AAECC (2018) 29:455–478
https://doi.org/10.1007/s00200-018-0352-4

ORIGINAL PAPER

Matrix-product structure of constacyclic codes over finite chain rings $\mathbb{F}_{p^m}[u]/\langle u^e\rangle$

Yuan Cao[1] · Yonglin Cao[1] · Fang-Wei Fu[2]

Received: 30 August 2017 / Accepted: 1 March 2018 / Published online: 6 March 2018

Abstract Let m, e be positive integers, p a prime number, $\mathbb{F}_{p^m}$ be a finite field of p^m elements and $R = \mathbb{F}_{p^m}[u]/\langle u^e\rangle$ which is a finite chain ring. For any $\omega \in R^\times$ and positive integers k, n satisfying $\gcd(p, n) = 1$, we prove that any $(1+\omega u)$-constacyclic code of length $p^k n$ over R is monomially equivalent to a matrix-product code of a nested sequence of p^k cyclic codes with length n over R and a $p^k \times p^k$ matrix A_{p^k} over $\mathbb{F}_p$. Using the matrix-product structures, we give an iterative construction of every $(1+\omega u)$-constacyclic code by $(1+\omega u)$-constacyclic codes of shorter lengths over R.

Keywords Repeated-root constacyclic code · Matrix-product code · Monomially equivalent codes · Finite chain ring

Mathematics Subject Classification 94B15 · 94B05 · 11T71

1 Introduction

Algebraic coding theory deals with the design of error-correcting and error-detecting codes for the reliable transmission of information across noisy channel. The class of constacyclic codes play a very significant role in the theory of error-correcting codes.

✉ Yonglin Cao
ylcao@sdut.edu.cn

Yuan Cao
yuancao@sdut.edu.cn

Fang-Wei Fu
fwfu@nankai.edu.cn

[1] School of Mathematics and Statistics, Shandong University of Technology, Zibo 255091, Shandong, China

[2] Chern Institute of Mathematics and LPMC, Nankai University, Tianjin 300071, China

Let Γ be a commutative finite chain ring with identity $1 \neq 0$, and $\Gamma^\times$ be the multiplicative group of invertible elements of Γ. For any $a \in \Gamma$, we denote by $\langle a \rangle_\Gamma$, or $\langle a \rangle$ for simplicity, the ideal of Γ generated by a, i.e. $\langle a \rangle_\Gamma = a\Gamma = \{ab \mid b \in \Gamma\}$. For any ideal I of Γ, we will identify the element $a + I$ of the residue class ring Γ/I with $a \pmod I$ for any $a \in \Gamma$.

A *code* of length N over Γ is a nonempty subset $\mathcal{C}$ of $\Gamma^N = \{(a_0, a_1, \ldots, a_{N-1}) \mid a_j \in \Gamma,\ j = 0, 1, \ldots, N-1\}$. Each element of $\mathcal{C}$ is called a *codeword* and the number of codewords in $\mathcal{C}$ is denoted by $|\mathcal{C}|$. The code $\mathcal{C}$ is said to be *linear* if $\mathcal{C}$ is a Γ-submodule of Γ^N. For any codeword $c = (c_0, c_1, \ldots, c_{N-1}) \in \mathcal{C}$, the *Hamming weight* of c is defined by $\mathrm{w}_H(c) = |\{j \mid c_j \neq 0,\ 0 \leq j \leq N-1\}|$. Then the *minimum Hamming distance* of a linear code $\mathcal{C}$ is equal to $d_H(\mathcal{C}) = \min\{\mathrm{w}_H(c) \mid c \neq 0,\ c \in \mathcal{C}\}$. If $M = |\mathcal{C}|$ and $d = d_H(\mathcal{C})$, $\mathcal{C}$ is called an (N, M, d)-code over Γ. All codes in this paper are assumed to be linear.

Let $\gamma \in \Gamma^\times$. A linear code $\mathcal{C}$ of length N over Γ is called a *γ-constacyclic code* if $(\gamma c_{N-1}, c_0, c_1, \ldots, c_{N-2}) \in \mathcal{C}$ for all $(c_0, c_1, \ldots, c_{N-1}) \in \mathcal{C}$. Particularly, $\mathcal{C}$ is called a *negacyclic code* if $\gamma = -1$, and $\mathcal{C}$ is called a *cyclic code* if $\gamma = 1$.

For any $a = (a_0, a_1, \ldots, a_{N-1}) \in \Gamma^N$, let $a(x) = a_0 + a_1 x + \cdots + a_{N-1}x^{N-1} \in \Gamma[x]/\langle x^N - \gamma \rangle$. We will identify a with $a(x)$ in this paper. It is well known that $\mathcal{C}$ is a γ-constacyclic code of length N over Γ if and only if $\mathcal{C}$ is an ideal of the residue class ring $\Gamma[x]/\langle x^N - \gamma \rangle$. Let p be the characteristic of the residue class field of Γ. If $\gcd(p, N) = 1$, $\mathcal{C}$ is called a *simple-root constacyclic code* while when $p \mid N$ it is called a *repeated-root constacyclic code*.

For any positive integer N, we denote $[N] = \{0, 1, \ldots, N-1\}$ in this paper. Let C_1 and C_2 be codes of length N over Γ. Recall that C_1 and C_2 are said to be *monomially equivalent* if there exists a permutation ϱ on the set $[N]$ and fixed elements $r_0, r_1, \ldots, r_{N-1} \in \Gamma^\times$ such that

$$C_2 = \{(r_0 c_{\varrho(0)}, r_1 c_{\varrho(1)}, \ldots, r_{N-1} c_{\varrho(N-1)}) \mid (c_0, c_1, \ldots, c_{N-1}) \in C_1\}$$

(cf. Huffman and Pless [13, Page 24]). Especially, C_1 and C_2 are said to be *permutation equivalent* when $r_0 = r_1 = \cdots = r_{N-1} = 1$ (cf. [13, Page 20]). Recall that a *monomial matrix* over Γ is a square matrix with exactly one invertible entry in each row and column. Hence C_1 and C_2 are monomially equivalent if and only if there is an $N \times N$ monomial matrix Q over Γ such that $Q \cdot C_1 = \{Q\xi \mid \xi \in C_1\} = C_2$ in which we regard each $\xi \in C_1$ as an $N \times 1$ column vector over Γ.

From now on, let m and e be positive integers, p a prime number, $\mathbb{F}_{p^m}$ be a finite field of p^m elements and denote

$$R = \mathbb{F}_{p^m}[u]/\langle u^e \rangle = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + \cdots + u^{e-1}\mathbb{F}_{p^m}\ (u^e = 0).$$

It is known that R is a finite chain ring with subfield $\mathbb{F}_{p^m}$, uR is the unique maximal ideal and e is the nilpotency index of u. All invertible elements of R are given by $a_0 + a_1 u + \cdots + a_{e-1}u^{e-1},\ a_0 \neq 0,\ a_0, a_1, \ldots, a_{e-1} \in \mathbb{F}_{p^m}$.

There are many research results on constacyclic codes over R, see [1], [5–10] and [14] for examples. Let $\omega \in R^\times$, k and n be positive integers satisfying $\gcd(p, n) = 1$. In this paper, we concentrate on $(1 + \omega u)$-constacyclic codes of length $p^k n$ over R,

i.e. ideals of the residue class ring $R[x]/\langle x^{p^k n} - (1+\omega u)\rangle$. Specifically, the algebraic structures and properties of $(1 + w\gamma)$-constacyclic codes of arbitrary length over an arbitrary finite chain ring Γ were given in [4], where w is a unit in Γ and γ generates the unique maximal ideal of Γ.

Blackford [2] classified all negacyclic codes over the finite chain ring $\mathbb{Z}_4$ of even length using a Discrete Fourier Transform approach. Using the concatenated structure given by [2, Theorem 3], we know that each negacyclic code of length $2^k n$, where n is odd, is monomially equivalent to a sequence of 2^k cyclic codes of length n over $\mathbb{Z}_4$.

As $-1 = 1 + 2 \in \mathbb{Z}_4$, negacyclic codes of even length over $\mathbb{Z}_4$ is a special subclass of the class of $(1 + w\gamma)$-constacyclic codes with arbitrary length over an arbitrary finite chain ring Γ. Now, we try to give a matrix-product structure for any $(1 + \omega u)$-constacyclic code of length $p^k n$ over R by us of the theory of finite chain rings. In this paper, we denote

$$\mathcal{R}_k := R[v]/\langle v^{p^k} - (1 + \omega u)\rangle.$$

As $R[x]/\langle f\rangle = R$ when $f = x - 1$, from Cao [4, Theorem 2.4] and Dinh et al. [10, Section 4] we deduce the following lemma.

Lemma 1.1 *Using the notations above, we have the following conclusions.*

(i) $v - 1$ *is nilpotent in the ring* $\mathcal{R}_k$.
(ii) $\mathcal{R}_k$ *is a commutative finite chain ring with maximal ideal* $(v - 1)\mathcal{R}_k$, *and* $p^k e$ *is the nilpotency index of* $v - 1$. *Furthermore,* $u\mathcal{R}_k = (v - 1)^{p^k}\mathcal{R}_k$.
(iii) $\mathcal{R}_k/(v - 1)\mathcal{R}_k \cong \mathbb{F}_{p^m}$.
(iv) All $p^k e + 1$ *distinct ideals of* $\mathcal{R}_k$ *are given by*

$$\{0\} = (v - 1)^{p^k e}\mathcal{R}_k \subset (v - 1)^{p^k e-1}\mathcal{R}_k \subset \cdots \subset (v - 1)\mathcal{R}_k \subset (v - 1)^0\mathcal{R}_k = \mathcal{R}_k.$$

Moreover, the number of elements in $(v - 1)^i\mathcal{R}_k$ *is equal to* $|(v - 1)^i\mathcal{R}_k| = p^{m(p^k e-i)}$ *for all* $i = 0, 1, \ldots, p^k e$.

We will construct a precise isomorphism of rings from $R[x]/\langle x^{p^k n} - (1 + \omega u)\rangle$ onto $\mathcal{R}_k[x]/\langle x^n - 1\rangle$, which induces a one-to-one correspondence between the set of $(1 + \omega u)$-constacyclic codes of length $p^k n$ over R onto the set of cyclic codes of length n over $\mathcal{R}_k$. By the theory of simple-root cyclic codes over finite chain rings (cf. Norton et al. [15]), any cyclic code of length n over $\mathcal{R}_k$ can be determined uniquely by a tower of $p^k e$ cyclic codes with length n over the finite field $\mathbb{F}_{p^m}$

$$\langle g_0(x)\rangle \subseteq \langle g_1(x)\rangle \subseteq \cdots \subseteq \langle g_{p^k e-1}(x)\rangle \subseteq \mathbb{F}_{p^m}[x]/\langle x^n - 1\rangle,$$

where $g_0(x), g_1(x), \ldots, g_{p^k e-1}(x)$ are monic divisors of $x^n - 1$ in $\mathbb{F}_{p^m}[x]$ satisfying $g_{p^k e-1}(x) \mid \cdots \mid g_1(x) \mid g_0(x) \mid (x^n - 1)$. Then we give a direct description of a monomially equivalence between a $(1 + \omega u)$-constacyclic code of length $p^k n$ over R and a matrix-product code of a sequence of p^k cyclic codes over R determined by $g_s(x), s = 0, 1, \ldots, p^k e - 1$.

In Sect. 2, we sketch the concept of matrix-product codes and structures of simple-root cyclic codes over the finite chain ring $\mathcal{R}_k$. In Sect. 3, we prove that any $(1+\omega u)$-constacyclic code of length $p^k n$ over R is monomially equivalent to a matrix-product code of a nested sequence of p^k cyclic codes with length n over R. Using this matrix-product structure, we give an iterative construction of every $(1+\omega u)$-constacyclic code by use of $(1+\omega u)$-constacyclic codes of shorter lengths over R in Sect. 4. In Sect. 5, we consider how to get the matrix-product structures of $(1+u)$-constacyclic codes of length 90 over $R = \mathbb{F}_3 + u\mathbb{F}_3$ $(u^2 = 0)$.

2 Preliminaries

In this section, we sketch the concept of matrix-product codes and structures of simple-root cyclic codes over the finite chain ring $\mathcal{R}_k$.

Let $R = \mathbb{F}_{p^m}[u]/\langle u^e \rangle$. We follow the notation in [3, Definition 2.1] for definition of matrix-product codes. Let $A = [a_{ij}]$ be an $\alpha \times \beta$ matrix with entries in R and let $C_1, \ldots, C_\alpha$ be codes of length n over R. The *matrix-product code* $[C_1, \ldots, C_\alpha] \cdot A$ is the set of all matrix products $[c_1, \ldots, c_\alpha] \cdot A$ defined by

$$\begin{aligned}[c_1, \ldots, c_\alpha] \cdot A &= [c_1, \ldots, c_\alpha] \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1\beta} \\ a_{21} & a_{22} & \ldots & a_{2\beta} \\ \vdots & \vdots & \vdots & \vdots \\ a_{\alpha 1} & a_{\alpha 2} & \ldots & a_{\alpha\beta} \end{bmatrix} \\ &= [a_{11}c_1 + a_{21}c_2 + \cdots + a_{\alpha 1}c_\alpha, a_{12}c_1 + a_{22}c_2 + \cdots + a_{\alpha 2}c_\alpha, \\ &\quad \ldots, a_{1\beta}c_1 + a_{2\beta}c_2 + \ldots + a_{\alpha\beta}c_\alpha]\end{aligned}$$

where $c_i \in C_i$ is an $n \times 1$ column vector for $1 \le i \le \alpha$. Any codeword $[c_1, \ldots, c_\alpha] \cdot A$ is an $n \times \beta$ matrix over R and we regard it as a codeword of length $n\beta$ by reading the entries of the matrix in column-major order. A code C over R is a matrix-product code if $C = [C_1, \ldots, C_\alpha] \cdot A$ for some codes $C_1, \ldots, C_\alpha$ and a matrix A.

In the rest of this paper, we assume that $A = [a_{ij}]$ is an $\alpha \times \beta$ matrix over $\mathbb{F}_{p^m}$, i.e. $a_{ij} \in \mathbb{F}_{p^m}$ for all i, j. If the rows of A are linearly independent over $\mathbb{F}_{p^m}$, A is called a *full-row-rank* (FRR) matrix. Let A_t be the matrix consisting of the first t rows of A. For $1 \le j_1 < j_2 < \cdots < j_t \le \beta$, we denote by $A(j_1, j_2, \ldots, j_t)$ the $t \times t$ submatrix consisting of the columns $j_1, j_2, \ldots, j_t$ of A_t. If every sub-matrix $A(j_1, j_2, \ldots, j_t)$ of A is non-singular for all $t = 1, \ldots, \alpha$, A is said to be *non-singular by columns* (NSC) (cf. [3, Definition 3.1]).

As a natural generalization of [12, Theorem 1] and results in [16], by [11, Theorem 3.1] we have the following properties of matrix-product codes.

Theorem 2.1 *Let A be an $\alpha \times \beta$ FRR matrix over $\mathbb{F}_{p^m}$, and C_i be a linear (n, M_i, d_i)-code over R for all $i = 1, \ldots, \alpha$. Then the matrix-product code $[C_1, \ldots, C_\alpha] \cdot A$ is a linear $(n\beta, \prod_{i=1}^{\alpha} M_i, d)$-code over R where the minimum Hamming distance d satisfies*

$$d \ge \delta := \min\{\delta_i d_i \mid i = 1, \ldots, \alpha\},$$

where δ_i is the minimum distance of the linear code with length β over $\mathbb{F}_{p^m}$ generated by the first i rows of the matrix A.

Moreover, when the matrix A is NSC, it holds that $\delta_i = \beta - i + 1$. Furthermore, if we assume that the codes C_i form a nested sequence $C_1 \supseteq C_2 \supseteq \cdots \supseteq C_\alpha$, then $d = \delta$.

Then we consider cyclic codes of length n over the finite chain ring $\mathcal{R}_k = R[v]/\langle v^{p^k} - (1 + \omega u)\rangle$, i.e. ideals of the residue class ring $\mathcal{R}_k[x]/\langle x^n - 1\rangle$. Let $\alpha \in \mathcal{R}_k$. By Lemma 1.1 and properties of finite chain rings, α has a unique $(v-1)$-expansion

$$\alpha = \sum_{s=0}^{p^k e-1} a_s (v-1)^s,\ a_s \in \mathbb{F}_{p^m},\ s = 0, 1, \ldots, p^k e - 1.$$

In this paper, we define $\tau : \mathcal{R}_k \to \mathbb{F}_{p^m}$ by

$$\tau(\alpha) = a_0 = \alpha \pmod{v-1},\ \forall \alpha \in \mathcal{R}_k.$$

Then τ is a surjective homomorphism of rings from $\mathcal{R}_k$ onto $\mathbb{F}_{p^m}$. As $u\mathcal{R}_k = (v-1)^{p^k}\mathcal{R}_k$ by Lemma 1.1(ii), there is an invertible element $\varepsilon \in \mathcal{R}_k^\times$ such that $u = (v-1)^{p^k}\varepsilon$, which implies $\tau(u) = 0$. Hence for any $\beta = b_0 + b_1 u + \cdots + b_{e-1}u^{e-1} \in R \subseteq \mathcal{R}_k$ where $b_0, b_1, \ldots, b_{e-1} \in \mathbb{F}_{p^m}$, we have

$$\tau(\beta) = b_0 = \beta \pmod{u}. \tag{1}$$

It is clear that τ can be extended to a surjective homomorphism of polynomial rings from $\mathcal{R}_k[x]$ onto $\mathbb{F}_{p^m}[x]$ by: $\sum \alpha_i x^i \mapsto \sum \tau(\alpha_i)x^i,\ \forall \alpha_i \in \mathcal{R}_k$. We still use τ to denote this homomorphism. Then τ induces a surjective homomorphism of rings from $\mathcal{R}_k[x]/\langle x^n - 1\rangle$ onto $\mathbb{F}_{p^m}[x]/\langle x^n - 1\rangle$ in the natural way

$$\tau\left(\sum_{i=0}^{n-1} \alpha_i x^i\right) = \sum_{i=0}^{n-1} \tau(\alpha_i)x^i,\ \forall \alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in \mathcal{R}_k.$$

Now, let $\mathcal{C}$ be a cyclic code of length n over $\mathcal{R}_k$. For any integer s, $0 \le s \le p^k e - 1$, define

$$(\mathcal{C} : (v-1)^s) = \left\{\alpha(x) \in \mathcal{R}_k[x]/\langle x^n - 1\rangle \mid (v-1)^s \alpha(x) \in \mathcal{C}\right\}$$

which is an ideal of $\mathcal{R}_k[x]/\langle x^n - 1\rangle$ as well. It is clear that

$$\mathcal{C} = (\mathcal{C} : (v-1)^0) \subseteq (\mathcal{C} : (v-1)) \subseteq \cdots (\mathcal{C} : (v-1)^{p^k e-1}). \tag{2}$$

Denote

$$\mathrm{Tor}_s(\mathcal{C}) = \tau(\mathcal{C} : (v-1)^s) = \{\tau(\alpha(x)) \mid \alpha(x) \in (\mathcal{C} : (v-1)^s)\}.$$

Then $\mathrm{Tor}_s(\mathcal{C})$ is an ideal of the ring $\mathbb{F}_{p^m}[x]/\langle x^n-1\rangle$, i.e. a cyclic code of length n over $\mathbb{F}_{p^m}$, which is called the *sth torsion code* of $\mathcal{C}$. Hence there is a unique monic divisor $g_s(x)$ of x^n-1 in $\mathbb{F}_{p^m}[x]$ such that

$$\mathrm{Tor}_s(\mathcal{C}) = \langle g_s(x)\rangle = \{b(x)g_s(x) \mid \deg(b(x)) < n - \deg(g_s(x)),\ b(x) \in \mathbb{F}_{p^m}[x]\},$$

where $g_s(x)$ is the generator polynomial of the cyclic code $\mathrm{Tor}_s(\mathcal{C})$. Hence $|\mathrm{Tor}_s(\mathcal{C})| = p^{m(n-\deg(g_s(x)))}$.

As $g_s(x) \in \mathrm{Tor}_s(\mathcal{C})$, we have $(v-1)^s(g_s(x)-(v-1)b_s(x)) \in \mathcal{C}$ for some $b_s(x) \in \mathcal{R}_k[x]$. Then by $(v-1)^{p^k e}=0$ in $\mathcal{R}_k$, it follows that

$$\begin{aligned}(v-1)^s g_s(x)^{p^k e-s} &= (v-1)^s\left(g_s(x)^{p^k e-s} - (v-1)^{p^k e-s} b_s(x)^{p^k e-s}\right)\\ &= (v-1)^s(g_s(x)-(v-1)b_s(x))\\ &\quad\cdot\left(\sum_{t=0}^{p^k e-s-1} g_s(x)^t\cdot((v-1)b_s(x))^{p^k e-s-1-t}\right).\end{aligned}$$

This implies $(v-1)^s g_s(x)^{p^k e-s} \in \mathcal{C}$. As $\gcd(p,n)=1$, x^n-1 has no repeated divisors in $\mathbb{F}_{p^m}[x]$. This implies $\gcd(x^n-1, g_s(x)^{p^k e-s}) = g_s(x)$. Hence there exist $a(x), b(x) \in \mathbb{F}_{p^m}[x]$ such that $g_s(x) = a(x)g_s(x)^{p^k e-s} + b(x)(x^n-1) = a(x)g_s(x)^{p^k e-s}$ in $\mathcal{R}_k[x]/\langle x^n-1\rangle$. Therefore, we have

$$(v-1)^s g_s(x) = a(x)\cdot(v-1)^s g_s(x)^{p^k e-s} \in \mathcal{C},\ s=0,1,\ldots,p^k e-1. \quad (3)$$

This implies $(v-1)^s\mathrm{Tor}_s(\mathcal{C}) \subseteq \mathcal{C}$ for all $s=0,1,\ldots,p^k e-1$. Moreover, by Eq. (2) we have a tower of cyclic codes over $\mathbb{F}_{p^m}$:

$$\mathrm{Tor}_0(\mathcal{C}) \subseteq \mathrm{Tor}_1(\mathcal{C}) \subseteq \cdots \subseteq \mathrm{Tor}_{p^k e-1}(\mathcal{C}) \subseteq \mathbb{F}_{p^m}[x]/\langle x^n-1\rangle.$$

This implies that $g_{p^k e-1}(x) \mid \cdots \mid g_1(x) \mid g_0(x) \mid (x^n-1)$ in $\mathbb{F}_{p^m}[x]$.

Now, let $c(x) \in \mathcal{C}$. Then $\tau(c(x)) \in \mathrm{Tor}_0(\mathcal{C}) = \langle g_0(x)\rangle$. Hence there exists a unique polynomial $b_0(x) \in \mathbb{F}_{p^m}[x]$ satisfying $\deg(b_0(x)) < n - \deg(g_0(x))$ such that $\tau(c(x)) = b_0(x)g_0(x)$. By Eq. (3), it follows that $b_0(x)g_0(x) \in \mathcal{C}$. Hence $c(x) - b_0(x)g_0(x) \in \mathcal{C}$.

As $\tau(c(x)-b_0(x)g_0(x)) = \tau(c(x)) - b_0(x)g_0(x) = 0$, there exists $\alpha_1(x) \in \mathcal{R}_k[x]/\langle x^n-1\rangle$ such that $(v-1)\alpha_1(x) = c(x) - b_0(x)g_0(x) \in \mathcal{C}$. This implies $\alpha_1(x) \in (\mathcal{C} : (v-1))$, and so $\tau(\alpha_1(x)) \in \mathrm{Tor}_1(\mathcal{C})$.

By $\mathrm{Tor}_1(\mathcal{C}) = \langle g_1(x)\rangle$, there exists a unique polynomial $b_1(x) \in \mathbb{F}_{p^m}[x]$ satisfying $\deg(b_1(x)) < n - \deg(g_1(x))$ such that $\tau(\alpha_1(x)) = b_1(x)g_1(x)$. Then by Eq. (3), it follows that $(v-1)b_1(x)g_1(x) = b_1(x)\cdot(v-1)g_1(x) \in \mathcal{C}$. By $\tau(\alpha_1(x)-b_1(x)g_1(x)) = 0$, there exists $\alpha_2(x) \in \mathcal{R}_k[x]/\langle x^n-1\rangle$ such that $(v-1)\alpha_2(x) = \alpha_1(x) - b_1(x)g_1(x)$ and

$$(v-1)^2\alpha_2(x) = (v-1)\alpha_1(x) - (v-1)b_1(x)g_1(x) \in \mathcal{C}.$$

This implies $\alpha_2(x) \in (\mathcal{C} : (v-1)^2)$, and so $\tau(\alpha_2(x)) \in \mathrm{Tor}_2(\mathcal{C}) = \langle g_2(x)\rangle$.

As stated above, we have

$$\begin{aligned} c(x) &= b_0(x)g_0(x) + (v-1)\alpha_1(x) \\ &= b_0(x)g_0(x) + (v-1)b_1(x)g_1(x) + (v-1)^2\alpha_2(x), \end{aligned}$$

where $c_0(x) = b_0(x)g_0(x) \in \mathrm{Tor}_0(\mathcal{C})$ and $c_1(x) = b_1(x)g_1(x) \in \mathrm{Tor}_1(\mathcal{C})$.

Let $2 \le s \le p^k e - 2$ and assume that there exist $c_i(x) \in \mathrm{Tor}_i(\mathcal{C})$, $i = 0, 1, \ldots, s$, and $\alpha_{s+1}(x) \in \mathcal{R}_k[x]/\langle x^n - 1\rangle$ such that

$$c(x) = \sum_{i=0}^{s} (v-1)^i c_i(x) + (v-1)^{s+1}\alpha_{s+1}(x).$$

Then by $(v-1)^i c_i(x) \in (v-1)^i \mathrm{Tor}_i(\mathcal{C}) \subseteq \mathcal{C}$, it follows that $(v-1)^{s+1}\alpha_{s+1}(x) \in \mathcal{C}$. This implies $\alpha_{s+1}(x) \in (\mathcal{C} : (v-1)^{s+1})$, and so $\tau(\alpha_{s+1}(x)) \in \mathrm{Tor}_{s+1}(\mathcal{C}) = \langle g_{s+1}(x)\rangle$. We denote $c_{s+1}(x) = \tau(\alpha_{s+1}(x))$. Then there exists $\alpha_{s+2}(x) \in \mathcal{R}_k[x]/\langle x^n - 1\rangle$ such that $\alpha_{s+1}(x) = c_{s+1}(x) + (v-1)\alpha_{s+2}(x)$, and hence $(v-1)^{s+1}\alpha_{s+1}(x) = (v-1)^{s+1}c_{s+1}(x) + (v-1)^{s+2}\alpha_{s+2}(x)$. Therefore,

$$c(x) = \sum_{i=0}^{s+1} (v-1)^i c_i(x) + (v-1)^{s+2}\alpha_{s+2}(x).$$

By mathematical induction on s, we conclude the following theorem.

Theorem 2.2 *Using the notations above, we have the following conclusions.*

(i) Let $\mathcal{C}$ be a cyclic code of length n over $\mathcal{R}_k = R[v]/\langle v^{p^k} - (1+\omega u)\rangle$. Then each codeword $c(x)$ in $\mathcal{C}$ has a unique $(v-1)$-adic expansion:

$$c(x) = \sum_{s=0}^{p^k e - 1} (v-1)^s c_s(x), \text{ where } c_s(x) \in \mathrm{Tor}_s(\mathcal{C}),\ \forall s = 0, 1, \ldots, p^k e - 1.$$

Hence $|\mathcal{C}| = \prod_{s=0}^{p^k e-1} |\mathrm{Tor}_s(\mathcal{C})| = p^{m(\sum_{s=0}^{p^k e-1}(n - \deg(g_s(x))))}$.

(ii) $\mathcal{C}$ is a cyclic code of length n over $\mathcal{R}_k$ if and only if there exists uniquely a tower of $p^k e$ cyclic codes with length n over $\mathbb{F}_{p^m}$, $C_0 \subseteq C_1 \subseteq \cdots \subseteq C_{p^k e-1}$, such that $\mathrm{Tor}_s(\mathcal{C}) = \tau(\mathcal{C} : (v-1)^s) = C_s$ for all $s = 0, 1, \ldots, p^k e - 1$. If the latter conditions are satisfied, then

$$\begin{aligned} \mathcal{C} &= \bigoplus_{s=0}^{p^k e-1} (v-1)^s C_s \\ &= \left\langle g_0(x), (v-1)g_1(x), \ldots, (v-1)^{p^k e} g_{p^k e-1}(x) \right\rangle_{\mathcal{R}_k[x]/\langle x^n-1\rangle} \\ &= \left\langle \sum_{s=0}^{p^k e-1} (v-1)^s g_s(x) \right\rangle_{\mathcal{R}_k[x]/\langle x^n-1\rangle} \end{aligned}$$

where $g_s(x) \in \mathbb{F}_{p^m}[x]$ being the generator polynomial of the cyclic code C_s for all $s = 0, 1, \ldots, p^k e - 1$.

Remark For a complete description of simple-root cyclic codes over arbitrary commutative finite chain rings, readers can refer to [15, Theorem 3.5] .

When $k = 0$, we have $\mathcal{R}_0 = R[v]/\langle v - (1 + \omega u)\rangle = R$ satisfying $v - 1 = \omega u$ or $u = \omega^{-1}(v - 1)$. Then from Lemma 1.1, Theorem 2.2 and Eq. (1), we deduce the following corollary which will be used in the following sections.

Corollary 2.3 *Using the notations above, we have the following conclusions.*

(i) Let $\mathcal{C}$ be a cyclic code of length n over $R = \mathbb{F}_{p^m}[u]/\langle u^e\rangle$. Then each codeword $c(x)$ in $\mathcal{C}$ has a unique u-adic expansion:

$$c(x) = \sum_{s=0}^{e-1} u^s c_s(x), \text{ where } c_s(x) \in \mathrm{Tor}_s(\mathcal{C}) = \tau(\mathcal{C} : u^s), \ \forall s = 0, 1, \ldots, e-1.$$

Hence $|\mathcal{C}| = \prod_{s=0}^{e-1} |\mathrm{Tor}_s(\mathcal{C})| = p^{m(\sum_{s=0}^{e-1}(n - \deg(g_s(x))))}$.

(ii) $\mathcal{C}$ is a cyclic code of length n over R if and only if there exists uniquely a tower of e cyclic codes with length n over $\mathbb{F}_{p^m}$, $C_0 \subseteq C_1 \subseteq \cdots \subseteq C_{e-1}$, such that $\mathrm{Tor}_s(\mathcal{C}) = C_s$ for all $s = 0, 1, \ldots, e-1$. If the latter conditions are satisfied, then $\mathcal{C} = \bigoplus_{s=0}^{e-1} u^s C_s$ and $|\mathcal{C}| = \prod_{i=0}^{e-1} |C_i|$. Furthermore, we have

$$\mathcal{C} = \left\langle g_0(x), ug_1(x), \ldots, u^{e-1}g_{e-1}(x)\right\rangle_{R[x]/\langle x^n-1\rangle} = \left\langle \sum_{s=0}^{e-1} u^s g_s(x)\right\rangle_{R[x]/\langle x^n-1\rangle}$$

where $g_s(x) \in \mathbb{F}_{p^m}[x]$ being the generator polynomial of the cyclic code C_s for all $s = 0, 1, \ldots, e-1$.

(iii) Let $\mathcal{C}$ and $\mathcal{C}'$ be cyclic codes of length n over R with $C_s = \mathrm{Tor}_s(\mathcal{C})$ and $C'_s = \mathrm{Tor}_s(\mathcal{C}')$ for all s. Then $\mathcal{C} \subseteq \mathcal{C}'$ if and only if $C_s \subseteq C'_s$ as ideals of the ring $\mathbb{F}_{p^m}[x]/\langle x^n - 1\rangle$ for all $s = 0, 1, \ldots, e-1$.

Proof We only need to prove (iii). If $C_s \subseteq C'_s$ for all $s = 0, 1, \ldots, e-1$, it is obvious that $\mathcal{C} = \bigoplus_{s=0}^{e-1} u^s C_s \subseteq \bigoplus_{s=0}^{e-1} u^s C'_s = \mathcal{C}'$.

Conversely, let $\mathcal{C} \subseteq \mathcal{C}'$. Then $(\mathcal{C} : u^s) \subseteq (\mathcal{C}' : u^s)$ for all s. From this, by $\mathrm{Tor}_s(\mathcal{C}) = \tau(\mathcal{C} : u^s)$ and $\mathrm{Tor}_s(\mathcal{C}') = \tau(\mathcal{C}' : u^s)$ we deduce that $C_s \subseteq C'_s$ for all $s = 0, 1, \ldots, e-1$. □

3 Matrix-product structure of $(1 + \omega u)$-constacyclic codes over R

Denote $[n) \times [p^k) = \{(j, t) \mid j \in [n), \ t \in [p^k)\}$. Then each integer $i \in [p^k n) = \{0, 1, \ldots, p^k n - 1\}$ can be uniquely expressed as

$$i = j + tn, \text{ were } j \equiv i \pmod n, \ j \in [n), \text{ and } t = \frac{i - j}{n} \in [p^k). \tag{4}$$

In this paper, we adopt the following notations.

Notation 3.1 Let l be the smallest positive integer such that $p^l \geq e$. Since $\gcd(p, n) = 1$, there exists a unique integer n', $1 \leq n' \leq p^{k+l} - 1$, such that

$$n'n \equiv 1 \pmod{p^{k+l}}. \tag{5}$$

We write $n' = qp^k + n''$, where $0 \leq q \leq p^l - 1$ and $1 \leq n'' \leq p^k - 1$ satisfying $\gcd(p, n'') = 1$. Then we define a transformation ϱ on the set $[p^k n)$ by

$$\varrho(j + \lambda n) = j + n\left(\lambda - jn'' \pmod{p^k}\right),\ \forall (j, \lambda) \in [n) \times [p^k),$$

and denote

$$\Lambda = \mathrm{diag}[1, (1 + \omega u)^q, (1 + \omega u)^{2q}, \ldots, (1 + \omega u)^{(n-1)q}]$$

which is a diagonal matrix of order n with $1, (1 + \omega u)^q, (1 + \omega u)^{2q}, \ldots, (1 + \omega u)^{(n-1)q} \in R^\times$ as its diagonal entries.

Lemma 3.2 *(i) The transformation ϱ is a permutation on the set $[p^k n)$.*
(ii) Let $P_{p^k n}$ be a matrix of order $p^k n$ defined by $P_{p^k n} = [\epsilon_{i,j}]$ where

$$\epsilon_{i,j} = 1 \text{ if } j = \varrho(i), \text{ and } \epsilon_{i,j} = 0 \text{ otherwise, for all } 0 \leq i, j \leq p^k n - 1,$$

and set $M_{p^k}(n, \omega) = \mathrm{diag}[\overbrace{\Lambda, \ldots, \Lambda}^{(p^k)\cdot \mathrm{s}}] \cdot P_{p^k n}$. Then $P_{p^k n}$ is a permutation matrix and $M_{p^k}(n, \omega)$ is a monomial matrix over R of order $p^k n$.
(iii) Define a transformation Θ on the R-module $R^{p^k n}$ by

$$\Theta(\xi) = M_{p^k}(n, \omega) \cdot \xi,\ \forall \xi = \begin{bmatrix} a_0 \\ a_1 \\ \cdots \\ a_{p^k n - 1} \end{bmatrix} \in R^{p^k n}.$$

Then Θ is an R-module automorphism on $R^{p^k n}$. Let C be an R-submodule of $R^{p^k n}$ and denote $\Theta(C) = M_{p^k}(n, \omega) \cdot C = \{M_{p^k}(n, \omega) \cdot c \mid c \in C\}$. Then $\Theta(C)$ and C are monomially equivalent linear codes of length $p^k n$ over R.

Proof (i) For any $(j, \lambda) \in [n) \times [p^k)$, let $t = \lambda - jn'' \pmod{p^k}$. Then by Equation (4) and $(j, t) = (j, \lambda)\begin{bmatrix} 1 & -n'' \\ 0 & 1 \end{bmatrix}$, we see that $\varrho : j + \lambda n \mapsto j + tn$ $(\forall (j, \lambda) \in [n) \times [p^k))$ is a a permutation on the set $[p^k n)$.
(ii) follows from (i) and Notation 3.1, and (iii) follows from (ii).

□

First, we establish an explicit relationship between the set of all $(1+\omega u)$-constacyclic codes of length $p^k n$ over the finite chain ring $R = \mathbb{F}_{p^m}[u]/\langle u^e\rangle$ and the set of all cyclic codes of length n over the finite chain ring $\mathcal{R}_k$.

Let $a(x) \in R[x]/\langle x^{p^k n} - (1+\omega u)\rangle$. By Eq. (4), $a(x)$ can be uniquely expressed as $a(x) = \sum_{j=0}^{n-1}\sum_{t=0}^{p^k-1} a_{j+tn}x^{j+tn}$, where $a_0, a_1, \ldots, a_{p^k n-1} \in R$. We will identify $a(x)$ with the column vector $[a_0, a_1, \ldots, a_{p^k n-1}]^{\mathrm{tr}} \in R^{p^k n}$ in this paper. By $x^{j+tn} = x^j(x^n)^t$, we can write $a(x)$ as a product of matrices

$$a(x) = [1, x, x^2, \ldots, x^{n-1}]M_{a(x)}X \tag{6}$$

where $X = [1, x^n, x^{2n}, \ldots, x^{(p^k-1)n}]^{\mathrm{tr}}$ is the transpose of the $1 \times p^k$ matrix $[1, x^n, x^{2n}, \ldots, x^{(p^k-1)n}]$ and $M_{a(x)} = \begin{bmatrix} a_0 & a_{0+n} & \cdots & a_{0+(p^k-1)n} \\ a_1 & a_{1+n} & \cdots & a_{1+(p^k-1)n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n-1} & a_{n-1+n} & \cdots & a_{n-1+(p^k-1)n} \end{bmatrix}$.

Set $v = x^n$ in Eq. (6). We obtain

$$a(x) = [1, x, x^2, \ldots, x^{n-1}]M_{a(x)}V.$$

where $V = [1, v, v^2, \ldots, v^{p^k-1}]^{\mathrm{tr}}$ is the transpose of the $1 \times p^k$ matrix $[1, v, v^2, \ldots, v^{p^k-1}]$. We define a map $\varphi : R[x]/\langle x^{p^k n} - (1+\omega u)\rangle \to \mathcal{R}_k/\langle x^n - v\rangle$ by

$$\varphi(a(x)) = [1, x, x^2, \ldots, x^{n-1}]\left(M_{a(x)}V\right) = \alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1}x^{n-1}$$

where $[\alpha_0, \alpha_1, \ldots, \alpha_{n-1}] = \left(M_{a(x)}V\right)^{\mathrm{tr}} \in \mathcal{R}_k^n$. Then from $\mathcal{R}_k = R[v]\langle v^{p^k} - (1+\omega u)\rangle$ and $R[x]/\langle x^{p^k n} - (1+\omega u)\rangle = R[x, v]/\langle v^{p^k} - (1+\omega u), x^n - v\rangle$ as residue class rings, we deduce the following conclusion.

Lemma 3.3 *The map φ is an isomorphism of rings from $R[x]/\langle x^{p^k n} - (1+\omega u)\rangle$ onto $\mathcal{R}_k/\langle x^n - v\rangle$.*

By Notation 3.1, we have $p^l \geq e$. From this, by $v^{p^k} = x^{p^k n} = 1 + \omega u$ and $u^e = 0$ in $\mathcal{R}_k$ we deduce that

$$v^{p^{k+l}} = (1+\omega u)^{p^l} = 1 + \omega^{p^l}u^{p^l} = 1 + \omega^{p^l}u^{p^l-e}u^e = 1.$$

Then by Eq. (5), it follows that $(v^{n'})^n = v^{n'n} = v$. Now, we define an automorphism of the polynomial ring $\mathcal{R}_k[x]$ by $\psi(\beta(x)) = \beta(v^{n'}x)$ $(\forall \beta(x) \in \mathcal{R}_k[x])$. Since $\psi(x^n - v) = (v^{n'}x)^n - v = v(x^n - 1)$ and $v \in \mathcal{R}_k^{\times}$, ψ induces an ring isomorphism of residue class rings from $\mathcal{R}_k[x]/\langle x^n - v\rangle$ onto $\mathcal{R}_k[x]/\langle x^n - 1\rangle$:

$$\alpha(x) \mapsto \alpha(v^{n'}x) = [1, x, \ldots, x^{n-1}]\mathrm{diag}(1, v^{n'}, \ldots, (v^{n'})^{n-1})[\alpha_0, \alpha_1, \ldots, \alpha_{n-1}]^{\mathrm{tr}}$$

for any $\alpha(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1}x^{n-1} \in \mathcal{R}_k[x]/\langle x^n - v\rangle$. We will still use ψ to denote this ring isomorphism. Hence $\psi(\alpha(x)) = \alpha(v^{n'}x)$ for all $\alpha(x) \in \mathcal{R}_k[x]/\langle x^n - v\rangle$. Then by Lemma 3.3, we conclude the following conclusion.

Lemma 3.4 *Using the notations above, the map $\psi\varphi$ define by*

$$\psi\varphi(a(x)) = [1, x, \ldots, x^{n-1}]\mathrm{diag}(1, v^{n'}, \ldots, (v^{n'})^{n-1})M_{a(x)}V$$

$(\forall a(x) \in R[x]/\langle x^{p^k n} - (1+\omega u)\rangle)$ is an isomorphism of rings from $R[x]/\langle x^{p^k n} - (1+\omega u)\rangle$ onto $\mathcal{R}_k[x]/\langle x^n - 1\rangle$. Therefore, C is a $(1+\omega u)$-constacyclic code of length $p^k n$ over R if and only if $\psi(\varphi(C))$ is a cyclic code of length n over $\mathcal{R}_k$.

Then by Lemma 3.4 and Theorem 2.2, we give a matrix-product structure of any $(1 + \omega u)$-constacyclic code of length $p^k n$ over R as follows.

Theorem 3.5 *Using the notations above, let C be a $(1 + \omega u)$-constacyclic code of length $p^k n$ over R, assume $\mathcal{C} = \psi(\varphi(C)) \subseteq \mathcal{R}_k[x]/\langle x^n - 1\rangle$ and $C_s = \mathrm{Tor}_s(\mathcal{C}) \subseteq \mathbb{F}_{p^m}[x]/\langle x^n - 1\rangle$ for all $s = 0, 1, \ldots, p^k e - 1$. Denote*

$$\mathcal{C}_\rho = \bigoplus_{i=0}^{e-1} u^i C_{ip^k+\rho} \subseteq R[x]/\langle x^n - 1\rangle,\ \rho = 0, 1, \ldots, p^k - 1.$$

(i) $\mathcal{C}_\rho$ is a cyclic code of length n over R satisfying $|\mathcal{C}_\rho| = \prod_{i=0}^{e-1} |C_{ip^k+\rho}|$ for all $\rho = 0, 1, \ldots, p^k - 1$. Moreover, we have that $\mathcal{C}_{p^k-1} \supseteq \cdots \supseteq \mathcal{C}_1 \supseteq \mathcal{C}_0$.

(ii) $\Theta(C) = M_{p^k}(n, \omega) \cdot C = [\mathcal{C}_{p^k-1}, \mathcal{C}_{p^k-2}, \ldots, \mathcal{C}_1, \mathcal{C}_0] \cdot A_{p^k}$, where

$$A_{p^k} = \left[(-1)^{p^k-i-j+1}\binom{p^k - i}{j-1}\right]_{1\le i,j\le p^k} \pmod p$$

in which we set $\binom{p^k - i}{j-1} = 0$ if $p^k - i < j - 1$ for all $1 \le i, j \le p^k$. Hence C is monomially equivalent to $[\mathcal{C}_{p^k-1}, \mathcal{C}_{p^k-2}, \ldots, \mathcal{C}_1, \mathcal{C}_0] \cdot A_{p^k}$.

Proof (i) By Theorem 2.2, C_s is a cyclic code of length n over $\mathbb{F}_{p^m}$, $0 \le s \le p^k e - 1$, and satisfies

$$C_0 \subseteq C_1 \subseteq \cdots \subseteq C_{p^k-1} \subseteq C_{p^k} \subseteq C_{p^k+1} \subseteq \cdots \subseteq C_{2p^k-1}$$
$$\subseteq \cdots \subseteq C_{(e-1)p^k} \subseteq C_{(e-1)p^k+1} \subseteq \cdots \subseteq C_{ep^k-1}.$$

This implies $C_\rho \subseteq C_{p^k+\rho} \subseteq \cdots \subseteq C_{(e-1)p^k+\rho}$. From this and by Corollary 2.3(ii), we deduce that $\mathcal{C}_\rho = \bigoplus_{i=0}^{e-1} u^i C_{ip^k+\rho}$ is a cyclic code of length n over R, i.e. an ideal of the ring $R[x]/\langle x^n - 1\rangle$, satisfying $|\mathcal{C}_\rho| = \prod_{i=0}^{e-1} |C_{ip^k+\rho}|$.

Let $0 \le \rho < \rho' \le e - 1$. Then $C_{ip^k+\rho} \subseteq C_{ip^k+\rho'}$ for all $i = 0, 1, \ldots, e - 1$. From this and by Corollary 2.3(iii), we deduce that $\mathcal{C}_\rho \subseteq \mathcal{C}_{\rho'}$.

(ii) As $\omega \in R^\times$, for each integer i, $0 \le i \le e-1$, $(\omega u)^i = \omega^i u^i$ can be uniquely expressed as $(\omega u)^i = \sum_{j=i}^{e-1} \lambda_{i,j} u^j$ for some $\lambda_{i,j} \in \mathbb{F}_{p^m}$ where $\lambda_{i,i} \neq 0, \forall j = i, i+1, \ldots, e-1$. Then we can write

$$\begin{bmatrix} 1 \\ \omega u \\ (\omega u)^2 \\ \cdots \\ (\omega u)^{e-1} \end{bmatrix} = TU \text{ with } U = [1, u, u^2, \ldots, u^{e-1}]^{\text{tr}} = \begin{bmatrix} 1 \\ u \\ u^2 \\ \cdots \\ u^{e-1} \end{bmatrix}, \quad (7)$$

where $T = \begin{bmatrix} \lambda_{0,0} & \lambda_{0,1} & \ldots & \lambda_{0,e-2} & \lambda_{0,e-1} \\ 0 & \lambda_{1,1} & \ldots & \lambda_{1,e-2} & \lambda_{1,e-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \lambda_{e-2,e-2} & \lambda_{e-2,e-1} \\ 0 & 0 & \ldots & 0 & \lambda_{e-1,e-1} \end{bmatrix}$ being an invertible $e \times e$ matrix over $\mathbb{F}_{p^m}$ (and R). By Theorem 2.2, we know that

$$\mathcal{C} = \psi\varphi(C) = C_0 \oplus (v-1)C_1 \oplus (v-1)^2 C_2 \oplus \cdots \oplus (v-1)^{p^k e-1} C_{p^k e-1}.$$

Let $a(x) = \sum_{j=0}^{n-1} \sum_{t=0}^{p^k-1} a_{j+tn} x^{j+tn} \in C$ where $a_{j+tn} \in R$, and assume $c(x) = \psi\varphi(a(x)) \in \mathcal{C}$. Then for each integer s, $0 \le s \le p^k e - 1$, there exists a unique codeword $c_s(x) \in C_s$ such that $c(x) = \sum_{s=0}^{p^k e-1} (v-1)^s c_s(x)$. By $(v-1)^{p^k} = \omega u$, we have $(v-1)^{ip^k} = (\omega u)^i$, for all $0 \le i \le e-1$. Hence

$$c(x) = \sum_{i=0}^{e-1} \sum_{\rho=0}^{p^k-1} (v-1)^{ip^k+\rho} c_{ip^k+\rho}(x) = \sum_{\rho=0}^{p^k-1} (v-1)^\rho \sum_{i=0}^{e-1} (\omega u)^i c_{ip^k+\rho}(x) \quad (8)$$

in which

$$\begin{aligned} \sum_{i=0}^{e-1} (\omega u)^i c_{ip^k+\rho}(x) &= [c_\rho(x), c_{p^k+\rho}(x), \ldots, c_{p^k(e-1)+\rho}(x)] \begin{bmatrix} 1 \\ \omega u \\ (\omega u)^2 \\ \cdots \\ (\omega u)^{e-1} \end{bmatrix} \\ &= [c_\rho(x), c_{p^k+\rho}(x), \ldots, c_{p^k(e-1)+\rho}(x)] TU \end{aligned}$$

by Equation (7). Let $0 \le \rho \le p^k - 1$. We denote the cartesian product of the e cyclic codes $C_\rho, C_{p^k+\rho}, \ldots, C_{p^k(e-1)+\rho}$ with length n over $\mathbb{F}_{p^m}$ by $\mathcal{S}_\rho$, i.e.

$$\mathcal{S}_\rho = C_\rho \times C_{p^k+\rho} \times C_{2p^k+\rho} \times \cdots \times C_{p^k(e-1)+\rho}.$$

For any $[c_\rho(x), c_{p^k+\rho}(x), \ldots, c_{p^k(e-1)+\rho}(x)] \in \mathcal{S}_\rho$, we denote

$$[c'_\rho(x), c'_{p^k+\rho}(x), \ldots, c'_{p^k(e-1)+\rho}(x)] = [c_\rho(x), c_{p^k+\rho}(x), \ldots, c_{p^k(e-1)+\rho}(x)]T$$

where

$$c'_{jp^k+\rho}(x) = \lambda_{0,j}c_\rho(x) + \lambda_{1,j}c_{p^k+\rho}(x) + \lambda_{2,j}c_{2p^k+\rho}(x) + \cdots + \lambda_{j,j}c_{jp^k+\rho}(x)$$

for all $j = 0, 1, \ldots, e-1$. By $C_\rho \subseteq C_{p^k+\rho} \subseteq C_{2p^k+\rho} \subseteq \cdots \subseteq C_{jp^k+\rho}$, it follows that

$$c'_{jp^k+\rho}(x) \in C_{jp^k+\rho},\ \forall j,\ 0 \le j \le e-1,$$

and hence $[c'_\rho(x), c'_{p^k+\rho}(x), \ldots, c'_{p^k(e-1)+\rho}(x)] \in \mathcal{S}_\rho$. From this and by the invertibility of the matrix T, we deduce that the map defined by

$$\xi \mapsto \xi \cdot T \quad (\forall \xi = [c_\rho(x), c_{p^k+\rho}(x), \ldots, c_{p^k(e-1)+\rho}(x)] \in \mathcal{S}_\rho)$$

is a bijection on $\mathcal{S}_\rho$. This implies $\mathcal{S}_\rho = \{\xi \cdot T \mid \xi \in \mathcal{S}_\rho\}$. Using the notations above, we have

$$\begin{aligned}
&\sum_{i=0}^{e-1}(\omega u)^i c_{ip^k+\rho}(x)\\
&\quad = [c'_\rho(x), c'_{p^k+\rho}(x), c'_{2p^k+\rho}(x), \ldots, c'_{p^k(e-1)+\rho}(x)]U\\
&\quad = c'_\rho(x) + uc'_{p^k+\rho}(x) + u^2c'_{2p^k+\rho}(x) + \cdots + u^{e-1}c'_{(e-1)p^k+\rho}(x) \in \mathcal{C}_\rho,
\end{aligned}$$

where

$$\mathcal{C}_\rho = C_\rho \oplus uC_{p^k+\rho} \oplus u^2C_{2p^k+\rho} \oplus \cdots \oplus u^{e-1}C_{p^k(e-1)+\rho} \subseteq R[x]/\langle x^n - 1\rangle.$$

Now, denote $\xi_\rho(x) = \sum_{i=0}^{e-1}(\omega u)^i c_{ip^k+\rho}(x) \in \mathcal{C}_\rho$ for all $\rho = 0, 1, \ldots, p^k - 1$. Then $c(x) = \sum_{\rho=0}^{p^k-1}(v-1)^\rho \xi_\rho(x)$. From this, by Eq. (8) and

$$(v-1)^{p^k-i} = ((-1)+v)^{p^k-i} = \sum_{j=1}^{p^k-i+1}\binom{p^k-i}{j-1}(-1)^{p^k-i-j+1}v^{j-1}$$

for all $i = 1, 2, \ldots, p^k$, we deduce that

$$c(x) = [1, x, \ldots, x^{n-1}][\xi_{p^k-1}, \ldots, \xi_1, \xi_0]A_{p^k}V, \tag{9}$$

where ξ_ρ is the unique $n \times 1$ column vector over R satisfying

$$\xi_\rho(x) = [1, x, \ldots, x^{n-1}] \cdot \xi_\rho,\ 0 \le \rho \le p^k - 1,$$

and $V = [1, v, v^2, \ldots, v^{p^k-1}]^{\mathrm{tr}}$. From now on, we will identify $\xi_\rho(x)$ with ξ_ρ as a codeword in the cyclic code $\mathcal{C}_\rho$ over R of length n. By replacing v with x^n in Eq. (9) we obtain

$$\pi(c(x)) = [1, x, \ldots, x^{n-1}][\xi_{p^k-1}, \ldots, \xi_1, \xi_0]A_{p^k}X \tag{10}$$

where $X = [1, x^n, \ldots, x^{(p^k-1)n}]^{\mathrm{tr}}$.

On the other hand, by Lemma 3.4 we have

$$c(x) = \psi\varphi(a(x)) = [1, x, \ldots, x^{n-1}]\mathrm{diag}(1, v^{n'}, \ldots, (v^{n'})^{n-1})M_{a(x)}V.$$

Replacing v with x^n, we obtain

$$\begin{aligned}\pi(c(x)) &= [1, x, \ldots, x^{n-1}]\mathrm{diag}(1, (x^n)^{n'}, (x^n)^{2n'}, \ldots, (x^n)^{(n-1)n'})M_{a(x)}X \\ &= [1, x^{1+n'n}, x^{2(1+n'n)}, \ldots, x^{(n-1)(1+n'n)}]M_{a(x)}X \\ &= \sum_{j=0}^{n-1}\sum_{t=0}^{p^k-1} a_{j+tn}x^{j(1+n'n)+tn} \\ &= \sum_{j=0}^{n-1}\sum_{t=0}^{p^k-1} a_{j+tn}x^{j+(t+jn')n}.\end{aligned}$$

By Notation 3.1, we have $n' = qp^k + n''$, where $0 \le q \le p^l - 1$ and $1 \le n'' \le p^k - 1$. By $x^{p^k n} = 1 + \omega u$ in the ring $R[x]/\langle x^{p^k n} - (1 + \omega u)\rangle$ it follows that

$$a_{j+tn}x^{j+(t+jn')n} = x^{jq\cdot p^k n}a_{j+tn}x^{j+(t+jn'')n} = (1+\omega u)^{jq}a_{j+tn}x^{j+(t+jn'')n}.$$

We denote $\lambda = t + jn'' \pmod{p^k}$. Then $\lambda \in [p^k)$ and $t = \lambda - jn'' \pmod{p^k}$. By Notation 3.1 and Lemma 3.2, the map ϱ defined by $\varrho(j + \lambda n) = j + tn = j + n\left(\lambda - jn'' \pmod{p^k}\right)$ $(\forall(j, \lambda) \in [n) \times [p^k))$ is a permutation on the set $[p^k n)$. This implies

$$\pi(c(x)) = \sum_{j=0}^{n-1}\sum_{\lambda=0}^{p^k-1}(1+\omega u)^{jq}a_{\varrho(j+\lambda n)}x^{j+\lambda n} = [1, x, \ldots, x^{n-1}]\Lambda\widetilde{M}_{a(x)}X \tag{11}$$

where $\Lambda = \mathrm{diag}[1, (1+\omega u)^q, (1+\omega u)^{2q}, \ldots, (1+\omega u)^{(n-1)q}]$ and

$$\widetilde{M}_{a(x)} = [b_{j,\lambda}] \text{ with } b_{j,\lambda} = a_{\varrho(j+\lambda n)},\ \forall(j, \lambda) \in [n) \times [p^k).$$

Now, from Eqs. (10) and (11) we deduces that

$$\Lambda \cdot \widetilde{M}_{a(x)} = [\xi_{p^k-1}, \ldots, \xi_1, \xi_0]A_{p^k},\ \forall a(x) \in C.$$

In this paper, we regard $\Lambda \cdot \widetilde{M}_{a(x)}$ and $[\xi_{p^k-1}, \ldots, \xi_1, \xi_0]A_{p^k}$ as a column vector of dimension $p^k n$ by reading the entries of the matrix in column-major order respectively. According to this view, by Lemma 3.2 it follows that

$$M_{p^k}(n, \omega) \cdot [a_0, a_1, \ldots, a_{p^k n-1}]^{\mathrm{tr}} = [\xi_{p^k-1}, \ldots, \xi_1, \xi_0]A_{p^k}, \forall a(x) \in C.$$

As stated above, we conclude that $\Theta(C) = [\mathcal{C}_{p^k-1}, \mathcal{C}_{p^k-2}, \ldots, \mathcal{C}_1, \mathcal{C}_0] \cdot A_{p^k}$. By Lemma 3.2(iii), C and the matrix-product code $[\mathcal{C}_{p^k-1}, \ldots, \mathcal{C}_1, \mathcal{C}_0] \cdot A_{p^k}$ are monomially equivalent codes over the finite chain ring R.

□

From Lemma 3.2 and the proof of Theorem 3.5, we deduce the following corollary which will be used in the next section.

Corollary 3.6 *Let $C \subseteq R^{p^k n}$. Then C is a $(1+\omega u)$-constacyclic code of length $p^k n$ over R if and only if there is a sequence of cyclic codes $\mathcal{C}_{p^k-1} \supseteq \cdots \supseteq \mathcal{C}_1 \supseteq \mathcal{C}_0$ over R of length n such that*

$$M_{p^k}(n,\omega) \cdot C := \{M_{p^k}(n,\omega) \cdot c \mid c \in C\} = [\mathcal{C}_{p^k-1}, \ldots, \mathcal{C}_1, \mathcal{C}_0] \cdot A_{p^k},$$

where we regard each $c \in C$ as a $p^k n \times 1$ column vector over R and each codeword $\xi = [\xi_{p^k-1}, \ldots, \xi_1, \xi_0] A_{p^k}$ in $[\mathcal{C}_{p^k-1}, \ldots, \mathcal{C}_1, \mathcal{C}_0] \cdot A_{p^k}$ as a $p^k n \times 1$ column vector over R by reading the entries of the matrix ξ in column-major order, respectively.

As $\gcd(p,n) = 1$, there are pairwise coprime monic irreducible polynomials $f_1(x), f_2(x), \ldots, f_r(x)$ in $\mathbb{F}_{p^m}[x]$ such that $x^n - 1 = f_1(x) f_2(x) \ldots f_r(x)$.

Lemma 3.7 (cf. [4, Theorem 3.4]) *Using the notations above, all $(p^k e + 1)^r$ distinct $(1+\omega u)$-constacyclic codes of length $p^k n$ over R are given by*

$$C_{(i_1,i_2,\ldots,i_r)} = \langle f_1(x)^{i_1} f_2(x)^{i_2} \ldots f_r(x)^{i_r} \rangle \subseteq R[x]/\langle x^{p^k n} - (1+\omega u) \rangle,$$

where $0 \le i_1, i_2, \ldots, i_r \le p^k e$. Furthermore, the number of codewords in $C_{(i_1,i_2,\ldots,i_r)}$ is equal to $|C_{(i_1,i_2,\ldots,i_r)}| = p^{m(\sum_{t=1}^{r}(p^k e - i_t)\deg(f_t(x)))}$.

Finally, we determine the nested sequences of p^k cyclic codes $\mathcal{C}_{p^k-1} \supseteq \cdots \supseteq \mathcal{C}_1 \supseteq \mathcal{C}_0$ with length n over R in the matrix-product structure of a $(1+\omega u)$-constacyclic code $C_{(i_1,i_2,\ldots,i_r)}$ over R with length $p^k n$.

Theorem 3.8 *Using the notations above, let $C = \langle f_1(x)^{i_1} f_2(x)^{i_2} \ldots f_r(x)^{i_r} \rangle$, $0 \le i_1, i_2, \ldots, i_r \le p^k e$, being a $(1+\omega u)$-constacyclic code C of length $p^k n$ over R. For each integer s, $0 \le s \le p^k e - 1$, denote*

$$g_s(x) = \prod_{i_t > s, 1 \le t \le r} f_t(x) \in \mathbb{F}_{p^m}[x].$$

Then C is monomially equivalent to $[\mathcal{C}_{p^k-1}, \ldots, \mathcal{C}_1, \mathcal{C}_0] \cdot A_{p^k}$, where A_{p^k} is given by Theorem 3.5 and for each integer ρ, $0 \le \rho \le p^k - 1$, $\mathcal{C}_\rho$ is a cyclic code of length n over R given by

$$\begin{aligned} \mathcal{C}_\rho &= \left\langle g_\rho(x), u g_{p^k+\rho}(x), u^2 g_{2p^k+\rho}(x), \ldots, u^{e-1} g_{(e-1)p^k+\rho}(x) \right\rangle \\ &= \left\langle g_\rho(x) + u g_{p^k+\rho}(x) + u^2 g_{2p^k+\rho}(x) + \cdots + u^{e-1} g_{(e-1)p^k+\rho}(x) \right\rangle. \end{aligned}$$

Proof Denote $G(x) = f_1(x)^{i_1} f_2(x)^{i_2} \ldots f_r(x)^{i_r} \in \mathbb{F}_{p^m}[x]$. By Theorem 3.5, it is suffices to prove that $C_s = \langle g_s(x) \rangle$ for all $s = 0, 1, \ldots, p^k e - 1$. Let $0 \le s \le p^k e - 1$. We first verify that

$$g_s(x) \in C_s = \mathrm{Tor}_s(\psi(\varphi(C))) = \tau(\psi(\varphi(C)) : (v-1)^s),$$

which is equivalent to that $(v-1)^s (g_s(x) + (v-1)w(x)) \in \psi(\varphi(C))$ for some $w(x) \in \mathcal{R}_k[x]/\langle x^n - 1 \rangle$. In the following, we denote

$$A_s = \{t \mid i_t > s,\ 1 \le t \le r\},\ B_s = \{t \mid i_t \le s,\ 1 \le t \le r\}.$$

and set

$$h_s(x) = \prod_{t \in B_s} f_t(x),\ \widehat{f_s}(x) = \prod_{t \in A_s} f_t(x)^{i_t - s - 1}.$$

Then $g_s(x) = \prod_{t \in A_s} f_t(x)$, and $h_s(x), \widehat{f_s}(x) \in \mathbb{F}_{p^m}[x]$ satisfying $x^n - 1 = g_s(x)h_s(x)$, $\gcd(g_s(x), h_s(x)) = \gcd(\widehat{f_s}(x), h_s(x)) = 1$.

As $G(x) = \prod_{t \in A_s \cup B_s} f_t(x)^{i_t}$ and $i_t \le s$ for all $t \in B_s$, we have

$$(x^n - 1)^s g_s(x) \widehat{f_s}(x) = \prod_{t \in A_s \cup B_s} f_t(x)^s \prod_{t \in A_s} f_t(x) \prod_{t \in A_s} f_t(x)^{i_t - s - 1} = \varepsilon(x) G(x)$$

where $\varepsilon(x) = \prod_{t \in B_s} f_t(x)^{s - i_t} \in \mathbb{F}_{p^m}[x] \subseteq R[x]$. This implies

$$(x^n - 1)^s g_s(x) \widehat{f_s}(x) \in \langle G(x) \rangle = C. \tag{12}$$

By $\gcd(\widehat{f_s}(x), h_s(x)) = 1$, there exist $a(x), b(x) \in \mathbb{F}_{p^m}[x]$ such that $a(x)\widehat{f_s}(x) + b(x)h_s(x) = 1$. This implies $a(x)\widehat{f_s}(x) = 1 - b(x)h_s(x)$. Then by Eq. (12) and $x^n - 1 = g_s(x)h_s(x)$, it follows that

$$\begin{aligned}
&(x^n - 1)^s g_s(x) - (x^n - 1)^{s+1} b(x) \\
&= (x^n - 1)^s g_s(x) - (x^n - 1)^s \cdot g_s(x)h_s(x) \cdot b(x) \\
&= (x^n - 1)^s g_s(x)(1 - b(x)h_s(x)) \\
&= (x^n - 1)^s g_s(x) \widehat{f_s}(x) \cdot a(x) \in C.
\end{aligned}$$

Replacing x^n with v, by the definition of φ we obtain

$$\begin{aligned}
&(v-1)^s g_s(x) - (v-1)^{s+1} \varphi(b(x)) \\
&= \varphi\left((x^n - 1)^s g_s(x) - (x^n - 1)^{s+1} b(x)\right) \in \varphi(C).
\end{aligned}$$

This implies $(v-1)^s g_s(x) + (v-1)^{s+1}\alpha(x) \in \varphi(C)$, where $\alpha(x) = -\varphi(b(x)) \in \mathcal{R}_k[x]/\langle x^n - v \rangle$. Then we replace x with $v^{n'}x$, by the definition of ψ we have

$$\begin{aligned}&(v-1)^s g_s(v^{n'}x) + (v-1)^{s+1}\alpha(v^{n'}x)\\ &\quad = \psi\left((v-1)^s g_s(x) + (v-1)^{s+1}\alpha(x)\right) \in \psi(\varphi(C)).\end{aligned}$$

From this and by

$$g_s(v^{n'}x) = g_s(x + x(v^{n'}-1)) = g_s(x + (v-1)\beta(x)) = g_s(x) + (v-1)\delta(x)$$

for some $\delta(x) \in \mathcal{R}_k[x]/\langle x^n - 1\rangle$, where $\beta(x) = x\sum_{i=0}^{n'-1} v^i$, we deduce that

$$\begin{aligned}&(v-1)^s g_s(v^{n'}x) + (v-1)^{s+1}\alpha(v^{n'}x)\\ &\quad = (v-1)^s\left(g_s(x) + (v-1)\delta(x)\right) + (v-1)^{s+1}\alpha(v^{n'}x)\\ &\quad = (v-1)^s\left(g_s(x) + (v-1)(\delta(x) + \alpha(v^{n'}x))\right).\end{aligned}$$

This implies $g_s(x) + (v-1)(\delta(x) + \alpha(v^{n'}x)) \in (\psi(\varphi(C)) : (v-1)^s)$, and hence

$$g_s(x) = \tau\left(g_s(x) + (v-1)(\delta(x) + \alpha(v^{n'}x))\right) \in \tau(\psi(\varphi(C)) : (v-1)^s) = C_s.$$

Therefore, $\langle g_s(x)\rangle \subseteq C_s$ as ideals of the ring $\mathbb{F}_{p^m}[x]/\langle x^n - 1\rangle$ for all $s = 0, 1, \ldots, p^k e - 1$.

On the other hand, by $x^n - 1 = \prod_{t=1}^{r} f_t(x)$ and $G(x) = \prod_{t=1}^{r} f_t(x)^{i_t} = \prod_{s=0}^{p^k e-1} g_s(x)$ it follows that

$$\sum_{t=1}^{r}(p^k e - i_t)\deg(f_t(x)) = p^k en - \deg(G(x)) = \sum_{s=0}^{p^k e-1}(n - \deg(g_s(x))). \quad (13)$$

By Lemma 3.7, Theorem 2.2 and $|\langle g_s(x)\rangle| = p^{m(n-\deg(g_s(x)))}$ for all s, we have

$$\begin{aligned}p^{m(\sum_{t=1}^{r}(p^k e-i_t)\deg(f_t(x)))} &= |C| = |\psi(\varphi(C))| = \prod_{s=0}^{p^k e-1}|C_s|\\ &\geq \prod_{s=0}^{p^k e-1}|\langle g_s(x)\rangle| = \prod_{s=0}^{p^k e-1}(p^m)^{n-\deg(g_s(x))}.\end{aligned}$$

From this and by Eq. (13), we deduce that $C_s = \langle g_s(x)\rangle$, i.e. $g_s(x)$ is the generator polynomial of C_s for all s.

Finally, let $0 \leq \rho \leq p^k - 1$. By Corollary 2.3(ii), it follows that $\mathcal{C}_\rho = \bigoplus_{i=0}^{e-1} u^i C_{ip^k+\rho} = \langle g_\rho(x) + ug_{p^k+\rho}(x) + u^2 g_{2p^k+\rho}(x) + \cdots + u^{e-1}g_{p^k(e-1)+\rho}(x)\rangle$ as ideals of $R[x]/\langle x^n - 1\rangle$. □

Remark As $\mathcal{C}_{p^k-1} \supseteq \cdots \supseteq \mathcal{C}_1 \supseteq \mathcal{C}_0$, by Theorem 2.1 the minimum Hamming distance of the $(1+\omega u)$-constacyclic code C of length $p^k n$ over R is equal to $d = \min\{\delta_{i+1} d_i \mid i = 0, 1, \ldots, p^k - 1\}$, where d_i is the minimum Hamming distance of the cyclic code $\mathcal{C}_i$ of length n over R and δ_{i+1} is the minimum distance of the linear code $\mathcal{L}_{i+1}$ with length p^k over $\mathbb{F}_{p^m}$ generated by the first $i+1$ rows of the matrix A_{p^k}, for all $i = 0, 1, \ldots, p^k - 1$. For each integer $1 \le j \le p^k$, it can be easily seen that $\mathcal{L}_j$ is exactly the cyclic code of length p^k over $\mathbb{F}_{p^m}$ generated by $(x-1)^{p^k-j}$. Since $a(x) \mapsto a(-x)$ $(\forall a(x) \in \mathbb{F}_{p^m}[x]/\langle x^{p^k} - 1\rangle)$ is a ring isomorphism and a Hamming distance-preserving map from $\mathbb{F}_{p^m}[x]/\langle x^{p^k} - 1\rangle$ onto $\mathbb{F}_{p^m}[x]/\langle x^{p^k} + 1\rangle$, δ_j is equal to the minimum Hamming distance of the negacyclic code of length p^k over $\mathbb{F}_{p^m}$ generated by $(x+1)^{p^k-j}$. From this and by Dinh [9] Theorem 4.11, we deduce that

$$\delta_j = \begin{cases} (t+1)p^s, & \text{if } p^{k-s} - tp^{k-s-1} \le j \le p^{k-s} - tp^{k-s-1} + p^{k-s-1} - 1, \\ & \text{where } 1 \le t \le p-1 \text{ and } 1 \le s \le k-1; \\ \gamma + 1, & \text{if } p^k - \gamma p^{k-1} \le j \le p^k - \gamma p^{k-1} + p^{k-1} - 1, \\ & \text{where } 1 \le \gamma \le p-1; \\ 1, & \text{if } j = p^k. \end{cases}$$

4 Iterative construction of $(1+\omega u)$-constacyclic codes over R

Let $A = [a_{ij}]_{1\le i,j\le m}$ and $B = [b_{st}]_{1\le s,t\le n}$ be $m \times m$ and $n \times n$ matrices over a commutative ring Γ, respectively. The *Kronecker product* of A and B is defined by $A \otimes B = [a_{ij}B]_{1\le i,j\le m} = \begin{bmatrix} a_{11}B & a_{12}B & \ldots & a_{1m}B \\ a_{21}B & a_{22}B & \ldots & a_{2m}B \\ \ldots & \ldots & \ldots & \ldots \\ a_{m1}B & a_{m2}B & \ldots & a_{mm}B \end{bmatrix}$ where $a_{ij}B = \begin{bmatrix} a_{ij}b_{11} & a_{ij}b_{12} & \ldots & a_{ij}b_{1n} \\ a_{ij}b_{21} & a_{ij}b_{22} & \ldots & a_{ij}b_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{ij}b_{n1} & a_{ij}b_{n2} & \ldots & a_{ij}b_{nn} \end{bmatrix}$, $i, j = 1, \ldots, m$. It is known from linear algebra that if A, B, C, D are matrix of appropriate sizes, then $(A \otimes B) \otimes C = A \otimes (B \otimes C)$ and $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$.

Using the notation in Theorem 3.5, we know that

$$A_{p^k} = \left[(-1)^{p^k-i-j+1}\binom{p^k - i}{j-1}\right]_{1\le i,j\le p^k} \pmod p, \ \forall k \ge 1.$$

Especially, $A_p = \left[(-1)^{p-i-j+1}\binom{p-i}{j-1}\right]_{1\le i,j\le p} \pmod p$, i.e.

$$A_p = \begin{bmatrix} (-1)^{p-1} & (-1)^{p-2}\binom{p-1}{p-2} & \dots & (-1)^2\binom{p-1}{2} & -\binom{p-1}{1} & 1 \\ (-1)^{p-2} & (-1)^{p-3}\binom{p-2}{p-3} & \dots & -\binom{p-2}{1} & 1 & 0 \\ (-1)^{p-3} & (-1)^{p-4}\binom{p-3}{p-4} & \dots & 1 & 0 & 0 \\ -1 & 1 & \dots & 0 & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 & 0 \end{bmatrix}$$

(mod p). As p is prime, by induction on j it follows that $\binom{p-i}{j-1} \not\equiv 0 \pmod{p}$, i.e. $\binom{p-i}{j-1} \in \mathbb{F}_{p^m}^{\times}$, for all integers i, j satisfying $i + j \leq p + 1$. Moreover, by [17, Proposition 1 and Lemma 3] we know the following conclusions.

Lemma 4.1 *(i) The matrix A_p is an NSC matrix over $\mathbb{F}_{p^m}$.*

(ii) $A_{p^k} = A_p \otimes A_{p^{k-1}} = \left[(-1)^{p-i-j+1}\binom{p-i}{j-1} A_{p^{k-1}}\right]_{1\leq i,j\leq p} \pmod{p}$ *for any integer $k \geq 2$.*

Every $(1 + \omega u)$-constacyclic code of length $p^k n$ over $R = \mathbb{F}_{p^m}[u]/\langle u^e\rangle$ can be constructed recursively from $(1 + \omega u)$-constacyclic codes of length $p^{k-1}n$ over R by the following theorem.

Theorem 4.2 *Let C be a $(1 + \omega u)$-constacyclic code of length $p^k n$ over R. Then there exist $(1 + \omega u)$-constacyclic codes $C^{(p-1)}, \dots, C^{(1)}, C^{(0)}$ of length $p^{k-1}n$ over R satisfying $C^{(p-1)} \supseteq \cdots \supseteq C^{(1)} \supseteq C^{(0)}$ such that C is monomially equivalent to the following matrix-product code over R*

$$[C^{(p-1)}, \dots, C^{(1)}, C^{(0)}] \cdot A_p.$$

Specifically, if $C = \langle f_1(x)^{i_1} f_2(x)^{i_2} \dots f_r(x)^{i_r}\rangle$ as an ideal of $R[x]/\langle x^{p^k n} - (1+\omega u)\rangle$, where $0 \leq i_1, i_2, \dots, i_r \leq p^k e$, then

$$C^{(j)} = \left\langle \prod_{\lambda=0}^{e-1} \prod_{l=0}^{p^{k-1}-1} \prod_{i_t > \lambda p^k + j p^{k-1} + l,\ 1\leq t\leq r} f_t(x) \right\rangle_{R[x]/\langle x^{p^{k-1}n} - (1+\omega u)\rangle} \tag{14}$$

for all $j = 0, 1, \dots, p - 1$. Furthermore, the minimum Hamming distance of C is equal to $\min\{pd^{(p-1)}, (p - 1)d^{(p-2)}, \dots, 2d^{(1)}, d^{(0)}\}$ where $d^{(j)}$ is the minimum Hamming distance of $C^{(j)}$ for all $j = 0, 1, \dots, p - 1$.

Proof Let C be a $(1 + \omega u)$-constacyclic code of length $p^k n$ over R. By Theorem 3.5 and Lemma 4.1(ii), there are p^k cyclic codes $\mathcal{D}_{p^k-1}, \cdots, \mathcal{D}_1, \mathcal{D}_0$ of length n over R satisfying $\mathcal{D}_{p^k-1} \supseteq \cdots \supseteq \mathcal{D}_1 \supseteq \mathcal{D}_0$ such that C is monomially equivalent to the following matrix-product code

$$
\begin{aligned}
&[\mathcal{D}_{p^k-1},\ldots,\mathcal{D}_1,\mathcal{D}_0]\cdot A_{p^k}\\
&\quad=\big[\mathcal{D}_{(p-1)p^{k-1}+p^{k-1}-1},\ldots,\mathcal{D}_{(p-1)p^{k-1}+1},\mathcal{D}_{(p-1)p^{k-1}},\ldots,\mathcal{D}_{p^{k-1}-1},\\
&\qquad\ldots,\mathcal{D}_1,\mathcal{D}_0\big]\cdot\left[(-1)^{p-1-s-t}\binom{p-s}{t-1}A_{p^{k-1}}\right]_{1\le s,t\le p}\pmod p\\
&\quad=[\mathcal{D}^{(p-1)},\ldots,\mathcal{D}^{(1)},\mathcal{D}^{(0)}]\cdot A_p,
\end{aligned}
$$

where $\mathcal{D}^{(j)}=[\mathcal{D}_{jp^{k-1}+p^{k-1}-1},\mathcal{D}_{jp^{k-1}+p^{k-1}-2},\ldots,\mathcal{D}_{jp^{k-1}+1},\mathcal{D}_{jp^{k-1}}]\cdot A_{p^{k-1}}$ for all $j=0,1,\ldots,p-1$. By Theorem 3.5, $\mathcal{D}^{(j)}$ is monomially equivalent to a $(1+\omega u)$-constacyclic code $C^{(j)}$ of length $p^{k-1}n$ over R for all $j=0,1,\ldots,p-1$. Then by Corollary 3.6 and Notation 3.1, there is a fixed $p^{k-1}n\times p^{k-1}n$ monomial matrix $M_{p^{k-1}}(n,\omega)$ over R such that $M_{p^{k-1}}(n,\omega)\cdot C^{(j)}=\mathcal{D}^{(j)}$ for all j. This implies

$$
\begin{aligned}
&[\mathcal{D}^{(p-1)},\ldots,\mathcal{D}^{(1)},\mathcal{D}^{(0)}]\cdot A_p\\
&\quad=[M_{p^{k-1}}(n,\omega)\cdot C^{(p-1)},\ldots,M_{p^{k-1}}(n,\omega)\cdot C^{(1)},M_{p^{k-1}}(n,\omega)\cdot C^{(0)}]\cdot A_p\\
&\quad=\big(I_p\otimes M_{p^{k-1}}(n,\omega)\big)\cdot\Big([C^{(p-1)},\ldots,C^{(1)},C^{(0)}]\cdot A_p\Big)
\end{aligned}
$$

in which we regard $[C^{(p-1)},\ldots,C^{(1)},C^{(0)}]\cdot A_p$ as a $p^kn\times 1$ column vector over R by reading the entries of the matrix in column-major order, and I_p is the identity matrix of order p. Since

$$
I_p\otimes M_{p^{k-1}}(n,\omega)=\operatorname{diag}(M_{p^{k-1}}(n,\omega),\ldots,M_{p^{k-1}}(n,\omega))
$$

is a $p^kn\times p^kn$ monomial matrix over R, $[\mathcal{D}^{(p-1)},\ldots,\mathcal{D}^{(1)},\mathcal{D}^{(0)}]\cdot A_p$ is monomially equivalent to $[C^{(p-1)},\ldots,C^{(1)},C^{(0)}]\cdot A_p$. Moreover, by

$$
\mathcal{D}_{jp^{k-1}+s}\supseteq\mathcal{D}_{ip^{k-1}+s},\ \forall i,j,s,\ \ p-1\ge j>i\ge 0,\ \ s=0,1,\ldots,p^{k-1}-1
$$

we conclude that $\mathcal{D}^{(j)}\supseteq\mathcal{D}^{(i)}$. This implies $C^{(j)}\supseteq C^{(i)}$ for all $0\le i\le j\le p-1$.

Since $C=\langle f_1(x)^{i_1}f_2(x)^{i_2}\ldots f_r(x)^{i_r}\rangle$ which is an ideal of $R[x]/\langle x^{p^kn}-(1+\omega u)\rangle$, in the matrix-product code $[\mathcal{D}_{p^k-1},\ldots,\mathcal{D}_1,\mathcal{D}_0]\cdot A_{p^k}$ we have $\mathcal{D}_\rho=\big\langle g_\rho(x),ug_{p^k+\rho}(x),u^2g_{2p^k+\rho}(x),\ldots,u^{e-1}g_{(e-1)p^k+\rho}(x)\big\rangle\subseteq R[x]/\langle x^n-1\rangle$ for all $\rho=0,1,\ldots,p^k-1$. By Theorem 3.8, we see that $g_s(x)=\prod_{i_t>s,1\le t\le r}f_t(x)\in\mathbb{F}_{p^m}[x]$, $0\le s\le p^ke-1$, satisfying $f_1(x)^{i_1}f_2(x)^{i_2}\ldots f_r(x)^{i_r}=\prod_{s=0}^{p^ke-1}g_s(x)=\prod_{\eta=0}^{p^k-1}\prod_{\lambda=0}^{e-1}g_{\lambda p^k+\eta}(x)$. Let $0\le j\le p-1$. Using Theorem 3.8 for the code $\mathcal{D}^{(j)}=[\mathcal{D}_{jp^{k-1}+p^{k-1}-1},\mathcal{D}_{jp^{k-1}+p^{k-1}-2},\ldots,\mathcal{D}_{jp^{k-1}+1},\mathcal{D}_{jp^{k-1}}]\cdot A_{p^{k-1}}$, we deduce that $\mathcal{D}^{(j)}$ is monomially equivalent to the $(1+\omega u)$-constacyclic code $C^{(j)}$ of length $p^{k-1}n$ over R generated by the following polynomial

$$
G^{(j)}(x)=\prod_{l=0}^{p^{k-1}-1}\prod_{\lambda=0}^{e-1}g_{\lambda p^k+jp^{k-1}+l}(x)=\prod_{\lambda=0}^{e-1}\prod_{l=0}^{p^{k-1}-1}\prod_{i_t>\lambda p^k+jp^{k-1}+l,\ 1\le t\le r}f_t(x).
$$

Hence $C^{(j)} = \langle G^{(j)}(x)\rangle$ as ideals of $R[x]/\langle x^{p^{k-1}n} - (1+\omega u)\rangle$.

Finally, the conclusion for minimum Hamming distance of C follows from Theorem 2.1 and Lemma 4.1(i) immediately. □

Remark Let $k = 0$. As $\gcd(p, n) = 1$ and $(1+\omega u)^{p^l} = 1$ by $p^l \geq e$ and $u^e = 0$ in R, there is uniquely $\eta \in R^\times$ such that $\eta^n = 1 + \omega u$. This implies $(\eta x)^n = (1 + \omega u)x^n$. Hence the map $\tau : a(x) \mapsto a(\eta x)$ $(\forall a(x) \in R[x]/\langle x^n - 1\rangle)$ is an isomorphism of rings from $R[x]/\langle x^n - 1\rangle$ onto $R[x]/\langle x^n - (1 + \omega u)\rangle$. Therefore, C is a $(1 + \omega u)$-constacyclic code of length n over R if and only if there is a unique cyclic code D of length n over R such that $\tau(D) = C$. Obviously, D and $\tau(D)$ are monomially equivalent codes over R.

5 An example

In this section, we explain the main results of the paper by considering $(1 + u)$-constacyclic codes of length 90 over $R = \mathbb{F}_3 + u\mathbb{F}_3$ $(u^2 = 0)$. In this case, we have $p = 3, m = 1, e = 2, k = 2, \omega = 1 \in R^\times$ and $n = 10$.

Using Notation 3.1, by $3^1 > e$ we have $l = 1$, $p^{k+l} = 3^{2+1} = 27$, and $n' = 19$ satisfying $1 \leq n' \leq 26$ and $n'n = 190 \equiv 1 \pmod{27}$. Obviously, $n' = qp^k + n''$ where $p^k = 9$, $q = 2$ and $n'' = 1$. Hence the permutation ϱ on the set $[90) = \{0, 1, \ldots, 89\}$ is defined by

$$\varrho(j + 10\lambda) = j + 10(\lambda - j \bmod 9),$$

for all $0 \leq j \leq 9$ and $0 \leq \lambda \leq 8$. Precisely, we have

$$\varrho = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 \\ 0 & 81 & 72 & 63 & 54 & 45 & 36 & 27 & 18 & 9 & 10 & 1 & 82 & 73 & 64 & 55 & 46 & 37 & 28 & 19 \\ 20 & 21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 & 29 & \ldots & 80 & 81 & 82 & 83 & 83 & 85 & 86 & 87 & 88 & 89 \\ 20 & 11 & 2 & 83 & 74 & 65 & 56 & 47 & 38 & 29 & \ldots & 80 & 71 & 62 & 53 & 44 & 35 & 26 & 17 & 8 & 89 \end{pmatrix}.$$

By $(1+u)^2 = 1+2u$, it follows that $\Lambda = \mathrm{diag}[1, 1+2u, (1+2u)^2, \ldots, (1+2u)^9]$. As $(1+u)^3 = 1$, we have

$$\Lambda = \begin{bmatrix} 1 & & & \\ & \Omega & & \\ & & \Omega & \\ & & & \Omega \end{bmatrix} \text{ where } \Omega = \begin{bmatrix} 1+2u & & \\ & 1+u & \\ & & 1 \end{bmatrix}.$$

Let $P_{90} = [\epsilon_{i,j}]$ be the 90×90 permutation matrix defined by: $\epsilon_{i,j} = 1$ if $j = \varrho(i)$, and $\epsilon_{i,j} = 0$ othwise, for all $0 \leq i, j \leq 89$, and set

$$M_9(10, 1) = \mathrm{diag}[\overbrace{\Lambda, \ldots, \Lambda}^{9\cdot s}] \cdot P_{90}.$$

By Lemma 3.2, we see that $M_9(10, 1)$ is a 90×90 monomial matrix over R, and

$$\Theta(\begin{bmatrix} a_0 \\ a_1 \\ \cdots \\ a_{89} \end{bmatrix}) = M_9(10, 1) \begin{bmatrix} a_0 \\ a_1 \\ \cdots \\ a_{89} \end{bmatrix}, \ \forall a_i \in R, \ i = 0, 1, \ldots, 89.$$

defines an R-module automorphism on R^{90}. By Corollary 3.6, we know that C is a $(1 + u)$-constacyclic code of length 90 over R if and only if there is a sequence $\mathcal{C}_8 \supseteq \cdots \supseteq \mathcal{C}_1 \supseteq \mathcal{C}_0$ of cyclic codes of length 10 over R such that

$$\Theta(C) = \{\Theta(c) \mid c \in C\} = [\mathcal{C}_8, \mathcal{C}_7, \mathcal{C}_6, \mathcal{C}_5, \mathcal{C}_5, \mathcal{C}_4, \mathcal{C}_3, \mathcal{C}_2, \mathcal{C}_1, \mathcal{C}_0] \cdot A_9.$$

Obviously, we have that $x^{10} - 1 = f_1(x) f_2(x) f_3(x) f_4(x)$ where $f_1(x) = x + 1$, $f_2(x) = x+2$, $f_3(x) = x^4+x^3+x^2+x+1$ and $f_4(x) = x^4+2x^3+x^2+2x+1$ being irreducible polynomials in $\mathbb{F}_3[x]$. By Lemma 3.7, the number of $(1+u)$-constacyclic codes with length 90 over R is $(3^2 \cdot 2 + 1)^4 = 130321$ and all these codes are given by:

$$C_{(i_1,i_2,i_3,i_4)} = \left\langle f_1(x)^{i_1} f_2(x)^{i_2} f_3(x)^{i_3} f_4(x)^{i_4} \right\rangle_{R[x]/\langle x^{90}-(1+u)\rangle}$$

where $0 \le i_1, i_2, i_3, i_4 \le 18$. The number of codewords in $C_{(i_1,i_2,i_3,i_4)}$ is equal to $|C_{(i_1,i_2,i_3,i_4)}| = 3^{(18-i_1)+(18-i_2)+4(18-i_3)+4(18-i_4)} = 3^{180-(i_1+i_2+4i_3+4i_4)}$.

Now, we consider $C = C_{(7,2,18,15)} = \langle f_1(x)^7 f_2(x)^2 f_3(x)^{18} f_4(x)^{15} \rangle$. In this case, $(i_1, i_2, i_3, i_4) = (7, 2, 18, 15)$, and hence $|C| = 3^{180-(7+2+4\cdot 18+4\cdot 15)} = 3^{39}$.

Using the notations of Theorem 3.8, we have $g_s(x) = \prod_{i_t > s, 1 \le t \le 4} f_t(x) \in \mathbb{F}_3[x]$ for all $s = 0, 1, \ldots, 17$. Specifically, we have

$$\begin{aligned}
g_0(x) &= g_1(x) = f_1(x) f_2(x) f_3(x) f_4(x) = x^{10} - 1, \\
g_2(x) &= g_3(x) = g_4(x) = g_5(x) = g_6(x) = f_1(x) f_3(x) \\
f_4(x) &= x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \\
g_7(x) &= g_8(x) = g_9(x) = g_{10}(x) = g_{11}(x) = g_{12}(x) = g_{13}(x) = g_{14}(x) \\
&= f_3(x) f_4(x) = x^8 + x^6 + x^4 + x^2 + 1, \\
g_{15}(x) &= g_{16}(x) = g_{17}(x) = f_3(x).
\end{aligned}$$

• By Theorem 3.5, we have that $\Theta(C) = [\mathcal{C}_8, \mathcal{C}_7, \mathcal{C}_6, \mathcal{C}_5, \mathcal{C}_4, \mathcal{C}_3, \mathcal{C}_2, \mathcal{C}_1, \mathcal{C}_0] \cdot A_9$ and C is monomially equivalent to the matrix-product code $[\mathcal{C}_8, \ldots, \mathcal{C}_1, \mathcal{C}_0] \cdot A_9$, where each $\mathcal{C}_\rho$ is a cyclic code of length 10 over R given by

$$\begin{aligned}
\mathcal{C}_8 &= \mathcal{C}_7 = \langle g_8(x) + u g_{9+8}(x) \rangle = \langle f_3(x) f_4(x) + u f_3(x) \rangle, \\
\mathcal{C}_6 &= \langle g_6(x) + u g_{9+6}(x) \rangle = \langle f_1(x) f_3(x) f_4(x) + u f_3(x) \rangle, \\
\mathcal{C}_5 &= \mathcal{C}_4 = \mathcal{C}_3 = \mathcal{C}_2 = \langle g_5(x) + u g_{9+5}(x) \rangle = \langle f_1(x) f_3(x) f_4(x) + u f_3(x) f_4(x) \rangle, \\
\mathcal{C}_1 &= \mathcal{C}_0 = \langle g_1(x) + u g_{9+1}(x) \rangle = \langle u f_3(x) f_4(x) \rangle
\end{aligned}$$

and $A_9 = A_3 \otimes A_3 = \begin{bmatrix} A_3 & A_3 & A_3 \\ 2A_3 & A_3 & 0 \\ A_3 & 0 & 0 \end{bmatrix} \pmod 3$ with $A_3 = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$. Let d_i be the minimum Hamming distance of the cyclic code $\mathcal{C}_i$ with length 10 over R. Then $d_8 = d_7 = 2$, $d_6 = 2$, $d_2 = d_3 = d_4 = d_5 = 5$ and $d_1 = d_0 = 5$.

• By Theorem 4.2, C is monomially equivalent to the matrix-product code $[C^{(2)}, C^{(1)}, C^{(0)}] \cdot A_3$ where $C^{(j)} = \langle G^{(j)}(x) \rangle$ is a $(1+u)$-constacyclic code of length 30 over R, i.e. an ideal of the ring $R[x]/\langle x^{30} - (1+u) \rangle$, generated by the polynomial $G^{(j)}(x) = \prod_{\lambda=0,1} \prod_{l=0}^{2} \prod_{i_t > 9\lambda + 3j + l,\ 1 \le t \le 4} f_t(x) \in \mathbb{F}_3[x]$. Specifically, we have

$$\begin{aligned}
G^{(2)}(x) &= \prod_{i_t>6,\ 1\le t\le 4} f_t(x) \prod_{i_t>7,\ 1\le t\le 4} f_t(x) \prod_{i_t>8,\ 1\le t\le 4} f_t(x) \\
&\quad \cdot \prod_{i_t>15,\ 1\le t\le 4} f_t(x) \prod_{i_t>16,\ 1\le t\le 4} f_t(x) \prod_{i_t>17,\ 1\le t\le 4} f_t(x) \\
&= f_1(x) f_3(x) f_4(x) \cdot f_3(x) f_4(x) \cdot f_3(x) f_4(x) \cdot f_3(x)^3 \\
&= f_1(x) f_3(x)^6 f_4(x)^3, \\
G^{(1)}(x) &= \prod_{i_t>3,\ 1\le t\le 4} f_t(x) \prod_{i_t>4,\ 1\le t\le 4} f_t(x) \prod_{i_t>5,\ 1\le t\le 4} f_t(x) \\
&\quad \cdot \prod_{i_t>12,\ 1\le t\le 4} f_t(x) \prod_{i_t>13,\ 1\le t\le 4} f_t(x) \prod_{i_t>14,\ 1\le t\le 4} f_t(x) \\
&= (f_1(x) f_3(x) f_4(x))^3 \cdot (f_3(x) f_4(x))^3 \\
&= f_1(x)^3 f_3(x)^6 f_4(x)^6, \\
G^{(0)}(x) &= \prod_{i_t>0,\ 1\le t\le 4} f_t(x) \prod_{i_t>1,\ 1\le t\le 4} f_t(x) \prod_{i_t>2,\ 1\le t\le 4} f_t(x) \\
&\quad \cdot \prod_{i_t>9,\ 1\le t\le 4} f_t(x) \prod_{i_t>10,\ 1\le t\le 4} f_t(x) \prod_{i_t>11,\ 1\le t\le 4} f_t(x) \\
&= (f_1(x) f_2(x) f_3(x) f_4(x))^2 \cdot f_1(x) f_3(x) f_4(x) \cdot (f_3(x) f_4(x))^3 \\
&= f_1(x)^3 f_2(x)^2 f_3(x)^6 f_4(x)^6.
\end{aligned}$$

Hence $C^{(2)} = \langle f_1(x) f_3(x)^6 f_4(x)^3 \rangle$, $C^{(1)} = \langle f_1(x)^3 f_3(x)^6 f_4(x)^6 \rangle$ and $C^{(0)} = \langle f_1(x)^3 f_2(x)^2 f_3(x)^6 f_4(x)^6 \rangle$. By Lemma 3.7, we have $|C^{(2)}| = 3^{60-(1+4\cdot6+4\cdot3)} = 3^{23}$, $|C^{(1)}| = 3^{60-(3+4\cdot6+4\cdot6)} = 3^9$, $|C^{(0)}| = 3^{60-(3+2+4\cdot6+4\cdot6)} = 3^7$. Moreover, from the proof of Theorem 4.2 we deduce the following conclusions:

- $C^{(2)}$ is monomially equivalent to $[\mathcal{C}_8, \mathcal{C}_7, \mathcal{C}_6] \cdot A_3$.
- $C^{(1)}$ is monomially equivalent to $[\mathcal{C}_5, \mathcal{C}_4, \mathcal{C}_3] \cdot A_3$.
- $C^{(0)}$ is monomially equivalent to $[\mathcal{C}_2, \mathcal{C}_1, \mathcal{C}_0] \cdot A_3$.

Let $d^{(j)}$ be the minimum Hamming distance of $C^{(j)}$ for $j = 0, 1, 2$. Since A_3 is NSC, by Theorems 4.2 and 2.1 it follows that $d^{(2)} = \min\{3d_8, 2d_7, d_6\} = 2$, $d^{(1)} = \min\{3d_5, 2d_4, d_3\} = 5$ and $d^{(0)} = \min\{3d_2, 2d_1, d_0\} = 5$.

By Theorem 2.1, the minimum Hamming distance of $C = C_{(7,2,18,15)}$ is equal to $d = \min\{3d^{(2)}, 2d^{(1)}, d^{(0)}\} = 5$.

6 Conclusion

For any positive integers m, e and a prime number p, denote $R = \mathbb{F}_{p^m}[u]/\langle u^e\rangle$ which is a finite chain ring. Let $\omega \in R^\times$, k and n be positive integers satisfying $\gcd(p, n) = 1$. We prove that any $(1 + \omega u)$-constacyclic code of length $p^k n$ over R is monomially equivalent to a matrix-product code of a nested sequence of p^k cyclic codes with length n over R and a $p^k \times p^k$ matrix A_{p^k} over $\mathbb{F}_p$. Then we give an iterative construction of every $(1 + \omega u)$-constacyclic code by $(1 + \omega u)$-constacyclic codes of shorter lengths over R. The next work is to rediscover new properties for minimum distance of the codes by use of their matrix-product structures.

Acknowledgements Part of this work was done when Yonglin Cao was visiting Chern Institute of Mathematics, Nankai University, Tianjin, China. Yonglin Cao would like to thank the institution for the kind hospitality. This research is supported in part by the National Natural Science Foundation of China (Grant Nos. 11671235, 61571243, 11471255).

References

1. Abualrub, T., Siap, I.: Constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$. J. Frankl. Inst. **346**, 520–529 (2009)
2. Blackford, T.: Negacyclic codes over Z_4 of even length. IEEE Trans. Inf. Theory **49**, 1417–1424 (2003)
3. Blockmore, T., Norton, G.H.: Matrix-product codes over $\mathbb{F}_q$. Appl. Algebra Eng. Commun. Comput. **12**, 477–500 (2001)
4. Cao, Y.: On constacyclic codes over finite chain rings. Finite Fields Appl. **24**, 124–135 (2013)
5. Cao, Y., Cao, Y., Fu, F.-W.: Cyclic codes over $\mathbb{F}_{2^m}[u]/\langle u^k\rangle$ of oddly even length. Appl. Algebra Eng. Commun. Comput. **27**, 259–277 (2016)
6. Cao, Y., Cao, Y., Dong, L.: Complete classification of $(\delta + \alpha u^2)$-constacyclic codes over $\mathbb{F}_{3^m}[u]/\langle u^4\rangle$ of length $3n$. Appl. Algebra Eng. Commun. Comput. **29**, 13–39 (2018)
7. Cao, Y., Cao, Y.: The Gray image of constacyclic codes over the finite chain ring $F_{p^m}[u]/\langle u^k\rangle$. J. Appl. Math. Comput. (2017). https://doi.org/10.1007/s12190-017-1107-2
8. Cao, Y., Cao, Y., Dinh, H. Q., Fu, F-W., Gao, J., Sriboonchitta, S.: Constacyclic codes of length np^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, https://www.researchgate.net/publication/320734899, October 2017. Accepted for publication in Adv. Math. Commun.
9. Dinh, H.Q.: On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions. Finite Fields Appl. **14**, 22–40 (2008)
10. Dinh, H.Q., Dhompongsa, S., Sriboonchitta, S.: Repeated-root constacyclic codes of prime power length over $\frac{\mathbb{F}_{p^m}[u]}{\langle u^a\rangle}$ and their duals. Discrete Math. **339**, 1706–1715 (2016)
11. Fan, Y., Ling, S., Liu, H.: Matrix product codes over finite commutative Frobenius rings. Des. Codes Cryptogr. **71**, 201–227 (2014)
12. Hernando, F., Lally, K., Ruano, D.: Construction and decoding of matrix-product codes from nested codes. Appl. Algebra Eng. Commun. Comput. **20**, 497–507 (2009)
13. Huffman, W.C., Pless, V.: Fundamentals of Error Correcting Codes. Cambridge University Press, Cambridge (2003)
14. Kai, X., Zhu, S., Li, P.: $(1 + \lambda u)$-constacyclic codes over $\mathbb{F}_p[u]/\langle u^k\rangle$. J. Frankl. Inst. **347**, 751–762 (2010)
15. Norton, G., Sălăgean-Mandache, A.: On the structure of linear and cyclic codes over finite chain rings. Appl. Algebra Eng. Commun. Comput. **10**, 489–506 (2000)
16. Özbudak, F., Stichtenoth, H.: Note on Niederreiter–Xing's propagation rule for linear codes. Appl. Algebra Eng. Commun. Comput. **13**, 53–56 (2002)
17. Sobhani, R.: Matrix-product structure of repeated-root cyclic codes over finite fields. Finite Fields Appl. **39**, 216–232 (2016)