, we obtain

$$\begin{aligned} d_M(U, V) &= \text{rank}_{\mathcal{R}}(U) + \text{rank}_{\mathcal{R}}(V) - 2\text{rank}_{\mathcal{R}}(U \cap V) = \dim_{\mathbb{F}_q} \overline{(U:\gamma^{t-1})} + \dim_{\mathbb{F}_q} \overline{(V:\gamma^{t-1})} - 2\dim_{\mathbb{F}_q} \overline{(U \cap V:\gamma^{t-1})} \\ &\geq \dim_{\mathbb{F}_q} \overline{(U:\gamma^{t-1})} + \dim_{\mathbb{F}_q} \overline{(V:\gamma^{t-1})} - 2\dim_{\mathbb{F}_q} (\overline{(U:\gamma^{t-1})} \cap \overline{(V:\gamma^{t-1})}) = d_s(\overline{(U:\gamma^{t-1})}, \overline{(V:\gamma^{t-1})}) \end{aligned}$$

This gives that $d_s(\overline{(C:\gamma^{t-1})}) \leq d_M(\mathcal{C})$.

2) In particular, if $2k \leq n$ and \mathcal{C} is an optimum distance constant rank code, for any $U, V \in \mathcal{C}$, we have $U \cap V = \{0\}$.

Let $\overline{(U:\gamma^{t-1})}$ and $\overline{(V:\gamma^{t-1})}$ be any two different elements of $\overline{(C:\gamma^{t-1})}$. We prove that $\overline{(U:\gamma^{t-1})} \cap \overline{(V:\gamma^{t-1})} = \{0\}$ by contradiction as follows.

Otherwise, there exists $0 \neq a \in \mathbb{F}_q^n$ such that $a \in \overline{(U:\gamma^{t-1})} \cap \overline{(V:\gamma^{t-1})}$. Hence, we can find that $b \in (U:\gamma^{t-1})$ and $c \in (V:\gamma^{t-1})$ satisfy $a = \bar{b} = \bar{c}$.

We assume that $b = b_0 + b_1\gamma + \dots + b_{t-1}\gamma^{t-1}$ and $c = c_0 + c_1\gamma + \dots + c_{t-1}\gamma^{t-1}$ with $b_0, b_1, \dots, b_{t-1}, c_0, c_1, \dots, c_{t-1} \in T^n$, where T is the Teichmüller set of \mathcal{R} . Then, by $\gamma^{t-1}b \in U$ and $\gamma^{t-1}c \in V$, we have $\gamma^{t-1}b_0 \in U$ and $\gamma^{t-1}c_0 \in V$. Thus, we obtain $\gamma^{t-1}a = \gamma^{t-1}\bar{b} = \gamma^{t-1}b_0 \in U$, and $\gamma^{t-1}a = \gamma^{t-1}\bar{c} = \gamma^{t-1}c_0 \in V$. This gives that $\gamma^{t-1}a \in U \cap V$. Obviously, $\gamma^{t-1}a \neq 0$. This is a contradiction. Thus, for any $\overline{(U:\gamma^{t-1})}, \overline{(V:\gamma^{t-1})} \in \overline{(C:\gamma^{t-1})}$, we have $d_s(\overline{(U:\gamma^{t-1})}, \overline{(V:\gamma^{t-1})}) = 2(k_0 + k_1 + \dots + k_{t-1}) = 2l$, which implies that $\overline{(C:\gamma^{t-1})}$ is an optimum distance constant dimension code with the minimum distance $2l$.

A linear code C over \mathcal{R} of length n is said to be cyclic if the following holds:

$$(c_0, c_1, \dots, c_{n-1}) \in C \Rightarrow (c_{n-1}, c_0, \dots, c_{n-2}) \in C.$$

It is well-known that a cyclic code of length n over \mathcal{R} can be identified with an ideal in the residue ring $\frac{\mathcal{R}[x]}{\langle x^n - 1 \rangle}$

via the \mathcal{R} -module isomorphism $\varphi: \mathcal{R}^n \rightarrow \frac{\mathcal{R}[x]}{\langle x^n - 1 \rangle}$ given by $(a_0, a_1, \dots, a_{n-1}) \mapsto a_0 + a_1x + \dots + a_{n-1}x^{n-1} \pmod{(x^n - 1)}$.

Customarily, for a polynomial $f(x) = \sum_{i=0}^l a_i x^i$ of degree l ($a_l \neq 0$ and a_0 is a unit) over \mathcal{R} , its monic reciprocal polynomial $a_0^{-1} x^l f\left(\frac{1}{x}\right)$ is denoted by $f^*(x)$, i.e.,

$$f^*(x) = a_0^{-1} x^t f\left(\frac{1}{x}\right) = a_0^{-1} \sum_{i=0}^t a_i x^{t-i}.$$

A polynomial $f(x)$ is self-reciprocal, if $f(x) = f^*(x)$.

The homomorphism from \mathcal{R} to \mathbb{F}_q extends naturally to a homomorphism $\mathcal{R}[x] \rightarrow \mathbb{F}_q[x]$, where $\mathcal{R}[x]$ and $\mathbb{F}_q[x]$ are the corresponding polynomial rings; for any $f \in \mathcal{R}[x]$ we denote by \bar{f} its image under this homomorphism; moreover, for a set $C \subset \mathcal{R}[x]$ we define $\bar{C} = \{\bar{f} \mid f \in C\}$.

It is well known that any $f \in \mathcal{R}[x]$ which is not divisible by γ can be written as $f = uf_1$, where $u \in \mathcal{R}[x]$ is a unit and f_1 is monic. We will therefore restrict our attention to monic polynomials.

The following is basic result of cyclic codes over \mathcal{R} .

Theorem 2 (Theorem 4.5 in Ref. [19]) Let $C = \langle \gamma^{a_0} g_{a_0}(x), \gamma^{a_1} g_{a_1}(x), \dots, \gamma^{a_s} g_{a_s}(x) \rangle$ be a cyclic code of length n over \mathcal{R} , where $g_{a_i}(x) \in \mathcal{R}[x]$ are monic. Then

- 1) $0 \leq a_0 < a_1 < \dots < a_s < t$, and a_0, a_1, \dots, a_s are unique.
- 2) $g_{a_i}(x) \mid g_{a_{i-1}}(x) \mid \dots \mid g_{a_1}(x) \mid g_{a_0}(x) \mid x^n - 1$, $\deg(g_{a_i}(x)) > \deg(g_{a_{i+1}}(x))$ for $i = 0, \dots, s-1$, and $g_{a_0}(x), g_{a_1}(x), \dots, g_{a_s}(x)$ are unique.
- 3) If $i < a_0$, then $\overline{(C:\gamma^i)} = \{\mathbf{0}\}$, otherwise $\overline{(C:\gamma^i)} = \{\overline{g_{a_j}}(x)\}$, where a_j is maximal with the property $a_j \leq i$.
- 4) $\dim_{\mathbb{F}_q}(\overline{(C:\gamma^i)}) = n - \deg(g_{a_j}(x))$, where a_j is maximal with the property $a_j \leq i$.

Combining Theorems 1 and 2, we obtain the following corollary.

Corollary 2 For $1 \leq i \leq r$, let $C_i = \langle g_0^{(i)}(x), \gamma g_1^{(i)}(x), \dots, \gamma^{t-1} g_{i-1}^{(i)}(x) \rangle$ be a cyclic code of length n over \mathcal{R} , where $g_{i-1}^{(i)}(x) \mid g_{i-2}^{(i)}(x) \mid \dots \mid g_1^{(i)}(x) \mid g_0^{(i)}(x) \mid x^n - 1$, and $\deg(g_j^{(i)}(x)) > \deg(g_{j+1}^{(i)}(x))$ for $j = 0, \dots, t-1$. Let $\mathcal{C} = \{C_i \mid i = 1, \dots, r\}$. If $\deg(g_j^{(i)}(x)) = \deg(g_j^{(2)}(x)) = \deg(g_j^{(r)}(x)) = k_j$ for $j = 1, 2, \dots, t-1$, then \mathcal{C} is a constant rank code over \mathcal{R} of rank k and length n , where $k = \frac{1}{t} \sum_{j=0}^{t-1} (t-j) \deg(g_j^{(i)}(x))$.

3 Orbit Constant Rank Codes over Finite Chain Rings

From now on, we denote by $\mathbf{GL}_m(\mathcal{R})$ the set $\mathbf{GL}_m(\mathcal{R}) = \{A \in M_{m \times m}(\mathcal{R}) \mid \det(A) \in \mathcal{R}^*\}$. It is well known that $A, B \in \mathbf{GL}_m(\mathcal{R})$ if and only if $AB \in \mathbf{GL}_m(\mathcal{R})$.

Let \mathcal{U} be a linear (submodule) code of length n over \mathcal{R} with a generator matrix \mathbf{G} in standard form in (1). Clearly, $\mathcal{U} = \text{im } \mathbf{G} = \{a\mathbf{G} \mid a \in \mathcal{R}^{K(C)}\}$, i.e., the submodule of \mathcal{R}^n generated by the rows of \mathbf{G} .

Definition 10 Let \mathcal{G} be a subgroup of $\mathbf{GL}_m(\mathcal{R})$, \mathcal{U} be a linear code (submodule) of length n over \mathcal{R} with a generator matrix \mathbf{G} in standard form in (1). The orbit submodule code generated by \mathcal{U} with respect to the subgroup \mathcal{G} , denoted by $\text{Orb}_{\mathcal{G}}(\mathcal{U})$, is defined as $\text{Orb}_{\mathcal{G}}(\mathcal{U}) = \{\text{im}(\mathbf{G}\mathbf{B}) \mid \mathbf{B} \in \mathcal{G}\}$.

Theorem 3 Let \mathcal{G} be a subgroup of $\mathbf{GL}_m(\mathcal{R})$, and \mathcal{U} be a linear code (submodule) of length n over \mathcal{R} with a generator matrix \mathbf{G} in standard form in (1). Set $k = \frac{1}{t} \sum_{i=0}^{t-1} (t-i)k_i$. Then orbit submodule code $\text{Orb}_{\mathcal{G}}(\mathcal{U})$ is a constant rank code over \mathcal{R} of rank k , length n . In particular, take $l = \sum_{i=0}^{t-1} k_i$, then $\overline{(\text{Orb}_{\mathcal{G}}(\mathcal{U}) : \gamma^{t-1})}$ is a constant dimension code over \mathbb{F}_q of dimension l , length n , and $d_s(\overline{(\text{Orb}_{\mathcal{G}}(\mathcal{U}) : \gamma^{t-1})}) \leq d_M(\mathcal{U})$. Moreover,

$$\overline{(\text{Orb}_{\mathcal{G}}(\mathcal{U}) : \gamma^{t-1})} = \{\text{im}(\overline{A}\overline{B}) \mid \mathbf{B} \in \mathcal{G}\} = \text{Orb}_{\overline{\mathcal{G}}}(\overline{\mathcal{U}} : \gamma^{t-1}),$$

where A is in (2), and $\overline{\mathcal{G}} = \{\overline{H} \mid H \in \mathcal{G}\}$.

Proof For any $\mathcal{V} \in \text{Orb}_{\mathcal{G}}(\mathcal{U})$, there exists $\mathbf{D} \in \mathcal{G}$ such that $\mathcal{V} = \text{im}(\mathbf{G}\mathbf{D})$. Since

$$\mathbf{G} = \begin{pmatrix} \mathbf{I}_{k_0} & \mathbf{A}_{0,1} & \mathbf{A}_{0,2} & \mathbf{A}_{0,3} & \cdots & \mathbf{A}_{0,t-1} & \mathbf{A}_{0,t} \\ 0 & \gamma \mathbf{I}_{k_1} & \gamma \mathbf{A}_{1,2} & \gamma \mathbf{A}_{1,3} & \cdots & \gamma \mathbf{A}_{1,t-1} & \gamma \mathbf{A}_{1,t} \\ 0 & 0 & \gamma^2 \mathbf{I}_{k_2} & \gamma^2 \mathbf{A}_{2,3} & \cdots & \gamma^2 \mathbf{A}_{2,t-1} & \gamma^2 \mathbf{A}_{2,t} \\ \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \gamma^{t-1} \mathbf{I}_{k_{t-1}} & \gamma^{t-1} \mathbf{A}_{t-1,t} \end{pmatrix} = \begin{pmatrix} \mathbf{A}_0 \\ \gamma \mathbf{A}_1 \\ \vdots \\ \gamma^{t-1} \mathbf{A}_{t-1} \end{pmatrix}$$

we have that $\text{rk}(\mathbf{A}_0 \mathbf{D}) = k_0, \text{rk}(\mathbf{A}_1 \mathbf{D}) = k_1, \dots, \text{rk}(\mathbf{A}_{t-1} \mathbf{D}) = k_{t-1}$ by Corollary 1.

On the other hand, we have

$$\mathbf{GD} = \begin{pmatrix} \mathbf{A}_0 \mathbf{D} \\ \gamma(\mathbf{A}_1 \mathbf{D}) \\ \vdots \\ \gamma^{t-1}(\mathbf{A}_{t-1} \mathbf{D}) \end{pmatrix}$$

Clearly, after a suitable permutation of coordinates, we obtain a generator matrix $\tilde{\mathbf{G}}$ in standard form of the submodule \mathcal{V} as follows

$$\tilde{\mathbf{G}} = \begin{pmatrix} \mathbf{I}_{k_0} & \widetilde{\mathbf{A}}_{0,1} & \widetilde{\mathbf{A}}_{0,2} & \widetilde{\mathbf{A}}_{0,3} & \cdots & \widetilde{\mathbf{A}}_{0,t-1} & \widetilde{\mathbf{A}}_{0,t} \\ 0 & \gamma \widetilde{\mathbf{I}}_{k_1} & \gamma \widetilde{\mathbf{A}}_{1,2} & \gamma \widetilde{\mathbf{A}}_{1,3} & \cdots & \gamma \widetilde{\mathbf{A}}_{1,t-1} & \gamma \widetilde{\mathbf{A}}_{1,t} \\ 0 & 0 & \gamma^2 \mathbf{I}_{k_2} & \gamma^2 \widetilde{\mathbf{A}}_{2,3} & \cdots & \gamma^2 \widetilde{\mathbf{A}}_{2,t-1} & \gamma^2 \widetilde{\mathbf{A}}_{2,t} \\ \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \gamma^{t-1} \mathbf{I}_{k_{t-1}} & \gamma^{t-1} \widetilde{\mathbf{A}}_{t-1,t} \end{pmatrix}$$

Thus, $\text{rank}_{\mathcal{R}}(\mathcal{V}) = k = \text{rank}_{\mathcal{R}}(\mathcal{U})$. This means that orbit submodule code $\text{Orb}_{\mathcal{G}}(\mathcal{U})$ is a constant rank code over \mathcal{R} of rank k , length n .

The second statement follows directly from Theorem 1.

By Lemma 9, $\overline{\mathbf{A}}$ is a generator matrix of the linear code $\overline{(\mathcal{U}:\gamma^{t-1})}$ over \mathbb{F}_q .

For any $\mathcal{V} \in \text{Orb}_{\mathcal{G}}(\mathcal{U})$, by Definition 10, there is a $\mathbf{P} \in \mathcal{G}$ such that $\mathcal{V} = \text{im}(\mathbf{GP})$. Then $\overline{\mathbf{A}} \cdot \overline{\mathbf{P}}$ is a generator matrix of the linear code $\overline{(\mathcal{V}:\gamma^{t-1})}$ over \mathbb{F}_q . This means that

$$\overline{(\text{Orb}_{\mathcal{G}}(\mathcal{U}):\gamma^{t-1})} = \{ \text{im}(\overline{\mathbf{A}} \overline{\mathbf{B}}) \mid \mathbf{B} \in \mathcal{G} \} = \text{Orb}_{\mathcal{G}}(\overline{(\mathcal{U}:\gamma^{t-1})}).$$

In the following, we give two examples to demonstrate Theorem 3. We use the Magma Computer Algebra System^[33] in our computations.

Example 1 Consider $\mathcal{R} = \mathbb{Z}_4$. Let \mathcal{U} be a linear (submodule) code of length 11 over \mathbb{Z}_4 with a generator matrix $\mathbf{G}_{\mathcal{U}}$ in standard form as follows:

$$\mathbf{G}_{\mathcal{U}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 2 & 1 & 2 & 1 \\ 0 & 0 & 2 & 0 & 2 & 0 & 0 & 2 & 2 & 0 & 2 \\ 0 & 0 & 0 & 2 & 2 & 2 & 0 & 2 & 2 & 0 & 2 \end{pmatrix}$$

Set $\mathcal{G} = \langle \mathbf{M} \rangle$. i.e., \mathcal{G} is a cyclic subgroup generated by \mathbf{M} of $\mathbf{GL}_{11}(\mathbb{Z}_4)$, where

$$\mathbf{M} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 3 & 0 & 0 & 3 & 0 & 0 & 3 & 3 & 0 & 3 & 3 \end{pmatrix}$$

Clearly, $|\mathcal{G}| = o(\mathbf{M}) = 178$ over $\mathbf{GL}_{11}(\mathbb{Z}_4)$.

It is easy to see that $\overline{\mathcal{G}} = \langle \overline{\mathbf{M}} \rangle$ over $\mathbf{GL}_{11}(\mathbb{F}_2)$, where

$$\overline{\mathbf{M}} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Thus, $|\overline{\mathcal{G}}| = o(\overline{\mathbf{M}}) = 89$ over $\mathbf{GL}_{11}(\mathbb{F}_2)$, and 89 is a prime.

Take

$$\overline{\mathbf{A}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

By Lemma 8, $\overline{\mathbf{A}}$ is a generator matrix of the linear code $\overline{(\mathcal{U}:2)}$. By Theorem 3, we know

$$\text{Orb}_{\overline{\mathcal{G}}}(\overline{(\mathcal{U}:2)}) = \left\{ \text{im}(\overline{\mathbf{A}} \overline{\mathbf{M}}^j) \mid j=0, 1, \dots, 88 \right\},$$

is a constant dimension code over \mathbb{F}_2 of dimension 4, length 11. One can check that $d_s(\overline{(\mathcal{U}:2)}) = 6$. This means that $\overline{(\mathcal{U}:2)}$ is a constant dimension code over \mathbb{F}_2 with parameters $(11, 89, 6; 4)_2$. Thus, by Theorem 3, $\text{Orb}_{\overline{\mathcal{G}}}(\overline{(\mathcal{U}:2)})$ is an optimum distance constant dimension code over \mathbb{Z}_4 with parameters $(11, 178, 6; 3)_2$.

Remark 4 In Refs. [4, 6, 10-12, 34-35], the authors have proved the existence of constant dimension codes with size $\frac{q^N-1}{q-1}$, or $r \frac{q^N-1}{q-1}$, or $(q^m-1) \frac{q^N-1}{q-1} + \frac{q^N-1}{q^k-1}$ and minimal distance $2k-2$ for any given k . Since $89 \neq 2^N-1$, $r(2^N-1), (2^m-1)(2^N-1) + \frac{2^N-1}{2^4-1}$ for any positive integers N and m , the constant dimension code over \mathbb{F}_2 with parameters $(11, 89, 6; 4)_2$ from Example 1 is new.

Example 2 Consider $\mathcal{R} = \mathbb{Z}_9$. Let \mathcal{U} be a linear (submodule) code of length 7 over \mathbb{Z}_9 , with a generator matrix $\mathbf{G}_{\mathcal{U}}$ in standard form as follows:

$$\mathbf{G}_{\mathcal{U}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 8 \\ 0 & 1 & 0 & 0 & 4 & 1 & 5 \\ 0 & 0 & 3 & 0 & 3 & 0 & 6 \end{pmatrix}.$$

Set $\mathcal{G} = \langle \mathbf{M} \rangle$. i.e., \mathcal{G} is a cyclic subgroup generated by \mathbf{M} of $\mathbf{GL}_7(\mathbb{Z}_9)$, where

$$\mathbf{M} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 4 & 4 & 4 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Clearly, $|\mathcal{G}| = o(\mathbf{M}) = 3 \cdot 279$ over $\mathbf{GL}_7(\mathbb{Z}_9)$.

It is easy to check that $\overline{\mathcal{G}} = \langle \overline{\mathbf{M}} \rangle$ over $\mathbf{GL}_7(\mathbb{F}_3)$, where

$$\overline{M} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Thus, $|\overline{\mathcal{G}}| = o(\overline{M}) = 1\,093$ over $\mathbf{GL}_7(\mathbb{F}_3)$, and $1\,093$ is a prime.

Take

$$\overline{A} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 2 \\ 0 & 1 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

By Lemma 8, \overline{A} is a generator matrix of the linear code $\overline{(\mathcal{U}:3)}$. Again by Theorem 3, we know $\text{Orb}_{\overline{\mathcal{G}}}(\overline{(\mathcal{U}:2)}) = \{\text{im}(\overline{A}\overline{M}^j) \mid j=0, 1, \dots, 1\,092\}$ is a constant dimension code over \mathbb{F}_3 of dimension 3, length 6. One can check that $d_s(\overline{(\mathcal{U}:3)}) = 4$. This means that $\overline{(\mathcal{U}:3)}$ is a constant dimension code over \mathbb{F}_2 with parameters $(7, 1\,093, 4; 3)$. Thus, by Theorem 3, $\text{Orb}_{\overline{\mathcal{G}}}(\mathcal{U})$ is a constant rank code over \mathbb{Z}_9 with parameters $(7, 3\,279, \geq 4; \frac{5}{2})_3$.

Remark 5 Glusing-Luerssen *et al*^[4] gave an open problem: Cyclic orbit codes with maximum distance, that is, $2k$, are spread codes (A subspace code C is called a spread of \mathbb{F}_q^n if $\bigcup_{V \in C} V = \mathbb{F}_q^n$ and $V \cap W = \{0\}$ for all distinct $V, W \in C$). Thus, the best distance a non-spread cyclic orbit code of dimension k can attain is $2(k-1)$, but the construction of such codes is unknown. Examples 1 and 2 obtain two special such codes.

Remark 6 When the length and rank of a constant rank code \mathcal{C} over \mathcal{R} and a constant dimension code $\overline{(\mathcal{C}:\gamma^{t-1})}$ over \mathbb{F}_q are same, we can see that $|\mathcal{C}| = h|\overline{(\mathcal{C}:\gamma^{t-1})}|$ for some integer $h > 1$ by Examples 1 and 2.

4 Gray Images of Constant Rank Code over $\mathbb{F}_q + \gamma\mathbb{F}_q$

The ring $\mathcal{R}_1 = \mathbb{F}_q + \gamma\mathbb{F}_q$ consists of all q -ary polynomials of degree 0 and 1 in an indeterminate γ , and it is closed under q -ary polynomial addition and multiplication modulo γ^2 . Thus $\mathcal{R}_1 = \frac{\mathbb{F}_q[\gamma]}{\langle \gamma^2 \rangle} = \{a + \gamma b \mid a, b \in \mathbb{F}_q\}$ is a local ring with maximal ideal $\gamma\mathbb{F}_q$. Therefore, it is a chain ring.

We first give the definition of the Gray map on \mathcal{R}_1^n . The Gray map $\Phi_1: \mathcal{R}_1 \rightarrow \mathbb{F}_q^2$ is given by $\Phi_1(a + \gamma b) = (b, a + b)$. This map can be extended to \mathcal{R}_1^n in a natural way: $\Phi: \mathcal{R}_1^n \rightarrow \mathbb{F}_q^{2n}, (a_1 + \gamma b_1, \dots, a_n + \gamma b_n) \mapsto (b_1, a_1 + b_1, \dots, b_n, a_n + b_n)$. The following corollary and lemma are from Refs. [13, 16].

Corollary 3 (Corollary 5.10 in Ref. [16]) If C is a linear code over \mathcal{R}_1 of length n and size q^k , then $\Phi(C)$ is a linear code over \mathbb{F}_q with parameters $[2n, k]$.

Lemma 11 (Theorem 3.4 in Ref. [13]) Let $C = \langle f(x)h(x), \gamma f(x) \rangle$ be a cyclic code of length n over \mathcal{R}_1 , where $x^n - 1 = f(x)g(x)h(x)$ and $f(x), g(x), h(x)$ are pairwise coprime. Then $|C| = q^{2(n - \deg(f(x)))}$.

Lemma 12 Let $C_i = \langle f_i(x)h_i(x), \gamma f_i(x) \rangle$ be a cyclic code of length n over \mathcal{R}_1 , where $x^n - 1 = f_i(x)g_i(x)h_i(x)$ and $f_i(x), g_i(x), h_i(x)$ are pairwise coprime for $i=1, 2$. Then $C_1 \cap C_2 = \langle \text{lcm}(f_1(x)h_1(x), f_2(x)h_2(x)), \gamma \text{lcm}(f_1(x), f_2(x))) \rangle$. Moreover, $|C_1 \cap C_2| = q^{2(n - \deg(\text{lcm}(f_1(x), f_2(x))))}$.

Proof Since $C_1 \cap C_2$ is a cyclic code of n over \mathcal{R} , there exist $u(x), v(x)$ and $w(x)$ in $\mathcal{R}[x]$ such that $C_1 \cap C_2 = \langle u(x)v(x), \gamma u(x) \rangle$, where $x^n - 1 = u(x)v(x)w(x)$ and $u(x), v(x), w(x)$ are pairwise coprime.

By $u(x)v(x) \in C_1 \cap C_2 \subset C_1$, there exist $a_1(x)$ and $b_1(x)$ in $\mathcal{R}[x]$ such that $u(x)v(x) = a_1(x)f_1(x)h_1(x) + \gamma b_1(x)f_1(x)$. Multiplying by γ , we obtain $\gamma u(x)v(x) = \gamma a_1(x)f_1(x)h_1(x)$, which implies $f_1(x)h_1(x)u(x)v(x)$.

Again by $\gamma u(x) \in C_1 \cap C_2 \subset C_1$, there exist $a_2(x)$ and $b_2(x)$ in $\mathcal{R}[x]$ such that $\gamma u(x) = a_2(x)f_1(x)h_1(x) + \gamma b_2(x)f_1(x)$.

Multiplying by $g_1(x)$, we obtain $\gamma u(x)g_1(x) = \gamma b_2(x)f_1(x)g_1(x)$, which implies $f_1(x)|u(x)$.

Similarly, $C_1 \cap C_2 \subset C_2$, which implies $f_2(x)h_2(x)|u(x)v(x)$ and $f_2(x)|u(x)$.

Consequently, $\text{lcm}(f_1(x)h_1(x), f_2(x)h_2(x))|u(x)v(x)$ and $\text{lcm}(f_1(x), f_2(x))|u(x)$. This means that

$$C_1 \cap C_2 \subset \langle \text{lcm}(f_1(x)h_1(x), f_2(x)h_2(x)), \gamma \text{lcm}(f_1(x), f_2(x)) \rangle.$$

On the other hand, clearly, we have $\langle \text{lcm}(f_1(x)h_2(x), f_2(x)h_2(x)), \gamma \text{lcm}(f_1(x), f_2(x)) \rangle \subset C_1 \cap C_2$.

To summarize, we have $C_1 \cap C_2 = \langle \text{lcm}(f_1(x)h_1(x), f_2(x)h_2(x), \gamma \text{lcm}(f_1(x), f_2(x)) \rangle$.

Set $f(x) = \text{lcm}(f_1(x), f_2(x))$, $h(x) = \frac{x^n - 1}{\text{lcm}(f_1(x), f_2(x)) \cdot \text{gcd}(g_1(x), f_2(x))}$, and $g(x) = \text{gcd}(g_1(x), f_2(x))$.

Then, $x^n - 1 = f(x)g(x)h(x)$ and the polynomials $f(x)$, $g(x)$ and $h(x)$ are pairwise coprime.

It is easy to check that $C_1 \cap C_2 = \langle f(x)h(x), \gamma f(x) \rangle$. Therefore, $|C_1 \cap C_2| = q^{2(n - \text{deg}(\text{lcm}(f_1(x), f_2(x))))}$.

Now combining Corollary 3 with Lemmas 11 and 12, we obtain the following proposition.

Proposition 1 Let $C_i = \langle f_i(x)h_i(x), \gamma f_i(x) \rangle$ be a cyclic code of length n over \mathcal{R}_1 , where $x^n - 1 = f_i(x)g_i(x)h_i(x)$, $f_i(x)$, $g_i(x)$, $h_i(x)$ are pairwise coprime for $i=1, 2, \dots, s$. Let $\mathcal{C} = \{C_i | i = 1, \dots, s\}$. If $\text{deg}(f_1(x)) = \text{deg}(f_2(x)) = \dots = \text{deg}(f_s(x))$ and $\text{deg}(\text{lcm}(f_1(x), f_2(x))) = \text{deg}(\text{lcm}(f_i(x), f_j(x)))$ for all $i \neq j$, then \mathcal{C} is a constant rank code over \mathcal{R}_1 with parameters $(n, s, d; k)_q$, where $k = n - \text{deg}(f_1(x))$ and $d = 2(\text{deg}(\text{lcm}(f_1(x), f_2(x))) - \text{deg}(f_1(x)))$.

Corollary 4 Let $x^n - 1 = l_1(x)l_2(x) \cdots l_r(x)$, where $l_1(x), l_2(x), \dots, l_r(x)$ are pairwise coprime. We assume that $\text{deg}(l_{j_1}(x)) = \dots = \text{deg}(l_{j_s}(x))$ for $\{j_1, \dots, j_s\} \subset \{1, 2, \dots, r\}$. Let $C_i = \langle l_{j_i}(x)h_i(x), \gamma l_{j_i}(x) \rangle$ be a cyclic code of length n over \mathcal{R}_1 where $x^n - 1 = l_{j_i}(x)g_i(x)h_i(x)$. Let $\mathcal{C} = \{C_i | i = 1, \dots, s\}$. Then \mathcal{C} is an optimum constant dimension code \mathbb{F}_q with parameters $(2n, s, d; k)_q$, where $d = 4\text{deg}(l_{j_i}(x))$, and $k = 2(n - \text{deg}(l_{j_i}(x)))$.

Proof It is easy to check that $\Phi(C_i \cap C_j) = \Phi(C_i) \cap \Phi(C_j)$ for $i, j = 1, 2, \dots, s$.

By Corollary 3 and Lemma 12, for $i, j = 1, 2, \dots, s$, $\Phi(C_i)$ is a linear code over \mathbb{F}_q with parameters $[2n, k]$, and $\Phi(C_i) \cap \Phi(C_j)$ is a linear code over \mathbb{F}_q with parameters $[2n, k - 2\text{deg}(l_{j_i}(x))]$. Thus, $d_s(\Phi(C_i)) = 2k - 2(k - 2\text{deg}(l_{j_i}(x))) = 4\text{deg}(l_{j_i}(x))$. So, \mathcal{C} is an optimum constant dimension code \mathbb{F}_q with parameters $(2n, s, d; k)_q$.

Example 3 Consider cyclic codes of length 71 over $\mathbb{F}_{5^2} + \gamma\mathbb{F}_{5^2}$. In $\mathbb{F}_{5^2} + \gamma\mathbb{F}_{5^2}$,

$$x^{71} - 1 = M_0(x)M_1(x)M_2(x) \cdots M_{14}(x),$$

where

$$\begin{aligned} M_0(x) &= x + 4, M_1(x) = x^5 + x^2 + 2x + 4, M_2(x) = x^5 + 4x^3 + 3x + 4, M_3(x) = x^5 + 4x^3 + 4x^2 + x + 4, \\ M_4(x) &= x^5 + 3x^3 + x^2 + 4x + 4, M_5(x) = x^5 + x^4 + x^3 + 3x^2 + 2x + 4, M_6(x) = x^5 + x^4 + 2x^3 + 3x^2 + 3x + 4, \\ M_7(x) &= x^5 + x^4 + 4x^3 + 2x^2 + 4, M_8(x) = x^5 + x^4 + 3x^3 + 2x^2 + 2x + 4, M_9(x) = x^5 + 2x^4 + x^2 + 4, \\ M_{10}(x) &= x^5 + 2x^4 + 2x^3 + 3x^2 + 4x + 4, M_{11}(x) = x^5 + 4x^4 + x^3 + x^2 + 4, M_{12}(x) = x^5 + 3x^4 + 2x^3 + 4x^2 + 4x + 4, \\ M_{13}(x) &= x^5 + 3x^4 + 4x^3 + 4, M_{14}(x) = x^5 + 3x^4 + 3x^3 + 2x^2 + 4x + 4. \end{aligned}$$

Let $C_i = \langle M_0(x)M_i(x), \gamma M_i(x) \rangle$ for $i = 1, 2, \dots, 14$. Using Corollary 4, we find that the subspace code $\mathcal{C} = \{\Phi(C_i) | i = 1, 2, \dots, 14\}$ is an optimum distance constant dimension code over \mathbb{F}_{5^2} with parameters $(142, 14, 20; 132)_{5^2}$.

Example 4 Consider cyclic codes of lengths 84 and 93 over $\mathbb{F}_4 + \gamma\mathbb{F}_4$, respectively. First,

$$x^{85} - 1 = M_0(x)M_1(x)M_2(x) \cdots M_{21}(x),$$

where

$$\begin{aligned} M_0(x) &= x + 1, M_1(x) = (x^2 + wx + 1)(x^2 + w^2x + 1), M_2(x) = x^4 + x^2 + wx + 1, \\ M_3(x) &= x^4 + w^2x^3 + x^2 + w^2x + 1, M_4(x) = x^4 + wx^2 + w^2x + 1, M_5(x) = x^4 + w^2x^2 + wx + 1, \\ M_6(x) &= x^4 + x^3 + wx + 1, M_7(x) = x^4 + x^3 + w^2x + 1, M_8(x) = x^4 + x^3 + wx^2 + x + 1, M_9(x) = x^4 + x^3 + w^2x^2 + x + 1, \\ M_{10}(x) &= x^4 + w^2x^3 + wx^2 + 1, M_{11}(x) = x^4 + x^2 + w^2x + 1, M_{12}(x) = x^4 + wx^3 + w^2x^2 + 1, M_{13}(x) = x^4 + w^2x^3 + x + 1, \\ M_{14}(x) &= x^4 + wx^3 + x + 1, M_{15}(x) = x^4 + w^2x^3 + x^2 + 1, M_{16}(x) = x^4 + wx^3 + x^2 + 1, M_{17}(x) = x^4 + wx^3 + x^2 + wx + 1, \\ M_{18}(x) &= x^4 + w^2x^3 + wx^2 + wx + 1, M_{19}(x) = x^4 + wx^3 + w^2x^2 + w^2x + 1, M_{20}(x) = x^4 + wx^3 + wx^2 + w^2x + 1, \end{aligned}$$

$$M_{21}(x) = x^4 + w^2x^3 + w^2x^2 + wx + 1.$$

Let $C_i = \langle M_0(x)M_i(x), \gamma M_i(x) \rangle$ for $i = 1, 2, \dots, 21$. Using Corollary 4, we find that the subspace code $\mathcal{C} = \{\Phi(C_i) \mid i = 1, 2, \dots, 21\}$ is an optimum distance constant dimension code over \mathbb{F}_4 with parameters $(170, 21, 16; 162)_4$.

Second, taking $n=93$, we have

$$x^{93} - 1 = N_0(x)N_1(x)N_2(x)\cdots N_{20}(x),$$

where

$N_0(x) = x + 1$, $N_1(x) = x + w$, $N_2(x) = x + w^2$, $N_3(x) = x^5 + x^2 + 1$, $N_4(x) = x^5 + x^2 + w$, $N_5(x) = x^5 + x^2 + w^2$, $N_6(x) = x^5 + x^3 + 1$,
 $N_7(x) = x^5 + x^3 + x + 1$, $N_8(x) = x^5 + wx^3 + w$, $N_9(x) = x^5 + w^2x^3 + w^2$, $N_{10}(x) = x^5 + x^4 + x^2 + x + 1$,
 $N_{11}(x) = x^5 + wx^3 + x^2 + w^2x + w$, $N_{12}(x) = x^5 + w^2x^3 + x^2 + wx + w^2$, $N_{13}(x) = x^5 + wx^4 + x^2 + wx + w^2$,
 $N_{14}(x) = x^5 + wx^4 + w^2x^3 + wx + w^2$, $N_{15}(x) = x^5 + wx^4 + w^2x^3 + x^2 + w^2$, $N_{16}(x) = x^5 + w^2x^4 + x^2 + w^2x + w$,
 $N_{17}(x) = x^5 + w^2x^4 + wx^3 + w^2x + w$, $N_{18}(x) = x^5 + w^2x^4 + wx^3 + x^2 + w$, $N_{19}(x) = x^5 + x^4 + x^3 + x + 1$, $N_{20}(x) = x^5 + x^4 + x^3 + x^2 + 1$.
Let $C_i = \langle M_0(x)M_i(x), \gamma M_i(x) \rangle$ for $i = 3, 4, \dots, 20$. Using Corollary 4, we find that the subspace code $\mathcal{C} = \{\Phi(C_i) \mid i = 3, \dots, 20\}$ is an optimum distance constant dimension code over \mathbb{F}_4 with parameters $(186, 17, 20; 176)_4$.

Remark 7 In Refs. [4, 6, 10-12, 34-35], the authors proved the existence of constant dimension codes with size $\frac{q^N - 1}{q - 1}$, or $r \frac{q^N - 1}{q - 1}$, or $(q^m - 1) \frac{q^N - 1}{q - 1} + \frac{q^N - 1}{q^k - 1}$ and minimal distance $2k - 2$ for any given k . Since $21, 17 \neq 4^N - 1, r \frac{4^N - 1}{3}, (4^m - 1) \frac{4^N - 1}{3} + \frac{4^N - 1}{4^k - 1}$ for any positive integers r, k, N and m , the constant dimension codes over \mathbb{F}_4 with parameters $(170, 21, 16; 162)_4$ and $(186, 17, 20; 176)_4$ from Example 4 are new.

Remark 8 The constant dimension codes from Examples 3 and 4 are optimum distance constant dimension codes.

5 Conclusion

In this paper, we studied submodule codes over finite chain rings, and gave two criteria for a submodule code \mathcal{C} over finite chain rings to be a constant rank code. Further, we constructed optimum distance constant dimension codes over \mathbb{F}_q by using submodule codes in finite chain rings. We believe that submodule codes over finite chain rings will be a good source for constructing new constant dimension codes over \mathbb{F}_q . In future work, in order to construct new constant dimension codes, we will use the computer algebra system MAGMA to search for more good submodule codes over finite chain rings.

References

- [1] Ahlswede R, Cai N, Li S R, *et al.* Network information flow [J]. *IEEE Transactions on Information Theory*, 2000, **46**(4): 1204-1216.
- [2] Koetter R, Kschischang F R. Coding for errors and erasures in random network coding[J]. *IEEE Transactions on Information Theory*, 2008, **54**(8): 3579-3591.
- [3] Gluesing-Luerssen H, Lehmann H. Distance distributions of cyclic orbit codes[J]. *Designs, Codes and Cryptography*, 2021, **89**(3): 447-470.
- [4] Gluesing-Luerssen H, Morrison K, Troha C. Cyclic orbit codes and stabilizer subfields[J]. *Advances in Mathematics of Communications*, 2015, **9**(2): 177-197.
- [5] Gluesing-Luerssen H, Troha C. Construction of subspace codes through linkage[J]. *Advances in Mathematics of Communications*, 2016, **10**(3): 525-540.
- [6] Chen B C, Liu H W. Constructions of cyclic constant dimension codes[J]. *Designs, Codes and Cryptography*, 2018, **86**(6): 1267-1279.
- [7] Heinlein D, Kurz S. Coset construction for subspace codes [J]. *IEEE Transactions on Information Theory*, 2017, **63**(12): 7651-7660.
- [8] Honold T, Kiermaier M, Kurz S. Optimal binary subspace codes of length 6, constant dimension 3 and minimum distance 4[EB/OL]. [2024-09-10]. <https://arxiv.org/abs/1311.0464v2>.
- [9] Trautmann A L, Manganiello F, Braun M, *et al.* Cyclic orbit codes[J]. *IEEE Transactions on Information Theory*, 2013, **59**(11): 7386-7404.
- [10] Ben-Sasson E, Etzion T, Gabizon A, *et al.* Subspace polynomials and cyclic subspace codes[J]. *IEEE Transactions on Information Theory*, 2016, **62**(3): 1157-1165.
- [11] Roth R M, Raviv N, Tamo I. Construction of Sidon spaces with applications to coding[J]. *IEEE Transactions on Information Theory*, 2018, **64**(6): 4412-4422.
- [12] Zhang H, Cao X W. Further constructions of cyclic subspace

- codes[J]. *Cryptography and Communications*, 2021, **13**(2): 245-262.
- [13] Dinh H Q, Lopez-Permouth S R. Cyclic and negacyclic codes over finite chain rings[J]. *IEEE Transactions on Information Theory*, 2004, **50**(8): 1728-1744.
- [14] Liu X S, Liu H L. LCD codes over finite chain rings[J]. *Finite Fields and Their Applications*, 2015, **34**: 1-19.
- [15] Hu P, Liu X S. Constacyclic codes of length p^s over finite rings $F_p^m + uF_p^m + vF_p^m + uvF_p^m$ [J]. *Wuhan University Journal of Natural Sciences*, 2020, **25**(4): 311-322.
- [16] Liu X S, Liu H L. σ -LCD codes over finite chain rings[J]. *Designs, Codes and Cryptography*, 2020, **88**(4): 727-746.
- [17] Liu X S, Liu H L. Quantum codes from linear codes over finite chain rings[J]. *Quantum Information Processing*, 2017, **16**(10): 240.
- [18] Liu Z H, Wang J L. Linear complementary dual codes over rings[J]. *Designs, Codes and Cryptography*, 2019, **87**(12): 3077-3086.
- [19] Norton G H, Sălăgean A. On the structure of linear and cyclic codes over a finite chain ring[J]. *Applicable Algebra in Engineering, Communication and Computing*, 2000, **10**(6): 489-506.
- [20] Abualrub T, Aydin N, Aydogdu I. Optimal binary codes derived from F_2F_4 -additivecyclic codes[J]. *Journal of Applied Mathematics and Computing*, 2020, **64**(1): 71-87.
- [21] Bonnacaze A, Udaya P. Cyclic codes and self-dual codes over $F_2 + uF_2$ [J]. *IEEE Transactions on Information Theory*, 1999, **45**(4): 1250-1255.
- [22] Norton G H, Salagean A. On the Hamming distance of linear codes over a finite chain ring[J]. *IEEE Transactions on Information Theory*, 2000, **46**(3): 1060-1067.
- [23] Dinh H Q, Bag T, Upadhyay A K, *et al.* Quantum codes from a class of constacyclic codes over finite commutative rings[J]. *Journal of Algebra and Its Applications*, 2020, **19**(12): 2150003.
- [24] Kal X S, Zhu S X. Quaternary construction of quantum codes from cyclic codes over $F_4 + uF_4$ [J]. *International Journal of Quantum Information*, 2011, **9**(2): 689-700.
- [25] Liu H L, Liu X S. New EAQEC codes from cyclic codes over $F_q + uF_q$ [J]. *Quantum Information Processing*, 2020, **19**(3): 85.
- [26] Ma F, Gao J, Fu F W. Constacyclic codes over the ring $F_p + vF_q$ and their applications of constructing new non-binary quantum codes[J]. *Quantum Information Processing*, 2018, **5**(2): 130-141.
- [27] Tang Y S, Zhu S X, Kai X S, *et al.* New quantum codes from dual-containing cyclic codes over finite rings[J]. *Quantum Information Processing*, 2016, **15**(11): 4489-4500.
- [28] Dougherty S T, Liu H W. Independence of vectors in codes over rings[J]. *Designs, Codes and Cryptography*, 2009, **51**(1): 55-68.
- [29] MacWilliams F J, Sloane N J A. *The Theory of Error-correcting Codes*[M]. Amsterdam: Elsevier, 1977.
- [30] Wood J A. Duality for modules over finite rings and applications to coding theory[J]. *American Journal of Mathematics*, 1999, **121**(3): 555-575.
- [31] Liu Z H. Galois LCD codes over rings[J]. *Advances in Mathematics of Communications*, 2024, **18**(1): 91-104.
- [32] Fan Y, Ling S, Liu H W. Matrix product codes over finite commutative Frobenius rings[J]. *Designs, Codes and Cryptography*, 2014, **71**(2): 201-227.
- [33] Bosma W, Cannon J, Playoust C. The magma algebra system I: The user language[J]. *Journal of Symbolic Computation*, 1997, **24**(3/4): 235-265.
- [34] Otal K, Özbudak F. Cyclic subspace codes via subspace polynomials[J]. *Designs, Codes and Cryptography*, 2017, **85**(2): 191-204.
- [35] Zhao W, Tang X L. A characterization of cyclic subspace codes via subspace polynomials[J]. *Finite Fields and Their Applications*, 2019, **57**: 1-12.

有限链环上常秩和轨道码的构造

郭焯， 刘修生[†]

湖北师范大学文理学院 理工学部, 湖北 黄石 435109

摘要: 本文将有限域上常维数和轨道码推广到有限链环上的常秩和轨道码。我们提供了有限链环的常秩码和它的剩余类域的常维数码之间的一种关系。特别地，证明了有限链环上的轨道子模码是一个常秩码。最后，对于特殊有限链环 $(F_q + \gamma F_q)^n$ ，定义了一个 Gray 映射从 $(F_q + \gamma F_q)^n$ 到 F_q^{2n} 的 Gray 映射 Φ ，借助 $F_q + \gamma F_q$ 上的循环码，得到域 F_q 上一种构造极优距离常维数码的办法。

关键词: 有限链环；线性码的秩；常秩码；轨道码

□