Computational and Applied Mathematics (2026) 45:246
https://doi.org/10.1007/s40314-026-03635-2

PIR Schemes from *n*D-Cyclic and *n*D-Constacyclic Codes and Their Monomial Equivalence

Markus Grassl[1] · Burcu Ecem Karakaş[2] · Ferruh Özbudak[3] · Buket Özkaya[2]

Received: 28 March 2025 / Revised: 12 December 2025 / Accepted: 6 January 2026

Abstract
Private Information Retrieval (PIR) scheme aims to retrieve data from a database without revealing any details about the identity of the data. The PIR scheme for coded storage systems with colluding servers gives a better PIR rate when the storage code and retrieval code have transitive automorphism groups. In this work, we study the transitivity of nD-cyclic codes and then PIR schemes from them together with several examples of nD-cyclic codes with better PIR rates. Then, we show the monomial equivalence between nD-cyclic codes and certain nD-constacyclic codes, which can be used as an alternative family of transitive codes.

Keywords Private information retrieval · Tansitive codes · nD-cyclic codes · nD-constacyclic codes

MSC subject classifications: 68P20 · 68P30 · 94B15 · 94B60

1 Introduction

Private Information Retrieval (PIR) allows data to be retrieved from a database without revealing the identity of the data items. The PIR rate is defined as the ratio of the information gained to the information downloaded, while upload costs are typically ignored. In modern distributed storage systems, communication between servers is necessary to recover data in case of node failure. Therefore, it is common for PIR schemes to assume that servers may collude, meaning they share information about their interaction with the user. The most

✉ Buket Özkaya
ozkayab@metu.edu.tr

Markus Grassl
markus.grassl@ug.edu.pl

Burcu Ecem Karakaş
burcuey@metu.edu.tr

Ferruh Özbudak
ferruh.ozbudak@sabanciuniv.edu

[1] International Centre for Theory of Quantum Technologies, University of Gdańsk, Gdańsk, Poland

[2] Institute of Applied Mathematics, Middle East Technical University, Ankara, Türkiye

[3] FENS, Faculty of Engineering and Natural Sciences, Sabancı University, Istanbul, Türkiye

Published online: 03 February 2026

common collusion model is t-collusion, where it is assumed that any subset of servers of size t can collude. The corresponding PIR scheme is called a t-private information retrieval scheme (Freij-Hollanti et al. 2018).

Throughout the paper, let q be a prime power and let $\mathbb{F}_q$ be the finite field with q elements. Let $\mathcal{C}$ and $\mathcal{D}$ be two linear codes over $\mathbb{F}_q$. Here, $\mathcal{C}$ is the storage code which is an $[n, k, d_\mathcal{C}]_q$ code with $k \times n$ generator matrix $G_\mathcal{C}$ and minimum distance $d_\mathcal{C}$. The retrieval code $\mathcal{D}$ has parameters $[n, k', d_\mathcal{D}]_q$.

In order to fix notation, in the following we describe the basic setup for a PIR scheme (for more details, see, *e. g.*, Freij-Hollanti et al. (2018)). Assume that there are n servers and M files, and that the user wants to download the w^{th} file.

Data Storage

This is the first step of PIR. The files are given by $x^{[1]}, \ldots, x^{[M]} \in \mathbb{F}_q^{b\times k}$, *i. e.*, all files consist of bk symbols over $\mathbb{F}_q$, which are partitioned into b blocks of length k. The total file X is of the form

$$X = \begin{bmatrix} x^{[1]} \\ \vdots \\ x^{[w]} \\ \vdots \\ x^{[M]} \end{bmatrix}_{bM\times k}.$$

After encoding with the code $\mathcal{C}$, these files are distributed to the n servers. So, each file $x^{[i]}$ is encoded as $y^{[i]} = x^{[i]}G_C \in \mathbb{F}_q^{b\times n}$. The encoded total file Y is

$$Y = XG_C = \begin{bmatrix} y^{[1]} \\ \vdots \\ y^{[w]} \\ \vdots \\ y^{[M]} \end{bmatrix}_{bM\times n} = \begin{bmatrix} y_1 & \cdots & y_j & \cdots & y_n \end{bmatrix}_{bM\times n} = \begin{bmatrix} y_1^{[1]} & \cdots & y_n^{[1]} \\ \vdots & \ddots & \vdots \\ y_1^{[w]} & \cdots & y_n^{[w]} \\ \vdots & \ddots & \vdots \\ y_1^{[M]} & \cdots & y_n^{[M]} \end{bmatrix}_{bM\times n},$$

written as collection of M encoded files $y^{[i]}$, as column vectors y_j, or as a block matrix with entries $y_j^{[i]}$, respectively. The block vector $y_j^{[i]} \in \mathbb{F}_q^{b\times 1}$ corresponds to the j^{th} coordinate of the i^{th} encoded file. The column vector $y_j \in \mathbb{F}_q^{bM\times 1}$ stored by the j^{th} server.

Request

The user selects a random query $q^{[w]} \in \mathbb{F}_q^{bM\times n}$ to retrieve the w^{th} file $x^{[w]}$ and then sends it to the servers:

$$q^{[w]} = \left(q_1^{[w]}, \ldots, q_n^{[w]}\right),$$

where the component $q_j^{[w]} \in \mathbb{F}_q^{bM\times 1}$ is sent to the j^{th} server.

Response

The servers compute responses as $r_j^{[w]} = q_j^{[w]} \cdot y_j \in \mathbb{F}_q$ and send them to the user. The total response vector is

$$r^{[w]} = \left(r_1^{[w]}, \cdots, r_n^{[w]}\right) \in \mathbb{F}_q^n.$$

Iteration

The steps *Request* and *Response* are repeated a total of s times until the desired file $x^{[w]}$ can be reconstructed from the s responses $r^{[w]}$.

Reconstruction

A reconstruction function takes as input all response vectors $r^{[w]} \in \mathbb{F}_q^n$ over all s iterations of the scheme, and outputs the desired file $x^{[w]}$.

Special case b = 1 and s = 1

Assume that $b = 1$ and the iteration number is $s = 1$. Then the arbitrary files amount to $x^{[i]} \in \mathbb{F}_q^{1\times k}$ and the w^{th} file is $x^{[w]}$. The stored data for each file is $y^{[i]} = x^{[i]}G_C \in \mathbb{F}_q^{1\times n}$. For every $x^{[i]}$, $i \in \{1, \ldots, M\}$, we choose a codeword $d^{[i]}$ uniformly at random from the retrieval code $\mathcal{D} \subseteq \mathbb{F}_q^n$. Let $e \in \mathbb{F}_q^n \setminus \mathcal{D}$ be suitably chosen, then we add e to $d^{[w]}$. Consider the following $M \times n$ matrix

$$\begin{bmatrix} d^{[1]} \\ d^{[2]} \\ \vdots \\ d^{[w]} + e \\ \vdots \\ d^{[M]} \end{bmatrix} = \begin{bmatrix} d_1^{[1]} & d_2^{[1]} & \cdots & d_j^{[1]} & \cdots & d_n^{[1]} \\ d_1^{[2]} & d_2^{[2]} & \cdots & d_j^{[2]} & \cdots & d_n^{[2]} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ d_1^{[w]} + e_1 & d_2^{[w]} + e_2 & \cdots & d_j^{[w]} + e_j & \cdots & d_n^{[w]} + e_n \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ d_1^{[M]} & d_2^{[M]} & \cdots & d_j^{[M]} & \cdots & d_n^{[M]} \end{bmatrix} = \begin{bmatrix} q_1^{[w]} & q_2^{[w]} & \cdots & q_n^{[w]} \end{bmatrix},$$

whose columns give us queries $q_j^{[w]}$, where $j = 1, \ldots, n$. Then the coded query $q_j^{[w]}$, which is of the form

$$q_j^{[w]} = \left(d_j^{[1]}, d_j^{[2]}, \ldots, d_j^{[w]} + e_j, \ldots, d_j^{[M]}\right)^T \in \mathbb{F}_q^{M\times 1},$$

is sent to the j^{th} server.

The servers send responses $r^{[w]}$,

$$\left(r_1^{[w]}, \ldots, r_n^{[w]}\right) = \left(q_1^{[w]} \cdot y_1, \ldots, q_n^{[w]} \cdot y_n\right) \in \mathcal{C}\star\mathcal{D} + \mathcal{C}\star e,$$

where $\star$ denotes the Schur product, so that $\mathcal{C}\star\mathcal{D} = \{c\star d = (c_1d_1, \ldots, c_nd_n) \mid c \in \mathcal{C}, d \in \mathcal{D}\}$.

The support of e is chosen so that right-multiplying the vector $\left(r_1^{[w]}, \ldots, r_n^{[w]}\right)$ with the parity check matrix of $\mathcal{C}\star\mathcal{D}$ reveals $d_{\mathcal{C}\star\mathcal{D}} - 1$ coordinates of $y^{[w]}$, coming from the $\mathcal{C}\star e$ summand in the above expression. The scheme protects against $(d_{\mathcal{D}^\perp} - 1)$-collusion because every $t = d_{\mathcal{D}^\perp} - 1$ columns of the generator matrix of $\mathcal{D}$ (which is a parity check matrix of $\mathcal{D}^\perp$) are linearly independent.

General case: b ≥ 1 and s ≥ 1

In general, assume that $b \geq 1$ and the iteration number is $s \geq 1$. Then, the arbitrary files are given by $x^{[i]} \in \mathbb{F}_q^{b\times k}$ and the w^{th} file is $x^{[w]}$. We have $y^{[i]} = x^{[i]}G_C = \left(y_1^{[i]}, \ldots, y_n^{[i]}\right) \in \mathbb{F}_q^{b\times n}$, for all i. For every $x^{[i]}$, we choose a codeword $d^{[i]} \in \mathcal{D} \subseteq \mathbb{F}_q^n$ for $i = 1, \ldots, M$. Let $E = (e^1, \ldots, e^s) \in (\mathbb{F}_q^{b\times n})^s$ be selected where $e_j^\gamma \in \mathbb{F}_q^{1\times b}$ denotes the j^{th} column of $e^\gamma \in \mathbb{F}_q^{b\times n}$. The PIR scheme proceeds as follows:

(1) Select Msb codewords independently and uniformly at random from $\mathcal{D}$ as

$$d^{[i],\gamma,\beta} \in \mathcal{D},$$

where $i \in \{1, \ldots, M\}$, $\gamma \in \{1, \ldots, s\}$, $\beta \in \{1, \ldots, b\}$.

(2) In round γ, send the query

$$q_j^{[w],\gamma} = \left(d_j^{[1],\gamma}, d_j^{[2],\gamma}, \ldots, d_j^{[w],\gamma} + e_j^\gamma, \ldots, d_j^{[M],\gamma}\right)^T \in \mathbb{F}_q^{Mb\times 1}$$

to the j^{th} server, where $d_j^{[i],\gamma} \in \mathbb{F}_q^{b\times 1}$ is the j^{th} row of the matrix

$$\begin{bmatrix} d_1^{[i],\gamma,1} & \cdots & d_1^{[i],\gamma,b} \\ \vdots & \ddots & \vdots \\ d_j^{[i],\gamma,1} & \cdots & d_j^{[i],\gamma,b} \\ \vdots & \ddots & \vdots \\ d_n^{[i],\gamma,1} & \cdots & d_n^{[i],\gamma,b} \end{bmatrix}.$$

Also, $q_j^{[w],\gamma}$ is the j^{th} column of the following matrix:

$$\begin{bmatrix} d_1^{[1],\gamma,1} & \cdots & d_j^{[1],\gamma,1} & \cdots & d_n^{[1],\gamma,1} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ d_1^{[1],\gamma,b} & \cdots & d_j^{[1],\gamma,b} & \cdots & d_n^{[1],\gamma,b} \\ & & \vdots & & \\ d_1^{[w],\gamma,1} + e_1^{\gamma,1} & \cdots & d_j^{[w],\gamma,1} + e_j^{\gamma,1} & \cdots & d_n^{[w],\gamma,1} + e_n^{\gamma,1} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ d_1^{[w],\gamma,b} + e_1^{\gamma,b} & \cdots & d_j^{[w],\gamma,b} + e_j^{\gamma,b} & \cdots & d_n^{[w],\gamma,b} + e_n^{\gamma,b} \\ & & \vdots & & \\ d_1^{[M],\gamma,1} & \cdots & d_j^{[M],\gamma,1} & \cdots & d_n^{[M],\gamma,1} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ d_1^{[M],\gamma,b} & \cdots & d_j^{[M],\gamma,b} & \cdots & d_n^{[M],\gamma,b} \end{bmatrix}.$$

(3) The servers send the responses

$$\left(r_1^{[w],\gamma}, \ldots, r_n^{[w],\gamma}\right) = \left(q_1^{[w],\gamma} \cdot y_1, \ldots, q_n^{[w],\gamma} \cdot y_n\right) \in \mathcal{C}\star\mathcal{D} + \left(e_1^{,\gamma} \cdot y_1, \ldots, e_n^{,\gamma} \cdot y_n\right).$$

and we retrive $(y_1, \ldots, y_n)$ via syndrome decoding after multiplying the parity check matrix H of $\mathcal{C}\star\mathcal{D}$ with the response vector above.

(4) This scheme retrieves the file $x^{[w]}$ from ns queries. Note that the number of y_i's that are recovered is $wt(e)$ at each round, therefore the required number of rounds s depends on $d_{\mathcal{C}\star\mathcal{D}}$ and the size of x (see the proof of (Freij-Hollanti et al. 2018, Theorem 2) for more details and exact formulations).

This scheme is called $(\mathcal{D}, E)$-retrieval scheme.

In Freij-Hollanti et al. (2018), Freij-Hollanti et al. have constructed a PIR scheme with rate $\frac{d_{\mathcal{C}\star\mathcal{D}}-1}{n}$ which protects against $(d_{\mathcal{D}^\perp} - 1)$-collusion. For some classes of $\mathcal{C}$ and $\mathcal{D}$, in particular when $\mathcal{C}$ and $\mathcal{C}\star\mathcal{D}$ have transitive automorphism groups (see below), they have shown that the rate of the scheme can be improved to the rate $\frac{\dim(\mathcal{C}\star\mathcal{D})^\perp}{n}$. In particular, they used Reed-Muller codes as transitive codes.

We repeat their main theorems for completeness. Recall that in the matrix X, each row corresponds to one of the files, but then the data in the matrix Y is partitioned into columns, and each column is stored at a different server.

Theorem 1.1 (Freij-Hollanti et al. 2018, Theorem 2) *Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be an $[n, k, d]_q$ linear storage code and let $\mathcal{D} \subseteq \mathbb{F}_q^n$ be any linear code. Then there exists a $(\mathcal{D}, E)$-retrieval scheme for the distributed storage system $Y = XG_{\mathcal{C}}$ with PIR rate*

$$\frac{d_{\mathcal{C}\star\mathcal{D}} - 1}{n},$$

which protects against $(d_{\mathcal{D}^\perp} - 1)$-collusion.

Before we can state the second main result from Freij-Hollanti et al. (2018), we need some definitions. Let S_n be the permutation group acting on $\mathcal{I} = \{1, \ldots, n\}$. Then, a group $G \leq S_n$ is transitive on the set I, if for any $1 \leq i_1 \leq i_2 \leq n$ there exists $g \in G$ such that $g(i_1) = i_2$. Let $\mathcal{C} \in \mathbb{F}_q^n$ be a linear code and let $\Gamma(\mathcal{C})$ be permutation automorphism of $\mathcal{C}$, then $\Gamma(\mathcal{C})$ is a subgroup of S_n. We say $\mathcal{C}$ is transitive on $\mathcal{I}$ if $\Gamma(\mathcal{C})$ is transitive on $\mathcal{I}$.

Theorem 1.2 (Freij-Hollanti et al. 2018, Theorem 4) *Let $\mathcal{C}$ and $\mathcal{D}$ be codes of length n such that $\Gamma(\mathcal{C})$ and $\Gamma(\mathcal{C}\star\mathcal{D})$ are transitive on I. Then there is a $(\mathcal{D}, E)$-retrieval scheme for the distributed storage system $Y = XG_{\mathcal{C}}$ with PIR rate*

$$\frac{\dim(\mathcal{C}\star\mathcal{D})^\perp}{n},$$

which protects against $(d_{\mathcal{D}^\perp} - 1)$-collusion.

In Bodur et al. (2022), Bodur et al. used cyclic codes, which are also transitive, to obtain better PIR rates. They also compared the performance of cyclic codes with punctured and shortened Reed-Muller codes as these are also known to be cyclic.

In this paper, we study nD-cyclic codes and PIR schemes from them. For this, we provide a formal proof of transitivity, which generalizes the case of cyclic codes. Then, we compare our scheme with the existing ones from cyclic codes. Finally, we generalize this idea further

to the constacyclic setup. By extending a known equivalence between cyclic and constacyclic codes, we investigate equivalent PIR schemes from nD-constacyclic codes.

The paper is organized as follows. Section 2 provides the necessary background on cyclic codes. In Section 3, we develop the transitivity of nD-cyclic codes and we present examples that PIR schemes obtained from nD-cyclic codes which perform better than the ones from cyclic codes. In Section 4, we extend the monomial equivalence between cyclic codes and certain constacyclic codes to nD case.

2 Preliminaries

Let q be a prime power and let $\mathbb{F}_q$ be the finite field with q elements. Let $m \geq 1$ be a positive integer such that $\gcd(m, q) = 1$ from this point on. Let r be the smallest integer satisfying $q^r \equiv 1 \mod m$ and let $\mathbb{F}_{q^r}$ be the extension of $\mathbb{F}_q$ such that $\mathbb{F}_{q^r} = \mathbb{F}_q(\xi)$, where $\xi \in \mathbb{F}_{q^r}$ is a primitive m^{th} root of unity (*i. e.*, $\mathbb{F}_{q^r}$ is the splitting field of $x^m - 1$ over $\mathbb{F}_q$).

Let $\mathcal{C}$ be an $[m, k]_q$-linear code over $\mathbb{F}_q$ (*i. e.*, $\mathcal{C}$ is a subspace of $\mathbb{F}_q^m$). The elements of $\mathcal{C}$ are the codewords $c = (c_0, c_1, \ldots, c_{m-1})$. An $[m, k]_q$-linear code $\mathcal{C}$ is a cyclic code if $c = (c_0, c_1, \ldots, c_{m-1}) \in \mathcal{C}$ implies $(c_{m-1}, c_0, c_1, \ldots, c_{m-2}) \in \mathcal{C}$. Let $R := \mathbb{F}_q[x]/\langle x^m - 1\rangle$ and $g(x) \in R$ be the generator polynomial of the $[m, k]_q$-cyclic code $\mathcal{C}$ with $\deg(g(x)) = m - k$. So, $\mathcal{C} = \langle g(x)\rangle$ and $\mathcal{C}^\perp = \langle h^*(x)\rangle$, where $h(x) = \frac{x^m-1}{g(x)}$ is a parity-check polynomial and its reciprocal is $h^*(x) = x^k h\left(\frac{1}{x}\right)$. The q-cyclotomic coset of ξ^j is $\left[\xi^j\right] = \left\{\xi^j, \xi^{qj}, \ldots, \xi^{q^{r-1}j}\right\}$ for any positive integer j.

For $w, p, d, s \in \mathbb{Z}^+$, we now set some notation:

- zero set of $\mathcal{C}$: $Z(\mathcal{C}) = \left\{\xi^j \in \mathbb{F}_{q^r} : g(\xi^j) = 0, 0 \leq j \leq m-1\right\} = \left\{\xi^{j_1}, \ldots, \xi^{j_w}\right\}$,
- defining set of $\mathcal{C}$: $J = \{j_1, \ldots, j_w\}$,
- generating set of $\mathcal{C}$: $\Omega \setminus J$, where $\Omega = \{0, 1, \ldots, m-1\}$,
- zero set of $\mathcal{C}^\perp$: $Z(\mathcal{C}^\perp) = \left\{\xi^i \in \mathbb{F}_{q^r} : h^*(\xi^i) = 0, 0 \leq i \leq m-1\right\} = \left\{\xi^{i_1}, \ldots, \xi^{i_p}\right\}$.

If ξ is a root of $g(x)$, then so is ξ^q. Therefore, the zero sets of $\mathcal{C}$ and $\mathcal{C}^\perp$ are disjoint unions of q-cyclotomic cosets which yields the following.

- basic zero set of $\mathcal{C}$: $BZ(\mathcal{C}) = \left\{\xi^{u_k} \in \mathbb{F}_{q^r} : \bigcup_{k=1}^{d} \left[\xi^{u_k}\right] = Z(\mathcal{C})\right\} = \{\xi^{u_1}, \ldots, \xi^{u_d}\}$,
- basic zero set of $\mathcal{C}^\perp$: $BZ(\mathcal{C}^\perp) = \left\{\xi^{v_k} \in \mathbb{F}_{q^r} : \bigcup_{k=1}^{s} \left[\xi^{v_k}\right] = Z(\mathcal{C}^\perp)\right\} = \{\xi^{v_1}, \ldots, \xi^{v_s}\}$.

Note that $f(\xi) = 0$ if and only if $f^*(\xi^{-1}) = 0$, which yields the following well-known result.

Theorem 2.1 *Let $\mathcal{C}$ be an $[m, k]_q$-cyclic code over $\mathbb{F}_q$ and ξ be the primitive m^{th} root of unity, $\xi \in \mathbb{F}_{q^r}$ and $\gcd(m, q) = 1$. Assume that the defining set of $\mathcal{C}$ is $J = \{j_1, \ldots, j_w\}$ and the generating set of $\mathcal{C}$ is $I = \{0, 1, \ldots, m-1\} \setminus \{j_1, \ldots, j_w\} = \{i_1, \ldots, i_t\}$. Then the defining set of $\mathcal{C}^\perp$ is $-I = \{-i_1, \ldots, -i_t\}$.*

We can represent any cyclic code as an evaluation code as follows.

Theorem 2.2 (Cascudo 2018, Lemma 4) *Let $\mathcal{C}$ be an $[m,k]_q$-cyclic code over $\mathbb{F}_q$, where* $\gcd(m,q)=1$. *Then $B(-I)|_{\mathbb{F}_q}=\mathcal{C}$ such that*

$$B(-I)=\left\{\left(f(1),f(\xi),\ldots,f(\xi^{m-1})\right): f(x)\in\mathbb{F}_{q^r}[x], f(x)=\sum_{j\in -I} f_j x^j\right\}$$
$$=\left\{\left(\sum_{j\in -I} f_j\xi^{ij}\right)_{0\le i\le m-1} : f_j\in\mathbb{F}_{q^r},\forall j\right\}.$$

A linear code $\mathcal{D}$ over $\mathbb{F}_{q^r}$ is *Galois closed* if $\mathcal{D}^q=\mathcal{D}$. Now we show that the code $B(-I)$ defined over $\mathbb{F}_{q^r}$ is Galois closed. For

$$f(\xi^i)=\sum_{j\in -I} f_j\xi^{ij},$$

we have

$$f(\xi^i)^q=\left(\sum_{j\in -I} f_j\xi^{ij}\right)^q=\sum_{j\in -I} f_j^q\xi^{qij}.$$

Remember that if $j\in -I$ then $qj\in -I$, therefore $q(-I)=-I$. Set $g_{qj}=f_j^q$, where $g(x)\in\mathbb{F}_{q^r}[x]$ then

$$f(\xi^i)^q=\sum_{j\in -I} g_{qj}\xi^{qij}=\sum_{k/q\in -I} g_k\xi^{ik}$$

with $g(x)=\sum_{k/q\in -I} g_k\xi^{ik}$. So, we have $B(-I)^q=B(-I)$.

By using Theorem 4 in Bierbrauer (2002), we can say that $\mathcal{C}=B(-I)|_{\mathbb{F}_q}=\mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(B(-I))$ and we arrive at the following equivalent characterization of cyclic codes.

Theorem 2.3 (Wolfmann 1989, Proposition 2.1) *Let $\mathcal{C}$ be an $[m,k]_q$-cyclic code over $\mathbb{F}_q$ and ξ be the primitive m^{th} root of unity, $\xi\in\mathbb{F}_{q^r}$ and* $\gcd(m,q)=1$. *Assume that the basic zero set of $\mathcal{C}^\perp$ is $BZ(\mathcal{C}^\perp)=\{\xi^{v_1},\ldots,\xi^{v_s}\}$. Then*

$$\mathcal{C}=\left\{\left(\mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}\left(c_1\xi^{iv_1}+\cdots+c_s\xi^{iv_s}\right)\right)_{0\le i\le m-1} : c_1,\ldots,c_s\in\mathbb{F}_{q^r}\right\}. \tag{2.1}$$

Remark 2.4 Note that $\{v_1,\ldots,v_s\}=-I$ by Theorem 2.1. Hence (2.1) can be rewritten in the polynomial representation as

$$\mathcal{C}=\left\{\sum_{i=0}^{m-1}\mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}\left(f\left(\xi^i\right)\right)x^i : f(x)\in\mathbb{F}_{q^r}[x], f(x)=\sum_{j\in -I} f_j x^j\right\}.$$

Given two vectors $u=(u_0,\ldots,u_{m-1}), v=(v_0,\ldots,v_{m-1})\in\mathbb{F}_q^m$, we define their *Schur product*, denoted by $u\star v$, as $u\star v=(u_0\cdot v_0,\ldots,u_{m-1}\cdot v_{m-1})$. In the polynomial representation over R, let $u(x)=\sum_{i\in\Omega} u_i x^i$ and $v(x)=\sum_{i\in\Omega} v_i x^i$, then $u(x)\star v(x)=\sum_{i\in\Omega} u_i v_i x^i$. If $\mathcal{C}_1$ and $\mathcal{C}_2$ are two linear codes of the same length over the same field, then their Schur product is $\mathcal{C}_1\star\mathcal{C}_2:=\{c_1\star c_2 : c_1\in\mathcal{C}_1, c_2\in\mathcal{C}_2\}$. For cyclic code pairs, we have the following result.

Theorem 2.5 (Cascudo 2018, Theorem 1) *Assume that* $\gcd(m, q) = 1$ *and that* $\mathcal{C}_1$ *and* $\mathcal{C}_2$ *are two cyclic codes of length* m *over* $\mathbb{F}_q$ *with generating sets* I_1 *and* I_2*, respectively. Let*

$$B(-I_1) = \left\{ \left(\sum_{j_1 \in -I_1} f_{j_1} \xi^{ij_1} \right)_{0 \le i \le m-1} : f_{j_1} \in \mathbb{F}_{q^r}, \forall j_1 \right\},$$

$$B(-I_2) = \left\{ \left(\sum_{j_2 \in -I_2} g_{j_2} \xi^{ij_2} \right)_{0 \le i \le m-1} : g_{j_2} \in \mathbb{F}_{q^r}, \forall j_2 \right\}.$$

Then we have $B(-(I_1 + I_2))|_{\mathbb{F}_q} = \mathcal{C}_1 \star \mathcal{C}_2$*, where* $I_1 + I_2 = \{i_1 + i_2 : i_1 \in I_1, i_2 \in I_2\}$.

Proof For any $i \in \Omega$, we have

$$\left(\sum_{j_1 \in -I_1} f_{j_1} \xi^{ij_1} \right) \star \left(\sum_{j_2 \in -I_2} g_{j_2} \xi^{ij_2} \right) = \sum_{j_1 \in -I_1} \sum_{j_2 \in -I_2} f_{j_1} g_{j_2} \xi^{i(j_1+j_2)} = \sum_{k \in -(I_1+I_2)} h_k \xi^{ik},$$

where $h_k = f_{j_1} g_{j_2}$ and $k = j_1 + j_2$. □

Let us now describe multidimensional cyclic codes. We will follow the notations and setup in Güneri and Özkaya (2016), starting with 2D and 3D-cyclic codes. Let ℓ be a positive integer, $\mathcal{C}$ be a linear code of length $m\ell$ over $\mathbb{F}_q$ and the codewords c of $\mathcal{C}$ be represented as $m \times \ell$ arrays,

$$c = \begin{pmatrix} c_{0,0} & \cdots & c_{0,\ell-2} & c_{0,\ell-1} \\ \vdots & \ddots & \vdots & \vdots \\ c_{m-2,0} & \cdots & c_{m-2,\ell-2} & c_{m-2,\ell-1} \\ c_{m-1,0} & \cdots & c_{m-1,\ell-2} & c_{m-1,\ell-1} \end{pmatrix}. \tag{2.2}$$

A linear code $\mathcal{C}$ of length $m\ell$ over $\mathbb{F}_q$ is a 2D-cyclic code if

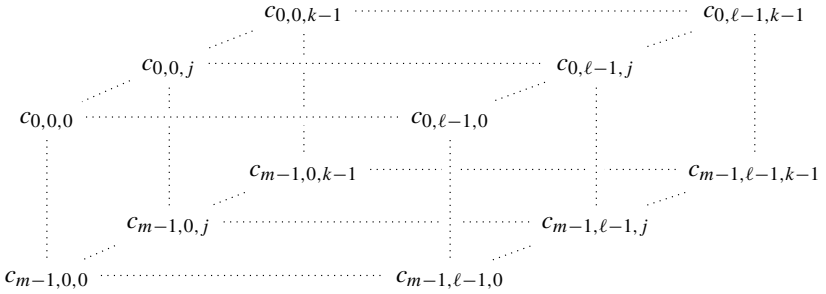
$$\begin{pmatrix} c_{m-1,0} & \cdots & c_{m-1,\ell-2} & c_{m-1,\ell-1} \\ c_{0,0} & \cdots & c_{0,\ell-2} & c_{0,\ell-1} \\ \vdots & \ddots & \vdots & \vdots \\ c_{m-2,0} & \cdots & c_{m-2,\ell-2} & c_{m-2,\ell-1} \end{pmatrix} \in \mathcal{C}$$

and

$$\begin{pmatrix} c_{0,\ell-1} & c_{0,0} & \cdots & c_{0,\ell-2} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m-2,\ell-1} & c_{m-2,0} & \cdots & c_{m-2,\ell-2} \\ c_{m-1,\ell-1} & c_{m-1,0} & \cdots & c_{m-1,\ell-2} \end{pmatrix} \in \mathcal{C}$$

In other words, a linear code of length $m \times \ell$ is 2D-cyclic if it is closed under row shifts and column shifts of codewords.

Let k be another positive integer and let $\mathcal{C}$ be a linear code of length $m\ell k$ over $\mathbb{F}_q$ and consider the codewords of $\mathcal{C}$ arranged as as $m \times \ell \times k$ cubes:



(2.3)

A linear code $\mathcal{C}$ of length $m\ell k$ over $\mathbb{F}_q$ is a 3D-cyclic code if $\forall c \in \mathcal{C}$, if it is closed under bottom-to-top shifts, right-to-left shifts and back-to-front shifts of codewords.

In general, an nD-cyclic code of length $m_1 \times \cdots \times m_n$ over $\mathbb{F}_q$ is defined to be an ideal in $R_n := \mathbb{F}_q[x_1, \ldots, x_n]/\langle x_1^{m_1} - 1, \ldots, x_n^{m_n} - 1\rangle$, where each m_i is a positive integer for $1 \leq i \leq n$. Throughout we will assume that $\gcd(m_i, q) = 1$ for $1 \leq i \leq n$.

For nD-cyclic codes, we will follow the notations and setup in Güneri and Özbudak (2008). Let $\boldsymbol{m} - \mathbf{1} = (m_1 - 1, \ldots, m_n - 1)$. Let $\boldsymbol{\Omega}$ be the set $\{0, \ldots, m_1 - 1\} \times \cdots \times \{0, \ldots, m_n - 1\}$,

$$\boldsymbol{\Omega} = \left\{(i_1, \ldots, i_n) : i_\nu \in \{0, \ldots, m_\nu - 1\} := \Omega_\nu, 1 \leq \nu \leq n, \text{ and } m_\nu \in \mathbb{Z}^+\right\}.$$

We denote $(i_1, \ldots, i_n) \in \boldsymbol{\Omega}$ as $\boldsymbol{i}$, $(x_1, \ldots, x_n)$ as $\boldsymbol{x}$ and the monomial $x_1^{i_1} \cdots x_n^{i_n}$ as $\boldsymbol{x}^{\boldsymbol{i}}$. Let $\xi_\nu \in \mathbb{F}_{q^r}$ be the primitive m_ν^{th} root of unity, for $1 \leq \nu \leq n$, then $(\xi_1, \ldots, \xi_n)$ is denoted as $\boldsymbol{\xi}$ and $(\xi_1^{i_1} \cdots \xi_n^{i_n})$ is denoted as $\boldsymbol{\xi}^{\boldsymbol{i}}$. With this setup, the notions of zero and basic zero sets as well as defining and generating sets given in the preliminaries for cyclic codes naturally extend to nD-cyclic codes. The following result generalizes Theorem 2.1.

Theorem 2.6 (Güneri and Özbudak 2008, Proposition 2.1) *Let $\mathcal{C}$ be an nD-cyclic code of length $m_1 \times \cdots \times m_n$ over $\mathbb{F}_q$, where $\gcd(m_i, q) = 1$ for $1 \leq i \leq n$ and let t, w be some positive integers. Assume that the defining set of $\mathcal{C}$ is $\boldsymbol{J} = \left\{\boldsymbol{j}_1, \ldots, \boldsymbol{j}_w\right\} \subseteq \boldsymbol{\Omega}$ and the generating set of $\mathcal{C}$ is $\boldsymbol{I} = \boldsymbol{\Omega} \setminus \boldsymbol{J} = \{\boldsymbol{i}_1, \ldots, \boldsymbol{i}_t\}$ then the defining set of $\mathcal{C}^\perp$ is $-\boldsymbol{I} = \{-\boldsymbol{i}_1, \ldots, -\boldsymbol{i}_t\}$.*

The trace representation of codewords given for cyclic codes in Theorem 2.3 is generalized to the nD case as follows.

Theorem 2.7 (Güneri and Özbudak 2008, Theorem 2.4) *Let $\mathcal{C}$ be an nD-cyclic code of length $m_1 \times \cdots \times m_n$ over $\mathbb{F}_q$, where $\gcd(m_i, q) = 1$ for $1 \leq i \leq n$ and let $\xi_\nu \in \mathbb{F}_{q^r}$ be a primitive m_ν^{th} root of unity for $1 \leq \nu \leq n$, $\boldsymbol{\xi} = (\xi_1, \ldots, \xi_n)$. Assume that the defining set of $\mathcal{C}^\perp$ is $-\boldsymbol{I} = \{-\boldsymbol{i}_1, \ldots, -\boldsymbol{i}_t\}$. Then*

$$\mathcal{C} = \left\{ \sum_{\boldsymbol{i} \in \boldsymbol{\Omega}} \mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}\left(f\left(\boldsymbol{\xi}^{\boldsymbol{i}}\right)\right) \boldsymbol{x}^{\boldsymbol{i}} \in R_n : f(\boldsymbol{x}) = \sum_{\boldsymbol{j} \in -\boldsymbol{I}} f_{\boldsymbol{j}} \boldsymbol{x}^{\boldsymbol{j}} \right\}.$$

This representation of $\mathcal{C}$ is called its trace representation.

We will also need the following notion. Two linear codes $\mathcal{C}$ and $\mathcal{D}$ of length n over $\mathbb{F}_q$ are monomially equivalent if there exists an $n \times n$ monomial matrix M such that $G_{\mathcal{C}} M = G_{\mathcal{D}}$,

where $G_{\mathcal{C}}$ and $G_{\mathcal{D}}$ are generator matrices of $\mathcal{C}$ and $\mathcal{D}$, respectively. We denote by $\mathtt{MAut}(\mathcal{C})$ the monomial automorphism group of $\mathcal{C}$, where

$$\mathtt{MAut}(\mathcal{C}) = \{M : n \times n \text{ monomial matrix}, \mathcal{C} = \mathcal{C}M\}\,.$$

Lemma 2.8 (Huffman and Pless 2010, Theorem 1.7.11 (ii)) *Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be codes over $\mathbb{F}_q$. If $\mathcal{C}_1 M = \mathcal{C}_2$, where M is a monomial matrix, then $M^{-1}\mathtt{MAut}(\mathcal{C}_1)M = \mathtt{MAut}(\mathcal{C}_2)$.*

3 PIR schemes from *n*D-cyclic codes

In this section, we study PIR schemes from nD-cyclic codes, which are transitive codes just like the cyclic codes.

Let S_m be a permutation group acting on $\mathcal{I} = \{1, \ldots, m\}$. Recall that a subgroup $G \leq S_m$ is *transitive* on the set $\mathcal{I}$ if, for any $1 \leq i_1 \leq i_2 \leq m$, there exists $g \in G$ such that $g(i_1) = i_2$. Let $\mathcal{C} \in \mathbb{F}_q^m$ be a linear code and let $\Gamma(\mathcal{C})$ be the permutation automorphism group of $\mathcal{C}$, then $\Gamma(\mathcal{C})$ is a subgroup of S_m. The code $\mathcal{C}$ is said to be transitive on $\mathcal{I}$ if $\Gamma(\mathcal{C})$ is transitive on $\mathcal{I}$.

The following lemma is straightforward.

Lemma 3.1 *Let $\mathcal{C}$ be an $[m, k]_q$-cyclic code over $\mathbb{F}_q$, where $\gcd(m, q) = 1$. Let $\Gamma(\mathcal{C}) \subseteq S_m$ be the permutation automorphism group of $\mathcal{C}$. Let $\delta \in S_m$ be the permutation cyclicly shifting a codeword by one unit, i.e., $\delta(i) = i + 1$, where $0 \leq i \leq m - 1$. Then, $\delta \in \Gamma(\mathcal{C})$, as $\mathcal{C}$ is cyclic and $\mathcal{C}$ is transitive on $\mathcal{I} = \{1, \ldots, n\}$, since for any i_1, i_2, $\sigma(i_1) = i_2$ for*

$$\sigma = \begin{cases} \delta^{i_2 - i_1}, & \text{if } i_2 \geq i_1; \\ \delta^{m + i_2 - i_1}, & \text{if } i_2 < i_1. \end{cases}$$

It means that, for $i_1 \geq i_2$ we have, $\delta^{i_2 - i_1}(i_1) = i_2$ so that

$$\left(\_ \overset{i_1}{\bullet} \_ \overset{i_2}{\bullet} \_ \_\right) \xrightarrow{\delta^{i_2 - i_1}} \left(\_ \_ \_ \overset{i_2}{\bullet} \_ \_\right)$$

and for $i_2 < i_1$ we have, $\delta^{m + i_2 - i_1}(i_1) = i_2$ so that

$$\underbrace{\left(\_ \overset{i_2}{\bullet} \_ \overset{i_1}{\bullet} \_ \_\right) \xrightarrow{\delta^{m - i_1}} \left(\_ \overset{i_2}{\bullet} \_ \_ \_ \overset{i_1}{\bullet}\right) \xrightarrow{\delta^{i_2}} \left(\_ \overset{i_2}{\bullet} \_ \_ \_ \_\right)}_{\delta^{m + i_2 - i_1}}.$$

In the polynomial representation, the action of σ on R can be viewed as $\sigma \cdot c(x) = xc(x)$, where $c(x) = \sum_{i=0}^{m-1} c_i x^i$ is a codeword of the cyclic code $\mathcal{C} \subseteq R$. Hence the coefficient c_i of $c(x)$ is moved to the j^{th} position when we multiply $c(x)$ by x^{j-i} or x^{m+j-i} suitably.

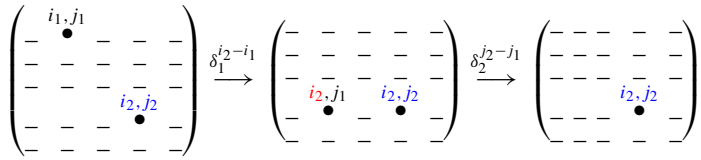
We will first generalize the above lemma to 2D case. Recall the $m \times \ell$ representation of 2D-cyclic codewords given in (2.2) and consider $S_m \times S_\ell$ acting on the set of tuples $\mathcal{I} \times \mathcal{J} = \{(i, j) : i \in \mathcal{I} = \{1, \ldots, m\}, j \in \mathcal{J} = \{1, \ldots, \ell\}\}$. We say the group $G \leq S_m \times S_\ell$ is *transitive* on the set $\mathcal{I} \times \mathcal{J}$ if for any $(i_1, j_1), (i_2, j_2) \in \mathcal{I} \times \mathcal{J}$, there exists $g \in G$ such that $g(i_1, j_1) = (i_2, j_2)$. Let $\mathcal{C} \in \mathbb{F}_q^{m \times \ell}$ be a linear code and let $\Gamma(\mathcal{C})$ be the permutation automorphism group of $\mathcal{C}$, then $\Gamma(\mathcal{C})$ is a subgroup of $S_m \times S_\ell$. The code $\mathcal{C}$ is transitive on $\mathcal{I} \times \mathcal{J}$ if $\Gamma(\mathcal{C})$ is transitive on $\mathcal{I} \times \mathcal{J}$.

Theorem 3.2 *Let $\mathcal{C}$ be a 2D-cyclic code in $\mathbb{F}_q^{m \times \ell}$ such that $\gcd(m, q) = \gcd(\ell, q) = 1$. Let $\Gamma(\mathcal{C}) \subseteq S_m \times S_\ell$ be the permutation automorphism group of $\mathcal{C}$. Let $\delta_1 \in S_m$ be the shifting*

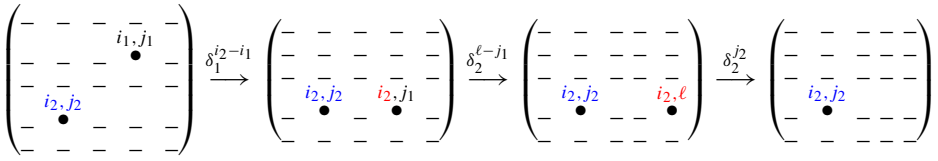
by 1 unit in a row in $\mathbb{F}_q^m$ *such that* $\delta_1(i) = i + 1$ *and let* $\delta_2 \in S_\ell$ *be the shifting by 1 unit in a column in* $\mathbb{F}_q^\ell$ *such that* $\delta_2(j) = j + 1$. *Then, a 2D-cyclic code* $\mathcal{C}$ *is transitive on* $\mathcal{I} \times \mathcal{J}$, *since* $\sigma(i_1, j_1) = (\sigma_1(i_1), \sigma_2(j_1)) = (i_2, j_2)$ *for*

$$\sigma_1 = \begin{cases} \delta_1^{i_2 - i_1}, & \text{if } i_2 \geq i_1; \\ \delta_1^{m + i_2 - i_1}, & \text{if } i_2 < i_1, \end{cases} \text{ and } \sigma_2 = \begin{cases} \delta_2^{j_2 - j_1}, & \text{if } j_2 \geq j_1; \\ \delta_2^{l + j_2 - j_1}, & \text{if } j_2 < j_1. \end{cases}$$

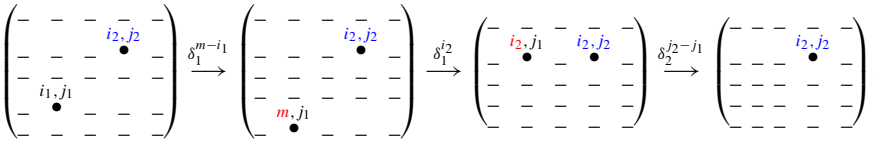
It means that, for $i_2 \geq i_1$ *and* $j_2 \geq j_1$ *we have,* $\delta_1^{i_2 - i_1}(i_1) = i_2$ *and* $\delta_2^{j_2 - j_1}(j_1) = j_2$.



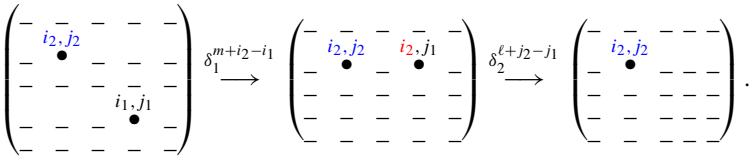
For $i_2 \geq i_1$ *and* $j_2 < j_1$ *we have,* $\delta_1^{i_2 - i_1}(i_1) = i_2$ *and* $\delta_2^{j_2 - j_1}(j_1) = j_2$.



For $i_2 < i_1$ *and* $j_2 \geq j_1$ *we have,* $\delta_1^{i_2 - i_1}(i_1) = i_2$ *and* $\delta_2^{j_2 - j_1}(j_1) = j_2$.



For $i_2 < i_1$ *and* $j_2 < j_1$ *we have,* $\delta_1^{i_2 - i_1}(i_1) = i_2$ *and* $\delta_2^{j_2 - j_1}(j_1) = j_2$.



In the polynomial representation, the actions of σ_1 and σ_2 on $R_2 = \mathbb{F}_q[x, y]/\langle x^m - 1, y^\ell - 1\rangle$ can be viewed as $\sigma_1 \cdot c(x, y) = x^{i_2 - i_1} c(x, y)$ or $\sigma_1 \cdot c(x, y) = x^{m + i_2 - i_1} c(x, y)$ and $\sigma_2 \cdot c(x, y) = y^{j_2 - j_1} c(x, y)$ or $\sigma_2 \cdot c(x, y) = y^{\ell + j_2 - j_1} c(x, y)$, respectively, where

$$c(x, y) = \sum_{i=0}^{m-1} \sum_{j=0}^{\ell-1} c_{i,j} x^i y^j$$

is a codeword of the 2D-cyclic code $\mathcal{C} \subseteq R_2$. Hence the coefficient c_{i_1, j_1} of $c(x, y)$ is moved to position i_2, j_2 when we multiply $c(x, y)$ by the suitable powers of x and y.

Now we are ready to state the transitivity of nD-cyclic codes which can be shown analogously. For this, we define $\mathcal{I}_1 \times \mathcal{I}_2 \times \cdots \times \mathcal{I}_n = \{(i_1, \ldots, i_n) : i_\nu \in \mathcal{I}_\nu = \{1, \ldots, m_\nu\}, 1 \leq \nu \leq n\}$. We say that a subgroup $G \leq S_{m_1} \times \cdots \times S_{m_n}$ is *transitive* on the set $\mathcal{I}_1 \times \mathcal{I}_2 \times \cdots \times \mathcal{I}_n$ if for any $(i_{1,1}, i_{1,2}, \ldots, i_{1,n}), (i_{2,1}, i_{2,2}, \ldots, i_{2,n}) \in \mathcal{I}_1 \times \mathcal{I}_2 \times \cdots \times \mathcal{I}_n$, there exists $g \in G$ such

that $g(i_{1,1}, i_{1,2}, \ldots, i_{1,n}) = (i_{2,1}, i_{2,2}, \ldots, i_{2,n})$. Let $\mathcal{C} \in \mathbb{F}_q^{m_1 \times \cdots \times m_n}$ be a linear code and let $\Gamma(\mathcal{C})$ be the permutation automorphism group of $\mathcal{C}$, then $\Gamma(\mathcal{C})$ is a subgroup of $S_{m_1} \times \cdots \times S_{m_n}$. The code $\mathcal{C}$ is transitive on $\mathcal{I}_1 \times \mathcal{I}_2 \times \cdots \times \mathcal{I}_n$ if $\Gamma(\mathcal{C})$ is transitive on $\mathcal{I}_1 \times \mathcal{I}_2 \times \cdots \times \mathcal{I}_n$.

Theorem 3.3 *Let $\mathcal{C}$ be an nD-cyclic code in $\mathbb{F}_q^{m_1 \times \cdots \times m_n}$, where $\gcd(m_i, q) = 1$ for $1 \le i \le n$. Let $\Gamma(\mathcal{C}) \subseteq S_{m_1} \times \cdots \times S_{m_n}$ be the permutation automorphism group of $\mathcal{C}$. For $1 \le \nu \le n$, let $\delta_\nu \in S_{m_\nu}$ be the shifting by 1 unit in $\mathbb{F}_q^{m_\nu}$ such that $\delta_\nu(i_\nu) = i_\nu + 1$. Then, an nD-cyclic code $\mathcal{C}$ is transitive on $\mathcal{I}_1 \times \mathcal{I}_2 \times \cdots \times \mathcal{I}_n$, since $\sigma(i_1, \ldots, i_n) = (\sigma_1(i_{1,1}), \ldots, \sigma_n(i_{1,n})) = (i_{2,1}, \ldots, i_{2,n})$ if for each $\nu \in \{1, \ldots, n\}$ we define*

$$\sigma_\nu = \begin{cases} \delta_\nu^{i_{2,\nu} - i_{1,\nu}}, & \text{if } i_{2,\nu} \ge i_{1,\nu}; \\ \delta_\nu^{m_\nu + i_{2,\nu} - i_{1,\nu}}, & \text{if } i_{2,\nu} < i_{1,\nu}. \end{cases}$$

In the polynomial representation, for each $\nu \in \{1, \ldots, n\}$, the action of ν^{th} permutation σ_ν on $R_n = \mathbb{F}_q[x_1, \ldots, x_n]/\langle x_1^{m_1} - 1, \ldots, x_n^{m_n} - 1\rangle$ is given by $\sigma_\nu \cdot c(x_1, \ldots, x_n) = x_\nu^{i_{2,\nu} - i_{1,\nu}} c(x_1, \ldots, x_n)$ or $\sigma_\nu \cdot c(x_1, \ldots, x_n) = x_\nu^{m_\nu + i_{2,\nu} - i_{1,\nu}} c(x_1, \ldots, x_n)$, where

$$c(x_1, \ldots, x_n) = \sum_{i_1=0}^{m_1-1} \cdots \sum_{i_n=0}^{m_n-1} c_{i_1, \ldots, i_n} x_1^{i_1} \cdots x_n^{i_n}$$

is a codeword of $\mathcal{C} \subseteq R_n$. Hence the coefficient $c_{i_{1,1}, \ldots, i_{1,n}}$ of $c(x_1, \ldots, x_n)$ is moved to position $i_{2,1}, \ldots, i_{2,n}$ when we multiply $c(x_1, \ldots, x_n)$ by the suitable powers of $x_1, \ldots, x_n$.

In order to build a PIR scheme from nD-cyclic codes, we need to show that their Schur product is also nD-cyclic. For this, we need to generalize Theorems 2.2 and 2.5 to the nD case.

We can represent nD-cyclic code as an evaluation code as follows (cf. Theorem 2.2).

Theorem 3.4 *Let $\mathcal{C}$ be an nD-cyclic code of length $m_1 \times \cdots \times m_n$ over $\mathbb{F}_q$, where $\gcd(m_i, q) = 1$ for $1 \le i \le n$. Then $B(-\boldsymbol{I})|_{\mathbb{F}_q} = \mathcal{C}$ such that*

$$\begin{aligned} B(-\boldsymbol{I}) &= \left\{ \left(f(\boldsymbol{\xi}^{\boldsymbol{0}}), \ldots, f(\boldsymbol{\xi}^{\boldsymbol{m}-\boldsymbol{1}}) \right) : f(\boldsymbol{x}) \in \mathbb{F}_{q^r}[x_1, \ldots, x_n],\ f(\boldsymbol{x}) = \sum_{\boldsymbol{j} \in -\boldsymbol{I}} f_{\boldsymbol{j}} \boldsymbol{x}^{\boldsymbol{j}} \right\} \\ &= \left\{ \left(\sum_{\boldsymbol{j} \in -\boldsymbol{I}} f_{\boldsymbol{j}} \boldsymbol{\xi}^{\boldsymbol{i}\boldsymbol{j}} \right)_{\boldsymbol{i} \in \boldsymbol{\Omega}} : f_{\boldsymbol{j}} \in \mathbb{F}_{q^r}, \forall \boldsymbol{j} \right\}, \end{aligned}$$

where $\boldsymbol{\xi}^{\boldsymbol{i}\boldsymbol{j}}$ means $(\xi_1^{i_1 j_1} \cdots \xi_n^{i_n j_n})$.

Proof Let $c(\boldsymbol{x}) = \sum_{\boldsymbol{i}=\boldsymbol{0}}^{\boldsymbol{m}-\boldsymbol{1}} f(\boldsymbol{\xi}^{\boldsymbol{i}}) \boldsymbol{x}^{\boldsymbol{i}}$. we want to show that $c(\boldsymbol{\xi}^{\boldsymbol{l}}) = 0$, where $\boldsymbol{l} \in \boldsymbol{J}$. Note that, $\boldsymbol{j} \in -\boldsymbol{I}$ and $\boldsymbol{l} \in \boldsymbol{J}$, we require $\boldsymbol{j} + \boldsymbol{l} \ne \boldsymbol{m} \bmod \boldsymbol{m}$. That is, $(j_1, \ldots, j_n) + (l_1, \ldots, l_n) \ne (0, \ldots, 0) \bmod (m_1, \ldots, m_n)$, where the addition and reduction are componentwise. By Theorem 2.1, we have $j_\nu + l_\nu \ne m_\nu \bmod m_\nu$, for each $1 \le \nu \le n$. To show that, let $-\boldsymbol{i}_a \in -\boldsymbol{I}$ and $\boldsymbol{j}_b \in \boldsymbol{J}$, where $1 \le a \le t$ and $1 \le b \le w$. Assume that $-\boldsymbol{i}_a + \boldsymbol{j}_b = \boldsymbol{0} \bmod \boldsymbol{m}$, or equivalently $\boldsymbol{j}_b = \boldsymbol{i}_a \bmod \boldsymbol{m}$. This is a contradiction, because $\boldsymbol{I} \cap \boldsymbol{J} = 0$. Therefore $-\boldsymbol{i}_a + \boldsymbol{j}_b \ne \boldsymbol{0} = \boldsymbol{m} \bmod \boldsymbol{m}$. For $d(\boldsymbol{x}) \in B(-\boldsymbol{I})$, we have

$$d(\boldsymbol{\xi}^{\boldsymbol{l}}) = \sum_{\boldsymbol{i}=\boldsymbol{0}}^{\boldsymbol{m}-\boldsymbol{1}} f(\boldsymbol{\xi}^{\boldsymbol{i}})(\boldsymbol{\xi}^{\boldsymbol{l}})^{\boldsymbol{i}} = \sum_{\boldsymbol{i}=\boldsymbol{0}}^{\boldsymbol{m}-\boldsymbol{1}} \left(\sum_{\boldsymbol{j} \in -\boldsymbol{I}} f_{\boldsymbol{j}} (\boldsymbol{\xi}^{\boldsymbol{i}})^{\boldsymbol{j}} \right) \boldsymbol{\xi}^{\boldsymbol{l}\boldsymbol{i}} = \sum_{\boldsymbol{j} \in -\boldsymbol{I}} f_{\boldsymbol{j}} \sum_{\boldsymbol{i}=\boldsymbol{0}}^{\boldsymbol{m}-\boldsymbol{1}} \boldsymbol{\xi}^{\boldsymbol{i}(\boldsymbol{j}+\boldsymbol{l})}.$$

Let $\boldsymbol{k} = \boldsymbol{j} + \boldsymbol{l}$. Since $\boldsymbol{j} \in -\boldsymbol{I}, \boldsymbol{l} \in \boldsymbol{J}$, $\boldsymbol{j} + \boldsymbol{l} \neq \boldsymbol{m} \bmod \boldsymbol{m}$, that is, $j_\nu + l_\nu \neq m_\nu \bmod m_\nu$, for all ν. Then $\xi_\nu^{j_\nu + l_\nu} \neq \xi_\nu^{m_\nu}$, for all ν. Also, for all ν, $\xi_\nu^{m_\nu} = 1$, because ξ_ν is an m_ν^{th} root of unity. So,

$$\begin{aligned}
\sum_{\boldsymbol{i}=\boldsymbol{0}}^{\boldsymbol{m}-\boldsymbol{1}} \boldsymbol{\xi}^{\boldsymbol{i}(j+l)} = \sum_{\boldsymbol{i}=\boldsymbol{0}}^{\boldsymbol{m}-\boldsymbol{1}} \boldsymbol{\xi}^{\boldsymbol{ik}} &= \sum_{i_1=0}^{m_1-1} \cdots \sum_{i_n=0}^{m_n-1} \xi_1^{i_1 k_1} \cdots \xi_n^{i_n k_n} \\
&= \sum_{i_2=0}^{m_2-1} \cdots \sum_{i_n=0}^{m_n-1} \frac{(\xi_1^{k_1})^{m_1} - 1}{\xi_1^{k_1} - 1} \xi_2^{i_2 k_2} \cdots \xi_n^{i_n k_n} \\
&= \sum_{i_2=0}^{m_2-1} \cdots \sum_{i_n=0}^{m_n-1} \frac{\overbrace{(\xi_1^{m_1})^{k_1} - 1}^{=0}}{\underbrace{\xi_1^{k_1} - 1}_{\neq 0}} \xi_2^{i_2 k_2} \cdots \xi_n^{i_n k_n} \\
&= \sum_{i_3=0}^{m_3-1} \cdots \sum_{i_n=0}^{m_n-1} 0 \cdot \frac{\overbrace{(\xi_2^{m_2})^{k_2} - 1}^{=0}}{\underbrace{\xi_2^{k_2} - 1}_{\neq 0}} \xi_3^{i_3 k_3} \cdots \xi_n^{i_n k_n} \\
&\vdots \\
&= 0
\end{aligned}$$

Therefore,

$$d(\boldsymbol{\xi}^{\boldsymbol{l}}) = \sum_{\boldsymbol{j} \in -\boldsymbol{I}} f_{\boldsymbol{j}} \overbrace{\sum_{\boldsymbol{i}=\boldsymbol{0}}^{\boldsymbol{m}-\boldsymbol{1}} \boldsymbol{\xi}^{\boldsymbol{i}(j+l)}}^{=0} = \boldsymbol{0}.$$

So, $B(-\boldsymbol{I}) \supseteq \mathcal{C}$. Therefore, the zeros of $\mathcal{C}$ are also zeros of $B(-\boldsymbol{I})$ and $B(-\boldsymbol{I})|_{\mathbb{F}_q} \supseteq \mathcal{C}$. Considered as vector spaces over $\mathbb{F}_q$, we have $\dim\left(B(-\boldsymbol{I})|_{\mathbb{F}_q}\right) = \dim(\mathcal{C})$. As a result, $B(-\boldsymbol{I})|_{\mathbb{F}_q} = \mathcal{C}$. □

Now we show that the code $B(-\boldsymbol{I})$ defined over $\mathbb{F}_{q^r}$ is Galois closed. For

$$f(\boldsymbol{\xi}^{\boldsymbol{i}}) = \sum_{\boldsymbol{j} \in -\boldsymbol{I}} f_{\boldsymbol{j}} \boldsymbol{\xi}^{\boldsymbol{ij}},$$

we have

$$f(\boldsymbol{\xi}^{\boldsymbol{i}})^q = \left(\sum_{\boldsymbol{j} \in -\boldsymbol{I}} f_{\boldsymbol{j}} \boldsymbol{\xi}^{\boldsymbol{ij}} \right)^q = \sum_{j \in -\boldsymbol{I}} f_{\boldsymbol{j}}^q \boldsymbol{\xi}^{q\boldsymbol{ij}}.$$

Note that if $\boldsymbol{j} \in -\boldsymbol{I}$ then $q\boldsymbol{j} \in -\boldsymbol{I}$, (we have $q\boldsymbol{j} = q(j_1, \ldots, j_n) = (qj_1, \ldots, qj_n)$), therefore $q(-\boldsymbol{I}) = -\boldsymbol{I}$. Set $g_{q\boldsymbol{j}} = f_{\boldsymbol{j}}^q$, where $g(\boldsymbol{x}) \in \mathbb{F}_{q^r}[\boldsymbol{x}]$ then

$$f(\boldsymbol{\xi}^{\boldsymbol{i}})^q = \sum_{\boldsymbol{j} \in -\boldsymbol{I}} g_{q\boldsymbol{j}} \boldsymbol{\xi}^{\boldsymbol{ij}} = \sum_{\boldsymbol{k}/q \in -\boldsymbol{I}} g_{\boldsymbol{k}} \boldsymbol{\xi}^{\boldsymbol{ik}}$$

with $g(x) = \sum_{\boldsymbol{k}/q \in -\boldsymbol{I}} g_{\boldsymbol{k}} \xi^{\boldsymbol{ik}}$. Therefore, we have $B(-\boldsymbol{I})^q = B(-\boldsymbol{I})$.

From Theorem 4 in Bierbrauer (2002), we obtain $\mathcal{C} = B(-\boldsymbol{I})|_{\mathbb{F}_q} = \mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(B(-\boldsymbol{I}))$ and we arrive at the equivalent characterization of nD-cyclic codes in terms of the trace map, given in Theorem 2.7.

Recall that $u(x) \star v(x) = \sum_{i \in \Omega} u_i v_i x^i$ in R. We naturally extend this to R_n as follows: let $u(\boldsymbol{x}) = \sum_{\boldsymbol{i} \in \boldsymbol{\Omega}} u_{\boldsymbol{i}} \boldsymbol{x}^{\boldsymbol{i}}$ and $v(\boldsymbol{x}) = \sum_{\boldsymbol{i} \in \boldsymbol{\Omega}} v_{\boldsymbol{i}} \boldsymbol{x}^{\boldsymbol{i}}$, then their *Schur product* is $u(\boldsymbol{x}) \star v(\boldsymbol{x}) = \sum_{\boldsymbol{i} \in \boldsymbol{\Omega}} u_{\boldsymbol{i}} v_{\boldsymbol{i}} \boldsymbol{x}^{\boldsymbol{i}}$. The following result generalizes Theorem 2.5.

Theorem 3.5 *Assume that $\mathcal{C}_1$ and $\mathcal{C}_2$ are two nD-cyclic codes over $\mathbb{F}_q$ with generating sets $\boldsymbol{I}_1$ and $\boldsymbol{I}_2$, respectively. Let*

$$B(-\boldsymbol{I}_1) = \left\{ \left(\sum_{\boldsymbol{j}_1 \in -\boldsymbol{I}_1} f_{\boldsymbol{j}_1} \xi^{\boldsymbol{i}\boldsymbol{j}_1} \right)_{\boldsymbol{i} \in \boldsymbol{\Omega}} : f_{\boldsymbol{j}_1} \in \mathbb{F}_{q^r}, \forall \boldsymbol{j}_1 \right\},$$

$$B(-\boldsymbol{I}_2) = \left\{ \left(\sum_{\boldsymbol{j}_2 \in -\boldsymbol{I}_2} g_{\boldsymbol{j}_2} \xi^{\boldsymbol{i}\boldsymbol{j}_2} \right)_{\boldsymbol{i} \in \boldsymbol{\Omega}} : g_{\boldsymbol{j}_2} \in \mathbb{F}_{q^r}, \forall \boldsymbol{j}_2 \right\}.$$

Then we have $B(-(\boldsymbol{I}_1 + \boldsymbol{I}_2))|_{\mathbb{F}_q} = \mathcal{C}_1 \star \mathcal{C}_2$.

Proof For any $\boldsymbol{i} \in \boldsymbol{\Omega}$, we have

$$\begin{aligned} \left(\sum_{\boldsymbol{j}_1 \in -\boldsymbol{I}_1} f_{\boldsymbol{j}_1} \xi^{\boldsymbol{i}\boldsymbol{j}_1} \right) \star \left(\sum_{\boldsymbol{j}_2 \in -\boldsymbol{I}_2} g_{\boldsymbol{j}_2} \xi^{\boldsymbol{i}\boldsymbol{j}_2} \right) &= \sum_{\boldsymbol{j}_1 \in -\boldsymbol{I}_1} \sum_{\boldsymbol{j}_2 \in -\boldsymbol{I}_2} f_{\boldsymbol{j}_1} g_{\boldsymbol{j}_2} \xi^{\boldsymbol{i}(\boldsymbol{j}_1 + \boldsymbol{j}_2)} \\ &= \sum_{\boldsymbol{k} \in -(\boldsymbol{I}_1 + \boldsymbol{I}_2)} h_{\boldsymbol{k}} \xi^{\boldsymbol{ik}}, \end{aligned}$$

where $h_{\boldsymbol{k}} = f_{\boldsymbol{j}_1} g_{\boldsymbol{j}_2}$ and $\boldsymbol{k} = \boldsymbol{j}_1 + \boldsymbol{j}_2$. □

Theorem 3.5 shows that the Schur product preserves the nD-cyclic property. By Theorem 1.2, along with the transitivity of nD-cyclic codes shown in Theorem 3.3, we conclude the following.

Corollary 3.6 *An nD-cyclic code pair $\mathcal{C}$ and $\mathcal{D}$ achieves the PIR rate $\frac{\dim(\mathcal{C} \star \mathcal{D})^\perp}{n}$ which protects against $(d_{\mathcal{D}^\perp} - 1)$-collusion.*

We note that if we have a 2D-cyclic code $\mathcal{C}$ of length $m \times \ell$ such that $\gcd(m, \ell) = 1$ then $\mathcal{C}$ is isomorphic to a cyclic code of the same length (see (Güneri and Özbudak 2012, Remark 3.6)). Therefore, we consider binary 2D-cyclic codes of length 63 in the following examples, where $m = 3$ and $\ell = 21$ or $m = 21$ and $\ell = 3$, so that at least one of the binary 2D-cyclic codes in consideration is not equivalent to a cyclic code.

We run a randomized search, via MAGMA (Bosma et al. 1997), over 2D-cyclic code pairs of length 63 over $\mathbb{F}_2$. We also list PIR parameters in Table 1 and 2 that have not been achieved using cyclic codes. In particular, it was listed in (Bodur et al. 2022, Example 2) that binary cyclic codes of length 63 can achieve the PIR rate $\frac{\dim(\mathcal{C} \star \mathcal{D})^\perp}{n}$ up to $6/63$ and collusion $d_{\mathcal{D}^\perp} - 1$ either 15 or 19. The generators for the codes with parameters given in our tables can be found in the Appendix.

Table 1 PIR rates and collusion numbers obtained by 2D-cyclic code pairs of length 63 over $\mathbb{F}_2$

	PIR rate	Collusion
1	7/63	15
2	8/63	15
3	9/63	15
4	11/63	15
5	6/63	17

The first approach is to search for a pair $\mathcal{C}$ and $\mathcal{D}$ of transitive codes and apply Corollary 3.6. This results in the PIR rate $\frac{\dim(\mathcal{C}\star\mathcal{D})^\perp}{n}$ and collusion parameter $d_{\mathcal{D}^\perp} - 1$. In the second approach, we fix the code $\mathcal{C}$ as a repetition code. Then $\mathcal{C}\star\mathcal{D} = \mathcal{D}$. It is not efficient to choose $\mathcal{C}$ to be a repetition code in terms of storage, but this choice yields better PIR rates since $\mathcal{C}\star\mathcal{D} = \mathcal{D}$.

Example 3.7 We consider the code $\mathcal{C} = [63, 2, 42]_2$ as data code and the retrieval code $\mathcal{D} = [63, 43, 5]_2$, whose generators can be found on item (1) of Codes from Table 1 in the Appendix. The dual code $\mathcal{D}^\perp$ has parameters $[63, 20, 16]_2$, and the dual of the Schur product is a $[63, 7, 24]_2$ code. Using Theorem 1.2, this results in a PIR rate of $7/63$ and collusion number 15.

We list parameters found by our randomized MAGMA search in Table 1 if the PIR rate is at least $6/63$ and the collusion number is at least 15, and one of the inequalities is strict. The parameters are ordered according to the collusion number first and then by the PIR rate.

Example 3.8 Now we consider the repetition code $\mathcal{C} = [63, 1, 63]_2$ as data code and the retrieval code $\mathcal{D} = [63, 51.3]_2$, whose generators can be found on item (1) of Codes from Table 2 in the Appendix. In this case $\mathcal{C}\star\mathcal{D} = \mathcal{D}$. The dual code $\mathcal{D}^\perp$ and the dual of the Schur product have parameters $[63, 12, 16]_2$. Using Theorem 1.2, this results in a PIR rate of $12/63$ and collusion number 15.

In Table 2, we list parameters obtained by our randomized search, where the storage code $\mathcal{C}$ is the repetition code (which is always 2D-cyclic), if the PIR rate is greater than $6/63$ and the collusion number is at least 15. The bold values in Table 2 improve both the PIR rate and the collusion number compared to the cyclic codes from (Bodur et al. 2022, Example 2).

4 Monomial Equivalence of *n*D-cyclic and *n*D-constacyclic codes

Let m be again a positive integer with $\gcd(m, q) = 1$. For a fixed $\alpha \in \mathbb{F}_q^*$, a linear code $\mathcal{C}_\alpha \subseteq \mathbb{F}_q^m$ is called a α-*constacyclic* code if it is invariant under the α-constashift of codewords, *i. e.*, $(c_0, \ldots, c_{m-1}) \in \mathcal{C}$ implies $(\alpha c_{m-1}, c_0, \ldots, c_{m-2}) \in \mathcal{C}$. In particular, if $\alpha = 1$ or $q = 2$, then $\mathcal{C}_\alpha$ is a cyclic code.

Consider the residue class ring $R_\alpha := \mathbb{F}_q[x]/\langle x^m - \alpha\rangle$. To an element $\mathbf{a} \in \mathbb{F}_q^m$, we associate an element of R_α via the following $\mathbb{F}_q$-module isomorphism:

$$\begin{aligned} \phi : \mathbb{F}_q^m &\longrightarrow R_\alpha \\ \mathbf{a} = (a_0, \ldots, a_{m-1}) &\longmapsto a(x) := a_0 + \cdots + a_{m-1}x^{m-1}. \end{aligned} \tag{4.1}$$

Observe that the α-constashift in $\mathbb{F}_q^m$ corresponds to multiplication by x in R_α. Therefore, an α-constacyclic code $\mathcal{C}_\alpha \subseteq \mathbb{F}_q^m$ can be viewed as an ideal of R_α. Since every ideal in R_α is

Table 2 PIR rates and collusion numbers obtained by 2D-cyclic code pairs of length 63 over $\mathbb{F}_2$ when the code $\mathcal{C}$ is a repetition code

	PIR rate	Collusion
1	12/63	15
2	16/63	15
3	17/63	15
4	19/63	15
5	8/63	17
6	16/63	17
7	11/63	19
8	13/63	19
9	**15/63**	**20**
10	**14/63**	**21**
11	**11/63**	**23**
12	**12/63**	**23**

principal, there exists a unique monic polynomial $g_\alpha(x) \in R_\alpha$ such that $\mathcal{C}_\alpha = \langle g_\alpha(x) \rangle$. The polynomial $g_\alpha(x)$, which is a divisor of $x^m - \alpha$, is called the *generator polynomial* of $\mathcal{C}_\alpha$.

Let r be the smallest divisor of $q-1$ with $\alpha^r = 1$ and let β be a primitive $(rm)^{\text{th}}$ root of unity such that $\beta^m = \alpha$. Then, $\xi := \beta^r$ is a primitive m^{th} root of unity and the roots of $x^m - \alpha$ are of the form $\beta, \beta\xi, \ldots, \beta\xi^{m-1}$. Let $\mathbb{F}$ be the smallest extension of $\mathbb{F}_q$ that contains β (equivalently, $\mathbb{F} = \mathbb{F}_q(\beta)$ so that $\mathbb{F}$ is the splitting field of $x^m - \alpha$). Given the α-constacyclic code $\mathcal{C}_\alpha = \langle g_\alpha(x) \rangle$, the set of roots of its generator polynomial, say $Z(\mathcal{C}_\alpha) := \{\beta\xi^k : g_\alpha(\beta\xi^k) = 0, 0 \le k \le m-1\}$, is called the *zero set* of $\mathcal{C}_\alpha$. All the results given in Section 2 can easily be adopted to constacyclic codes.

Recall that $\delta \in S_m$ represents the cyclic shift by 1 unit. Similarly, we can define $\delta_\alpha = \delta \cdot \mathrm{diag}(1, 1, \ldots, 1, \alpha)$ as the α-constacyclic shift by 1 unit operator. If X and X_α are the matrix representations of δ and δ_α, respectively, then

$$X = \overbrace{\begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}}^{\text{cyclic shift}}_{m\times m}, \quad X_\alpha = \overbrace{\begin{bmatrix} 0 & 0 & \cdots & 0 & \alpha \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}}^{\alpha\text{-constacyclic shift}}_{m\times m}.$$

Clearly, invariance under multiplication by X means being cyclic, and invariance under multiplication by X_α means being α-constacyclic. We would like to find a monomial matrix that demonstrates the monomial equivalence between cyclic and α-constacyclic codes. Observe that $X_\alpha = X \cdot \mathrm{diag}(1, 1, \ldots, 1, \alpha)$.

Given a cyclic code $\mathcal{C}$ and an α-constacyclic code $\mathcal{C}_\alpha$, let $G_\mathcal{C}$ and $G_{\mathcal{C}_\alpha}$ denote their generator matrices, respectively. We will find a monomial matrix M satisfying $G_{\mathcal{C}_\alpha} = G_\mathcal{C} M$ by using Lemma 2.8. If the matrix M is of the form

$$M = \begin{bmatrix} \mu_1 & 0 & \cdots & 0 \\ 0 & \mu_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mu_m \end{bmatrix}_{m\times m},$$

then we know that its inverse M^{-1} is

$$M^{-1} = \begin{bmatrix} \frac{1}{\mu_1} & 0 & \cdots & 0 \\ 0 & \frac{1}{\mu_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \frac{1}{\mu_m} \end{bmatrix}_{m\times m}.$$

In order to use Lemma 2.8, we first compute MXM^{-1}, as $X \in \mathtt{MAut}(\mathcal{C})$:

$$\begin{aligned} MXM^{-1} &= \begin{bmatrix} \mu_1 & 0 & \cdots & 0 \\ 0 & \mu_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mu_m \end{bmatrix} \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{\mu_1} & 0 & \cdots & 0 \\ 0 & \frac{1}{\mu_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \frac{1}{\mu_m} \end{bmatrix} \\ &= \begin{bmatrix} 0 & 0 & \cdots & 0 & \mu_1 \\ \mu_2 & 0 & \cdots & 0 & 0 \\ 0 & \mu_3 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \mu_m & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{\mu_1} & 0 & \cdots & 0 \\ 0 & \frac{1}{\mu_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \frac{1}{\mu_m} \end{bmatrix} \\ &= \begin{bmatrix} 0 & 0 & \cdots & 0 & \frac{\mu_1}{\mu_m} \\ \frac{\mu_2}{\mu_1} & 0 & \cdots & 0 & 0 \\ 0 & \frac{\mu_3}{\mu_2} & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \frac{\mu_m}{\mu_{m-1}} & 0 \end{bmatrix}. \end{aligned}$$

Since MXM^{-1} cannot be equal to some proper power of X_α, considering the support of the matrices, in order to satisfy $MXM^{-1} = X_\alpha$, we have to set $\mu_i = 1$, for all $1 \le i \le m$, which yields equality of X and X_α, but this does not hold unless $\alpha = 1$. Therefore, we multiply the left-hand-side by some nonzero element $\beta \in \mathbb{F}_q$ to avoid this. Now we solve for $\beta MXM^{-1} = X_\alpha$ as follows

$$\begin{bmatrix} 0 & 0 & \cdots & 0 & \frac{\mu_1}{\mu_m}\beta \\ \frac{\mu_2}{\mu_1}\beta & 0 & \cdots & 0 & 0 \\ 0 & \frac{\mu_3}{\mu_2}\beta & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \frac{\mu_m}{\mu_{m-1}}\beta & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & \cdots & 0 & \alpha \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}$$

From this equality, we get the following:

$$\begin{aligned}
&\frac{\mu_m}{\mu_{m-1}}\beta = 1 \Longrightarrow \mu_m = \mu_{m-1}\beta^{-1}\\
&\frac{\mu_{m-1}}{\mu_{m-2}}\beta = 1 \Longrightarrow \mu_{m-1} = \mu_{m-2}\beta^{-1} \Longrightarrow \mu_m = (\mu_{m-2}\beta^{-1})\beta^{-1} = \mu_{m-2}\beta^{-2}\\
&\qquad\vdots\\
&\frac{\mu_2}{\mu_1}\beta = 1 \Longrightarrow \mu_2 = \mu_1\beta^{-1} \qquad \Longrightarrow \mu_m = \mu_1\beta^{-(m-1)}\\
&\frac{\mu_1}{\mu_m}\beta = \alpha \Longrightarrow \mu_1 = \mu_m\beta^{-1}\alpha \qquad \Longrightarrow \mu_1 = \mu_1\beta^{-(m-1)}\beta^{-1}\alpha \qquad\qquad \Longrightarrow \alpha = \beta^m.
\end{aligned}$$

As a result, the variables μ_i can be written as

$$\begin{aligned}
\mu_1 &= \mu_m\beta^{m-1},\\
\mu_2 &= \mu_1\beta^{-1} = \mu_n\beta^{m-2},\\
&\vdots\\
\mu_{m-1} &= \mu_m\beta^{m-(m-1)} = \mu_m\beta.
\end{aligned}$$

Since $\alpha = \beta^m$, β is an m^{th} root of α. For a given $m \in \mathbb{N}$, an element $a \in \mathbb{F}_q^*$ has an m^{th} root in $\mathbb{F}_q$ if and only if $a^{(q-1)/d} = 1$, where $d = \gcd(q-1, m)$ (Lidl and Niederreiter 1997, Exercise 2.14). For $d = 1$, the following equivalence was shown in Bierbrauer (2002), and for $d \geq 1$, it was done in (Dastbasteh et al. 2025, Corollary 3.6).

Theorem 4.1 *Let* $\gcd(m, q) = 1$ *and* $\alpha \in \mathbb{F}_q^*$ *such that* $\alpha^{(q-1)/d} = 1$, *where* $d = \gcd(q-1, m)$. *Let* $\beta \in \mathbb{F}_q$ *be an* m^{th} *root of* α, *(i. e.,* $\alpha = \beta^m$*). Then, a* α*-constacyclic code* $\mathcal{C}_\alpha \subseteq \mathbb{F}_q^m$ *is monomially equivalent to a cyclic code* $\mathcal{C} \subseteq \mathbb{F}_q^m$, *where the equivalence is obtained via the matrix*

$$M = \begin{bmatrix} \beta^{m-1} & 0 & \cdots & 0 & 0\\ 0 & \beta^{m-2} & \cdots & 0 & 0\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ 0 & 0 & \cdots & \beta & 0\\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix}_{m\times m}.$$

In other words, if $\mathcal{C}_\alpha = \mathcal{C}M$ *such that* $\mathcal{C}$ *is a cyclic code, then* $\mathcal{C}_\alpha$ *is an* α*-constacyclic code. Moreover, if*

$$\mathcal{C} = \langle g(x)\rangle \subseteq R = \mathbb{F}_q[x]/\langle x^m - 1\rangle,$$

where $g(x) \mid (x^m - 1)$ *and* $g(x) = g_0 + g_1x + \cdots + g_{m-1}x^{m-1} \in R$, *then we have*

$$\mathcal{C}_\alpha = \langle g_\alpha(x)\rangle \subseteq R_\alpha = \mathbb{F}_q[x]/\langle x^m - \alpha\rangle,$$

where $g_\alpha(x) \mid (x^m - \alpha)$ *and*

$$g_\alpha(x) = \beta^{m-1}g_0 + \beta^{m-2}g_1x + \cdots + g_{m-1}x^{m-1} \in R_\alpha.$$

Proof First, we will show the monomial equivalence of codewords. Let $c \in \mathcal{C}$, then

$$c = (c_0, c_1, \ldots, c_{m-1}) \in \mathcal{C} \Longrightarrow c' = (c_{m-1}, c_0, c_1, \ldots, c_{m-2}) \in \mathcal{C}.$$

For $\mathcal{C}_\alpha = \{cM : c \in \mathcal{C}\}$, we want to show that $\mathcal{C}_\alpha$ is α-constacyclic. For this, we need

$$\begin{aligned} cM &= (\beta^{m-1}c_0, \beta^{m-2}c_1, \ldots, \beta c_{m-2}, c_{m-1}) \in \mathcal{C}_\alpha \\ &\Longrightarrow (\alpha c_{m-1}, \beta^{m-1}c_0, \beta^{m-2}c_1, \ldots, \beta c_{m-2}) \in \mathcal{C}_\alpha. \end{aligned}$$

By cyclicity of $\mathcal{C}$, $c'M \in \mathcal{C}_\alpha$, therefore

$$(\beta^{m-1}c_{m-1}, \beta^{m-2}c_0, \beta^{m-3}c_1, \ldots, \beta c_{m-3}, c_{m-2}) \in \mathcal{C}_\alpha, \tag{4.2}$$

and since $\mathcal{C}_\alpha$ is linear code and $\beta c'M \in \mathcal{C}_\alpha$, we have

$$(\beta^m c_{m-1}, \beta^{m-1}c_0, \beta^{m-2}c_1, \ldots, \beta c_{m-2}) = (\alpha c_{m-1}, \beta^{m-1}c_0, \beta^{m-2}c_1, \ldots, \beta c_{m-2}) \in \mathcal{C}_\alpha. \tag{4.3}$$

Now we will prove the relation between the generator polynomials. Let $g(x) = g_0 + g_1x + \cdots + g_{m-1}x^{m-1}$ be the generator polynomial of $\mathcal{C}$ such that $g(x) \mid (x^m - 1)$. For $\alpha = \beta^m$, let $g_\alpha(x) = \beta^{m-1}g_0 + \beta^{m-2}g_1x + \cdots + g_{m-1}x^{m-1}$. Assume that $x = \beta y$, then

$$x^m - \alpha = \beta^m y^m - \alpha = \alpha y^m - \alpha = \alpha(y^m - 1)$$

and

$$\begin{aligned} g_\alpha(x) &= g_0\beta^{m-1} + g_1\beta^{m-2}x + \cdots + g_{m-1}x^{m-1} \\ &= g_0\beta^{m-1} + g_1\beta^{m-2}\beta y + g_2\beta^{m-3}\beta^2 y + \cdots \\ &\quad + g_{m-2}\beta\beta^{m-2}y^{m-2} + g_{m-1}\beta^{m-1}y^{m-1} \\ &= \beta^{m-1}(g_0 + g_1y + \cdots + g_{m-1}y^{m-1}) \\ &= \beta^{m-1}g(y). \end{aligned}$$

So,

$$y^m - 1 = \left(\frac{x}{\beta}\right)^m - 1 = \frac{x^m - \beta^m}{\beta^m} = \frac{x^m - \alpha}{\alpha}.$$

Since $g(x) \mid (x^m - 1)$, it is obvious that $g(y) \mid (y^m - 1)$. Then

$$\begin{aligned} g(y) \mid \left(y^m - 1\right) \text{ and } y^m - 1 = \frac{x^m - \alpha}{\alpha} &\Longrightarrow \beta^{m-1}g(y) \left| \frac{\beta^{m-1}(x^m - \alpha)}{\alpha} \right. \\ &\Longrightarrow \beta^{m-1}g(y) \left| \frac{x^m - \alpha}{\beta} \right. \\ &\Longrightarrow g_\alpha(x) \left| \frac{x^m - \alpha}{\beta} \right. \\ &\Longrightarrow g_\alpha(x) \mid \left(x^m - \alpha\right) \end{aligned}$$

since β is constant. □

We can start generalizing Theorem 4.1 above to the 2D setup as follows. An nD constacyclic code of length $m_1 \times \cdots \times m_n$ is an ideal in $\mathbb{F}_q[x_1, \ldots, x_n]/\langle x_1^{m_1} - \alpha_1, \ldots, x_n^{m_n} - \alpha_n\rangle$ (see Ling and Özkaya (2019)).

Theorem 4.2 *Let $s \geq 1$ and $\gcd(m\ell, q) = 1$. Let $\alpha, \delta \in \mathbb{F}_q^*$ such that $\alpha^{(q-1)/d_1} = 1$ and $\delta^{(q-1)/d_2} = 1$, where $d_1 = \gcd(q-1, m)$ and $d_2 = \gcd(q-1, \ell)$. Let $\beta, \gamma \in \mathbb{F}_q$ be an m^{th}*

root of α and an ℓ^{th} root of δ, respectively (i. e., $\alpha = \beta^m$ and $\delta = \gamma^\ell$). If the 2D-cyclic code $\mathcal{C}$ is generated by $g_1(x, y), \ldots, g_s(x, y) \in \mathbb{F}_q[x, y]/\langle x^m - 1, y^\ell - 1\rangle$, where

$$g_t(x, y) = \sum_{i=0}^{m-1} \sum_{j=0}^{l-1} g_{i,j,t} x^i y^j$$

for $1 \le t \le s$, then the monomially equivalent (α, δ)-constacyclic code $\mathcal{C}_{\alpha,\delta}$ is generated by $g_{\alpha,\delta,1}(x, y), \ldots, g_{\alpha,\delta,s}(x, y) \in \mathbb{F}_q[x, y]/\langle x^m - \alpha, y^\ell - \delta\rangle$, where

$$g_{\alpha,\delta,t}(x, y) = \sum_{i=0}^{m-1} \sum_{j=0}^{l-1} \beta^{m-1-i} \gamma^{l-1-j} g_{i,j,t} x^i y^j$$

for $1 \le t \le s$.

Proof Any non-zero ideal in $\mathbb{F}_q[x, y]/\langle x^m - 1, y^\ell - 1\rangle$ is of the form $\langle \{g_t(x, y) : t \in I\}, x^m - 1, y^\ell - 1\rangle$ with $\emptyset \ne I \subseteq \mathbb{Z}^+$. It can be shown that the codewords of $\mathcal{C}_{\alpha,\delta}$ generated by $g_{\alpha,\delta,1}(x, y), \ldots, g_{\alpha,\delta,s}(x, y) \in \mathbb{F}_q[x, y]/\langle x^m - \alpha, y^\ell - \delta\rangle$ are invariant under α-row-constashift and δ-column-constashift by following the steps in (4.2) and (4.3).

Moreover the map $g_{\alpha,\delta,t}(x, y) \longmapsto g_{\alpha,\delta,t}(\beta x, \gamma y)$ for $t \in I$ sends the ideal in $\mathbb{F}_q[x, y]/\langle x^m - \alpha, y^\ell - \delta\rangle$ to an ideal in $\mathbb{F}_q[u, v]/\langle u^m - 1, v^\ell - 1\rangle$, where $u = \beta x$ and $v = \gamma y$ as in the proof of Theorem 4.1 above. □

Theorem 4.2 can be generalized to the nD case as follows:

Theorem 4.3 *Let $s \ge 1$ and $\gcd(m_1 \cdots m_n, q) = 1$. Let $\boldsymbol{\alpha} = (\alpha_1, \ldots \alpha_n) \in (\mathbb{F}_q^*)^n$ such that $\alpha_\nu^{(q-1)/d_\nu} = 1$, where $d_\nu = \gcd(q - 1, m_\nu)$ for $1 \le \nu \le n$. Let $\boldsymbol{\beta} \in (\mathbb{F}_q^*)^n$ be an $\boldsymbol{m}^{\text{th}}$ root of $\boldsymbol{\alpha}$ (i. e., $\alpha_\nu = \beta_\nu^{m_\nu}$ for $1 \le \nu \le n$). If the nD-cyclic code $\mathcal{C}$ is generated by $g_1(\boldsymbol{x}), \ldots, g_s(\boldsymbol{x}) \in \mathbb{F}_q[x_1, \ldots, x_n]/\langle x_1^{m_1} - 1, \ldots, x_n^{m_n} - 1\rangle$, then the monomially equivalent $(\boldsymbol{\alpha})$-constacyclic code $\mathcal{C}_{\boldsymbol{\alpha}}$ is generated by $g_{\boldsymbol{\alpha},1}(\boldsymbol{x}), \ldots, g_{\boldsymbol{\alpha},s}(\boldsymbol{x}) \in \mathbb{F}_q[x_1, \ldots, x_n]/\langle x_1^{m_1} - \alpha_1, \ldots, x_n^{m_n} - \alpha_n\rangle$, where*

$$g_{\boldsymbol{\alpha},t}(x) = \sum_{\boldsymbol{i} \in \boldsymbol{\Omega}} \boldsymbol{\beta}^{\boldsymbol{m}-1-\boldsymbol{i}} g_{\boldsymbol{i},t} \boldsymbol{x}^{\boldsymbol{i}}$$

for $1 \le t \le s$.

Using monomial equivalence of codes, one obtains equivalent PIR schemes. In some cases, with a suitable choice of monomial matrices or polynomial coefficients, nD-constacyclic codes can be transformed to nD-cyclic codes. Both families can be considered as transitive codes under the constraints of Theorem 4.3.

Appendix

Codes from Table 1

Let $R_{63} := \mathbb{F}_q[x]/\langle x^{21} - 1, y^3 - 1\rangle$. The following generators correspond to Table 1.

(1) For PIR rate $7/63$ and collusion number 15, the generators of $\mathcal{C} = [63, 2, 42]_2$ are

$$\begin{aligned}&\langle y^2\left(x^{19}+x^{18}+x^{16}+x^{15}+x^{13}+x^{12}+x^{10}+x^9+x^7+x^6+x^4+x^3+x+1\right)\\&+y\left(x^{20}+x^{18}+x^{17}+x^{15}+x^{14}+x^{12}+x^{11}+x^9+x^8+x^6+x^5+x^3+x^2+1\right)\\&+x^{20}+x^{19}+x^{17}+x^{16}+x^{14}+x^{13}+x^{11}\\&+x^{10}+x^8+x^7+x^5+x^4+x^2+x\rangle \in R_{63}\end{aligned}$$

and the generators of $\mathcal{D}$ are

$$\begin{aligned}&\langle y^2+y\left(x^7+x^6+x^5+x^4+x^2\right)+x^9+x^8+x^7+x^5+x^4+x^2+x+1,\\&y\left(x^9+x^8+x^5+x^4+x^2+x+1\right)+x^{10}+x^8+x^6+x^4+x^3+1,\\&x^{11}+x^8+x^7+x^2+1\rangle \in R_{63}.\end{aligned}$$

The dual $(\mathcal{C}\star\mathcal{D})^\perp$ of the Schur product and the code $\mathcal{D}^\perp$ have parameters $[63, 7, 24]_2$ and $[63, 20, 16]_2$, respectively.

(2) For PIR rate $8/63$ and collusion number 15, the generators of $\mathcal{C} = [63, 2, 42]_2$ are

$$\begin{aligned}&\langle y^2\left(x^{19}+x^{18}+x^{16}+x^{15}+x^{13}+x^{12}+x^{10}+x^9+x^7+x^6+x^4+x^3+x+1\right)\\&+y\left(x^{20}+x^{18}+x^{17}+x^{15}+x^{14}+x^{12}+x^{11}+x^9+x^8+x^6+x^5+x^3+x^2+1\right)\\&+x^{20}+x^{19}+x^{17}+x^{16}+x^{14}+x^{13}+x^{11}+x^{10}\\&+x^8+x^7+x^5+x^4+x^2+x\rangle \in R_{63}\end{aligned}$$

and the generators of $\mathcal{D}$ are

$$\begin{aligned}&\langle y^2(x+1)+y\left(x^6+x^5+x^4+1\right)+x^7+x^3+x+1,\\&y\left(x^7+x^6+x^5+x^4+x^3+1\right)+x^8+x^7+x^6+x^5+x^4+x,\\&x^9+x^7+x^6+x^5+x^3+x^2+x+1\rangle \in R_{63}.\end{aligned}$$

The dual $(\mathcal{C}\star\mathcal{D})^\perp$ of the Schur product and the code $\mathcal{D}^\perp$ have parameters $[63, 8, 24]_2$ and $[63, 17, 16]_2$, respectively.

(3) For PIR rate $9/63$ and collusion number 15, the generators of $\mathcal{C} = [63, 2, 42]_2$ are

$$\begin{aligned}&\langle(y^2+y+1)(x^{19}+x^{18}+x^{16}+x^{15}+x^{13}+x^{12}\\&+x^{10}+x^9+x^7+x^6+x^4+x^3+x+1)\rangle \in R_{63}\end{aligned}$$

and the generators of $\mathcal{D}$ are

$$\begin{aligned}&\langle y^2+y+x^{11}+x^9+x^8+x^4+x,\\&y\left(x^7+x^4+x^3+x^2+x+1\right)+x^7+x^4+x^3+x^2+x+1,\\&x^{13}+x^{11}+x^{10}+x^8+x^7+x^6+x^5+x^3+x^2+1\rangle \in R_{63}.\end{aligned}$$

The dual $(\mathcal{C}\star\mathcal{D})^\perp$ of the Schur product and the code $\mathcal{D}^\perp$ have parameters $[63, 9, 24]_2$ and $[63, 20, 16]_2$, respectively.

(4) For PIR rate 11/63 and collusion number 15, the generators of $\mathcal{C} = [63, 2, 42]_2$ are

$$\begin{aligned}\langle y^2 &\left(x^{19}+x^{18}+x^{16}+x^{15}+x^{13}+x^{12}+x^{10}+x^9+x^7+x^6+x^4+x^3+x+1\right)\\ &+y\left(x^{20}+x^{19}+x^{17}+x^{16}+x^{14}+x^{13}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x\right)\\ &+x^{20}+x^{18}+x^{17}+x^{15}+x^{14}+x^{12}+x^{11}\\ &+x^9+x^8+x^6+x^5+x^3+x^2+1\rangle \in R_{63}\end{aligned}$$

and the generators of $\mathcal{D}$ are

$$\begin{aligned}&\langle y^2(x+1)+y(x+1)+x^{15}+x^{14}+x^{13}+x^{12}+x^8+x^6+x^4+x^3+x+1,\\ &y\left(x^4+x^2+x+1\right)+x^{17}+x^{16}+x^{14}+x^{11}+x^{10}+x^9+x^7+x^5+x^4+x^3+x^2+x,\\ &x^{18}+x^{16}+x^{15}+x^{14}+x^{11}+x^9+x^8+x^7+x^4+x^2+x+1\rangle \in R_{63}.\end{aligned}$$

The dual $(\mathcal{C}\star\mathcal{D})^\perp$ of the Schur product and the code $\mathcal{D}^\perp$ have parameters $[63, 11, 24]_2$ and $[63, 23, 16]_2$, respectively.

(5) For PIR rate 6/63 and collusion number 17, the generators of $\mathcal{C} = [63, 2, 42]_2$ are

$$\begin{aligned}\langle y^2 &\left(x^{20}+x^{19}+x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}\right.\\ &\left.+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1\right)\\ &+x^{20}+x^{19}+x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}\\ &+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1,\\ &y\left(x^{20}+x^{19}+x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}\right.\\ &\left.+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1\right)\\ &+x^{20}+x^{19}+x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}\\ &+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1\rangle \in R_{63}\end{aligned}$$

and the generators of $\mathcal{D}$ are

$$\begin{aligned}&\langle y^2(x+1)+y(x+1)+x+1,\\ &y\left(x^4+x^2+x+1\right)+x^5+x^3+x^2+x,\\ &+x^6+x^5+x^2+1\rangle \in R_{63}.\end{aligned}$$

The dual $(\mathcal{C}\star\mathcal{D})^\perp$ of the Schur product and the code $\mathcal{D}^\perp$ have parameters $[63, 6, 21]_2$ and $[63, 11, 18]_2$, respectively.

Codes from Table 2

Let the code $\mathcal{C} = [63, 1, 63]_2$ be the repetition code and let $\langle g(x, y)\rangle \in R_{63}$ be the generator of $\mathcal{C}$, where

$$\begin{aligned}g(x,y) =&(y^2+y+1)\left(x^{20}+x^{19}+x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}\right.\\ &\left.+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1\right).\end{aligned}$$

We have found the following generators for the 2D-cyclic code $\mathcal{D}$ which give the parameters listed in Table 2, where $\mathcal{C}$ is fixed as the repetition code of length 63. In this case $\mathcal{C}\star\mathcal{D} = \mathcal{D}$.

(1) For PIR rate 12/63 and collusion number 15, the generators of $\mathcal{D}$ are

$$\begin{aligned}&\langle y^2 + y + 1,\\ &y\left(x^6 + x^5 + x^4 + x^2 + 1\right),\\ &x^6 + x^5 + x^4 + x^2 + 1\rangle \in R_{63}\end{aligned}$$

The dual code $\mathcal{D}^{\perp}$ has parameters $[63, 12, 16]_2$.

(2) For PIR rate 16/63 and collusion number 15, the generators of $\mathcal{D}$ are

$$\begin{aligned}&\langle y^2 + y\left(x^4 + x^3 + x^2 + x + 1\right) + x^8 + x^6 + x^4 + x^2 + 1,\\ &y\left(x^7 + x^4 + x^3 + x^2 + x + 1\right) + x^7 + x^4 + x^3 + x^2 + x + 1,\\ &x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + 1\rangle \in R_{63}\end{aligned}$$

The dual code $\mathcal{D}^{\perp}$ has parameters $[63, 16, 16]_2$.

(3) For PIR rate 17/63 and collusion number 15, the generators of $\mathcal{D}$ are

$$\begin{aligned}&\langle y^2 + y\left(x^4 + x^3 + x^2 + x\right) + x^4 + x^3 + x^2 + x + 1,\\ &y\left(x^6 + x^5 + x^4 + x^2 + 1\right) + x^9 + x^8 + x^6 + x,\\ &x^{11} + x^8 + x^7 + x^2 + 1\rangle \in R_{63}\end{aligned}$$

The dual code $\mathcal{D}^{\perp}$ has parameters $[63, 17, 16]_2$.

(4) For PIR rate 19/63 and collusion number 15, the generators of $\mathcal{D}$ are

$$\begin{aligned}&\langle y^2 + y + x^12 + x^6 + x^3,\\ &y\left(x^4 + x^3 + x^2 + 1\right) + x^{14} + x^{13} + x^{12} + x^9 + x^7 + x^6 + x^5 + x^4 + x^3 + 1,\\ &x^{15} + x^{14} + x^{12} + x^9 + x^8 + x^5 + x^2 + 1\rangle \in R_{63}\end{aligned}$$

The dual code $\mathcal{D}^{\perp}$ has parameters $[63, 19, 16]_2$.

(5) For PIR rate 8/63 and collusion number 17, the generators of $\mathcal{D}$ are

$$\begin{aligned}&\langle y^2 + x^7,\\ &y + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,\\ &x^8 + x^6 + x^5 + x^4 + x^3 + x^2 + 1\rangle \in R_{63}\end{aligned}$$

The dual code $\mathcal{D}^{\perp}$ has parameters $[63, 8, 18]_2$.

(6) For PIR rate 16/63 and collusion number 17, the generators of $\mathcal{D}$ are

$$\begin{aligned}&\langle y^2 + y + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^3 + x,\\ &y\left(x^4 + x^3 + x^2 + 1\right) + x^{11} + x^9 + x^8 + x^7 + x^6 + x^2,\\ &x^{12} + x^{11} + x^9 + x^7 + x^3 + x^2 + x + 1\rangle \in R_{63}\end{aligned}$$

The dual code $\mathcal{D}^{\perp}$ has parameters $[63, 16, 18]_2$.

(7) For PIR rate $11/63$ and collusion number 19, the generators of $\mathcal{D}$ are

$$\begin{aligned}&\langle y^2\,(x+1)+x^8+x^4+x^3+x^2,\\ &\ y\,(x+1)+x^7+x^5+x^4+x^3+x^2+x,\\ &\ x^9+x^8+x^7+x^6+x^4+x^3+x^2+1\rangle \in R_{63}\end{aligned}$$

The dual code $\mathcal{D}^\perp$ has parameters $[63, 11, 20]_2$.

(8) For PIR rate $13/63$ and collusion number 19, the generators of $\mathcal{D}$ are

$$\begin{aligned}&\langle y^2+y+x^{11}+x^{10}+x^9+x^6+x^5+x+1,\\ &\ y\,(x+1)+x^6+x^5+x^4+1,\\ &\ x^{12}+x^{11}+x^{10}+x^9+x^5+x^3+x+1\rangle \in R_{63}\end{aligned}$$

The dual code $\mathcal{D}^\perp$ has parameters $[63, 13, 20]_2$.

(9) For PIR rate $15/63$ and collusion number 20, the generators of $\mathcal{D}$ are

$$\begin{aligned}&\langle y^2+y+x^{10}+x^9+x^6+x^5+x^3+x^2+x+1,\\ &\ y\left(x^3+x+1\right)+x^{11}+x^9+x^6+x^5+x^3+x+1,\\ &\ x^{12}+x^{11}+x^9+x^7+x^3+x^2+x+1\rangle \in R_{63}\end{aligned}$$

The dual code $\mathcal{D}^\perp$ has parameters $[63, 15, 21]_2$.

(10) For PIR rate $14/63$ and collusion number 21, the generators of $\mathcal{D}$ are

$$\begin{aligned}&\langle y^2+y+1,\\ &\ y\left(x^3+x+1\right)+x^7+x^6+x^4+x,\\ &\ x^{11}+x^8+x^7+x^2+1\rangle \in R_{63}\end{aligned}$$

The dual code $\mathcal{D}^\perp$ has parameters $[63, 14, 22]_2$.

(11) For PIR rate $11/63$ and collusion number 23, the generators of $\mathcal{D}$ are

$$\begin{aligned}&\langle y^2+y+x^7+x^6+x^5+x^3,\\ &\ y\left(x^3+x^2+1\right)+x^6+x^5+x^4+x,\\ &\ x^8+x^6+x^5+x^4+x^3+x^2+1\rangle \in R_{63}\end{aligned}$$

The dual code $\mathcal{D}^\perp$ has parameters $[63, 11, 24]_2$.

(12) For PIR rate $12/63$ and collusion number 23, the generators of $\mathcal{D}$ are

$$\begin{aligned}&\langle y^2+x^9+x^7+x^4+x^2+x+1,\\ &\ y+x^{11}+x^8+x^7+x^2,\\ &\ x^{12}+x^{11}+x^9+x^8+x^6+x^4+x^3+x+1\rangle \in R_{63}\end{aligned}$$

The dual code $\mathcal{D}^\perp$ has parameters $[63, 12, 24]_2$.

Acknowledgements Markus Grassl is supported by grant no. FENG.02.01-IP.05-0006/23, financed by the European Funds for a Smart Economy 2021-2027 (FENG), Priority FENG.02 Innovation-friendly environment, Measure FENG.02.01. The last three authors were supported by TÜBİTAK project 223N065. This work was presented at the International Conference on Finite Fields and Their Applications 2025 (Fq16), where the travel was supported by TÜBİTAK 2224-A program. The authors have no relevant financial or non-financial interests to disclose.

Funding Open access funding provided by the Scientific and Technological Research Council of Türkiye (TüBiTAK).

Data Availability Not applicable.

References

Bierbrauer J (2002) The theory of cyclic codes and a generalization to additive codes. Des Codes Crypt 25:189–206

Bodur Ş, Martínez-Moro E, Ruano D (2022) Private information retrieval schemes using cyclic codes. In International Workshop on the Arithmetic of Finite Fields, pages 194–207. Springer,

Bosma W, Cannon J, Playoust C (1997) The Magma algebra system.I. The user language. J. Symbolic Comput. 24(3–4):235–265 (**Computational algebra and number theory (London, 1993)**)

Cascudo I (2018) On squares of cyclic codes. IEEE Trans Inf Theory 65(2):1034–1047

Dastbasteh R, Padashnick F, Crespo P, Grassl M, Sharafi J (2025) Equivalence of constacyclic codes with shift constants of different orders. Des Codes Crypt 93(1):79–93

Freij-Hollanti R, Gnilke OW, Hollanti C, Horlemann-Trautmann A-L, Karpuk D, Kubjas I (2018) t-private information retrieval schemes using transitive codes. IEEE Trans Inf Theory 65(4):2107–2118

Güneri C, Özbudak F (2008) Multidimensional cyclic codes and Artin-Schreier type hypersurfaces over finite fields. Finite Fields Appl 14(1):44–58

Güneri C, Özbudak F (2012) A relation between quasi-cyclic codes and 2-D cyclic codes. Finite Fields Appl 18(1):123–132

Güneri C, Özkaya B (2016) Multidimensional quasi-cyclic and convolutional codes. IEEE Trans Inf Theory 62(12):6772–6785

Huffman WC, Pless V (2010) Fundamentals of error-correcting codes. Cambridge University Press

Lidl R, Niederreiter H (1997) Finite Fields. Cambridge University Press

Ling S, Özkaya B (2019) Multidimensional quasi-twisted codes: equivalent characterizations and their relation to multidimensional convolutional codes. Des Codes Crypt 87:2941–2965

Wolfmann J (1989) New bounds on cyclic codes from algebraic curves. In Lecture Notes in Computer Science, volume 388, pages 47–62. New York: Springer-Verlag