Hindawi
Security and Communication Networks
Volume 2022, Article ID 9294459, 16 pages
https://doi.org/10.1155/2022/9294459

Research Article

Characterizations and Properties of Monic Principal Skew Codes over Rings

Mhammed Boulagouaz [1] and Abdulaziz Deajim [2]

[1]Department of Mathematics, Faculty of Sciences and Technologies, University of Sidi Mohamed Ben Abdellah, B.P. 2202, Fes, Morocco
[2]Department of Mathematics, King Khalid University, P.O. Box 9004, Abha, Saudi Arabia

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

Received 15 January 2022; Revised 9 March 2022; Accepted 16 April 2022; Published 31 July 2022

Academic Editor: Lu Ou

Let A be a ring with identity, σ a ring endomorphism of A that maps the identity to itself, δ a σ-derivation of A, and consider the skew-polynomial ring $A[X;\sigma,\delta]$. When A is a finite field, a Galois ring, or a general ring, some fairly recent literature used $A[X;\sigma,\delta]$ to construct new interesting codes (e.g., skew-cyclic and skew-constacyclic codes) that generalize their classical counterparts over finite fields (e.g., cyclic and constacyclic linear codes). This paper presents results concerning *monic principal skew codes*, called herein *monic principal* (f,σ,δ)*-codes*, where $f \in A[X;\sigma,\delta]$ is monic. We provide recursive formulas that compute the entries of both a generator matrix and a control matrix of such a code $\mathscr{C}$. When A is a finite commutative ring and σ is a ring automorphism of A, we also give recursive formulas for the entries of a parity-check matrix of $\mathscr{C}$. Also, in this case, with $\delta = 0$, we present a characterization of monic principal σ-codes whose dual codes are also monic principal σ-codes, and we deduce a characterization of self-dual monic principal σ-codes. Some corollaries concerning monic principal σ-constacyclic codes are also given, and a good number of highlighting examples is provided.

1. Introduction

1.1. State of the Art. Let A be a ring with identity, σ a ring endomorphism of A that maps the identity to itself, and δ a σ-derivation of A (i.e., $\delta(a+b) = \delta(a) + \delta(b)$ and $\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$ for all $a, b \in A$). Denote by $A_{\sigma,\delta}$ the skew-polynomial ring

$$A[X;\sigma,\delta] = \left\{ \sum_{i=0}^{n-1} a_i X^i | n \in \mathbb{N}, a_i \in A \right\}. \tag{1}$$

Recall that $A_{\sigma,\delta}$ has the same additive-group structure as that of the usual ring of polynomials $A[X]$ but has multiplication twisted based on the rule $Xa = \sigma(a)X + \delta(a)$ for $a \in A$ and extended associatively and distributively to all elements of $A_{\sigma,\delta}$. This obviously makes $A_{\sigma,\delta}$ a noncommutative ring unless $\delta = 0$, σ is the identity, and A is commutative (in which case $A_{\sigma,\delta}$ is nothing but $A[X]$). In case $\delta = 0$, we use the notation A_σ instead of $A_{\sigma,0}$.

For a finite field $\mathbb{F}$ and a ring automorphism σ of $\mathbb{F}$, Boucher et al. [1] used $\mathbb{F}_\sigma$ to introduce the notion of a skew-cyclic code $\mathscr{C}$ over $\mathbb{F}$ of length n as a code satisfying $(\sigma(a_{n-1}), \sigma(a_0), \sigma(a_1), \ldots, \sigma(a_{n-2})) \in \mathscr{C}$ for any $(a_0, a_1, \ldots, a_{n-2}, a_{n-1}) \in \mathscr{C}$. This is obviously a generalization of the classical notion of cyclic codes over finite fields (when σ is the identity). It is also shown therein that the class of skew-cyclic codes over finite fields gives a supply of codes with good coding and decoding properties (see also [2–5]). When a monic $f \in \mathbb{F}_\sigma$ generates a two-sided ideal in $\mathbb{F}_\sigma$, then, $\mathbb{F}_\sigma/(f)$ is a (noncommutative) principal left-ideal ring. In particular, when the order of σ divides n, then, $(X^n - 1)$ is a two-sided ideal in $\mathbb{F}_\sigma$ (see [1]). When, further, $g \in \mathbb{F}_\sigma$ is a right divisor of $X^n - 1$, Boucher et al. [1] studied the skew-cyclic code generated by g, which is associated with the principal left ideal $(g)/(X^n-1)$ of $\mathbb{F}_\sigma/(X^n-1)$. The structure of such an ideal puts some restrictions on the code (for instance, (X^n-1) must be a two-sided ideal, which is ensured by some arithmetical condition on n).

To further generalize the notion of skew-cyclic codes, Boucher and Ulmer [2] introduced codes defined as modules over $\mathbb{F}_\sigma$. Among other things, this new construction has the advantage of removing some of the constraints on the lengths of skew-cyclic codes alluded to above. Boucher et al. [6] relaxed the requirement on the field of coefficients by considering skew-polynomial rings over Galois rings enabling further generalizations and improvements (see also [7]). Boulagouaz and Leroy [8] took this generalization further by letting the ring of coefficients be any ring A with σ a ring endomorphism of A and δ a σ-derivation of A. A nice recent generalization in a different direction may be found in [9]. For other references on skew codes over rings, see [10, 11]; and for more references, see ([12], Chapter 6) and ([13], Chapter 11).

1.2. Contributions and Map of the Article

(i) For a ring A (not necessarily finite nor commutative), an endomorphism σ of A, and a σ-derivation δ of A, the following is performed:

(1) In Section 2, we revisit the main definitions of [8] and, particularly, make precise the notions of monic principal (f,σ,δ)-codes, σ-codes, (f,σ,δ)-constacyclic codes, and σ-constacyclic codes over A.

(2) Section 3 aims mainly at improving ([8], Theorem 1) computationally by giving a generator matrix of a monic principal (f,σ,δ)-code (resp. a monic principal σ-code) over A using recursive formulas introduced by means of a list of lemmas; see Theorem 1 (resp. Corollary 5).

(3) In Section 4, we present precise and more practical recursive formulas which yield, in Theorem 2, the entries of a control matrix of a monic principal (f,σ,δ)-code $\mathscr{C}$ over A whose generating polynomial is both a right and left divisor of f. This gives Theorem 2 a practicality advantage over ([8], Corollary 1). Furthermore, for a monic principal σ-code (resp. a monic principal σ-constacyclic code) over A, the control matrix given in Theorem 2 takes a better shape; see Corollary 6 (resp. Corollary 7).

(ii) For a finite commutative ring A and an automorphism σ of A, the following is performed:

(1) In Section 5, we characterize the monic principal σ-codes over A whose dual codes are also monic principal σ-codes, strengthening and extending ([3], Theorem 1); see Theorem 3 and the paragraph that precedes it. Consequently, we give in Corollary 8 a generator matrix of the dual of a monic principal σ-constacyclic code over A, and we further introduce, in Corollary 9, a characterization of self-dual monic principal σ-codes over A in such a way that generalizes and strengthens ([2], Corollary 4).

(2) In Section 6, we begin by introducing the notion of a parity-check matrix of a free (f,σ,δ)-code over a general ring with an endomorphism σ. We then go back to the assumptions on the ring A being finite and commutative and σ an automorphism of A, where we construct a parity-check matrix of a monic principal (f,σ,δ)-code $\mathscr{C}$ over A showing also how to extract such a matrix from a control matrix of $\mathscr{C}$; see Theorem 4. Furthermore, for a monic principal σ-code (resp. a monic principal σ-constacyclic code) over A, the parity-check matrix given in Theorem 4 takes a better shape; see Corollary 10 (resp. Corollary 11). On the other hand, with the crucial assumption that σ is an automorphism of A, we show in Corollary 12 that the parity-check matrix given in Corollary 11 can be obtained without the assumption that the monic principal σ-constacyclic code is generated by some monic $g \in A_\sigma$ that is also a left divisor of X^n-a.

(iii) Throughout the article, a good number of highlighting examples is given. An earlier preprint of this article is in reference [14]. Some results from this article were used in [15] to construct novel matrix-product codes arising from (σ,δ)-codes. Other applications of skew codes over rings can be found in ([12], Chapter 6) and ([13], Chapter 11) and the references therein.

2. Preliminaries

Let A be a ring with identity, σ a ring endomorphism of A that maps the identity to itself, δ a σ-derivation of A, and $U(A)$ the multiplicative group of units of A. Fix a monic skew-polynomial $f(X)=\sum_{i=0}^{n} a_i X^i \in A_{\sigma,\delta}$ of degree n. In order to define the notion of a skew (f,σ,δ)-code, we begin by using f to endow A^n with a structure of a left $A_{\sigma,\delta}$-module. Let C_f be the usual companion matrix of f; that is,

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

The map $T_f\colon A^n \longrightarrow A^n$ defined by

$$T_f(x_0,\dots,x_{n-1}) = (\sigma(x_0),\dots,\sigma(x_{n-1}))C_f + (\delta(x_0),\dots,\delta(x_{n-1})), \quad (3)$$

is a (σ,δ)-*pseudo-linear transformation* (*associated to* f); that is, considering A^n as a left A-module, we have $T_f(ax) = \sigma(a)T_f(x) + \delta(a)x$ for all $a \in A$ and $x \in A^n$. It can also be easily checked that T_f is a group endomorphism of A^n (see

[8] for more details and examples on this notion). For a skew-polynomial $P(X)=\sum_{i=0}^{n-1}b_iX^i\in A_{\sigma,\delta}$, the map $P(T_f)=\sum_{i=0}^{n-1}b_iT_f^i$ is obviously a group endomorphism of A^n as well. Now, the map $(P(X),(c_0,\ldots,c_{n-1}))\mapsto P\ (T_f)(c_0,\ldots,c_{n-1})$ defines a left action of $A_{\sigma,\delta}$ on A^n, which in turn endows A^n with a left $A_{\sigma,\delta}$-module structure as desired.

Let $(f)_l$ denote the principal left ideal of $A_{\sigma,\delta}$ generated by f. With A^n and $A_{\sigma,\delta}/(f)_l$ as left $A_{\sigma,\delta}$-modules, the map $\phi_f\colon A^n\longrightarrow A_{\sigma,\delta}/(f)_l$ defined by $(d_0,\ldots,d_{n-1})\mapsto\sum_{i=0}^{n-1}d_iX^i+(f)_l$ is a left $A_{\sigma,\delta}$-module isomorphism. The coset $\sum_{i=0}^{n-1}d_iX^i+(f)_l$ is called the *polynomial representation* of $(d_0,\ldots,d_{n-1})$ in $A_{\sigma,\delta}/(f)_l$. On the other hand, we know that for each $t(X)\in A_{\sigma,\delta}$, there exists a unique $p(X)=\sum_{i=0}^{n-1}d_iX^i\in A_{\sigma,\delta}$ of degree at most $n-1$ such that $t(X)+(f)_l=p(X)+(f)_l$. The n-tuple $(d_0,\ldots,d_{n-1})\in A^n$ is called the *coordinates* of $t(X)+(f)_l$ (with respect to the basis $\mathscr{B}=\{1+(f)_l, X+(f)_l,\ldots,X^{n-1}+(f)_l\}$). Note that $(d_0,\ldots,d_{n-1})=\phi_f^{-1}(t(X)+(f)_l)$.

A skew (f,σ,δ)*-code* (or an (f,σ,δ)*-code* for short) of length n over A is a linear code $\mathscr{C}\subseteq A^n$ such that $(x_0,\ldots,x_{n-1})\in\mathscr{C}$ implies that $T_f(x_0,\ldots,x_{n-1})\in\mathscr{C}$ (see [8]). With the above notation, an (f,σ,δ)*-code of length noverA* is a subset $\mathscr{C}$ of A^n consisting of the coordinates of a left $A_{\sigma,\delta}$-submodule $\mathscr{M}$ of $A_{\sigma,\delta}/(f)_l$ with respect to $\mathscr{B}$, i.e., $\mathscr{C}=\phi_f^{-1}(\mathscr{M})$ for some left $A_{\sigma,\delta}$-submodule $\mathscr{M}$ of $A_{\sigma,\delta}/(f)_l$. Equivalently, $\mathscr{C}\subseteq A^n$ is an (f,σ,δ)-code if and only if the set $\phi_f(\mathscr{C})$ of polynomial representations of elements of $\mathscr{C}$ is a left $A_{\sigma,\delta}$-submodule of $A_{\sigma,\delta}/(f)_l$. So, there is a one-to-one correspondence between (f,σ,δ)-codes over A and left $A_{\sigma,\delta}$-submodules of $A_{\sigma,\delta}/(f)_l$. If $\delta=0$, an (f,σ,δ)-code may be called an (f,σ)-code, or just a σ-code if f is irrelevant to the context. A linear code $\mathscr{C}\subseteq A^n$ is called a (σ,δ)-code of length n if there exists a monic skew-polynomial $f\in A_{\sigma,\delta}$ of degree n such that $\mathscr{C}$ is an (f,σ,δ)-code.

A ring over which every two bases of any finitely generated free (right) module have the same (finite) number of elements is said to have (right) *Invariant Basis Number* (IBN for short). This common number is defined to be *the rank* of such a module. Examples of such rings include nonzero commutative rings, nonzero finite rings, division rings, and local rings. For more on IBN rings, see ([16], Chapter 1). From now on, whenever we mention the finite rank of a free module, we implicitly assume without mention that the underlying ring has IBN.

As $\mathscr{M}$ is a left $A_{\sigma,\delta}$-submodule of $A_{\sigma,\delta}/(f)_l$, $\mathscr{C}$ is a left $A_{\sigma,\delta}$-submodule of A^n. Then, note *a priori* that $\mathscr{M}$ and $\mathscr{C}$ are left A-modules, and $\mathscr{M}$ is free over A of rank r if and only if $\mathscr{C}$ is free over A of rank r.

We call an (f,σ,δ)-code $\mathscr{C}=\phi_f^{-1}(\mathscr{M})$ over A *monic principal* if the left $A_{\sigma,\delta}$-submodule $\mathscr{M}$ of $A_{\sigma,\delta}/(f)_l$ is generated by a right divisor $g\in A_{\sigma,\delta}$ of f whose leading coefficient is a unit u; in which case $\mathscr{M}=(g)_l/(f)_l=(u^{-1}g)_l/(f)_l$, where $u^{-1}g$ is obviously monic, and so we can equivalently assume sometimes that $\mathscr{M}$ is generated by a monic right divisor of f. Note that if $g,h\in A_{\sigma,\delta}$ are such that $f=hg$ with a unit leading coefficient of g, then, the leading coefficient of h is a unit as well and $\deg(h)=\deg(f)-\deg(g)$. On the other hand, a linear code $\mathscr{C}\subseteq A^n$ is called a monic principal (σ,δ)-code of length n if there exists a monic skew-polynomial $f\in A_{\sigma,\delta}$ of degree n such that $\mathscr{C}$ is a monic principal (f,σ,δ)-code. Rephrased according to our terminology, ([8], Theorem 1) shows that a monic principal (f,σ,δ)-code generated by a monic skew-polynomial g is free over A of rank equal to $\deg(f)-\deg(g)$. It should be noted, however, that not all (f,σ,δ)-codes are monic principal since not all left $A_{\sigma,\delta}$-submodules of $A_{\sigma,\delta}/(f)_l$ are principal to begin with, and even if a left $A_{\sigma,\delta}$-submodule of $A_{\sigma,\delta}/(f)_l$ happens to be a principal submodule generated by a right divisor g of f, g may have a non-unit leading coefficient (unless A has no zero divisors). Being *free* codes has played an important factor on our choice of working with monic principal (f,σ,δ)-codes in this article. As such, we could deal with their related notions of generator matrices (Section 3), control matrices (Section 4), and under certain extra conditions, their *free* dual codes (Section 5) and parity-check matrices (Section 6).

In the special case, when $f(X)=X^n-a$ for some $a\in U(A)$ and $\mathscr{M}$ is a left $A_{\sigma,\delta}$-submodule (resp. a principal left $A_{\sigma,\delta}$-submodule generated by a right divisor of X^n-a whose leading coefficient is a unit) of $A_{\sigma,\delta}/(X^n-a)_l$, the (X^n-a,σ,δ)-code $\mathscr{C}=\phi_{X^n-a}^{-1}(\mathscr{M})$ is called an (X^n-a,σ,δ)*-constacyclic* (resp. a monic principal (X^n-a,σ,δ)*-constacyclic*) code. In this paper, we deal with such a code only when $\delta=0$ and thus call it an (X^n-a,σ)-constacyclic (resp. a monic principal (X^n-a,σ)-constacyclic) code. A linear code $\mathscr{C}\subseteq A^n$ is called a σ-constacyclic code (resp. a monic principal σ-constacyclic code) of length n if there exists $a\in U(A)$ such that $\mathscr{C}$ is an (X^n-a,σ)-code (resp. a monic principal (X^n-a,σ)-code). A monic principal σ-constacyclic code generated by a right divisor $g\in A_\sigma$ of X^n-a, for some $a\in U(A)$, is denoted by $(g)_{n,\sigma}^a$.

3. Generator Matrix of a Monic Principal (f,σ,δ)-Code over a Ring

In this section, we assume that A is a ring with identity, σ is a ring endomorphism of A that maps the identity to itself, and δ is a σ -derivation of A. For an A-free (f,σ,δ)-code $\mathscr{C}$ of rank $n-r$, define a *generator matrix* of $\mathscr{C}$ as a matrix $G\in M_{n-r,n}(A)$ whose rows form an A-basis of $\mathscr{C}$ (see [17]) for the classical definition of a generator matrix of a linear code over a field). In set notation, we have $\mathscr{C}=\{xG|x\in A^{n-r}\}$.

Let $f(X)=\sum_{i=0}^n a_iX^i\in A_{\sigma,\delta}$ be monic and $\mathscr{C}$ a monic principal (f,σ,δ)-code generated by a monic $g(X)=\sum_{i=0}^r g_iX^i\in A_{\sigma,\delta}$ of degree r. Then, by ([8], Theorem 1), $\mathscr{C}$ is free over A of rank $n-r$. Using g and the map T_f introduced in Section 1, Boulagouaz and Leroy [8] gave a way of computing G as in Lemma 1. The main aim of this section is to introduce, in Theorem 1, more practical recursive formulas that compute the entries of G using g, σ, and δ. Corollary 5 deals with the case when $\delta=0$.

Lemma 1 (see [8], Theorem 1). *With the assumptions as above, the monic principal (f,σ,δ) -code $\mathscr{C}$ has a generator matrix $G\in M_{n-r,n}(A)$ whose rows are given by*

$$T_f^i(g_0,\ldots,g_r,0,\ldots,0), \tag{4}$$

for $0\le i\le n-r-1$.

The following results aim at giving the set-up for producing formulas that compute

$$T_f^i(g_0,\ldots,g_r,0,\ldots,0), \tag{5}$$

much more easily, which among other things gives an obvious programming advantage to the process of computing G, for instance.

To simplify notation, for $i\ge 0$ and $(x_0,\ldots,x_{n-1})\in A^n$, we set

$$\left(x_0^{(i)},\ldots,x_{n-1}^{(i)}\right)=T_f^i(x_0,\ldots,x_{n-1}). \tag{6}$$

Lemma 2. *For* $(x_0,\ldots,x_{n-1})\in A^n$ *and* $i\in\mathbb{N}$, *we have*

(a) $x_0^{(i)}=\delta(x_0^{(i-1)})-\sigma(x_{n-1}^{(i-1)})a_0$;

(b) $x_j^{(i)}=\delta(x_j^{(i-1)})+\sigma(x_{j-1}^{(i-1)})-\sigma(x_{n-1}^{(i-1)})a_j$, *for*$1\le j\le n-1$.

Proof. By definition,

$$\begin{aligned}T_f(x_0,x_1,\ldots,x_{n-1})&=(\sigma(x_0),\sigma(x_1),\ldots,\sigma(x_{n-1}))C_f+(\delta(x_0),\delta(x_1),\ldots,\delta(x_{n-1}))\\&=(\delta(x_0)-\sigma(x_{n-1})a_0,\delta(x_1)+\sigma(x_0)-\sigma(x_{n-1})a_1,\ldots,\delta(x_{n-1})+\sigma(x_{n-2})-\sigma(x_{n-1})a_{n-1}).\end{aligned} \tag{7}$$

As $(x_0^{(i)},x_1^{(i)},\ldots,x_{n-1}^{(i)})=T_f^i(x_0,\ldots,x_{n-1})=T_f(x_0^{(i-1)},x_1^{(i-1)},\ldots,x_{n-1}^{(i-1)})$, we have

$$\begin{aligned}\left(x_0^{(i)},x_1^{(i)},\ldots,x_{n-1}^{(i)}\right)=&\left(\delta\left(x_0^{(i-1)}\right)-\sigma\left(x_{n-1}^{(i-1)}\right)a_0,\delta\left(x_1^{(i-1)}\right)\right.\\&+\sigma\left(x_0^{(i-1)}\right)-\sigma\left(x_{n-1}^{(i-1)}\right)a_1,\ldots,\delta\left(x_{n-1}^{(i-1)}\right)\\&\left.+\sigma\left(x_{n-2}^{(i-1)}\right)-\sigma\left(x_{n-1}^{(i-1)}\right)a_{n-1}\right).\end{aligned} \tag{8}$$

□

Corollary 1. *For* $(x_0,\ldots,x_{n-1})\in A^n$ *with* $x_{n-1}=0$, *we have*

(a) $x_0^{(1)}=\delta(x_0)$;

(b) $x_j^{(1)}=\delta(x_j)+\sigma(x_{j-1})$ *for* $1\le j\le n-2$;

(c) $x_{n-1}^{(1)}=\sigma(x_{n-2})$.

Proof. This follows directly from Lemma 2 and properties of σ and δ. □

Corollary 2. *For* $(x_0,\ldots,x_{n-1})\in A^n$ *with* $x_{s+1}=\ldots=x_{n-1}=0$ *for some* $0\le s\le n-2$, *we have*

(a) $x_{s+i}^{(i)}=\sigma^i(x_s)$ *for* $1\le i<n-s-1$;

(b) $x_{s+j}^{(i)}=0$ *for* $1\le i<j\le n-s-1$.

Proof. We proceed by (finite) induction on i. For $i=1$, it follows from Corollary 1 that

$$x_{s+1}^{(1)}=\delta(x_{s+1})+\sigma(x_s)=\delta(0)+\sigma(x_s)=\sigma(x_s). \tag{9}$$

For $1=i<j\le n-s-1$, we have $s+1\le s+j-1\le n-2$ and (by Corollary 1)

$$x_{s+j}^{(1)}=\delta\left(x_{s+j}\right)+\sigma\left(x_{s+j-1}\right)=\delta(0)+\sigma(0)=0. \tag{10}$$

Assume now, for $1<i<n-s-1$, that $x_{s+i-1}^{(i-1)}=\sigma^{i-1}(x_s)$ and, for $i-1<t\le n-s-1$, that $x_{s+t}^{(i-1)}=0$. Then, it follows from Lemma 2 that

$$\begin{aligned}x_{s+i}^{(i)}&=\delta\left(x_{s+i}^{(i-1)}\right)+\sigma\left(x_{s+i-1}^{(i-1)}\right)-\sigma\left(x_{n-1}^{(i-1)}\right)a_{s+i}\\&=\delta(0)+\sigma\left(\sigma^{i-1}(x_s)\right)-\sigma(0)a_{s+i}=\sigma^i(x_s).\end{aligned} \tag{11}$$

We also have (by Lemma 2), for $1<i<j\le n-s-1$,

$$\begin{aligned}x_{s+j}^{(i)}&=\delta\left(x_{s+j}^{(i-1)}\right)+\sigma\left(x_{s+j-1}^{(i-1)}\right)-\sigma\left(x_{n-1}^{(i-1)}\right)a_{s+j}\\&=\delta(0)+\sigma\left(x_{s+j-1}^{(i-1)}\right)-\sigma(0)a_{s+j}=\sigma\left(x_{s+j-1}^{(i-1)}\right).\end{aligned} \tag{12}$$

As $i-1<j-1$, $x_{s+j-1}^{(i-1)}=0$ by assumption. Thus, $x_{s+j}^{(i)}=0$ as claimed. □

Corollary 3. *Let* $(x_0,\ldots,x_{n-1})\in A^n$ *and* $\delta=0$.

(a) If $x_{n-1}=0$, *then,* $x_0^{(1)}=0$ *and* $x_j^{(1)}=\sigma(x_{j-1})$ *for* $1\le j\le n-1$.

(b) If $x_{s+1}=\ldots=x_{n-1}=0$ *for some* $0\le s\le n-2$, *then for any* $1\le i\le n-s-1$,

(i) $x_j^{(i)}=0$ *for* $0\le j\le i-1$, *and*

(ii) $x_j^{(i)}=\sigma(x_{j-1}^{(i-1)})$ *for* $0\le i-1<j\le n-1$.

Proof

(a) A direct application of Corollary 1 yields the claim.

(b) We proceed by (finite) induction on i. Let $i=1$. If $0\le j\le i-1$, then, $j=0$. So, $x_0^{(i)}=x_0^{(1)}=0$ by part (1) above. From part (1) again, for $0=i-1<j\le n-1$, $x_j^{(i)}=x_j^{(1)}=\sigma(x_{j-1})=\sigma(x_{j-1}^{(0)})=\sigma(x_{j-1}^{(i-1)})$ as desired. Assume now that the result holds for all $1\le i<n-s-1$. Set $y_j=x_j^{(i)}$ for each $0\le j\le n-1$, and note that $y_j^{(t)}=(x_j^{(i)})^{(t)}=x_j^{(i+t)}$ for all $t\ge 1$. By the inductive assumption, we see that

$$\begin{aligned}y_{n-1}&=x_{n-1}^{(i)}=\sigma\left(x_{n-2}^{(i-1)}\right)=\sigma^2\left(x_{n-3}^{(i-2)}\right)=\cdots=\sigma^i\left(x_{n-1-i}^{(0)}\right)\\&=\sigma^i(x_{n-1-i}).\end{aligned} \tag{13}$$

As $i<n-s-1$, $n-1-i>s$. So, $x_{n-1-i}=0$ and, thus, $y_{n-1}=0$. It now follows from part (1) applied to

$(y_0, \ldots, y_{n-1})$ that $x_0^{(i+1)} = y_0^{(1)} = 0$, and for $1 \le j \le n-1$, $x_j^{(i+1)} = y_j^{(1)} = \sigma(y_{j-1}) = \sigma(x_{j-1}^{(i)})$. Note, in particular, that for $1 \le j \le i+1$, $0 \le j-1 \le i$. So, $x_{j-1}^{(i)} = 0$ by the inductive assumption, and therefore, $x_j^{(i+1)} = \sigma(0) = 0$ in this case. □

Corollary 4. *Let $(x_0, \ldots, x_{n-1}) \in A^n$, $\delta = 0$, and $a_1 = \cdots = a_{n-1} = 0$. Then,*

(a) For $i \in \mathbb{N}$, we have

(1) $x_0^{(i)} = -\sigma(x_{n-1}^{(i-1)})a_0$;
(2) $x_j^{(i)} = \sigma(x_{j-1}^{(i-1)})$ for $1 \le j \le n-1$.

(b) If, further, $x_0 = x_1 = \ldots x_s = 0$ for some $0 \le s \le n-2$, then, we have

(i) (1) $x_0^{(1)} = -\sigma(x_{n-1})a_0$
(2) $x_j^{(1)} = 0$ for $1 \le j \le s+1$
(3) $x_j^{(1)} = \sigma(x_{j-1})$ for $s+2 \le j \le n-1$

(ii) For $2 \le i \le n-s-1$, we have
(1) $x_0^{(i)} = -\sigma(x_{n-1}^{(i-1)})a_0$
(2) $x_j^{(i)} = \sigma(x_{j-1}^{(i-1)})$ for $1 \le j \le i-1$
(3) If $s \ge 1$, then $x_j^{(i)} = 0$ for $i \le j \le i+s-1$
(4) $x_j^{(i)} = \sigma(x_{j-1}^{(i-1)})$ for $i+s \le j \le n-1$.

Proof

(a) This follows directly from Lemma 2 with $\delta = 0$ and $a_1 = \cdots = a_{n-1} = 0$.

(b) By part (a), we have

(i) $x_0^{(1)} = -\sigma(x_{n-1}^{(0)})a_0 = -\sigma(x_{n-1})a_0$
(2) For $1 \le j \le s+1$, $x_j^{(1)} = \sigma(x_{j-1}^{(0)}) = \sigma(x_{j-1}) = \sigma(0) = 0$
(3) For $s+2 \le j \le n-1$, $x_j^{(1)} = \sigma(x_{j-1}^{(0)}) = \sigma(x_{j-1})$.

(ii) Items 1, 2, and 4 are immediate from part (a). As for item 3, assume that $s \ge 1$. We use (finite) induction on i. For $i = 2$ and $2 \le j \le s+1$, we have $1 \le j-1 \le s$ and it thus follows from part (a) and part (b-i-2) that $x_j^{(2)} = \sigma(x_{j-1}^{(1)}) = \sigma(0) = 0$. Suppose now that $x_j^{(i)} = 0$ for $2 \le i \le n-s-2$ and $i \le j \le i+s-1$. Then, for $i+1 \le j \le i+s$, we have $i \le j-1 \le i+s-1$. So, it follows from part (a) and the inductive step that $x_j^{(i+1)} = \sigma(x_{j-1}^{(i)}) = \sigma(0) = 0$.

Now comes the main result of this section, which gives precise recursive formulas for the entries of a generator matrix of $\mathscr{C}$ enhancing ([8], Theorem 1). □

Theorem 1. *Keep the assumptions mentioned at the beginning of this section. Then, a generator matrix $G \in M_{n-r,n}(A)$ of $\mathscr{C}$ is*

$$\begin{pmatrix} g_0 & \cdots & g_r & 0 & 0 & \cdots & 0 \\ g_0^{(1)} & \cdots & g_r^{(1)} & \sigma(g_r) & 0 & \cdots & 0 \\ g_0^{(2)} & \cdots & g_r^{(2)} & g_{r+1}^{(2)} & \sigma^2(g_r) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ g_0^{(n-r-1)} & \cdots & g_r^{(n-r-1)} & g_{r+1}^{(n-r-1)} & g_{r+2}^{(n-r-1)} & \cdots & \sigma^{n-r-1}(g_r) \end{pmatrix}, \tag{14}$$

where

(1) $g_j = 0$ for $r+1 \le j \le n-1$,
(2) $g_0^{(i)} = \delta(g_0^{(i-1)})$ for $1 \le i \le n-r-1$
(3) $g_j^{(i)} = \delta(g_j^{(i-1)}) + \sigma(g_{j-1}^{(i-1)})$ for $1 \le i \le n-r-1$ and $1 \le j \le n-1$.

Proof. Using Lemma 1 and applying Corollaries 1 and 2 with $s = r$, $(x_0, \ldots, x_{n-1}) = (g_0, \ldots, g_{n-1})$, and $g_{r+1} = \cdots = g_n = 0$ yield the claim of the theorem. □

If $\mathscr{C}$ of Theorem 1 is a monic principal σ-code (i.e., $\delta = 0$), then, a generator matrix of $\mathscr{C}$ takes a more beautiful form as the following result shows, the proof of which is just a direct application of Theorem 1 in this special case.

Corollary 5. *Keep all the assumptions of Theorem 1 with $\delta = 0$. Then, a generator matrix $G \in M_{n-r,n}(A)$ of $\mathscr{C}$ is*

$$\begin{pmatrix} g_0 & \cdots & g_r & 0 & 0 & \cdots & 0 \\ 0 & \sigma(g_0) & \cdots & \sigma(g_r) & 0 & \cdots & 0 \\ \vdots & \ddots & & & \ddots & & \vdots \\ 0 & 0 & \cdots & 0 & \sigma^{n-r-1}(g_0) & \cdots & \sigma^{n-r-1}(g_r) \end{pmatrix}. \tag{15}$$

Example 1. Let R be a ring with identity and A the ring $\left\{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} | a, b \in R\right\}$. Letting $\sigma: \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mapsto \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ and $\delta: \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mapsto \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$, it can be checked that σ is a ring endomorphism of A that maps the identity to itself and δ is a σ-derivation of A. Let $\mathscr{C}$ a monic principal (σ, δ)-code of length 4 generated by $g(X) = X - \alpha \in A_{\sigma,\delta}$ with $\alpha = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Noting that $g_0 = -\alpha$, $g_1 = 1$, $g_2 = g_3 = 0$, we get from Theorem 1 that a generator matrix of $\mathscr{C}$ is

$$\begin{aligned} G &= \begin{pmatrix} g_0 & g_1 & 0 & 0 \\ g_0^{(1)} & g_1^{(1)} & \sigma(g_1) & 0 \\ g_0^{(2)} & g_1^{(2)} & g_2^{(2)} & \sigma^2(g_1) \end{pmatrix} \\ &= \begin{pmatrix} g_0 & 1 & 0 & 0 \\ \delta(g_0) & \delta(1) + \sigma(g_0) & 1 & 0 \\ (\delta(g_0))^{(1)} & (\delta(1) + \sigma(g_0))^{(1)} & (1)^{(1)} & (0)^{(1)} \end{pmatrix} \\ &= \begin{pmatrix} g_0 & 1 & 0 & 0 \\ \delta(g_0) & \delta(g_1) + \sigma(g_0) & 1 & 0 \\ \delta^2(g_0) & \delta^2(1) + (\delta\sigma + \sigma\delta)(g_0) & (\delta\sigma + \sigma\delta)(1) + \sigma^2(g_0) & 1 \end{pmatrix} \\ &= \begin{pmatrix} -\alpha & 1 & 0 & 0 \\ \delta(-\alpha) & \sigma(-\alpha) & 1 & 0 \\ \delta^2(-\alpha) & 0 & \sigma^2(-\alpha) & 1 \end{pmatrix} = \begin{pmatrix} -\alpha & 1 & 0 & 0 \\ 1-\alpha & -1 & 1 & 0 \\ 1-\alpha & 0 & -1 & 1 \end{pmatrix}. \end{aligned} \tag{16}$$

On the other hand, if $\delta = 0$, then, it follows from Corollary 5 that a generator matrix of $\mathscr{C}$ is

$$G = \begin{pmatrix} g_0 & g_1 & 0 & 0 \\ 0 & \sigma(g_0) & \sigma(g_1) & 0 \\ 0 & 0 & \sigma^2(g_0) & \sigma^2(g_1) \end{pmatrix} = \begin{pmatrix} -\alpha & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{pmatrix}. \quad (17)$$

Example 2. Let $A = \mathbb{F}_3 \times \mathbb{F}_3$, $\sigma(x, y) = (y, x)$, and $f(X) = X^6 + 1 \in A_\sigma$. Denoting $(a, a) \in A$ by a, we can see that $f(X) = (X^2 + 1)(X^4 + 2X^2 + 1) = (X^4 + 2X^2 + 1)(X^2 + 1)$. The σ-code generated by $g(X) = X^4 + 2X^2 + 1$ is a monic principal σ-constacyclic (or negacyclic if one wishes), which is a self-orthogonal $[6, 4, 2]$ code over A with generator matrix $\begin{pmatrix} 1 & 0 & 2 & 0 & 1 & 0 \\ 0 & 1 & 0 & 2 & 0 & 1 \end{pmatrix}$. Using the obvious Gray map on Magma ([18]), this code yields a ternary $[12, 4, 3]$ code whose dual is a $[12, 8, 2]$ code, which is quasioptimal (see [19]).

4. Control Matrix of a Monic Principal (f, σ, δ)-Code over a Ring

In this section, we assume that A is a ring with identity, σ is a ring endomorphism of A that maps the identity to itself, and δ is a σ-derivation of A. The results of Section 3 are utilized here to give control matrices (defined below) of a monic principal (f, σ, δ)-code, a monic principal σ-code, and a monic principal σ-constacyclic code.

For $H \in M_{n,t}(A)$ with $t \leq n$, denote by $\mathrm{Ann}_l(H)$ the left A-submodule of A^n:

$$\mathrm{Ann}_l(H) := \{x \in A^n \mid xH = 0\}. \quad (18)$$

If $\mathscr{C}$ is an (f, σ, δ)-code of length n over A, a matrix $H \in M_{n,t}(A)$, with $t \leq n$, is called a *control matrix* of $\mathscr{C}$ if $\mathscr{C} = \mathrm{Ann}_l(H)$. Consequently, for an A-free code $\mathscr{C}$, if G is a generator matrix of $\mathscr{C}$ and H is a control matrix of $\mathscr{C}$, then, $GH = 0$.

For a monic principal (f, σ, δ)-code $\mathscr{C}$ over A that is generated by some monic $g \in A_{\sigma,\delta}$ which is both a right and left divisor of f, Boulagouaz and Leroy [8] gave a way of computing a control matrix of $\mathscr{C}$, as in Lemma 3, using T_f and h, where $h \in A_{\sigma,\delta}$ is such that $gh = f$. Theorem 2 gives precise and more practical recursive formulas that compute a control matrix of $\mathscr{C}$ using f, h, σ and δ. Corollary 6 deals with the special case when $\delta = 0$, while Corollary 7 handles the more special case when $\mathscr{C}$ is monic principal σ-constacyclic.

Lemma 3 (see [8], Corollary 1). *Let $\mathscr{C}$ be a monic principal (f, σ, δ)-code of length n generated by some monic $g \in A_{\sigma,\delta}$ of degree $n-k$ which is also a left divisor of f, with $f = gh$ for some $h(X) = \sum_{i=0}^{k} h_i X^i \in A_{\sigma,\delta}$. Then, a control matrix of $\mathscr{C}$ is the matrix $H \in M_{n,n}(A)$ whose rows are $T_f^i(h_0, \ldots, h_k, 0, \ldots, 0)$ for $0 \leq i \leq n-1$.*

Remark 1. Lemma 3 is still valid if we assume that the leading coefficient of g is a unit in A.

With the assumptions of Lemma 3, the following theorem gives explicit and more practical recursive formulas to compute a control matrix.

Theorem 2. *Keep the assumptions of Lemma 3 with $f(X) = \sum_{i=0}^{n} a_i X^i$. Then, a control matrix $H \in M_{n,n}(A)$ of $\mathscr{C}$ is given by*

$$\begin{pmatrix} h_0 & \ldots & h_k & 0 & 0 & \ldots & 0 \\ h_0^{(1)} & \ldots & h_k^{(1)} & \sigma(h_k) & 0 & \ldots & 0 \\ h_0^{(2)} & \ldots & h_k^{(2)} & h_{k+1}^{(2)} & \sigma^2(h_k) & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ h_0^{(n-k-1)} & \ldots & h_k^{(n-k-1)} & h_{k+1}^{(n-k-1)} & h_{k+2}^{(n-k-1)} & \ldots & \sigma^{n-k-1}(h_k) \\ h_0^{(n-k)} & \ldots & h_k^{(n-k)} & h_{k+1}^{(n-k)} & h_{k+2}^{(n-k)} & \ldots & h_{n-1}^{(n-k)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ h_0^{(n-1)} & \ldots & h_k^{(n-1)} & h_{k+1}^{(n-1)} & h_{k+2}^{(n-1)} & \ldots & h_{n-1}^{(n-1)} \end{pmatrix}, \quad (19)$$

where,

(1) $h_j = 0$ for $k + 1 \leq j \leq n - 1$,

(2) for $2 \leq n - k$, $1 \leq i \leq n - k - 1$, and $1 \leq j \leq n - 1$,

(i) $h_0^{(i)} = \delta(h_0^{(i-1)})$,

(ii) $h_j^{(i)} = \delta(h_j^{(i-1)}) + \sigma(h_{j-1}^{(i-1)})$,

(3) for $n - k \leq i \leq n - 1$ and $1 \leq j \leq n - 1$

(i) $h_0^{(i)} = \delta(h_0^{(i-1)}) - \sigma(h_{n-1}^{(i-1)})a_0$, and

(ii) $h_j^{(i)} = \delta(h_j^{(i-1)}) + \sigma(h_{j-1}^{(i-1)}) - \sigma(h_{n-1}^{(i-1)})a_j$.

Proof. By Lemma 3, a control matrix of $\mathscr{C}$ is the matrix $H \in M_{n,n}(A)$ whose rows are

$$T_f^i(h_0, \ldots, h_k, 0, \ldots, 0) = (h_0^{(i)}, \ldots, h_{n-1}^{(i)}), \quad \text{for } 0 \leq i \leq n-1. \quad (20)$$

Now applying Lemma 2 and Corollaries 1 and 2 with $s = k$ and $(h_0, \ldots, h_{n-1})$ in place of $(x_0, \ldots, x_{n-1})$ yields the desired conclusion. □

Remark 2. In Theorem 2, case (1) deals with the first row of H, case (2) deals with the rows (beyond the first row) which end with consecutive zeros, and case (3) deals with the remaining rows. It is obvious that in case $n - k = 1$, we disregard case (2) and consider only cases (1) and (3). In such a case, as $n = k + 1$, the last column of H is the $(k+1)^{\text{st}}$ which has h_k at the top, and so the upper triangle of zeros does not exist (see the example below).

Example 3. Let R be a ring of characteristic 3 with identity and $A = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \middle| a, b \in R \right\}$. Take $\sigma: \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ and $\delta: \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mapsto \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$. Let $f(X) = X^3 + 2X \in A_{\sigma,\delta}$ where 2 obviously denotes $2\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Consider $g(X) = X +$

$2\beta \in A_{\sigma,\delta}$ and $h(X) = X^2 + \beta X + \alpha \in A_{\sigma,\delta}$ with $\alpha = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. A simple verification shows that $f = gh = hg$. Let $\mathscr{C}$ be the monic principal (f, σ, δ)-code generated by g. Noting that $h_0 = \alpha$, $h_1 = \beta$, and $h_2 = 1$, it follows from Theorem 2 (cases (1) and (3); see the above remark) that a control matrix of $\mathscr{C}$ is

$$H = \begin{pmatrix} h_0 & h_1 & h_2 \\ h_0^{(1)} & h_1^{(1)} & h_2^{(1)} \\ h_0^{(2)} & h_1^{(2)} & h_2^{(2)} \end{pmatrix} = \begin{pmatrix} \alpha & \beta & 1 \\ \alpha & 2\alpha + 1 & \beta \\ \alpha & \beta & 1 \end{pmatrix}. \quad (21)$$

To double-check that H is a correct control matrix, it follows from Theorem 1 that a generator matrix of $\mathscr{C}$ is $G = \begin{pmatrix} 2\beta & 1 & 0 \\ 2\alpha & 2\beta & 1 \end{pmatrix}$. Making use of the characteristic of R and properties of σ, δ, α, and β, it is straightforward to check that $GH = 0$.

Corollary 6. *Keep the assumptions of Theorem 2 with $\delta = 0$. Then, a control matrix $H \in M_{n,n}(A)$ of $\mathscr{C}$ is given by*

$$\begin{pmatrix} h_0 & h_1 & h_2 & \dots & h_k & 0 & 0 & 0 & \dots & 0 \\ 0 & \sigma(h_0) & \sigma(h_2) & \dots & \sigma(h_{k-1}) & \sigma(h_k) & 0 & 0 & \dots & 0 \\ 0 & 0 & \sigma^2(h_0) & \dots & \sigma^2(h_{k-2}) & \sigma^2(h_{k-1}) & \sigma^2(h_k) & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \dots & 0 & \sigma^{n-k-1}(h_0) & \dots & \dots & \dots & \sigma^{n-k-1}(h_k) \\ h_0^{(n-k)} & h_1^{(n-k)} & \dots & \dots & h_k^{(n-k)} & h_{k+1}^{(n-k)} & h_{k+2}^{(n-k)} & \dots & \dots & h_{n-1}^{(n-k)} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ h_0^{(n-1)} & h_1^{(n-1)} & \dots & \dots & h_k^{(n-1)} & h_{k+1}^{(n-1)} & h_{k+2}^{(n-1)} & \dots & \dots & h_{n-1}^{(n-1)} \end{pmatrix}, \quad (22)$$

where the number of initial consecutive zeros in the ith row is precisely $i - 1$ for $i = 2, \dots, n - k$, and

(1) $h_j = 0$ for $k + 1 \le j \le n - 1$,

(2) for $2 \le n - k$, $1 \le i \le n - k - 1$, and $1 \le j \le n - 1$,

(i) $h_0^{(i)} = 0$,
(ii) $h_j^{(i)} = \sigma(h_{j-1}^{(i-1)})$,

(3) for $n - k \le i \le n - 1$ and $1 \le j \le n - 1$,

(i) $h_0^{(i)} = -\sigma(h_{n-1}^{(i-1)})a_0$, and
(ii) $h_j^{(i)} = \sigma(h_{j-1}^{(i-1)}) - \sigma(h_{n-1}^{(i-1)})a_j$.

Proof. Use Theorem 2 and Corollary 3. □

Corollary 7. *Keep the assumptions of Corollary 6. Let $\mathscr{C}$ be a monic principal σ-constacyclic code $\mathscr{C} = (g)_{n,\sigma}^a$ for some $a \in U(A)$ such that g is also a left divisor of $X^n - a$ with $X^n - a = g(X)h(X)$ for some $h(X) = \sum_{i=0}^k h_i X^i \in A_{\sigma,\delta}$. Then, the entries of a control matrix $H = (H_{i,j}) \in M_{n,n}(A)$ of $\mathscr{C}$ are as follows:*

(a) If $n - k = 1$, then,

$$H_{1,j} = h_{j-1}; \text{if } 1 \le j \le n, \quad (23)$$

and , for $2 \le i \le n$,, then,

$$H_{i,j} = \begin{cases} -\sigma^{i-1}(h_{n-i+j})a & ;\text{if } 1 \le j \le i-1, \\ \sigma^{i-1}(h_{j-i}) & ;\text{if } i \le j \le n. \end{cases} \quad (24)$$

(b) If $n - k \ge 2$, then,

(i) for $i = 1$,

$$H_{1,j} = \begin{cases} h_{j-1} & ;\text{if } 1 \le j \le k+1, \\ 0 & ;\text{if } k+2 \le j \le n. \end{cases} \quad (25)$$

(ii) for $2 \le i \le n - k$,

$$H_{i,j} = \begin{cases} 0 & ;\text{if } 1 \le j \le i-1, \\ \sigma^{i-1}(h_{j-i}) & ;\text{if } i \le j \le i+k, \\ 0 & ;\text{if } i+k+1 \le j \le n. \end{cases} \quad (26)$$

(iii) for $n - k + 1 \le i \le n$,

$$H_{i,j} = \begin{cases} -\sigma^{i-1}(h_{n-i+j})a & ;\text{if } 1 \le j \le i-(n-k), \\ 0 & ;\text{if } i-(n-k)+1 \le j \le i-1, \\ \sigma^{i-1}(h_{j-i}) & ;\text{if } i \le j \le n. \end{cases} \quad (27)$$

Proof. Apply Corollary 4 and Corollary 6. □

5. The Dual of a Monic Principal σ-Code over a Finite Commutative Ring

In this section, we assume that A is a finite commutative ring with identity and σ is an automorphism of A. We give in Theorem 3 a characterization of monic principal σ-codes over A whose duals are also monic principal σ-codes, strengthening and extending ([3], Theorem 1). Furthermore, Corollary 8 utilizes Theorem 3 and Corollary 5 to give a generator matrix of the dual of a monic principal σ-constacyclic code. Finally, Corollary 9 characterizes self-dual monic principal σ-codes over A in such a way that generalizes and strengthens ([2], Corollary 4).

For a linear code $\mathscr{C}\subseteq A^n$, the set $\{y \in A^n | \langle x, y\rangle = 0 \text{ for all } x \in \mathscr{C}\}$ of elements of A^n orthogonal to $\mathscr{C}$ with respect to the Euclidean inner product on A^n is called the dual of $\mathscr{C}$ and is denoted by $\mathscr{C}^\perp$. It can be checked that $\mathscr{C}^\perp$ is a left A-submodule of A^n and so is a linear code. It is noted that if $\mathscr{C}$ is free with a generator matrix G and a control matrix H, then, it follows from the equality $GH = 0$ (see Section 4) that the columns of H are elements of the dual code $\mathscr{C}^\perp$.

For a skew-polynomial $h(X) = \sum_{i=0}^{s} h_i X^i \in A_\sigma$, define the following skew-polynomials:

$$\sigma^n(h(X)) = \sum_{i=0}^{s} \sigma^n(h_i)X^i \ (\text{for } n \in \mathbb{N}) \text{and } h^*(X) = \sum_{i=0}^{s} \sigma^i(h_{s-i})X^i. \tag{28}$$

Consider the ring of Laurent skew-polynomials:

$$A\left[X, X^{-1}; \sigma\right] = \left\{ \sum_{i=-m}^{n} a_i X^i | m, n \in \mathbb{N}\cup\{0\}, a_i \in A \right\}, \tag{29}$$

where addition is given by the usual rule and multiplication is given by the rule:

$$\left(a_i X^i\right)\left(b_j X^j\right) = a_i\sigma^i\left(b_j\right)X^{i+j} \ (\text{for } i, j \in \mathbb{Z}), \tag{30}$$

and then extending associatively and distributively to all elements of $A[X, X^{-1}; \sigma]$. It is obvious that A_σ is a subring of $A[X, X^{-1}; \sigma]$. It is worth noting that $X^{-1}a = \sigma^{-1}(a)X^{-1}$ and $aX^{-1} = X^{-1}\sigma(a)$ for all $a \in A$.

The following result and its proof are similar, in part, to their counterparts over finite fields appearing in the literature (see for instance [3], Lemma 1]).

Lemma 4. *Let ψ: $A[X, X^{-1}; \sigma] \longrightarrow A[X, X^{-1}; \sigma]$ be the map defined by*

$$\sum_{i=-m}^{n} a_i X^i \mapsto \sum_{i=-m}^{n} X^{-i} a_i, \tag{31}$$

Also, let $h(X) = \sum_{i=0}^{s} h_i X^i \in A_\sigma$ be of degree s. Then, the following holds:

(i) ψ is a ring antiautomorphism,
(ii) $h^*(X) = X^s\psi(h(X))$,
(iii) for any $n \in \mathbb{N}$, $X^n h(X) = \sigma^n(h(X))X^n$, and
(iv) if h_s is not a zero divisor in A, then, $h(X)$ is not a zero divisor in A_σ.

Proof

(i) It is straightforward to show that ψ is bijective and additive. Consider two Laurent skew-polynomials $S(X) = \sum_{i=-m_1}^{n_1} s_i X^i$ and $T(X) = \sum_{j=-m_2}^{n_2} t_j X^j$. Letting $k = \max\{m_1, m_2\}$, we may add zero terms if necessary to set $S(X) = \sum_{i=-k}^{n_1} s_i X^i$ and $T(X) = \sum_{j=-k}^{n_2} t_j X^j$. Then,

$$\begin{aligned}\psi(S(X)T(X)) &= \psi\left(\left(\sum_{i=-k}^{n_1} s_i X^i\right)\left(\sum_{j=-k}^{n_2} t_j X^j\right)\right) = \psi\left(\sum_{i=-k}^{n_1}\sum_{j=-k}^{n_2} s_i X^i t_j X^j\right)\\ &= \psi\left(\sum_{j=-k}^{n_2}\sum_{i=-k}^{n_1} s_i\sigma^i\left(t_j\right)X^{i+j}\right) = \sum_{j=-k}^{n_2}\sum_{i=-k}^{n_1} X^{-(i+j)} s_i\sigma^i\left(t_j\right).\end{aligned} \tag{32}$$

On the other hand,

$$\begin{aligned}\psi(T(X))\psi(S(X)) &= \left(\sum_{j=-k}^{n_2} X^{-j} t_j\right)\left(\sum_{i=-k}^{n_1} X^{-i} s_i\right) = \sum_{j=-k}^{n_2}\sum_{i=-k}^{n_1} X^{-j} t_j X^{-i} s_i\\ &= \sum_{j=-k}^{n_2}\sum_{i=-k}^{n_1} X^{-(i+j)}\sigma^i\left(t_j\right)s_i = \sum_{j=-k}^{n_2}\sum_{i=-k}^{n_1} X^{-(i+j)} s_i\sigma^i\left(t_j\right).\end{aligned} \tag{33}$$

Thus, $\psi(S(X)T(X)) = \psi(T(X))\psi(S(X))$.

(ii) We see that

$$X^s\psi(h(X)) = X^s\left(\sum_{i=0}^{s} X^{-i}h_i\right) = \sum_{i=0}^{s} X^{s-i}h_i = \sum_{i=0}^{s} \sigma^{s-i}(h_i)X^{s-i} = \sum_{j=0}^{s} \sigma^j(h_{s-j})X^j = h^*(X). \quad (34)$$

(iii) $X^n h(X) = \sum_{i=0}^{s} X^n h_i X^i = \sum_{i=0}^{s} \sigma^n(h_i)X^{i+n} = \sigma^n(h(X))X^n$.

(iv) Let $r(X) = \sum_{j=0}^{t} r_j X^j \in A_\sigma$ be such that $r_t \neq 0$ and $h(X)r(X) = 0$ (resp. $r(X)h(X) = 0$). Then, $\sigma^s(r_t)h_s = 0$ (resp. $r_t\sigma^t(h_s) = 0$). Note that since h_s is not a zero divisor in A and σ^t is an automorphism of A, $\sigma^t(h_s)$ is not a zero divisor in A either. It then follows that $\sigma^s(r_t) = 0$ (resp. $r_t = 0$). Since σ^s is an automorphism of A, it follows in both cases that $r_t = 0$, a contradiction. Thus, $r(X) = 0$.

Special cases of the following two results (in the context of finite fields) appear in [3]. □

Lemma 5. *Let $g(X) = \sum_{i=0}^{n-k} g_i X^i \in A_\sigma$ be of degree $n-k$, $g_{n-k} \in U(A)$, $h(X) = \sum_{i=0}^{k} h_i X^i \in A_\sigma$ of degree k, and $b \in U(A)$. Then, $X^n - b = g(X)h(X)$ if and only if $X^n - a = \sigma^n(h(X))g(X)$ for $a = \sigma^k(b)\sigma^{k-n}(g_{n-k})\sigma^k(g_{n-k}^{-1})$.*

Proof. Either of the claimed equivalent statements imply that $h_k \in U(A)$. We first prove the lemma for the case when g is monic. Assume that $X^n - b = g(X)h(X)$. Then, h is monic too. It follows from Lemma 4 (iii) that,

$$\sigma^n(h(X))g(X)h(X) = \sigma^n(h(X))X^n - \sigma^n(h(X))b = X^n h(X) - \sigma^n(h(X))b. \quad (35)$$

So, $[X^n - \sigma^n(h(X))g(X)]h(X) = \sigma^n(h(X))b$. Since $\deg(h) = \deg(\sigma^n(h)b)$ and h is monic, $\deg(X^n - \sigma^n(h(X))g(X)) = 0$ regardless of the characteristic of A. So, $X^n - \sigma^n(h(X))g(X) = a$ for some nonzero $a \in A$, and $ah(X) - \sigma^n(h(X))b = 0$. Since h and $\sigma^n(h)$ are monic, the leading coefficient of $ah(X) - \sigma^n(h(X))b$ is $a - \sigma^k(b)$. Thus, $a = \sigma^k(b)$ and $X^n - \sigma^k(b) = \sigma^n(h(X))g(X)$ as claimed.

Conversely, suppose that $X^n - \sigma^k(b) = \sigma^n(h(X))g(X)$. Applying the above argument for $\sigma^n(h)$ and $\sigma^k(b)$ instead of g and b, respectively, yields

$$X^n - \sigma^{n-k}\left(\sigma^k(b)\right) = \sigma^n(g(X))\sigma^n(h(X)). \quad (36)$$

So, $\sigma^n(X^n - b) = \sigma^n(g(X)h(X))$ and, thus, $X^n - b = g(X)h(X)$ as claimed.

We now drop the assumption that g is monic. Assume that $X^n - b = g(X)h(X)$ and let $G = g_{n-k}^{-1}g$. Then, $G \in A_\sigma$ is monic, and

$$G(X)h(X) = g_{n-k}^{-1}X^n - g_{n-k}^{-1}b = X^n\sigma^{-n}\left(g_{n-k}^{-1}\right) - bg_{n-k}^{-1} = \left[X^n - b\sigma^{-n}(g_{n-k})g_{n-k}^{-1}\right]\sigma^n\left(g_{n-k}^{-1}\right). \quad (37)$$

Letting $H = h\sigma^{-n}(g_{n-k}) \in A_\sigma$, we then have $G(X)H(X) = X^n - b\sigma^{-n}(g_{n-k})g_{n-k}^{-1}$. Since G is monic and $b\sigma^{-n}(g_{n-k})g_{n-k}^{-1} \in U(A)$, it follows from the argument in the first paragraph of this proof that

$$\begin{aligned} X^n - \sigma^k(b)\sigma^{k-n}(g_{n-k})\sigma^k\left(g_{n-k}^{-1}\right) &= X^n - \sigma^k\left(b\sigma^{-n}(g_{n-k})g_{n-k}^{-1}\right) \\ &= \sigma^n(H(X))G(X) \\ &= \sigma^n(h(X))g_{n-k}G(X) \\ &= \sigma^n(h(X))g(X), \end{aligned} \quad (38)$$

as claimed.

Conversely, suppose that $X^n - a = \sigma^n(h(X))g(X)$ with $a = \sigma^k(b)\sigma^{k-n}(g_{n-k})\sigma^k(g_{n-k}^{-1})$. Note that $a \in U(A)$ since σ is an automorphism of A and $g_{n-k} \in U(A)$. Let $G = g_{n-k}^{-1}g$. Then, $G \in A_\sigma$ is monic and $X^n - a = \sigma^n(h(X))g_{n-k}G(X)$. As $hg_{n-k} \in A_\sigma$ and σ^k and σ^n are automorphisms of A (and also additive automorphisms when extended to A_σ), let $c \in U(A)$ and $H \in A_\sigma$ be such that $a = \sigma^k(c)$ and $\sigma^n(h)g_{n-k} = \sigma^n(H)$. So, $X^n - \sigma^k(c) = H(X)G(X)$. It now follows from the argument in the first paragraph of this proof that $X^n - c = G(X)H(X)$; that is,

$$X^n - \sigma^{-k}(a) = G(X)h(X)\sigma^{-n}(g_{n-k}) = g_{n-k}^{-1}g(X)h(X)\sigma^{-n}(g_{n-k}). \quad (39)$$

So,

$$\begin{aligned} g_{n-k}\left[X^n - \sigma^{-k}(a)\right] &= g(X)h(X)\sigma^{-n}(g_{n-k}), \\ X^n\sigma^{-n}(g_{n-k}) - g_{n-k}\sigma^{-k}(a) &= g(X)h(X)\sigma^{-n}(g_{n-k}), \\ \left[X^n - g_{n-k}\sigma^{-k}(a)\sigma^{-n}\left(g_{n-k}^{-1}\right)\right]\sigma^{-n}(g_{n-k}) &= g(X)h(X)\sigma^{-n}(g_{n-k}), \\ X^n - g_{n-k}\sigma^{-k}(a)\sigma^{-n}\left(g_{n-k}^{-1}\right) &= g(X)h(X)\sigma^{-n}(g_{n-k})\sigma^{-n}\left(g_{n-k}^{-1}\right), \\ X^n - g_{n-k}b\sigma^{-n}(g_{n-k})g_{n-k}^{-1}\sigma^{-n}\left(g_{n-k}^{-1}\right) &= g(X)h(X). \end{aligned} \quad (40)$$

Hence, $X^n - b = g(X)h(X)$ as claimed. □

Remark 3. If we do not want to be so specific about the nature of a, b, and h as they appear above, we could rephrase Lemma 5 as follows:

A skew-polynomial $g \in A_\sigma$, whose leading coefficient is a unit in A, is a left divisor of $X^n - b \in A_\sigma$ for some $b \in U(A)$ if and only if g is a right divisor of $X^n - a \in A_\sigma$ for some $a \in U(A)$.

Example 4. Let σ be an automorphism of A, and $\alpha \in U(A)$ with $\sigma(\alpha) = \alpha$. For $g(X) = X - \alpha$ and $h(X) = X^3 + \alpha X^2 + \alpha^2 X + \alpha^3$, we have $X^4 - \alpha^4 = g(X)h(X)$ in A_σ. On the other hand,

$$\begin{aligned}\sigma^4(h(X))g(X) &= h(X)g(X)\\ &= X^4 - \sigma^3(\alpha^4)\sigma^{-1}(1)\sigma^3(1^{-1}) = X^4 - \alpha^4,\end{aligned} \tag{41}$$

as asserted by Lemma 5.

Lemma 6. *Let $h(X) = \sum_{i=0}^{k} h_i X^i \in A_\sigma$ be of degree k with $h_k, h_0 \in U(A)$. If h is a right divisor of $X^n - b$ for some $b \in U(A)$, then, h^* is a left divisor of $X^n - \sigma^{k-n}(b^{-1})$ and a right divisor of $X^n - b^{-1}\sigma^{-k}(h_0)\sigma^{n-k}(h_0^{-1})$.*

Proof. Suppose that h is a right divisor of $X^n - b$ for some $b \in U(A)$. So, $l(X)h(X) = X^n - b$ for some $l \in A_\sigma$ with $\deg(l) = n - k$ (as $h_k \in U(A)$). We then have from Lemma 4:

$$\begin{aligned}\psi(h(X))\psi(l(X)) &= X^{-n} - b,\\ X^k[\psi(h(X))\psi(l(X))]X^{n-k} &= 1 - X^k b X^{n-k},\\ h^*(X)\psi(l(X))X^{n-k} &= 1 - X^n \sigma^{k-n}(b),\\ &= \left[\sigma^{k-n}\left(b^{-1}\right) - X^n\right]\sigma^{k-n}(b),\\ h^*(X)\psi(l(X))X^{n-k}\sigma^{k-n}\left(b^{-1}\right) &= \sigma^{k-n}\left(b^{-1}\right) - X^n,\\ h^*(X)\left[-\psi(l(X))X^{n-k}\sigma^{k-n}\left(b^{-1}\right)\right] &= X^n - \sigma^{k-n}\left(b^{-1}\right).\end{aligned} \tag{42}$$

Since $\deg(l) = n - k$, $-\psi(l(X))X^{n-k}\sigma^{k-n}(b^{-1}) \in A_\sigma$. It is now obvious that h^* is a left divisor of $X^n - \sigma^{k-n}(b^{-1})$. Now, keeping in mind that $\deg(h^*) = \deg(h) = k$ and the leading coefficient of h^* is $h_0 \in U(A)$, it follows from Lemma 5 that h^* is a right divisor of $X^n - a$, where

$$a = \sigma^{n-k}\left(\sigma^{k-n}\left(b^{-1}\right)\right)\sigma^{-k}(h_0)\sigma^{n-k}\left(h_0^{-1}\right) = b^{-1}\sigma^{-k}(h_0)\sigma^{n-k}\left(h_0^{-1}\right), \tag{43}$$

as claimed. □

Example 5. Keep the notations of Example 4. By Lemma 6, $h^*(X) = \alpha^3 X^3 + \alpha^2 X^2 + \alpha X + 1$ is a left divisor of $X^4 - \sigma^{-1}(\alpha^{-4}) = X^4 - \alpha^{-4}$. In fact, we have

$$\left(\alpha^3 X^3 + \alpha^2 X^2 + \alpha X + 1\right)\left(\alpha^{-3} X + \alpha^{-4}\right) = X^4 - \alpha^{-4}. \tag{44}$$

We also deduce from Lemma 6 that h^* is a right divisor of $X^4 - \sigma^3(\alpha^3)/\alpha^4\sigma(\alpha^3) = X^4 - \alpha^{-4}$ too. In fact, $(\alpha^{-3}X + \alpha^{-4})(\alpha^3 X^3 + \alpha^2 X^2 + \alpha X + 1) = X^4 - \alpha^{-4}$.

The following is a very important and interesting fact concerning the A-module orthogonal to a free A-module over a finite commutative ring A, where orthogonality is with respect to the Euclidean inner product. This result is a rephrasing of ([20], Proposition 2.9). It should be noted that the authors of [20] assumed that the finite commutative ring is Frobenius. However, going through their proof and the results they utilized, it becomes clear that such an assumption is unnecessary. It is, however, a necessary assumption for the converse of ([20], Proposition 2.9) to hold, which we do not need here (see [20], Remark 2.10) and the few lines following it).

Lemma 7. *If A is a finite commutative ring with identity, M is a free A-submodule of A^n of rank k, and $M^\perp$ is the A-submodule of A^n orthogonal to M with respect to the Euclidean inner product on A^n, then, $M^\perp$ is free of rank $n - k$.*

Proof. Let $G \in M_{k,n}(A)$ be a matrix whose rows are the k elements of an A-basis of M. Then, G is a full-row-rank matrix (that is, the rows of G form a linearly independent set). As it is obvious that $M^\perp = \{x \in A^n | Gx^t = 0\}$, it follows from ([20], Proposition 2.9) that $M^\perp$ is free of rank $n - k$. □

In the terminology of this paper, ([3], Theorem 1) characterizes the monic principal σ-codes over a finite field $\mathbb{F}$ (with σ an automorphism of $\mathbb{F}$) whose duals are also monic principal σ-codes, extending ([2], Theorem 2). It is claimed in ([3], p. 240) that ([3], Theorem 1) remains valid over finite rings (not even assuming commutativity!) if one assumes that the constant term of g is a unit. Yet, when looking at the proof of ([3], Theorem 1), we see that a crucial underlying assumption is that the dual of a linear code over a finite field is free (as both are vector spaces) and the sum of the dimensions of the two codes is equal to their length. However, the freeness assumption on the dual does not necessarily hold over rings in general even if the original linear code is free, let alone talking about the sum of the dimensions. So, the same proof of ([3], Theorem 1) cannot be adopted for finite rings and, thus, we can not see at the moment how the aforementioned claim can be verified. To the best of the authors' knowledge, however, it was not until the appearance of ([20], Proposition 2.9) (Lemma 7) three years after the study by Boucher and Ulmer [3] that we were able to extend ([3], Theorem 1) to *finite commutative* rings (Theorem 3).

Theorem 3. *Let A be a finite commutative ring with identity, σ a ring automorphism of A, and $\mathscr{C}$ a monic principal σ-code of length n generated by some monic $g(X) = \sum_{i=0}^{n-k} g_i X^i \in A_\sigma$ with $g_0 \in U(A)$.*

(i) If the dual $\mathscr{C}^\perp$ of $\mathscr{C}$ is a monic principal σ-code generated by some $h(X) = \sum_{i=0}^{k} h_i X^i \in A_\sigma$ with $h_0, h_k \in U(A)$, then, $\mathscr{C}$ is monic principal σ-constacyclic with $\mathscr{C} = (g)_{n,\sigma}^{\sigma^k(g_0)\sigma^{2k}(h_k)}$.

(ii) If for some $a \in U(A)$, $\mathscr{C} = (g)^{a}_{n,\sigma}$ is monic principal σ-constacyclic, then, the dual $\mathscr{C}^{\perp}$ of $\mathscr{C}$ is the monic principal σ-constacyclic code $\mathscr{C}^{\perp} = (h^{*})^{c}_{n,\sigma}$, where $h(X) = \sum_{i=0}^{k} h_i X^i \in A_\sigma$ is such that $X^n - \sigma^{-k}(a) = g(X)h(X)$ with $h_0 \in U(A)$, and $c = \sigma^{-k}(a^{-1})\sigma^{-k}(h_0)\sigma^{n-k}(h_0^{-1})$.

Proof

(i) Let $\mathscr{C}^{\perp}$ be a monic principal σ-code generated by some $h(X) = \sum_{i=0}^{k} h_i X^i \in A_\sigma$ with $h_k, h_0 \in U(A)$. Since $h_0^{-1}h \in A_\sigma$ also generates $\mathscr{C}^{\perp}$, we assume that $h_0 = 1$, set $h^{\perp}(X) = \sum_{i=0}^{k} \sigma^{k-i}(h_{k-i})X^i$, and note that $h^{\perp}$ is monic. We claim that $g(X)h^{\perp}(X) = X^n - g_0\sigma^k(h_k)$. Suppose that $g(X)h^{\perp}(X) = \sum_{i=0}^{n} c_i X^i$. Notice that $c_n = 1$ and $c_0 = g_0\sigma^k(h_k)$. To settle the claim, it remains to show that $c_l = 0$ for $l \in \{1, \ldots, n-1\}$. Since $\{X^i g(X)\}_{0 \le i \le k-1}$ and $\{X^j h(X)\}_{0 \le j \le n-k-1}$ are A-generators of $\mathscr{C}$ and $\mathscr{C}^{\perp}$, respectively, it follows that

$$\langle X^{i_0} g(X), X^{i_1} h(X) \rangle = 0. \tag{45}$$

For any $i_0 \in \{0, \ldots, k-1\}$ and $i_1 \in \{0, \ldots, n-k-1\}$. So, for every such i_0 and i_1, we have

$$\begin{aligned}
0 &= \langle X^{i_0} g(X), X^{i_1} h(X) \rangle \\
&= \langle \sum_{i=0}^{n-k} \sigma^{i_0}(g_i) x^{i+i_0}, \sum_{i=0}^{k} \sigma^{i_1}(h_i) X^{i+i_1} \rangle \\
&= \langle \sum_{i=0}^{n-k} \sigma^{i_0}(g_i) x^{i+i_0}, \sum_{i=i_1-i_0}^{k+i_1-i_0} \sigma^{i_1}\left(h_{i-i_1+i_0}\right) X^{i+i_0} \rangle \\
&= \sum_{i=\max\{0,i_1-i_0\}}^{\min\{n-k,k+i_1-i_0\}} \sigma^{i_0}(g_i)\sigma^{i_1}\left(h_{i-i_1+i_0}\right) \\
&= \sigma^{i_0}\left[\sum_{i=\max\{0,i_1-i_0\}}^{\min\{n-k,k+i_1-i_0\}} g_i \sigma^{i_1-i_0}\left(h_{i-i_1+i_0}\right)\right].
\end{aligned} \tag{46}$$

Since σ^{i_0} is an automorphism of A, $\sum_{i=\max\{0,i_1-i_0\}}^{\min\{n-k,k+i_1-i_0\}} g_i \sigma^{i_1-i_0}(h_{i-i_1+i_0}) = 0$. Let $l = k + i_1 - i_0$. Then, $l \in \{1, \ldots, n-1\}$ and

$$\sigma^{i}(h_{l-i}) = \sigma^{i}\left(\sigma^{l-i-k}(h_{k-l+i})\right) = \sigma^{l-k}(h_{k-l+i}) = \sigma^{i-i_0}\left(h_{i-i_1+i_0}\right). \tag{47}$$

So,

$$\begin{aligned}
0 &= \sum_{i=\max\{0,i_1-i_0\}}^{\min\{n-k,k+i_1-i_0\}} g_i \sigma^{i_1-i_0}\left(h_{i-i_1+i_0}\right) \\
&= \sum_{i=\max\{0,l-k\}}^{\min\{n-k,l\}} g_i \sigma^{l-k}(h_{k-l+i}) \\
&= \sum_{i=\max\{0,l-k\}}^{\min\{n-k,l\}} g_i \sigma^{i}(h_{l-i}) \\
&= c_l,
\end{aligned} \tag{48}$$

as desired. It now follows from Lemma 5 that $X^n - \sigma^k(g_0)\sigma^{2k}(h_k) = \sigma^n(h^{\perp}(X))g(X)$, and hence, $\mathscr{C} = (g)^{\sigma^k(g_0)\sigma^{2k}(h_k)}_{n,\sigma}$ is σ-constacyclic.

(ii) As g is a right divisor of $X^n - a$ whose leading coefficient is a unit, it follows from Lemma 5 that there exists some $h(X) = \sum_{i=0}^{k} h_i X^i \in A_\sigma$ such that $X^n - \sigma^{-k}(a) = g(X)h(X)$. Since $g_0 h_0 = \sigma^{-k}(a)$ and A is commutative with $\sigma^{-k}(a) \in U(A)$, $h_0 \in U(A)$. It then follows from Lemma 6 that h^* is a right divisor of $X^n - c$ with $c = \sigma^{-k}(a^{-1})\sigma^{-k}(h_0)\sigma^{n-k}(h_0^{-1})$. Let $\mathscr{C}^* = (h^*)^{c}_{n,\sigma}$ be the monic principal σ-constacyclic code generated by h^*. We show that $\mathscr{C}^* = \mathscr{C}^{\perp}$. As $\mathscr{C}$ is a monic principal σ-code generated by g, which is of degree $n-k$, $\mathscr{C}$ is A-free of rank k ([8], Theorem 1). Since A is a finite commutative ring, it follows from Lemma 7 that $\mathscr{C}^{\perp}$ is A-free of rank $n-k$. On the other hand, as $\mathscr{C}^*$ is a monic principal σ-code generated by h^*, which is of degree k, $\mathscr{C}^*$ is A-free of rank $n-k$ too. So, $|\mathscr{C}^*| = |\mathscr{C}^{\perp}| < \infty$. It, thus, suffices to show that $\mathscr{C}^* \subseteq \mathscr{C}^{\perp}$. Since $\{X^i g(X)\}_{0 \le i \le k-1}$ and $\{X^j h^*(X)\}_{0 \le j \le n-k-1}$ are A-generators of $\mathscr{C}$ and $\mathscr{C}^*$, respectively, it suffices to show that $< X^i g(X), X^j h^*(X) > = 0$ for each such i and j. An argument like that in part (i) above will do. Hence, $\mathscr{C}^{\perp} = (h^*)^{c}_{n,\sigma}$. □

Remark 4. If we do not want to be so detailed in Theorem 3, we would rephrase it as follows (with some obvious additions):

Let A be a finite commutative ring with identity, σ a ring automorphism of A, and $\mathscr{C}$ a monic principal σ-code of length n generated by some monic $g(X) = \sum_{i=0}^{n-k} g_i X^i \in A_\sigma$ with $g_0 \in U(A)$. Then, the following are equivalent (assuming in each case that the constant term of the generating skew-polynomial is a unit in A):

(i) $\mathscr{C}^{\perp}$ is a monic principal σ-code.

(ii) $\mathscr{C}^{\perp}$ is a monic principal σ-constacyclic code.

(iii) $\mathscr{C}$ is a monic principal σ-constacyclic code.

Note that "$(i) \longrightarrow (iii)$" is part (i) of Theorem 3, "$(iii) \longrightarrow (ii)$" is part (ii) of Theorem 3, and "$(ii) \longrightarrow (i)$" is trivial.

Example 6. Keep the notations of Examples 4 and 5. As $(X^3+\alpha X^2+\alpha^2 X+\alpha^3)(X-\alpha) = X^4-\alpha^4$, let $\mathscr{C}$ be the monic principal σ-constacyclic code $\mathscr{C} = (X-\alpha)^{\alpha^4}_{4,\sigma}$. It then follows from Theorem 3 that $\mathscr{C}^{\perp} = (\alpha^3 X^3+\alpha^2 X^2+\alpha X+1)^{\alpha^{-4}}_{4,\sigma}$.

Remark 5. Note that in part (ii) of Theorem 3, if $a\sigma^{-k}(a) = \sigma^{-k}(h_0)\sigma^{n-k}(h_0^{-1})$, then, $\mathscr{C}^{\perp}$ is the monic principal σ-constacyclic code $\mathscr{C}^{\perp} = (h^*)^{a}_{n,\sigma}$. That is, both $\mathscr{C}$ and $\mathscr{C}^{\perp}$ are generated by right divisors of the same polynomial $X^n - a$.

If a σ-code $\mathscr{C}$ is monic principal σ-constacyclic over a finite commutative ring with identity (where σ is an automorphism of the ring), Theorem 3 asserts that the dual code $\mathscr{C}^{\perp}$ is monic principal σ-constacyclic as well. The following theorem gives a generator matrix of the dual code in such a case.

Corollary 8. *Let A be a finite commutative ring with identity, σ a ring automorphism of A, $a \in U(A)$, and $\mathscr{C} = (g)^{a}_{n,\sigma}$ a monic principal σ-constacyclic code generated by some monic $g(X) = \sum_{i=0}^{n-k} g_i X^i \in A_\sigma$ with $g_0 \in U(A)$. Let $h(X) = \sum_{i=0}^{k} h_i X^i \in A_\sigma$ be such that $g(X)h(X) = X^n - \sigma^{-k}(a)$, as ensured by Theorem 3. Then, a generator matrix $H \in M_{n-k,n}(A)$ of $\mathscr{C}^{\perp}$ is*

$$\begin{pmatrix} h_k & \sigma(h_{k-1}) & \dots & \sigma^k(h_0) & 0 & \dots & 0 \\ 0 & \sigma(h_k) & \sigma^2(h_{k-1}) & \dots & \sigma^{k+1}(h_0) & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & & & \\ 0 & \dots & \dots & 0 & \sigma^{n-k-1}(h_k) & \dots & \sigma^{n-1}(h_0) \end{pmatrix}. \tag{49}$$

Proof. By Theorem 3, the dual code $\mathscr{C}^{\perp}$ is a monic principal σ-constacyclic code generated by h^*. Now, applying Corollary 5 yields the desired conclusion. □

Example 7

(a) Keep the notations of Example 5. It follows from Corollary 8 that a generator matrix of $\mathscr{C}^{\perp}$ is $H = \begin{pmatrix} h_3 & \sigma(h_2) & \sigma^2(h_1) & \sigma^3(h_0) \end{pmatrix} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \end{pmatrix}$.

(b) Let $A = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in \mathbb{Z}_6 \right\}$ and $\sigma: \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mapsto \begin{pmatrix} a & -b \\ 0 & a \end{pmatrix}$. Let $\alpha = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in U(A)$, $g(X) = X^2 + \alpha \in A_\sigma$, and $h(X) = X^2 - \alpha \in A_\sigma$. We then get

$$h(X)g(X) = g(X)h(X) = X^4 - \alpha^2. \tag{50}$$

Letting $\mathscr{C} = (g)^{\alpha^2}_{4,\sigma}$, it follows from Theorem 3 that $\mathscr{C}^{\perp} = (h^*)^{\alpha^{-2}}_{4,\sigma}$ and from Corollary 8 that $\mathscr{C}^{\perp}$ has the following generator matrix:

$$\begin{aligned} H &= \begin{pmatrix} h_2 & \sigma(h_1) & \sigma^2(h_0) & 0 \\ 0 & \sigma(h_2) & \sigma^2(h_1) & \sigma^3(h_0) \end{pmatrix} \\ &= \begin{pmatrix} 1 & \sigma(0) & \sigma^2(-\alpha) & 0 \\ 0 & \sigma(1) & \sigma^2(0) & \sigma^3(-\alpha) \end{pmatrix} = \begin{pmatrix} 1 & 0 & -\alpha & 0 \\ 0 & 1 & 0 & -\alpha \end{pmatrix}. \end{aligned} \tag{51}$$

Due to Theorem 3, the following result gives a characterization of self-dual σ-codes over finite commutative rings in such a way that generalizes ([2], Corollary 4) and further strengthens it.

Corollary 9. *Keep the assumptions of Theorem 3 with $n = 2k$. Then, the following statements are equivalent:*

(i) $\mathscr{C}$ is a self-dual σ-code.

(ii) $\mathscr{C}$ is a monic principal σ-constacyclic code with $\mathscr{C} = (g)^{a}_{n,\sigma}$, $a \in U(A)$, and $\sigma^k(h_0^{-1})h^* = g$, where $g(X)h(X) = X^n - \sigma^{-k}(a)$.

(iii) For any $l \in \{0, \dots, k\}$, $\sum_{i=0}^{l} \sigma^{k-l}(g_i) g_{i+k-l} = 0$.

Proof. (i)⇔(ii): assume that $\mathscr{C} = \mathscr{C}^{\perp}$. It follows from Theorem 3 and its proof that $\mathscr{C}^{\perp}$ is σ-constacyclic generated by $h^* \in A_\sigma$, where $h(X) = \sum_{i=0}^{k} h_i X^i$ is satisfying $h_0 \in U(A)$ and $g(X)h(X) = X^n - \sigma^{-k}(a)$ for some $a \in U(A)$. As $\sigma^k(h_0^{-1})h^*$ also generates $\mathscr{C}^{\perp}$ and both g and $\sigma^k(h_0^{-1})h^*$ are monic and generate the same code, we must have $g = \sigma^k(h_0^{-1})h^*$. Conversely, assume that $\mathscr{C} = (g)^{a}_{n,\sigma}$, for some $a \in U(A)$, and $\sigma^k(h_0^{-1})h^* = g$ where $g(X)h(X) = X^n - \sigma^{-k}(a)$. Then, by Theorem 3, $\mathscr{C}^{\perp}$ is monic principal and generated by h^*. Since h^* and $\sigma^k(h_0^{-1})h^* = g$ generate the same code, we conclude that $\mathscr{C} = \mathscr{C}^{\perp}$.

(i)⇔(iii): follow the proof of Corollary 4 of [2] verbatim with the use of Theorem 3 and the obvious adjustments. □

Example 8. Let $A = \mathbb{F}_3 \times \mathbb{F}_3$, $\sigma(x, y) = (y, x)$, and denote $(a, a) \in A$ by a. Taking $h(X) = X^2 + 2X + 2 \in A_\sigma$, we get $h^*(X) = 2X^2 + 2X + 1$ and $\sigma^2(h_0^{-1})h^*(X) = 2(2X^2 + 2X + 1) = X^2 + X + 2$. Letting $g(X) = X^2 + X + 2$, a simple verification shows that $g(X)h(X) = X^4 + 1$. We then deduce from Corollary 9 (ii) that $\mathscr{C} = (X^2 + X + 2)_{4,\sigma}^{-1}$ is a self-dual σ-constacyclic code over A, which is negacyclic over A of length 4. Using Magma [18], this yields, after the obvious Gray map, a negacyclic $[8, 4, 3]$ ternary code over A with the generator matrix in systematic form $\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 0 & 2 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 0 & 2 & 0 & 2 \end{pmatrix}$. So, we get a new construction of the unique self-dual code with these parameters [21], which is classically obtained as a direct sum of two copies of the tetracode [22], (Table XII).

Example 9. Consider $\mathbb{F}_4 = \mathbb{F}_2(w)$ with $w^2 + w + 1 = 0$. Let $A = \mathbb{F}_4 \times \mathbb{F}_4$, $\sigma(x, y) = (x, y^2)$, and $f(X) = X^6 + 1 \in A_\sigma$ where 1 denotes $(1, 1)$. Letting

$$\begin{aligned}
g_1(X) &= h_1(X) = X^3 + 1,\\
g_2(X) &= 1 + \left(0, w^2\right)x + \left(0, w^2\right)x^2 + x^3,\\
h_2(X) &= 1 + \left(0, w^2\right)x + (0, w)x^2 + x^3,\\
g_3(X) &= 1 + (0, w)x + (0, w)x^2 + x^3,\\
h_3(X) &= 1 + (0, w)x + \left(0, w^2\right)x^2 + x^3,
\end{aligned} \tag{52}$$

we see that $f = g_i h_i$ for every $i = 1, 2, 3$. So, by Corollary 9, the three codes $\mathscr{C}_1 = (g_1)_{6,\sigma}^{-1}$, $\mathscr{C}_2 = (g_2)_{6,\sigma}^{-1}$, and $\mathscr{C}_3 = (g_3)_{6,\sigma}^{-1}$ are self-dual σ-constacyclic codes over A. Generator matrices of $\mathscr{C}_1$, $\mathscr{C}_2$, and $\mathscr{C}_3$ are, respectively, as follows:

$$\begin{aligned}
G_1 &= \begin{pmatrix} (1,1) & (0,0) & (0,0) & (1,1) & (0,0) & (0,0) \\ (0,0) & (1,1) & (0,0) & (0,0) & (1,1) & (0,0) \\ (0,0) & (0,0) & (1,1) & (0,0) & (0,0) & (1,1) \end{pmatrix},\\
G_2 &= \begin{pmatrix} (1,1) & \left(0,w^2\right) & \left(0,w^2\right) & (1,1) & (0,0) & (0,0) \\ (0,0) & (1,1) & (0,w) & (0,w) & (1,1) & (0,0) \\ (0,0) & (0,0) & (1,1) & \left(0,w^2\right) & \left(0,w^2\right) & (1,1) \end{pmatrix},\\
G_3 &= \begin{pmatrix} (1,1) & (0,w) & (0,w) & (1,1) & (0,0) & (0,0) \\ (0,0) & (1,1) & \left(0,w^2\right) & \left(0,w^2\right) & (1,1) & (0,0) \\ (0,0) & (0,0) & (1,1) & (0,w) & (0,w) & (1,1) \end{pmatrix}.
\end{aligned} \tag{53}$$

Moreover, using the obvious Gray map to $\mathbb{F}_4$, we get from $\mathscr{C}_2$ a self-dual $[12, 6, 2]$ code over $\mathbb{F}_4$. For this, Magma [18] was used.

6. Parity-Check Matrix of a Monic Principal (f, σ, δ)-Code over a Finite Commutative Ring

Let A be a ring, σ a ring endomorphism of A that maps the identity to itself, and δ a σ-derivation of A. If $\mathscr{C}$ is an A-free (f, σ, δ)-code of length n and rank k, a matrix $H_* \in M_{n-k,n}(A)$ is called a *parity-check matrix* of $\mathscr{C}$ if

(1) H_*^T is a control matrix of $\mathscr{C}$, and

(2) H_* is a generator matrix of the dual $\mathscr{C}^\perp$.

In classical coding theory over finite fields, the dual code of a linear code is also linear, and hence, a parity-check matrix of such a code always exists. However, for a monic principal (f, σ, δ)-code $\mathscr{C}$ over a ring A (despite being A-free), the dual $\mathscr{C}^\perp$ may not be A-free, and thus, a parity-check matrix of $\mathscr{C}$ may not exist (due to the lack of requirement (2) above). Nonetheless, when A is a finite commutative ring with identity and σ is a ring automorphism of A, nice things happen. With this assumption added to the hypotheses of Theorem 2, Theorem 4 shows that the transpose of the matrix consisting of the last $n - k$ columns of H of Theorem 2 is indeed a parity-check matrix of $\mathscr{C}$. This is a dramatic improvement of Theorem 2 in this important and widely used case.

Theorem 4. *Let A be a finite commutative ring with identity, σ a ring automorphism of A, and keep the other notations and assumptions of Theorem 2. Then, a parity-check matrix $H_* \in M_{n-k,n}(A)$ of $\mathscr{C}$ is given by*

$$\begin{pmatrix}
h_k & h_k^{(1)} & h_k^{(2)} & \dots & h_k^{(n-k-1)} & h_k^{(n-k)} & \dots & h_k^{(n-1)} \\
0 & \sigma(h_k) & h_{k+1}^{(2)} & \dots & h_{k+1}^{(n-k-1)} & h_{k+1}^{(n-k)} & \dots & h_{k+1}^{(n-1)} \\
0 & 0 & \sigma^2(h_k) & \dots & h_{k+2}^{(n-k-1)} & h_{k+2}^{(n-k)} & \dots & h_{k+2}^{(n-1)} \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \dots & \sigma^{n-k-1}(h_k) & h_{n-1}^{(n-k)} & \dots & h_{n-1}^{(n-1)}
\end{pmatrix}, \tag{54}$$

where $h_j^{(i)}$ is as in Theorem 2.

Proof. Note that H_* is the transpose of the last $n - k$ columns of H of Theorem 2. The rows $H_1, \dots, H_{n-k}$ of H_* are A-linearly independent since H_* is in echelon form. Let $\mathscr{C}_*$ be the free left A-submodule of A^n a basis of which is $H_1, \dots, H_{n-k}$. Then, $\mathscr{C}_*$ has cardinality equal to $|A|^{n-k}$. On the other hand, it follows from Lemma 7 that $\mathscr{C}^\perp$ is A-free of rank $n - k$. So, $\mathscr{C}^\perp$ has cardinality equal to $|A|^{n-k}$ as well. With H of Theorem 2, we have $\mathscr{C} = \mathrm{Ann}_l(H) \subseteq \mathrm{Ann}_l(H_*^T)$. By Lemma 7 again, $\mathrm{Ann}_l(H_*^T)$ is A-free of rank k. Then, $|\mathrm{Ann}_l(H_*^T)| = |A|^k = |\mathscr{C}|$ and so $\mathscr{C} = \mathrm{Ann}_l(H_*^T)$. Thus, H_*^T is a control matrix of $\mathscr{C}$. This, in particular, implies that $H_1, \dots, H_{n-k} \in \mathscr{C}^\perp$. So, $\mathscr{C}^* \subseteq \mathscr{C}^\perp$. Since $\mathscr{C}^*$ and $\mathscr{C}^\perp$ are of the same finite cardinality, $\mathscr{C}^* = \mathscr{C}^\perp$. So, H_* is a generator matrix of $\mathscr{C}^\perp$ and thus a parity-check matrix of $\mathscr{C}$. □

Example 10. Keep the notation and assumptions of Example 3 with A finite and commutative and σ a ring automorphism of A. By Theorem 4, the matrix $H_* = \begin{pmatrix} 1 & \beta & 1 \end{pmatrix}$ is a parity-check matrix of $\mathscr{C}$. By Theorem 1, a generator matrix of $\mathscr{C}$ is $G = \begin{pmatrix} 2\beta & 1 & 0 \\ 2\alpha & 2\beta & 1 \end{pmatrix}$. It can be easily checked that $GH_*^T = 0$.

When $\delta = 0$, H_* takes a nicer form.

Corollary 10. *Keep the assumptions of Theorem 4 with $\delta = 0$. Then, a parity-check matrix $H_* \in M_{n-k,n}(A)$ of the monic principal σ-code $\mathscr{C}$ is given by*

$$\begin{pmatrix} h_k & \sigma(h_{k-1}) & \sigma^2(h_{k-2}) & \dots & \sigma^k(h_0) & h_k^{(k+1)} & h_k^{(k+2)} & \dots & h_k^{(n-1)} \\ 0 & \sigma(h_k) & \sigma^2(h_{k-1}) & \dots & \sigma^k(h_1) & \sigma^{k+1}(h_0) & h_{k+1}^{(k+2)} & \dots & h_{k+1}^{(n-1)} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \dots & \sigma^{n-k-1}(h_k) & \dots & \dots & \sigma^{n-1}(h_0) \end{pmatrix}, \tag{55}$$

where $h_j^{(i)}$ is as in Theorem 2.

Proof. Follows immediately from Theorem 4 and Corollary 6.

A special, yet important, case of Corollary 10 is when $\mathscr{C}$ is a monic principal σ-constacyclic code, in which case H_* takes a much better form. □

Corollary 11. *Keep the assumptions of Theorem 4 with $\mathscr{C}$ a monic principal σ-constacyclic code, $\mathscr{C} = (g)_{n,\sigma}^a$ for some $a \in U(A)$. Then, a parity-check matrix $H_* \in M_{n-k,n}(A)$ of $\mathscr{C}$ is given by*

$$\begin{pmatrix} h_k & \sigma(h_{k-1}) & \sigma^2(h_{k-2}) & \dots & \sigma^k(h_0) & 0 & 0 & \dots & 0 \\ 0 & \sigma(h_k) & \sigma^2(h_{k-1}) & \dots & \sigma^k(h_1) & \sigma^{k+1}(h_0) & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \dots & \sigma^{n-k-1}(h_k) & \dots & \dots & \sigma^{n-1}(h_0) \end{pmatrix}. \tag{56}$$

Proof. For $j = 1, \dots, n$, let C_j denote the jth column of H in Corollary 7. If $n - k = 1$, then, $H_* = (C_{k+1}^T)$, where (by Corollary 7 (a))

$$C_{k+1}^T = C_n^T = \left(h_k, \sigma(h_{k-1}), \sigma^2(h_{k-2}), \dots, \sigma^k(h_0)\right). \tag{57}$$

Suppose now that $n - k \geq 2$. Then, the rows of H_* are precisely $C_{k+1}^T, C_{k+2}^T, \dots, C_n^T$. We begin by specifying the entries of C_{k+1}, where we show that

$$C_{k+1}^T = \left(H_{i,k+1}\right)_{1\leq i\leq n}^T = \left(h_k, \sigma(h_{k-1}), \sigma^2(h_{k-2}), \dots, \sigma^k(h_0), 0, \dots, 0\right), \tag{58}$$

that is, $H_{i,k+1} = \sigma^{i-1}(h_{k-(i-1)})$ for $1 \leq i \leq k+1$, and $H_{i,k+1} = 0$ for $k+2 \leq i \leq n$. By Corollary 7 (b)-(i), $H_{1,k+1} = h_k$. Let $2 \leq i \leq n$. We deal with the following three cases:

Case ($j = k+1 = n-k$): for $2 \leq i \leq n-k = k+1$, we have $2 \leq i \leq k+1 = j \leq i+k$, so we are in the second case of Corollary 7 (b)-(ii). Thus, $H_{i,k+1} = \sigma^{i-1}(h_{k-(i-1)})$ here. For $n-k+1 \leq i \leq n$, we have $j = k+1 = n-k \leq i-1 \leq n-1$ and $i - (n-k) + 1 \leq k+1 = j$. So $i - (n-k) + 1 \leq j \leq i-1$, and we are in the second case of Corollary 7 (b)-(iii). Thus, $H_{i,k+1} = 0$ here. This fully verifies the asserted entries of C_{k+1} when $j = k+1 = n-k$.

Case ($j = k+1 > n-k$): for $2 \leq i \leq n-k$, we have $i \leq n-k < j = k+1$ and $i + k \geq 2 + k > j$. So, $i \leq j \leq i+k$, and we are in the second case of Corollary 7 (b)-(ii). Thus, $H_{i,k+1} = \sigma^{i-1}(h_{j-1}) = \sigma^{i-1}(h_{k-(i-1)})$ here. Let $n-k+1 \leq i \leq n$. If $i \leq j \leq n$, then, we are in third case of Corollary 7 (b)-(iii). Thus, $H_{i,k+1} = \sigma^{i-1}(h_{j-1}) = \sigma^{i-1}(h_{k-(i-1)})$ here as well. If $n-k+1 \leq j \leq i-1$, then, $i - (n-k) + 1 \leq n - (n-k) + 1 = k+1 = j$. So $i - (n-k) + 1 \leq j \leq i-1$, and we are in the second case of Corollary 7 (b)-(iii). Thus, $H_{i,k+1} = 0$ here. This fully verifies the asserted entries of C_{k+1} when $j = k+1 > n-k$.

Case ($j = k+1 < n-k$): let $2 \leq i \leq n-k$. If $i \leq k+1 = j < n-k$, then, $i + k \leq n-k+k = n$. So, we have $i \leq j \leq i+k$, and we are in the second case of Corollary 7 (b)-(ii). Thus, $H_{i,k+1} = \sigma^{i-1}(h_{k+1-i}) = \sigma^{i-1}(h_{k-(i-1)})$ here. If $j = k+1 < i \leq n-k$, then $1 \leq j \leq i-1$, and we are in the first case of Corollary 7 (b)-(ii). Thus, $H_{i,k+1} = 0$ here. For $n-k+1 \leq i \leq n$, we have $j = k+1 < n-k < n-k+1 \leq i$. So, $j \leq i-1$. Also, $i - (n-k) + 1 \leq n - (n-k) + 1 = k+1 = j$. So, we have $i - (n-k) + 1 \leq j \leq i-1$, and we are in the second case of Corollary 7 (b)-(iii). Thus, $H_{i,k+1} = 0$ here as well. This fully verifies the asserted entries of C_{k+1} when $j = k+1 < n-k$.

Now, as for C_{k+1+t} with $t = 1, \ldots, n-k-1$, note that (by Corollary 7) $H_{i,k+1+t} = 0$ for $1 \le i \le t$. For $t+1 \le i \le k+1+t$, Corollary 4 (a) yields $H_{i,k+1+t} = \sigma^{i-1}(h_{k+1+t-i})$. For $k+1+t+1 \le i \le n$, Corollary 4 (a) again yields $H_{i,k+1+t} = 0$. This completes the proof.

Note that a requirement in the above corollary is that g be both a right and left divisor of $X^n - a$ (according to Theorem 4). The following corollary deals with the case when g is a right divisor of $X^n - a$ and a left divisor of $X^n - \sigma^{-k}(a)$ and $g_0 \in U(A)$ (see the assumptions of Corollary 8). □

Corollary 12. *Keep the assumptions of Corollary 8. Then, a parity-check matrix $H_* \in M_{n-k,n}(A)$ of $\mathscr{C}$ is given by*

$$\begin{pmatrix} h_k & \sigma(h_{k-1}) & \sigma^2(h_{k-2}) & \ldots & \sigma^k(h_0) & 0 & 0 & \ldots & 0 \\ 0 & \sigma(h_k) & \sigma^2(h_{k-1}) & \ldots & \sigma^k(h_1) & \sigma^{k+1}(h_0) & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & \ldots & \sigma^{n-k-1}(h_k) & \ldots & \ldots & \sigma^{n-1}(h_0) \end{pmatrix}. \tag{59}$$

Proof. By Corollary 8, H_* is a generator matrix of $\mathscr{C}^\perp$. Furthermore, it is clear that $z \in \mathrm{Ann}_l(H_*^T)$ if and only if $z \in \{x \in A^n | \langle x, y\rangle = 0 \text{ for all } y \in \mathscr{C}^\perp\} = (\mathscr{C}^\perp)^\perp$. Since $(\mathscr{C}^\perp)^\perp$ and $\mathscr{C}$ are both free of the same rank (thanks to Lemma 7) and $\mathscr{C} \subseteq (\mathscr{C}^\perp)^\perp$, we conclude that $\mathscr{C} = \mathrm{Ann}_l(H_*^T)$. Hence, H_* is a parity-check matrix of $\mathscr{C}$ as claimed. □

7. Conclusion and Future Work

7.1. Conclusion. In this article, recursive formulas were provided to compute the entries of generator and control matrices of a monic principal (f, σ, δ)-code $\mathscr{C}$ over a ring A. When A is finite and commutative with an automorphism σ and the generator polynomial of $\mathscr{C}$ is both a right and a left divisor of f, a parity-check matrix of $\mathscr{C}$ was also given. When further $\delta = 0$, a characterization was given for such codes whose dual codes were also monic principal. Particularly, self-dual codes of this kind as well as monic principal skew-constacyclic were discussed.

7.2. Future Work. Some of the issues that can be worked on are the following:

(i) Despite the importance of the generator matrices, control matrices, and parity-check matrices in identifying certain monic principal skew codes over rings, improvements on other coding-theoretic parameters are still to be discussed.

(ii) What can be said about monic principal dual codes of monic principal skew codes in case $\delta \ne 0$, and what can be said about the non-monic-principal dual codes of monic principal skew codes in both cases $\delta = 0$ and $\delta \ne 0$?

(iii) In case $\delta \ne 0$, what can be said about self-dual monic principal (σ, δ)-codes and constacyclic (σ, δ)-codes in terms of their characterizations or properties?

Data Availability

All the needed data are included in the manuscript.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors would like to thank Patrick Solé and Felix Ulmer for some useful conversations and suggestions.

References

[1] D. Boucher, W. Geiselmann, and F. Ulmer, "Skew-cyclic codes," *Applicable Algebra in Engineering, Communication and Computing*, vol. 18, no. 4, pp. 379–389, 2007.

[2] D. Boucher and F. Ulmer, "Codes as modules over skew polynomial rings," in *Proceedings of the Cryptography and Coding*, M. G. Parker, Ed., pp. 38–55pp. 38–, Cirencester, UK, December 2009.

[3] D. Boucher and F. Ulmer, "A note on the dual codes of module skew codes," *Lecture Notes in Computer Science*, vol. 7089, pp. 230–243, 2011.

[4] D. Boucher and F. Ulmer, "Linear codes using skewp polynomials with automorphisms and derivations," *Designs, Codes and Cryptography*, vol. 70, pp. 405–431, 2014.

[5] D. Boucher and F. Ulmer, "Coding with skew polynomial rings," *Journal of Symbolic Computation*, vol. 44, pp. 1644–1656, 2009.

[6] D. Boucher, P. Solé, and P. Solé, "Skew constacyclic codes over Galois rings," *Advances in Mathematics of Communications*, vol. 2, pp. 273–292, 2008.

[7] H. Dinh, B. Nguyen, and S. Sriboonchitta, "Skew constacyclic codes over finite fields and finite chain rings," *Mathematical Problems in Engineering*, vol. 2016, Article ID 3965789, 17 pages, 2016.

[8] M. Boulagouaz and A. Leroy, "σ, δ-codes," *Advances in Mathematics of Communications*, vol. 7, pp. 463–474, 2013.

[9] S. Bedir, F. Gursoy, and I. Siap, "On generalizations of skew quasi-cyclic codes," *Bull. Korean Math. Soc.*vol. 57, pp. 459–479, 2020.

[10] M. Ezerman, S. Ling, P. Solé, and O. Yemen, "From skew-cyclic codes to asymmetric quantum codes," *Advances in Mathematics of Communications*, vol. 5, pp. 41–57, 2011.

[11] P. Solé and O. Yemen, "Binary quasi-cyclic codes of index 2 and skew polynomial rings," *Finite Fields Appls*, vol. 18, pp. 685–699, 2012.

[12] S. Dougherty, *Algebraic Coding Theory over Finite Commutative Rings*Springer, Berlin, Germany, 2017.

[13] M. Shi, A. Alahmadi, and P. Solé, *Codes and Rings, Theory and Practice*, Academic Press, Massachusetts, MA, USA, 2017.

[14] M. Boulagouaz and A. Deajim, "Characterizations and properties of principal f, σ, δ-codes over rings," 2021, https://arxiv.org/abs/1809.10409.

[15] M. Boulagouaz and A. Deajim, "Matrix-product codes over commutative rings and constructions arising from σ, δ-codes," *Journal of Mathematics*, vol. 2021, Article ID 5521067, 10 pages, 2021.

[16] T. Lam, "Lectures on modules and rings," *Grad. Texts in Math*, Springer-Verlag, Berlin, Germany, 1st edition, 1999.

[17] J. H. van Lint, "Introduction to Coding Theory," *Grad. Texts in Math*, Springer-Verlag, Berlin, Germany, 3rd edition, 1999.

[18] Magma, "Magma computational algebra system," 2021, https://magma.maths.usyd.edu.au/magma/.

[19] M. Grassl, "Tables of parameters of linear codes," 2019, https://www.codetables.de.

[20] Y. Fan, S. Ling, and H. Liu, "Matrix product codes over finite commutative Frobenius rings," *Designs, Codes and Cryptography*, vol. 71, pp. 201–227, 2014.

[21] P. Gaborit, "Tables of self-dual codes," 1998, https://www.unilim.fr/pages_perso/philippe.gaborit/SD/.

[22] E. M. Rains and N. J. A. Sloane, "Self-dual codes," in *Handbook of Coding Theory*, W. C. Hufman and V. Pless, Eds., vol. I, North-Holland, 1998.