Research Article

Matrix-Product Codes over Commutative Rings and Constructions Arising from (σ, δ) -Codes

Mhammed Boulagouaz¹ and Abdulaziz Deajim²

¹Department of Mathematics, Faculty of Sciences and Technologies, University of Sidi Mohamed Ben Abdellah, B.P. 2202, Fes, Morocco

²Department of Mathematics, King Khalid University, P.O. Box 9004, Abha, Saudi Arabia

Correspondence should be addressed to Abdulaziz Deajim; deajim@gmail.com

Received 28 January 2021; Accepted 11 February 2021; Published 3 March 2021

Academic Editor: Marco Fontana

Copyright © 2021 Mhammed Boulagouaz and Abdulaziz Deajim. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

A well-known lower bound (over finite fields and some special finite commutative rings) on the Hamming distance of a matrix-product code (MPC) is shown to remain valid over any commutative ring R . A sufficient condition is given, as well, for such a bound to be sharp. It is also shown that an MPC is free when its input codes are all free, in which case a generator matrix is given. If R is finite, a sufficient condition is provided for the dual of an MPC to be an MPC, a generator matrix for such a dual is given, and characterizations of LCD, self-dual, and self-orthogonal MPCs are presented. Finally, the results of this paper are used along with previous results of the authors to construct novel MPCs arising from (σ, δ) -codes. Some properties of such constructions are also studied.

1. Introduction

Over the past two decades, studying codes over commutative rings (especially finite ones) and their properties has been attracting a great deal of attention. As far as engineering applications are concerned, it is understood that codes over special types of commutative rings are more relevant; namely, finite Frobenius rings. For a very nice survey of such development, and for relevant references, one can check [1–3]. From a purely mathematical point of view, however, the authors believe that when certain results can be verified over more general commutative rings, then it would be reasonable to pursue such approach for the sake of mathematical interest (an example of such approach is seen in [3]).

1.1. Linear Codes. In this work, if not otherwise specified, R denotes a commutative ring with identity and $U(R)$ the multiplicative group of all invertible elements of R . A nonempty subset C of the free R -module R^n is called a code

over R of length n , and an element of C is called a codeword. If C is an R -submodule of R^n , then C is called a linear code over R . The R -submodule of R^n generated by a code in R^n is obviously a linear code over R , so all codes considered in this paper are linear. If C is a free R -submodule of R^n of rank k (i.e., C has an R -basis whose cardinality is k), then C is called a free linear code over R of rank k , and we express this by saying that C is an $[n, k]$ -linear code over R . If C is an $[n, k]$ -linear code over R , we say that a matrix $G \in M_{k,n}(R)$ is a generator matrix of C if the rows of G form an R -basis of C . We, thus, write $C = \{xG \mid x \in R^k\}$.

On the free R -module R^n , consider the (Euclidean) bilinear form $\langle \cdot, \cdot \rangle: R^n \times R^n \rightarrow R$ defined by $\langle (x_1, \dots, x_n), (y_1, \dots, y_n) \rangle = \sum_{i=1}^n x_i y_i$. With respect to this bilinear form, define the dual $C^\perp$ of any code C over R by $C^\perp = \{x \in R^n \mid \langle x, y \rangle = 0 \text{ for all } y \in C\}$. It is easy to check that $C^\perp$ is a linear code over R if C is so. When $C \subseteq C^\perp$ (resp. $C = C^\perp$), we say that C is self-orthogonal (resp., self-dual). A code C is called linear complementary dual (LCD for short) if $C \cap C^\perp = \{0\}$ (see [4]).

1.2. Matrix-Product Codes. Constructing codes (with certain properties) from smaller ones has lately been an important problem in pursuit by coding theorists. In particular, studying the effect of the properties of the smaller codes on the properties of the constructed codes is crucial. An interesting such construction is the construction of matrix-product codes over finite fields first introduced by Blackmore and Norton in [5]. Ever since the introduction, researchers have been trying to pave new tracks in this area. Particularly relevant to us here are constructions of matrix-product codes over various commutative rings (see, for instance, [6–11]).

Let C_i be an $[n, k_i]$ -linear code over R , for $i = 1, \dots, s$. Writing codewords of the codes C_i in column form, let $(c_1, \dots, c_s)$ be the $n \times s$ matrix whose columns are $c_1 \in C_1, \dots, c_s \in C_s$. Consider the following subset of the set $M_{n \times s}(R)$ of $n \times s$ matrices with entries in R :

$$[C_1, \dots, C_s] = \{(c_1, \dots, c_s) | c_i \in C_i, i = 1, \dots, s\}. \quad (1)$$

For $s \leq l$ and a matrix $A \in M_{s \times l}(R)$, define the matrix-product code associated with $C_1, \dots, C_s$ and A to be

$$[C_1, \dots, C_s]A := \{(c_1, \dots, c_s)A | c_i \in C_i, i = 1, \dots, s\} \subseteq M_{n \times l}(R). \quad (2)$$

As the three R -modules $M_{n \times l}(R)$, R^{nl} , and $(R^n)^l$ are isomorphic, $[C_1, \dots, C_s]A$ can be thought of as a code of length nl over R in an obvious way, and we can look at codewords of $[C_1, \dots, C_s]A$ as elements of either of these three modules. More specifically, if $A = (a_{ij})$ and $c_i = (x_{1i}, \dots, x_{ni})^t \in C_i$ for $i = 1, \dots, s$, then the codeword $(c_1, \dots, c_s)A$ of $[C_1, \dots, C_s]A$ is the matrix:

$$\left(\sum_{i=1}^s x_{1i}a_{i1} \cdots \sum_{i=1}^s x_{1i}a_{il} \sum_{i=1}^s x_{2i}a_{i1} \cdots \sum_{i=1}^s x_{2i}a_{il} : \cdots : \sum_{i=1}^s x_{ni}a_{i1} \cdots \sum_{i=1}^s x_{ni}a_{il} \right) \in M_{n \times l}(R). \quad (3)$$

This matrix can be identified with the its corresponding element of R^{nl} , so the codeword $(c_1, \dots, c_s)A$ can be looked at as the following element:

$$\left(\sum_{i=1}^s x_{1i}a_{i1}, \dots, \sum_{i=1}^s x_{1i}a_{il}, \dots, \sum_{i=1}^s x_{ni}a_{i1}, \dots, \sum_{i=1}^s x_{ni}a_{il} \right) \in R^{nl}. \quad (4)$$

On the contrary, as the k th column of the above matrix is $\sum_{i=1}^s a_{ik}c_i \in R^n$, the codeword $(c_1, \dots, c_s)A$ can be looked at as the following l -tuple with coordinates from R^n :

$$\left(\sum_{i=1}^s a_{i1}c_i, \dots, \sum_{i=1}^s a_{il}c_i \right) \in (R^n)^l. \quad (5)$$

It should be noted that $[C_1, \dots, C_s]A$ is linear if all C_i are linear.

Some of the well-known code constructions turned out to be matrix-product codes. For instance, the Plotkins $(u|u+v)$ -construction and the ternary $(u+v+w|2u+v|u)$ -construction are only examples of matrix-product codes with matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 2 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$, respectively (see [5]). Moreover, recent new constructions of linear codes arising from matrix-product codes have been evolving (see [7, 12–16]).

1.3. Points of Investigation and Contributions. In general, some of the serious differences between linear codes over fields versus linear codes over commutative rings are apparent from the following:

- (1) A linear code $C \subseteq R^n$ may not be free. Due to this, it is not possible to talk about a generator matrix of a nonfree code in the sense of the definition of such a matrix we have given. In this regard, we give in Proposition 2 sufficient conditions for a matrix-product code over a commutative ring to be free, and we also give its generator matrix in Corollary 1.
- (2) When a code C is free over R , its dual $C^\perp$ may not be free. Even if C and $C^\perp$ are both free codes over R of length n , the equality $\text{rank}(C) + \text{rank}(C^\perp) = n$ may not hold. With respect to these issues, it follows from [10, Proposition 2.9] that if R is a finite commutative ring and C is an $[n, k]$ -linear code over R , then $C^\perp$ is an $[n, n-k]$ -linear code over R . So, in our relevant results, we work over finite commutative rings. Nonetheless, as was stated earlier, whenever a result can be proved valid over more general rings, then we state it and prove in such generality.
- (3) In an effort to extend results on the minimum Hamming distance of matrix-product codes over finite fields to those over general commutative rings, we prove in Theorem 1 that a well-known lower bound for the minimum distance of a matrix-product code over a finite field or a finite chain ring remains valid over a commutative ring and we, further, give a sufficient condition for such a lower bound to be sharp.
- (4) When we impose finiteness on R , more results are proved. Over such a ring, we generalize in Proposition 3 a well-know fact that tells when the dual of a matrix-product code is also a matrix-product code. This is used in Corollary 2 to give a generator matrix of the dual for a matrix-product code, and it is also used in Corollary 3 to give characterizations of self-dual, self-orthogonal, and LCD matrix-product codes.

- (5) As an interesting application, we study in Section 4 matrix-product codes arising from (σ, δ) -codes over finite commutative rings. In this section, we bring together results from the authors' work [17] and results proved in this paper to construct matrix-product codes out of (σ, δ) -codes, give generator matrices for such codes and their dual codes (Propositions 4 and 5), and give a criterion in Proposition 6 which tests when such a code is self-dual. Appropriate highlighting examples are also given throughout.

2. Matrix-Product Codes over Commutative Rings

In this section, unless further assumptions are stated, R stands for a commutative ring with identity.

Definition 1. Let $A \in M_{s \times l}(R)$ with $s \leq l$.

- (i) If the rows of A are linearly independent over R , we say that A has full rank over R .
- (ii) If there is $B \in M_{l \times s}(R)$ such that $AB = I_s$ (the $s \times s$ identity matrix), we say that A is right invertible and B is the right inverse of A . Left invertibility is defined similarly. If $s = l$, we say that A is invertible if it has both right and left inverses.

$$\phi: \prod_{i=1}^s C_i \subseteq (R^n)^s \longrightarrow [C_1, \dots, C_s]A \subseteq M_{n \times l}(R) \cong R^{nl}, \quad (c_1, \dots, c_s) \mapsto (c_1, \dots, c_s)A \quad (6)$$

is a homomorphism of R -modules. If $(c_1, \dots, c_s) \in \prod_{i=1}^s C_i$ is such that $\phi(c_1, \dots, c_s) = 0$, then for each $1 \leq k \leq n$ and $1 \leq t \leq l$, we have $\sum_{j=1}^s x_{kj} a_{jt} = 0$. As A has full rank over R , it follows that for each $1 \leq k \leq n$ and $1 \leq t \leq l$, we have $x_{kj} = 0$. Therefore ϕ is injective. It is clear, by construction, that ϕ is surjective and, therefore, the rank of $[C_1, \dots, C_s]A$ is equal to the rank of $\prod_{i=1}^s C_i$, which is $k_1 + \dots + k_s$. Finally, the last statement follows from the bijectivity of ϕ . $\square$

Lemma 1. Let M be a free R -module of rank k , and S a system of k elements of M . If S generates M over R , then S is a basis of M over R .

Proof. Assume that $S = (s_1, \dots, s_k)$, and let $B = (e_1, \dots, e_k)$ be an R -basis of M . Consider the R -module homomorphism

$$f: M = \sum_{i=1}^k R s_i \longrightarrow M = \bigoplus_{i=1}^k R e_i, \quad a_1 s_1 + \dots + a_k s_k \mapsto a_1 e_1 + \dots + a_k e_k. \quad (7)$$

If $\sum_{i=1}^k a_i s_i = 0$ with $a_i \in R$, then $f(\sum_{i=1}^k a_i s_i) = \sum_{i=1}^k a_i e_i = 0$. Since $e_1, \dots, e_k$ are linearly independent over R , $a_1 = \dots = a_k = 0$. Thus, S is linearly independent and, hence, S is an R -basis of M . $\square$

- (iii) If $s = l$ and the determinant $\det(A)$ is a unit of R , then we say that A is nonsingular.

Proposition 1. If $A \in M_{s \times s}(R)$, then the following statements are equivalent:

(i) A is invertible.

(ii) A is nonsingular.

If, further, R is finite, then the above two statements are equivalent to the following:

(iii) A has full rank.

Proof. The equivalence of the first two statements follows from the standard argument of computing the inverse of a square matrix ([18]). For the last statement, see [10, Corollary 2.8]. $\square$

Proposition 2. Let $A = (a_{ij}) \in M_{s \times l}(R)$ be of full rank and C_i be $[n, k_i]$ -linear codes over R for $i = 1, \dots, s$. Then the matrix-product code $[C_1, \dots, C_s]A$ is an $[nl, \sum_{i=1}^s k_i]$ -linear code over R . If, further, R is finite, then $|[C_1, \dots, C_s]A| = \prod_{i=1}^s |C_i|$.

Proof. The map

Remark 1. In contrast with vector spaces over fields, one should be warned that with M as in Lemma 1, a linearly independent system whose cardinality is k is not necessarily an R -basis of M . For instance, looking at $\mathbb{Z}$ as a free $\mathbb{Z}$ -module of rank 1, we notice that 2 is linearly independent over $\mathbb{Z}$ but does not generate $\mathbb{Z}$.

Corollary 1. Let $A = (a_{ij}) \in M_{s \times l}(R)$ be of full rank, and $C_1, \dots, C_s$ be $[n, k_i]$ -linear codes over R , respectively. If $G_i \in M_{k_i \times n}(R)$ is a generator matrix of C_i for $i = 1, \dots, s$, respectively, then $[C_1, \dots, C_s]A$ is free with the following generator matrix ($k = \sum_{i=1}^s k_i$):

$$G = \begin{pmatrix} a_{11}G_1 & a_{12}G_1 & \dots & a_{1l}G_1 \\ a_{21}G_2 & a_{22}G_2 & \dots & a_{2l}G_2 \\ \vdots & \vdots & \dots & \vdots \\ a_{s1}G_s & a_{s2}G_s & \dots & a_{sl}G_s \end{pmatrix} \in M_{k, ln}(R). \quad (8)$$

Proof. By Proposition 2, $[C_1, \dots, C_s]A$ is free of rank $k = \sum_{i=1}^s k_i$ over R . The set S consisting of the rows of the matrix G is clearly a generating system of the code $[C_1, \dots, C_s]A$ over R . Since the cardinality of S is equal to the rank of $[C_1, \dots, C_s]A$, it follows from Lemma 1 that S is a basis of

$[C_1, \dots, C_s]A$ over R . Hence, G is a generator matrix of $[C_1, \dots, C_s]A$.

Let $A = (a_{ij}) \in M_{s \times l}(R)$. For $i = 1, \dots, s$, let $L_i = (a_{i1}, \dots, a_{il}) \in R^l$ be the i th row of A and C_{L_i} the left R -submodule of R^l generated by $L_1, \dots, L_i$ (so, $C_{L_i} = \sum_{j=1}^i RL_j$). Let d_i be the minimum Hamming distance of C_i and D_i the minimum Hamming distance of C_{L_i} . Generalizing its counterparts over a finite field ([5]) and a finite chain ring ([6]), the theorem below gives a lower bound for the minimum Hamming distance of a matrix-product code $[C_1, \dots, C_s]A$ over a commutative ring when A has full rank. It, further, gives a sufficient condition under which the bound is sharp, generalizing [14, Theorem 1]. Note that, in the following theorem, we use the multiplication map $R^l \times R^n \longrightarrow R^{ln}$ defined by

$$UV = (u_1v_1, \dots, u_1v_n, u_2v_1, \dots, u_2v_n, \dots, u_lv_1, \dots, u_lv_n), \quad (9)$$

for $U = (u_1, \dots, u_l) \in R^l$ and $V = (v_1, \dots, v_n) \in R^n$. $\square$

$$\begin{aligned} wt(c) &= wt((x_1, x_2, \dots, x_s)A) = wt((x_{11}, x_{12}, \dots, x_{1s})A, (x_{21}, x_{22}, \dots, x_{2s})A, \dots, (x_{n1}, x_{n2}, \dots, x_{ns})A) \\ &= \sum_{k=1}^n wt((x_{k1}, x_{k2}, \dots, x_{ks})A) \\ &\geq \sum_{t=1}^{d_r} wt((x_{i_t,1}, x_{i_t,2}, \dots, x_{i_t,s})A) \\ &= \sum_{t=1}^{d_r} wt(y_t) \geq d_r D_r \\ &\geq \min\{d_1 D_1, d_2 D_2, \dots, d_s D_s\}. \end{aligned} \quad (12)$$

Now assume, further, that $C_s \subseteq C_{s-1} \subseteq \dots \subseteq C_1$ and, for every $i = 1, \dots, s$, there exist $x_i \in C_i$ and $X_i \in C_{L_i}$ such that $wt(x_i) = d_i$, $wt(X_i) = D_i$, and $X_i x_i \neq 0$. By the first part of this proof, we have $d(C) \geq \min\{d_1 D_1, d_2 D_2, \dots, d_s D_s\}$. Let $r \in \{1, \dots, s\}$ be such that $d_r D_r = \min\{d_1 D_1, d_2 D_2, \dots, d_s D_s\}$. Take $x_r \in C_r$ and $X_r \in C_{L_r}$ so that $wt(x_r) = d_r$, $wt(X_r) = D_r$, and $x_r X_r \neq 0$. We show that $X_r x_r \in [C_1, \dots, C_s]A$ and $wt(X_r x_r) = d_r D_r$, which settles the proof. Write $x_r = (x_{1,r}, \dots, x_{n,r})$ and $X_r = \sum_{i=1}^r \lambda_i L_i \in C_{L_r}$ for $\lambda_i \in R$. Set $y_i = \lambda_i x_r$ for $i = 1, \dots, s$ with $\lambda_i = 0$ for $i = r+1, \dots, s$. As $y_i \in C_r$, $y_i \in C_i$ for all $i = 1, \dots, r$. Also, $y_i = 0 \in C_i$ for all $i = r+1, \dots, s$. Thus, $[y_1, \dots, y_s]A \in [C_1, \dots, C_s]A$ and

$$\begin{aligned} [y_1, \dots, y_s]A &= \left(\sum_{i=1}^s y_i a_{i1}, \sum_{i=1}^s y_i a_{i2}, \dots, \sum_{i=1}^s y_i a_{il} \right) \\ &= \left(\sum_{i=1}^r \lambda_i a_{i1}, \sum_{i=1}^r \lambda_i a_{i2}, \dots, \sum_{i=1}^r \lambda_i a_{il} \right) x_r \\ &= X_r x_r. \end{aligned} \quad (13)$$

Theorem 1. *Keep the above notation. If $A \in M_{s \times l}(R)$ is of full rank, then the minimum distance of the matrix-product code $[C_1, \dots, C_s]A$ satisfies the following inequality:*

$$d([C_1, \dots, C_s]A) \geq \min\{d_1 D_1, d_2 D_2, \dots, d_s D_s\}. \quad (10)$$

If, furthermore, $C_s \subseteq C_{s-1} \subseteq \dots \subseteq C_1$ and, for every $i = 1, \dots, s$, there exist $x_i \in C_i$ and $X_i \in C_{L_i}$ such that $wt(x_i) = d_i$, $wt(X_i) = D_i$, and $X_i x_i \neq 0$, then

$$d([C_1, \dots, C_s]A) = \min\{d_1 D_1, d_2 D_2, \dots, d_s D_s\}. \quad (11)$$

Proof. Let $0 \neq c = (x_1, \dots, x_s)A \in [C_1 \dots C_s]A$. There exist some $r \in \{1, \dots, s-1\}$, $x_r \neq 0$, and $x_i = 0$ for $r < i \leq s$ (so, $c = (x_1, \dots, x_r, 0, \dots, 0)A$); otherwise set $r = s$. Since $0 \neq x_r \in C_r$, $wt(x_r) \geq d_r$ and, thus, x_r has at least d_r nonzero components, $x_{i_1,r}, \dots, x_{i_{d_r},r}$ say. Now, for each $t = 1, \dots, d_r$, we have $y_t = (x_{i_t,1}, x_{i_t,2}, \dots, x_{i_t,s})A \in C_{L_r}$ because $x_{j,k} = 0$ for each $j = 1, \dots, l$ and $r < k \leq s$. Since $x_{i_t,r} \neq 0$ and A has a full rank over R , we deduce that $y_t \neq 0$. So, $wt(y_t) \geq D_r$. Hence,

As $0 \neq X_r x_r \in [C_1, \dots, C_s]A$, $wt(X_r x_r) \geq \min\{d_1 D_1, d_2 D_2, \dots, d_s D_s\} = d_r D_r$. On the contrary, as precisely d_r components of x_r are nonzero and precisely D_r components of X_r are nonzero, it follows from the definition of the multiplication $X_r x_r$ that $wt(X_r x_r) \leq d_r D_r$. Hence, $wt(X_r x_r) = d_r D_r$ as claimed. $\square$

Remark 2. Note that if R is a field (or even an integral domain), then the requirement on x_i and X_i in Theorem 1 holds automatically. On the contrary, we present here an example which shows that such a requirement is sufficient but not necessary. Let $R = \mathbb{Z}_4$ and consider the matrix

$$A = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 2 & 1 \end{pmatrix} \in M_{2 \times 3}(\mathbb{Z}_4). \text{ It is clear that } A \text{ is of full rank.}$$

Consider $C_{L_1} = \mathbb{Z}_4(1, 2, 0)$ and $C_{L_2} = \mathbb{Z}_4(1, 2, 0) + \mathbb{Z}_4(0, 2, 1)$. It can be checked that $D_1 = D_2 = 1$, the only codeword in C_{L_1} of weight 1 is $(2, 0, 0)$, and the only codewords in C_{L_2} of weight 1 are $(2, 0, 0)$ and $(0, 0, 2)$. Set $C_1 = C_{L_2}$ and $C_2 = C_{L_1}$, so $C_2 \subseteq C_1$ and $d^* = 1$. It is easily seen that $x_1 X_1 = x_2 X_1 = (0, 0, 0, 0, 0, 0)$. Nonetheless, $d([C_1 C_2]A) = 1 = d^*$ since the codeword

$$c = \begin{pmatrix} 0 & 2 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} A = \begin{pmatrix} 0 & 0 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in [C_1 C_2] A, \quad (14)$$

has weight 1.

3. On the Dual of a Matrix-Product Code over a Finite Commutative Ring

Throughout this section, R denotes a finite commutative ring with identity. A nonempty subset of the free R -module $M_{n \times m}(R) \cong R^{nm}$ can be looked at as a code over R of length nm , where a codeword (which is a matrix $A \in M_{n \times m}(R)$) is thought of as a word over R of length nm in the obvious way. We consider the following bilinear form on $M_{n \times m}(R)$:

$$\langle A, B \rangle = \text{tr}(AB^T) = \sum_{i=1}^n \sum_{j=1}^m a_{ij} b_{ij}, \quad (15)$$

for $A = (a_{ij})$ and $B = (b_{ij})$, where B^T is the transpose of B and $\text{tr}(AB^T)$ is the trace of the $n \times n$ matrix AB^T .

Our next goal is to give sufficient conditions for the dual of a matrix-product code to also be a matrix-product code, generalizing similar results over finite fields and finite chain rings (see [5, 6]).

Lemma 2 (see [10, Proposition 2.9]). *If C is an $[n, k]$ -linear code over R , then $C^\perp$ is an $[n, n-k]$ -linear code over R .*

Proposition 3. *If $A \in M_{s \times s}(R)$ is nonsingular, and $C_1, \dots, C_s$ are free linear codes over R of length n , then $([C_1, \dots, C_s]A)^\perp = [C_1^\perp, \dots, C_s^\perp](A^{-1})^T$.*

Proof. Let $\text{rank}(C_j) = k_j$ for $j = 1, \dots, s$. Since R is finite, it follows from Lemma 2 that $C_j^\perp$ are free over R of rank $n - k_j$ for $j = 1, \dots, s$. Thus, by Proposition 2, both $[C_1, \dots, C_s]A$ and $[C_1^\perp, \dots, C_s^\perp](A^{-1})^T$ are free with

$$\begin{aligned} \text{rank}\left([C_1^\perp, \dots, C_s^\perp](A^{-1})^T\right) &= \sum_{j=1}^s (n - k_j) \\ &= ns - \sum_{j=1}^s k_j = ns - \text{rank}([C_1, \dots, C_s]A). \end{aligned} \quad (16)$$

From now on, just follow the proof of [2, Lemma 6.1] with the obvious notational adjustments. $\square$

Remark 3. Freeness of the input codes is necessary for the conclusion of Proposition 3 to hold, as the following example shows: let $R = \mathbb{Z}_{20}$, $C_1 = 10\mathbb{Z}_{20}$, $C_2 = 2\mathbb{Z}_{20}$, and $A = \begin{pmatrix} 3 & 0 \\ 0 & 7 \end{pmatrix}$. It can be easily seen that $C_1^\perp = C_2$, $C_2^\perp = C_1$,

and A is nonsingular with $(A^{-1})^T = \begin{pmatrix} 7 & 0 \\ 0 & 3 \end{pmatrix}$. Now, for $(8, 2) \in [C_1 C_2]A$ and $(2, 0) \in [C_1^\perp C_2^\perp](A^{-1})^T$, it is clear that

$\langle (8, 2), (2, 0) \rangle = 16 \neq 0$ in $\mathbb{Z}_{20}$. So, $([C_1 C_2]A)^\perp \neq [C_1^\perp C_2^\perp](A^{-1})^T$. Notice that all assumptions of Proposition 3 are satisfied here except that C_1 and C_2 are not free over $\mathbb{Z}_{20}$.

Corollary 2. *Keep the assumptions of Proposition 3. If $G'_1, \dots, G'_s$ are generator matrices of $C_1^\perp, \dots, C_s^\perp$, respectively, and $(A^{-1})^T = (b_{ij})$, then a generator matrix of $([C_1, \dots, C_s]A)^\perp$ is*

$$G' = \begin{pmatrix} b_{11}G'_1 & b_{12}G'_1 & \cdots & b_{1l}G'_1 \\ b_{21}G'_2 & b_{22}G'_2 & \cdots & b_{2l}G'_2 \\ \vdots & \vdots & \cdots & \vdots \\ b_{s1}G'_s & b_{s2}G'_s & \cdots & b_{sl}G'_s \end{pmatrix}. \quad (17)$$

Proof. If C_i is of rank k_i over R for $i = 1, \dots, s$, it follows from Lemma 2 that $C_i^\perp$ is free of rank $n - k_i$ for $i = 1, \dots, s$. Letting $G'_i \in M_{(n-k_i), n}(R)$ be the respective generator matrices of $C_i^\perp$, the result now follows from Corollary 1 and Proposition 3.

For $r_1, \dots, r_s \in R$, let $\text{Diag}(r_1, \dots, r_s)$ denote the diagonal matrix of size $s \times s$ whose principal-diagonal entry in position i is r_i for $i = 1, \dots, s$. $\square$

Lemma 3. *If $C_1, \dots, C_s$ are linear codes over R of the same length, $Y \in M_{s \times l}(R)$, and $X = \text{Diag}(r_1, \dots, r_s)Y$ for some $r_1, \dots, r_s \in U(R)$. Then, $[C_1, \dots, C_s]X = [C_1, \dots, C_s]Y$.*

Proof. As $X = \text{Diag}(r_1, \dots, r_s)Y$, $[C_1, \dots, C_s]X = [(r_1 C_1), \dots, (r_s C_s)]Y$. Since r_i is a unit, $r_i C_i = C_i$ for $i = 1, \dots, s$, and thus the claimed conclusion follows immediately.

The following result gives characterizations of self-dual, self-orthogonal, and LCD matrix-product codes over finite commutative rings (for part 3, see [8] as well). $\square$

Corollary 3. *Let $A \in M_{s \times s}(R)$ be such that $AA^T = \text{Diag}(r_1, \dots, r_s)$ with $r_i \in U(R)$ for $i = 1, \dots, s$, and let $C_1, \dots, C_s$ be linear codes over R of the same length. Then*

- (1) $[C_1, \dots, C_s]A$ is self-dual if and only if C_i is self-dual for every $i = 1, \dots, s$.
- (2) $[C_1, \dots, C_s]A$ is self-orthogonal if and only if C_i is self-orthogonal for every $i = 1, \dots, s$.
- (3) $[C_1, \dots, C_s]A$ is LCD if and only if C_i is LCD for every $i = 1, \dots, s$.

Proof. To begin with, as $\text{Diag}(r_1, \dots, r_s)$ is invertible and A is a square matrix over a commutative ring ([18]), A and A^T are invertible too, with

$$(A^T)^{-1} = (A^{-1})^T = \text{Diag}(r_1^{-1}, \dots, r_s^{-1})A. \quad (18)$$

By Lemma 3,

$$[C_1, \dots, C_s]A = [C_1, \dots, C_s](A^{-1})^T. \quad (19)$$

Also, by Proposition 3,

$$([C_1, \dots, C_s]A)^\perp = [C_1^\perp, \dots, C_s^\perp](A^{-1})^T. \quad (20)$$

(1) By (19) and (20),

$$\begin{aligned} [C_1, \dots, C_s]A \text{ is self-dual} &\text{ iff } [C_1, \dots, C_s]A = ([C_1, \dots, C_s]A)^\perp, \\ &\text{ iff } [C_1, \dots, C_s](A^{-1})^T = [C_1^\perp, \dots, C_s^\perp](A^{-1})^T, \\ &\text{ iff } C_i = C_i^\perp \text{ for every } 1 \leq i \leq s \text{ (as } A \text{ is invertible),} \\ &\text{ iff } C_i \text{ is self-dual for every } 1 \leq i \leq s. \end{aligned} \quad (21)$$

(2) Proving the self-orthogonality statement is similar.

(3) We have

$$\begin{aligned} [C_1, \dots, C_s]A \text{ is LCD} &\text{ iff } [C_1, \dots, C_s]A \cap ([C_1, \dots, C_s]A)^\perp = \{0_{R^m}\}, \\ &\text{ iff } [C_1, \dots, C_s](A^{-1})^T \cap [C_1^\perp, \dots, C_s^\perp](A^{-1})^T = \{0_{R^m}\}, \\ &\text{ iff } [C_1, \dots, C_s] \cap [C_1^\perp, \dots, C_s^\perp] = \{0_{R^m}\} \text{ (as } A \text{ is invertible),} \\ &\text{ iff } C_i \cap C_i^\perp = \{0_{R^n}\} \text{ for every } i = 1, \dots, s, \\ &\text{ iff } C_i \text{ is LCD for every } i = 1, \dots, s. \end{aligned} \quad (22)$$

4. Matrix-Product Codes Arising From (σ, δ) -Codes over Finite Commutative Rings

Throughout this section, R denotes a finite commutative ring with identity. We use here some results from the authors' paper [17] combined with results from the previous sections to construct matrix-product codes based on (σ, δ) -codes over R and, further, give a criterion for self-duality of such codes. We start off by recalling some terminologies and results from [17, 19].

4.1. (σ, δ) -Codes. For a ring endomorphism σ of R that maps the identity to itself and a σ -derivation δ of R , let $R_{\sigma, \delta}$ denote the (noncommutative) ring of skew-polynomials $\sum_{i=0}^m a_i X^i$ over R with the usual addition of polynomials and multiplication based on the rule $Xa = \sigma(a)X + \delta(a)$ for $a \in R$. Let $g(X) = \sum_{i=0}^{n-k} g_i X^i \in R_{\sigma, \delta}$ be a monic skew-polynomial, for some $1 \leq k \leq n-1$. Fix any monic $f(X) = \sum_{i=0}^n a_i X^i \in R_{\sigma, \delta}$ of degree n of which $g(X)$ is a right divisor in $R_{\sigma, \delta}$, and let $(f)_l$ be the left principal ideal of $R_{\sigma, \delta}$ generated by f . Then, $R_{\sigma, \delta}/(f)_l$ is both a left $R_{\sigma, \delta}$ -module as well as a free left R -module with an R -basis $\mathcal{B} = \{1 + (f)_l, X + (f)_l, \dots, X^{n-1} + (f)_l\}$. On the contrary, letting

$$C_f = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 \\ -a_0 & -a_1 & \dots & -a_{n-2} & -a_{n-1} \end{pmatrix}, \quad (23)$$

be the companion matrix of f , define the group endomorphism $T_f: R^n \rightarrow R^n$ by

$$(t_0, \dots, t_{n-1}) \mapsto (\sigma(t_0), \dots, \sigma(t_{n-1}))C_f + (\delta(t_0), \dots, \delta(t_{n-1})). \quad (24)$$

Then the map $R_{\sigma, \delta} \times R^n \rightarrow R^n$ given by $(P(X), (t_0, \dots, t_{n-1})) \mapsto P(T_f)(t_0, \dots, t_{n-1})$ defines a left action of $R_{\sigma, \delta}$ on R^n which makes R^n a left $R_{\sigma, \delta}$ -module in an obvious way. Now, the map $\phi_f: R^n \rightarrow R_{\sigma, \delta}/(f)_l$ given by $(t_0, \dots, t_{n-1}) \mapsto \sum_{i=0}^{n-1} t_i X^i + (f)_l$ is a left $R_{\sigma, \delta}$ -module isomorphism. For every $p(X) \in R_{\sigma, \delta}$, there is a unique $q(X) = \sum_{i=0}^{n-1} t_i X^i \in R_{\sigma, \delta}$ (of degree at most $n-1$) such that $p(X) + (f)_l = q(X) + (f)_l$. We can see that $(t_0, \dots, t_{n-1}) = \phi_f^{-1}(p(X) + (f)_l)$, and we call $(t_0, \dots, t_{n-1})$ the coordinates of $p(X) + (f)_l$ with respect to the basis $\mathcal{B}$.

If $\mathcal{M}$ is a left $R_{\sigma, \delta}$ -submodule of $R_{\sigma, \delta}/(f)_l$, the left $R_{\sigma, \delta}$ -submodule $C = \phi_f^{-1}(\mathcal{M})$ of R^n is called an (f, σ, δ) -code (or just a (σ, δ) -code) of length n over R . Note that C consists of the coordinates of all the elements of $\mathcal{M}$. As R is a subring of $R_{\sigma, \delta}$, $\mathcal{M}$ and C are also left R -modules. A linear code $C \subseteq R^n$ is called a principal (f, σ, δ) -code (or just a principal (σ, δ) -code) generated by g if there exist monic skew-polynomials $f, g \in R_{\sigma, \delta}$ of degrees n and $n-k$, respectively, such that g is a right divisor of f in $R_{\sigma, \delta}$ and $C = \phi_f^{-1}((g)_l/(f)_l)$. Such a code is free over R of rank k (see [5, Theorem 1]). A (σ, δ) -code is called a principal (σ, δ) -constacyclic code if it is generated by some monic right divisor of $X^n - a$ for some $a \in U(R)$.

Starting with a set of monic skew-polynomials $g_1, \dots, g_s$ over R , we give here a construction of a free matrix-product code C over R whose input codes are principal (σ, δ) -codes generated by the g_i 's and, further, give its generator matrix in terms of the matrix of the code and the coefficients of the g_i 's. We also give a construction of the dual $C^\perp$ of C under certain extra assumptions and give its generator matrix (a parity-check matrix of C).

For every $j = 1, \dots, s$, let σ_j be a ring endomorphism of R that maps the identity to itself, δ_j a σ_j -derivation of R , $g_j(X) = \sum_{i=0}^{n-k_j} g_{i,j} X^i \in R_{\sigma_j, \delta_j}$ monic, and C_j the principal (σ_j, δ_j) -code over R generated by $g_j(X)$ (so, there exists a monic $f_j(X) \in R_{\sigma_j, \delta_j}$ of degree n of which $g_j(X)$ is a right divisor in R_{σ_j, δ_j}). By [3, Theorem 2.7], a generator matrix $G_j \in M_{k_j \times n}(R)$ of C_j is given by

$$G_j = \begin{pmatrix} g_{0,j} & \cdots & g_{n-k_j,j} & 0 & 0 & \cdots & 0 \\ g_{0,j}^{(1)} & \cdots & g_{n-k_j,j}^{(1)} & \sigma_j(g_{n-k_j,j}) & 0 & \cdots & 0 \\ g_{0,j}^{(2)} & \cdots & g_{n-k_j,j}^{(2)} & g_{n-k_j+1,j}^{(2)} & \sigma_j^2(g_{n-k_j,j}) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ g_{0,j}^{(k_j-1)} & \cdots & g_{n-k_j,j}^{(k_j-1)} & g_{n-k_j+1,j}^{(k_j-1)} & g_{n-k_j+2,j}^{(k_j-1)} & \cdots & \sigma_j^{k_j-1}(g_{n-k_j,j}) \end{pmatrix}, \quad (25)$$

where

- (1) $g_{i,j} = 0$ for $n - k_j + 1 \leq i \leq n - 1$
- (2) $g_{0,j}^{(i)} = \delta_j(g_{0,j}^{(i-1)})$ for $1 \leq i \leq k_j - 1$

$$(3) \ g_{t,j}^{(i)} = \delta_j(g_{t,j}^{(i-1)}) + \sigma_j(g_{t-1,j}^{(i-1)}) \text{ for } 1 \leq i \leq k_j - 1 \text{ and } 1 \leq t \leq n - 2$$

The matrices G_j take more elegant shapes if $\delta_j = 0$ where, by [3, Corollary 2.8], we would have

$$G_j = \begin{pmatrix} g_{0,j} & \cdots & g_{n-k_j,j} & 0 & 0 & \cdots & 0 \\ 0 & \sigma_j(g_{0,j}) & \cdots & \sigma_j(g_{n-k_j,j}) & 0 & \cdots & 0 \\ \vdots & \ddots & & & \ddots & & \vdots \\ 0 & 0 & \cdots & 0 & \sigma_j^{k_j-1}(g_{0,j}) & \cdots & \sigma_j^{k_j-1}(g_{n-k_j,j}) \end{pmatrix}. \quad (26)$$

On the contrary, if further σ_j are ring automorphisms of R and $g_j(X)$ are also left divisors in R_{σ_j, δ_j} of $f_j(X) = \sum_{i=0}^n a_{i,j} X^i$ for all $j = 1, \dots, s$ with

$f_j(X) = g_j(X)h_j(X)$ for $h_j(X) = \sum_{i=0}^{k_j} h_{i,j} X^i \in R_{\sigma_j, \delta_j}$, then (by [3, Theorem 5.1]) a generator matrix $H_j \in M_{n-k_j,n}(R)$ of $C_j^\perp$, for $j = 1, \dots, s$, is

$$H_j = \begin{pmatrix} h_{k_j,j} & h_{k_j,j}^{(1)} & h_{k_j,j}^{(2)} & \cdots & h_{k_j,j}^{(n-k_j-1)} & h_{k_j,j}^{(n-k_j)} & \cdots & h_{k_j,j}^{(n-1)} \\ 0 & \sigma_j(h_{k_j,j}) & h_{k_j+1,j}^{(2)} & \cdots & h_{k_j+1,j}^{(n-k_j-1)} & h_{k_j+1,j}^{(n-k_j)} & \cdots & h_{k_j+1,j}^{(n-1)} \\ 0 & 0 & \sigma_j^2(h_{k_j,j}) & \cdots & h_{k_j+2,j}^{(n-k_j-1)} & h_{k_j+2,j}^{(n-k_j)} & \cdots & h_{k_j+2,j}^{(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \sigma_j^{n-k_j-1}(h_{k_j,j}) & h_{n-1,j}^{(n-k_j)} & \cdots & h_{n-1,j}^{(n-1)} \end{pmatrix}, \quad (27)$$

where

- (1) $h_{i,j} = 0$ for $k_j + 1 \leq i \leq n - 1$
- (2) for $1 \leq i \leq n - k_j - 1$ and $1 \leq t \leq n - 2$
  - (i) $h_{0,j}^{(i)} = \delta_j(h_{0,j}^{(i-1)})$
  - (ii) $h_{t,j}^{(i)} = \delta_j(h_{t,j}^{(i-1)}) + \sigma_j(h_{t-1,j}^{(i-1)})$
- (3) for $n - k_j \leq i \leq n - 1$ and $1 \leq t \leq n - 1$
  - (i) $h_{0,j}^{(i)} = \delta_j(h_{0,j}^{(i-1)}) - a_{0,j} \sigma_j(h_{n-1,j}^{(i-1)})$
  - (ii) $h_{t,j}^{(i)} = \delta_j(h_{t,j}^{(i-1)}) + \sigma_j(h_{t-1,j}^{(i-1)}) - a_{t,j} \sigma_j(h_{n-1,j}^{(i-1)})$

$[C_1, \dots, C_s]A$ by $[g_1, \dots, g_s]A$ in order to emphasize a way of constructing a free matrix-product over R out of a well-chosen set of skew-polynomials over R , as the following results indicate.

Proposition 4. Keep the notations and assumptions of Section 4.1. Let $A = (a_{ij}) \in M_{s \times l}(R)$ be of full rank. Then, the matrix $G \in M_{r \times \ln}(R)$ ($r = \sum_{i=1}^s k_i$) given by

$$G = \begin{pmatrix} a_{11}G_1 & a_{12}G_1 & \cdots & a_{1l}G_1 \\ a_{21}G_2 & a_{22}G_2 & \cdots & a_{2l}G_2 \\ \vdots & \vdots & \cdots & \vdots \\ a_{s1}G_s & a_{s2}G_s & \cdots & a_{sl}G_s \end{pmatrix} \quad (28)$$

4.2. Matrix-Product Codes Arising from (σ, δ) -Codes. Keep the notations and assumptions of Section 4.1. For $A \in M_{s \times l}(R)$, we denote the matrix-product code

is a generator matrix for the matrix-product code $[g_1, \dots, g_s]A$.

Proof. By [5, Theorem 1] (see also [17]), C_i is free of rank k_i for every $i = 1, \dots, s$. Now, applying Corollary 1 yields the claimed conclusion. $\square$

Proposition 5. Besides the assumptions of Proposition 4, assume further that σ_i is a ring automorphism of R , $g_i(X)$ is also a left divisor of $f_i(X)$ for $i = 1, \dots, s$, and $A \in M_{s \times s}(R)$ is nonsingular with $(A^{-1})^T = (b_{ij})$. Then the matrix $H \in M_{r' \times \ln}(R)$ ($r' = \sum_{i=1}^s (n - k_i)$) given by

$$H = \begin{pmatrix} b_{11}H_1 & b_{12}H_1 & \dots & b_{1l}H_1 \\ b_{21}H_2 & b_{22}H_2 & \dots & b_{2l}H_2 \\ \vdots & \vdots & \dots & \vdots \\ b_{s1}H_s & b_{s2}H_s & \dots & b_{sl}H_s \end{pmatrix} \quad (29)$$

is a generator matrix for the dual matrix-product code $([g_1, \dots, g_s]A)^\perp$.

Proof. By the presentation in Subsection 4.1, H_i is a generator matrix of $C_i^\perp$ for $i = 1, \dots, s$. Now, apply Corollary 2 to get the desired conclusion. $\square$

Example 1. Let R be finite of characteristic 2, $\alpha, \beta \in R$ with $\alpha^2 + \alpha + 1 = 0$, and σ_1, σ_2 ring automorphisms of R with $\sigma_1(\alpha) = \alpha^2$ and $\sigma_2(\beta) = \beta$. We present several principal σ_i -codes of length 4 and use them to construct many matrix-product codes.

Step 1. Consider $f_1(X), g_1(X), h_1(X) \in R_{\sigma_1}$, with $f_1(X) = X^4 + X^2 + 1$, $g_1(X) = X^2 + \alpha$, and $h_1(X) = X^2 + \alpha^2$. It can be checked that

$$f_1(X) = g_1(X)h_1(X) = h_1(X)g_1(X). \quad (30)$$

Let C_1 and C_2 be the principal σ_1 -codes of length 4 over R generated, respectively, by g_1 and h_1 . By Section 4.1,

$$G_1 = \begin{pmatrix} g_{0,1} & g_{1,1} & g_{2,1} & 0 \\ 0 & \sigma_1(g_{0,1}) & \sigma_1(g_{1,1}) & \sigma_1(g_{2,1}) \end{pmatrix} = \begin{pmatrix} \alpha & 0 & 1 & 0 \\ 0 & \alpha^2 & 0 & 1 \end{pmatrix} \quad (31)$$

is a generator matrix of C_1 , and

$$G_2 = \begin{pmatrix} h_{0,1} & h_{1,1} & h_{2,1} & 0 \\ 0 & \sigma_1(h_{0,1}) & \sigma_1(h_{1,1}) & \sigma_1(h_{2,1}) \end{pmatrix} = \begin{pmatrix} \alpha^2 & 0 & 1 & 0 \\ 0 & \alpha & 0 & 1 \end{pmatrix} \quad (32)$$

is a generator matrix of C_2 . On the contrary,

$$H_1 = \begin{pmatrix} h_{2,1} & h_{2,1}^{(1)} & h_{2,1}^{(2)} & h_{2,1}^{(3)} \\ 0 & \sigma_1(h_{2,1}) & h_{3,1}^{(2)} & h_{3,1}^{(3)} \end{pmatrix} = \begin{pmatrix} 1 & 0 & \alpha & 0 \\ 0 & 1 & 0 & \alpha^2 \end{pmatrix} \quad (33)$$

is a generator matrix of $C_1^\perp$, and

$$H_2 = \begin{pmatrix} g_{2,1} & g_{2,1}^{(1)} & g_{2,1}^{(2)} & g_{2,1}^{(3)} \\ 0 & \sigma_1(g_{2,1}) & g_{3,1}^{(2)} & g_{3,1}^{(3)} \end{pmatrix} = \begin{pmatrix} 1 & 0 & \alpha^2 & 0 \\ 0 & 1 & 0 & \alpha \end{pmatrix} \quad (34)$$

is a generator matrix of $C_2^\perp$. Notice that

$$G_1 H_1^T = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = G_2 H_2^T.$$

Step 2. Consider $f_2(X), g_2(X), h_2(X) \in R_{\sigma_2}$, with $f_2(X) = X^4 + \beta^4$, $g_2(X) = X + \beta$, and $h_2(X) = X^3 + \beta X^2 + \beta^2 X + \beta^3$. It can be checked that

$$f_2(X) = g_2(X)h_2(X) = h_2(X)g_2(X). \quad (35)$$

Let C_3 and C_4 be the principal σ_2 -codes of length 4 over R generated, respectively, by g_2 and h_2 . By Section 4.1,

$$G_3 = \begin{pmatrix} g_{0,2} & g_{1,2} & 0 & 0 \\ 0 & \sigma_2(g_{0,2}) & \sigma_2(g_{1,2}) & 0 \\ 0 & 0 & \sigma_2^2(g_{0,2}) & \sigma_2^2(g_{1,2}) \end{pmatrix} = \begin{pmatrix} \beta & 1 & 0 & 0 \\ 0 & \beta & 1 & 0 \\ 0 & 0 & \beta & 1 \end{pmatrix} \quad (36)$$

is a generator matrix of C_3 , and

$$G_4 = (h_{0,2} \ h_{1,2} \ h_{2,2} \ h_{3,2}) = (\beta^3 \ \beta^2 \ \beta 1) \quad (37)$$

is a generator matrix of C_4 . On the contrary,

$$H_3 = (h_{3,2} \ h_{3,2}^{(1)} \ h_{3,2}^{(2)} \ h_{3,2}^{(3)}) = (1 \ \beta \ \beta^2 \ \beta^3) \quad (38)$$

is a generator matrix of $C_3^\perp$, and

$$H_4 = \begin{pmatrix} g_{1,2} & g_{1,2}^{(1)} & g_{1,2}^{(2)} & g_{1,2}^{(3)} \\ 0 & \sigma_2(g_{1,2}) & g_{2,2}^{(2)} & g_{2,2}^{(3)} \\ 0 & 0 & \sigma_2^2(g_{1,2}) & g_{3,2}^{(3)} \end{pmatrix} = \begin{pmatrix} 1 & \beta & 0 & 0 \\ 0 & 1 & \beta & 0 \\ 0 & 0 & 1 & \beta \end{pmatrix} \quad (39)$$

is a generator matrix of $C_4^\perp$. Notice that $G_3 H_3^T = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ and $G_4 H_4^T = \begin{pmatrix} 0 & 0 & 0 \end{pmatrix}$.

Step 3. Let $A = (a_{i,j}) \in M_{2 \times l}(R)$, $B = (b_{i,j}) \in M_{3 \times l}(R)$, $D = (d_{i,j}) \in M_{4 \times 3}(R)$ be all full-rank matrices. By Proposition 4, we can easily construct the generator matrices of many matrix-product codes out of different combinations of the above principal σ_i -codes such as $[g_i g_j]A$ and $[g_i h_j]A$, $[g_i h_j g_k]B$, $[h_i g_j h_k]B$, $[g_i h_j h_k g_p]D$, and $[g_i g_j g_k h_p]B$ for $i, j, k, p = 1, 2$. For instance,

$\begin{pmatrix} a_{1,1}G_1 & \dots & a_{1,l}G_1 \\ a_{2,1}G_4 & \dots & a_{2,l}G_4 \end{pmatrix} \in M_{3 \times 4l}(R)$ is a generator matrix of

$[g_1 h_2]A$, $\begin{pmatrix} b_{1,1}G_4 & \dots & b_{1,l}G_4 \\ b_{2,1}G_3 & \dots & b_{2,l}G_3 \\ b_{3,1}G_2 & \dots & b_{3,l}G_2 \end{pmatrix} \in M_{6 \times 4l}(R)$ is a generator

matrix of $[h_2 g_2 h_1]B$, and $\begin{pmatrix} d_{1,1}G_3 & \dots & d_{1,l}G_3 \\ d_{2,1}G_4 & \dots & d_{2,l}G_4 \\ d_{3,1}G_4 & \dots & d_{3,l}G_4 \\ d_{4,1}G_1 & \dots & d_{4,l}G_1 \end{pmatrix} \in M_{7 \times 4l}(R)$

is a generator matrix of $[g_2 h_2 h_2 g_1]D$. In a similar manner,

we can construct generator matrices of different combinations of the codes C_i and their dual codes for $i = 1, 2, 3, 4$.

Step 4. Utilizing Proposition 3, we can give the generator matrices of the dual codes of all of the above matrix-product codes when the matrices A , B , and D are square and nonsingular. For instance, following Remark 3, let R be $\mathbb{Z}_{20}$ and $A = \begin{pmatrix} 3 & 0 \\ 0 & 7 \end{pmatrix}$. Then A is nonsingular and $(A^{-1})^T = \begin{pmatrix} 7 & 0 \\ 0 & 3 \end{pmatrix}$. As in Step 3, a generator matrix of $[g_1 g_2]A$ is

$$G = \begin{pmatrix} 3G_1 & 0 \\ 0 & 7G_2 \end{pmatrix} \in M_{4 \times 8}(R). \quad (40)$$

By Proposition 3, a generator matrix of $([g_1 g_2]A)^\perp$ is

$$H = \begin{pmatrix} 7H_1 & 0 \\ 0 & 3H_2 \end{pmatrix} \in M_{4 \times 8}(R). \quad (41)$$

Note that

$$GH^T = \begin{pmatrix} 21G_1H_1^T & 0 \\ 0 & 21G_2H_2^T \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in M_{4 \times 4}(R). \quad (42)$$

Besides the assumptions of Proposition 5, let us now assume further that, for every $j = 1, \dots, s$, $\delta_j = 0$, $g_{0,j} \in U(R)$, $k = k_1 = k_2 = \dots = k_s$ with $n = 2k$, and denote $R_{\sigma_j,0}$ by R_{σ_j} .

Proposition 6. *Keep the assumptions as above. Assume further that $A = (a_{ij}) \in M_{s \times s}(R)$ is such that $AA^T = \text{Diag}(r_1, \dots, r_s)$ with $r_1, \dots, r_s \in U(R)$ and that, for every $j = 1, \dots, s$, either of the following statements holds:*

- (i) $g_j(X)$ is a right divisor in R_{σ_j} of $X^n - a_j$ for some $a_j \in U(R)$, C_j is the principal $(X^n - a_j, \sigma_j)$ -constacyclic code generated by $g_j(X)$, and

$$\sigma_j^{k_j}(h_{0,j}^{-1})h_j^*(X) = g_j(X), \text{ where } g_j(X)h_j(X) = X^n - \sigma_j^{k_j}(a_j).$$

- (ii) For any $l_j \in \{0, \dots, k_j\}$, $\sum_{i=0}^{l_j} \sigma_j^{k_j-i}(g_{i,j})g_{i+k_j-l_j,j} = 0$.

Then, the matrix-product code $[g_1, \dots, g_s]A$ is self-dual.

Proof. By [3, Corollary 3.7], the statements (i) and (ii) are equivalent and, further, they are equivalent to the condition of C_j being self-dual. Now, apply Corollary 1 to get that $[g_1, \dots, g_s]A$ is self-dual. $\square$

Example 2. Let $R = \mathbb{F}_3 \times \mathbb{F}_3$, $\sigma(x, y) = (y, x)$, and $\alpha = (2, 2)$. Note that σ is a ring automorphism of R of order 2, $1 = 1_R = (1, 1)$, and α is a unit in R of order 2. Set $h(X) = X^2 + \alpha X + \alpha$. Then $h_0 = \alpha = h_0^{-1}$ and $h^*(X) = \alpha X^2 + \alpha X + 1$. Let $g(X) = \sigma^2(h_0^{-1})h^*(X)$. So, $g(X) = \alpha(\alpha X^2 + \alpha X + 1) = X^2 + X + \alpha$. Using the multiplication rule in R_σ , we have

$$\begin{aligned} g(X)h(X) &= (X^2 + X + \alpha)(X^2 + \alpha X + \alpha) \\ &= X^4 + \sigma(\alpha)X^3 + \sigma(\alpha)X^2 + X^3 + \sigma(\alpha)X^2 \\ &\quad + \sigma(\alpha)X + \alpha X^2 + \alpha^2 X + \alpha^2 \\ &= X^4 + (\alpha + 1)X^3 + (3\alpha)X^2 + (\alpha + \alpha^2)X + 1 \\ &= X^4 + 1 \\ &= X^4 + 1. \end{aligned} \quad (43)$$

Thus, $g(X)$ satisfies condition (2) of Proposition 6 and, hence, it generates a self-dual $(X^4 + 1, \sigma)$ -constacyclic code C of length 4 over R . It follows from the paragraph following Proposition 4 that a generator matrix of C is

$$M = \begin{pmatrix} \alpha & 1 & 1 & 0 \\ 0 & \alpha & 1 & 1 \end{pmatrix}. \quad \text{Given the matrix}$$

$$A = \begin{pmatrix} (1, 0) & (0, 1) \\ (0, 2) & (1, 0) \end{pmatrix} \in M_{2 \times 2}(R), \text{ which is orthogonal and,}$$

thus, quasiorthogonal, we conclude from Propositions 6 and 4, respectively, that the matrix-product code $[gg]A$ is self-dual with the following generator matrix:

$$G = \begin{pmatrix} (1, 0)M & (0, 1)M \\ (0, 2)M & (1, 0)M \end{pmatrix} = \begin{pmatrix} (2, 0) & (1, 0) & (1, 0) & (0, 0) & (0, 2) & (0, 1) & (0, 1) & (0, 0) \\ (0, 0) & (2, 0) & (1, 0) & (1, 0) & (0, 0) & (0, 2) & (0, 1) & (0, 1) \\ (0, 1) & (0, 2) & (0, 2) & (0, 0) & (2, 0) & (1, 0) & (1, 0) & (0, 0) \\ (0, 0) & (0, 1) & (0, 2) & (0, 2) & (0, 0) & (2, 0) & (1, 0) & (1, 0) \end{pmatrix}. \quad (44)$$

Data Availability

All data are contained in the manuscript.

Disclosure

An earlier version of this manuscript was posted on arXiv (see [20]).

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors deeply thank the many colleagues and experts whose valuable comments helped them in improving the paper.

References

- [1] S. Dougherty, *Algebraic Coding Theory over Finite Commutative Rings*, Springer Briefs in Mathematics, Berlin, Germany, 2017.
- [2] M. Shi, A. Alahmadi, and P. Solé, *Codes and Rings, Theory and Practice*, Academic Press, Cambridge, MA, USA, 2017.
- [3] J. A. Wood, "Duality for modules over finite rings and applications to coding theory," *American Journal of Mathematics*, vol. 121, no. 3, pp. 555–575, 1999.
- [4] J. L. Massey, "Linear codes with complementary duals," *Discrete Mathematics*, vol. 106–107, pp. 337–342, 1992.
- [5] T. Blackmore and G. H. Norton, "Matrix-product codes over q ," *Applicable Algebra in Engineering, Communication and Computing*, vol. 12, no. 6, pp. 477–500, 2001.
- [6] B. van Asch, "Matrix-product codes over finite chain rings," *Applicable Algebra in Engineering, Communication and Computing*, vol. 19, no. 1, pp. 39–49, 2008.
- [7] Y. Cao, Y. Cao, and F.-W. Fu, "Matrix-product structure of constacyclic codes over finite chain rings $\mathbb{F}_p[x]/\langle x^u - u \rangle$," *Applicable Algebra in Engineering, Communication and Computing*, vol. 29, no. 6, pp. 455–478, 2018.
- [8] A. Deajim, M. Bouye, and K. Guenda, "The hulls of matrix-product codes over commutative rings and applications," *Journal of Applied Mathematics and Computing*, <https://arxiv.org/pdf/1910.12440.pdf>, 2020.
- [9] Y. Fan, S. Ling, and H. Liu, "Matrix product codes over finite commutative Frobenius rings," *Designs, Codes and Cryptography*, vol. 71, no. 2, pp. 201–227, 2014.
- [10] Y. Fan, S. Ling, and H. Liu, "Homogeneous weights of matrix product codes over finite principal ideal rings," *Finite Fields and Their Applications*, vol. 29, pp. 247–267, 2014.
- [11] F. Hernando, K. Lally, and D. Ruano, "Construction and decoding of matrix-product codes from nested codes," *Applicable Algebra in Engineering, Communication and Computing*, vol. 20, no. 5–6, pp. 497–507, 2009.
- [12] M. Cao and J. Cui, "Construction of new quantum codes via Hermitian dual-containing matrix-product codes," *Quantum Information Science*, vol. 19, Article ID 427, 2020.
- [13] C. Galindo, F. Hernando, and D. Ruano, "New quantum codes from evaluation and matrix-product codes," *Finite Fields and Their Applications*, vol. 36, pp. 98–120, 2015.
- [14] X. Liu, H. Q. Dinh, H. Liu, and L. Yu, "On new quantum codes from matrix product codes," *Cryptography and Communications*, vol. 10, no. 4, pp. 579–589, 2018.
- [15] R. Sobhani, "Matrix-product structure of repeated-root cyclic codes over finite fields," *Finite Fields and Their Applications*, vol. 39, pp. 216–232, 2016.
- [16] H. Song, R. Li, J. Wang, and J. Lv, "Construction of new matrix-product codes and their applications," *IEEE Access*, vol. 7, pp. 164044–164050, 2019.
- [17] M. Boulagouaz and A. Deajim, "On principal (f, σ, δ) -codes over rings," <https://arxiv.org/abs/1809.10409v1>.
- [18] B. McDonald, *Linear Algebra over Commutative Rings*, Marcel Dekker Inc., New York and Basel, NY, USA, 1984.
- [19] M. Boulagouaz and A. Leroy, "–codes," *Advances in Mathematics of Communications*, vol. 7, pp. 463–474, 2013.
- [20] M. Boulagouaz and A. Deajim, "Matrix-product codes over commutative rings and constructions arising from (σ, δ) -codes," <https://arxiv.org/abs/1910.08899v1>.