On Cyclic Convolutional Codes

Heide Gluesing-Luerssen* and Wiland Schmale*

February 9, 2004

Abstract

We investigate the notion of cyclicity for convolutional codes as it has been introduced in the papers [19, 22]. Codes of this type are described as submodules of $\mathbb{F}[z]^n$ with some additional generalized cyclic structure but also as specific left ideals in a skew polynomial ring. Extending a result of [19], we show in a purely algebraic setting that these ideals are always principal. This leads to the notion of a generator polynomial just like for cyclic block codes. Similarly a parity check polynomial can be introduced by considering the right annihilator ideal. An algorithmic procedure is developed which produces unique reduced generator and parity check polynomials. We also show how basic code properties and a minimal generator matrix can be read off from these objects. A close link between polynomial and vector description of the codes is provided by certain generalized circulant matrices.

Keywords: Algebraic convolutional coding theory, cyclic codes, skew polynomial ring

MSC (2000): 94B10, 94B15, 16S36

1 Introduction

Convolutional codes (CC's) and block codes are the most widely used types of codes in engineering practice, a fact which leads to a continuing need for a thorough mathematical basis for the design of useful codes. In consequence, coding theory has become one of the various young branches of mathematics which are attractive because of the active interplay between sophisticated engineering inventions and high level mathematics. This is particularly true for the theory of cyclic block codes.

The algebraic theory of CC's was initiated mainly by the articles of Forney [4] and Massey et al. [16, 17], and, as can be seen from the books [12, 20] and the article [18], a lot of material has been accumulated since. In the last decade Rosenthal and co-workers began a successful project, dedicated to a better and deeper mathematical understanding of CC's

*Department of Mathematics, University of Oldenburg, 26 111 Oldenburg, Germany, email: gluesing@mathematik.uni-oldenburg.de, wiland.schmale@uni-oldenburg.de

by exploiting more systematically the existing links to control theory, see [24, 26, 23]. Yet, up to now the mathematical theory of CC's is not nearly as developed as that of block codes. This gap is even larger when it comes to the notion of cyclicity. Despite the well-known and frequently exploited efficiency of cyclic block codes, almost nothing is known about cyclic structures for convolutional codes and their possible impact on applications.

In 1976 Piret showed in his fundamental paper [19] how cyclicity has to be understood for CC's and laid the basis for a mathematical theory of cyclic CC's. The first important discovery of Piret was that classical cyclicity — as common for block codes — is trivial for CC's (see Proposition 2.7 in the next section). He also showed that a more sophisticated "graded cyclicity" leads to interesting examples of good convolutional codes, some of which can be found in [19, Sect. IV] and in [9]. His second main discovery was that irreducible graded cyclic CC's can algebraically be described by one-sided principal ideals in a noncommutative algebra $A[z;\sigma]$. This algebra will be introduced in the next section. For the moment we only mention that $A[z;\sigma]$ is equal to $A[z]$ as a left $\mathbb{F}[z]$-module where $A \cong \mathbb{F}[x]/(x^n-1)$, $\mathbb{F}$ is a finite field and n is the length of the code. Only the multiplication in the algebra $A[z;\sigma]$ is quite different from the ordinary one. It depends on an $\mathbb{F}$-automorphism σ of A and is typically non-commutative.

The results of Piret indicate a surprising analogy to the theory of block codes where cyclic codes are described as principal ideals, see [15, 1], with the only difference that the latter are in the commutative ring A.

Shortly after Piret, a thorough analysis of his results was undertaken by Roos [22] in a module theoretic framework, avoiding thereby cumbersome matrix manipulations. At the same time Roos considerably extended Piret's notion to what will be called σ-cyclicity later on in this paper. But apart from this, no substantially new results could be added and Piret's idea of a generating polynomial [19, Thm.3.10] could not be incorporated. Furthermore, Roos' results are partly non-constructive.

After the work of Piret and Roos no substantial effort has been made towards a concise mathematical description of cyclic CC's — as far as we know. This may partly be due to the limited mathematical readership of the journals in question and to the circumstance that Piret's article is quite cumbersome to read.

Yet, we think that this topic is worth being investigated in more detail. We realized that Piret's results may serve as a good basis for a theory of σ-cyclic CC's, which we would like to re-initiate with this paper. Although we do not consider distance properties of cyclic CC's, we will present the exact free distance of all codes constructed in the examples. Moreover, in the paper [8] plenty of cyclic CC's are presented, all of which have optimal distance with respect to their parameters. This way we hope to indicate that the big class of σ-cyclic CC's contains quite some good codes and, therefore, deserves to be investigated further.

We proceed with an outline of the paper. In Section 2 we will trace the steps which lead to the definition of σ-cyclicity for CC's. We think it is worthwhile recalling also the original idea of Piret before going into the more general setting initiated by Roos. We will construct the (generalized) Piret algebra $A[z;\sigma]$ and develop the representation of σ-cyclic

CC's as left ideals in $A[z;\sigma]$. As the Piret algebra is based on an automorphism σ of A, we have to collect some information about the group of automorphisms of A and about how the structure of the Piret algebra depends on σ. This will be done in Section 3. In Section 4 we give an algebraic and extended version of Piret's main result which states that σ-cyclic CC's are left principal ideals in $A[z;\sigma]$. Thereafter we investigate as to what extent a generator of a left ideal in $A[z;\sigma]$ is unique and in Section 5 we show how this unique generator can be computed by means of a finite algorithmic procedure. The basic algebraic tool for these sections is a decomposition of the Piret algebra by idempotents of A and a reduction procedure based on a monomial order of the skew polynomials. In Section 6 we introduce a new type of non-commuting σ-circulant matrices along with a thorough investigation of their properties. These matrices are just the proper medium for the interplay between left ideals together with their principal generators on the one side and CC's as submodules of $\mathbb{F}[z]^n$ along with their generating matrices on the other. They also turn out to be a canonical, yet nontrivial, generalization of classical circulants as they are common in the theory of cyclic block codes. This becomes in particularly clear when we derive our results on generator and parity check polynomials and dual codes in Section 7. Indeed, we arrive at a scenario very similar to that of cyclic block codes. The notion of a parity check polynomial is also included in this framework, it is obtained via (right) annihilator ideals in the Piret algebra. Beyond this algebraic structure, convolutional coding requires to also discuss some other properties and invariants of the codes, as there are non-catastrophicity, minimal generator matrices and the complexity (overall constraint length) of the given code. All these issues can nicely be dealt with in our algebraic context. As it turns out, the reduced principal generator polynomials for left ideals in $A[z;\sigma]$, as constructed in Section 4 and 5, also suits well when it comes to the properties of the associate circulant matrix. The latter leads in a canonical way to a basic minimal generator matrix of the given code, and, consequently, the complexity can be computed in terms of the generator polynomial. In order to derive these results one has to combine the techniques for circulant matrices with the algebraic methods from Section 3– 5. In the final Section 8 we give a short outline of several future research topics.

2 What is a cyclic convolutional code?

In this section we will shortly recall the basic definitions and properties of convolutional codes and cyclic block codes and then develop — along the lines of the articles [19, 22] — the notion of a cyclic convolutional code.

Throughout this paper, $\mathbb{F}$ denotes a fixed finite field and n a positive integer such that

$$\text{the characteristic of } \mathbb{F} \text{ does not divide } n. \tag{2.1}$$

The number n is going to be the length of the code and (2.1) is the familiar assumption from the theory of cyclic block codes guaranteeing that the polynomial $x^n - 1$ factors into different prime polynomials over $\mathbb{F}$.

As is well-known, a block code is simply a subspace of the vector space $\mathbb{F}^n$. Analogously, convolutional codes are direct summands of $\mathbb{F}[z]^n$. Of course, only additional properties single out the codes which are relevant for applications. Before presenting the according notions, we first collect some basic facts about submodules and direct summands of $\mathbb{F}[z]^n$.

As usual in coding theory, all vectors are regarded as row vectors, thus

$$\mathbb{F}[z]^n := \{(v_1, \ldots, v_n) \mid v_i \in \mathbb{F}[z] \text{ for } i = 1, \ldots, n\}.$$

Consequently, images and kernels of matrices will always denote *left* images and *left* kernels. The following facts will be used freely.

Proposition 2.1
Let V be a submodule of $\mathbb{F}[z]^n$.

(a) V has a finite basis and all bases of V have the same length, called the rank of V.

(b) If $v_1, \ldots, v_r \in \mathbb{F}[z]^n$ form a generating set of V, then $V = \operatorname{im} M := \{uM \mid u \in \mathbb{F}[z]^r\}$ where

$$M := \begin{bmatrix} v_1 \\ \vdots \\ v_r \end{bmatrix} \in \mathbb{F}[z]^{r \times n}. \tag{2.2}$$

We call M a generating matrix of V.

(c) Let $P \in \mathbb{F}[z]^{r \times r}$ and M as in (b). Then $V = \operatorname{im}(PM) \Longleftrightarrow P$ is invertible over $\mathbb{F}[z]$.

The following properties about direct summands are easily obtained from linear algebra over the Euclidean domain $\mathbb{F}[z]$.

Proposition 2.2
Let $V \subseteq \mathbb{F}[z]^n$ be a submodule and $v_1, \ldots, v_r \in \mathbb{F}[z]^n$ a generating set of V. Put $M \in \mathbb{F}[z]^{r \times n}$ as in (2.2). Then the following are equivalent.

(1) V is a direct summand of $\mathbb{F}[z]^n$.

(2) Any basis of V can be completed to a basis of $\mathbb{F}[z]^n$.

(3) The Smith-form of M is given by $\left(\begin{smallmatrix} I_k & 0 \\ 0 & 0 \end{smallmatrix}\right)$, where k is the rank of V.

(4) If $v_1, \ldots, v_r$ is a basis of V (equivalently, if r is the rank of V), then M is right invertible over $\mathbb{F}[z]$.

(5) For all $v \in \mathbb{F}[z]^n$ and all $\lambda \in \mathbb{F}[z] \backslash \{0\}$ one has

$$\lambda v \in V \Longrightarrow v \in V. \tag{2.3}$$

(6) There exists some matrix $N \in \mathbb{F}[z]^{n \times l}$ such that $V = \ker N := \{v \in \mathbb{F}[z]^n \mid vN = 0\}$.

(7) For all submodules $W \in \mathbb{F}[z]^n$ having the same rank as V one has

$$V \subseteq W \Longrightarrow V = W.$$

A matrix M with property (3) will be called basic.

For the definition of Smith-forms see e. g. [6, p. 141] or [11, Sec. 3.7].

A convolutional code is simply defined to be a direct summand of $\mathbb{F}[z]^n$. But of course only various additional notions lead to useful coding theoretical concepts.

Definition 2.3

(1) *A convolutional code (CC) of length n and dimension k is a direct summand $\mathcal{C}$ of $\mathbb{F}[z]^n$ of rank k.*

(2) *Any generating matrix $G \in \mathbb{F}[z]^{k\times n}$ having rank k of $\mathcal{C}$ is called a generator matrix or encoder of $\mathcal{C}$. Hence*

$$\mathcal{C} = \operatorname{im} G = \{uG \mid u \in \mathbb{F}[z]^k\}$$

and the vector $uG \in \mathbb{F}[z]^n$ is said to be the codeword associated with the message word $u \in \mathbb{F}[z]^k$.

(3) *A matrix $H \in \mathbb{F}[z]^{n\times(n-k)}$ satisfying $\mathcal{C} = \ker H = \{v \in \mathbb{F}^n \mid vH = 0\}$ is said to be a parity check matrix of the code $\mathcal{C}$.*

(4) *The maximal degree of the k-minors of an encoder G is called the (encoding) complexity of the code. A code of complexity zero is said to be a block code.*

We need to make some comments. So far no uniform notation has been established in the literature for what we call *complexity*. Often different phrases are used, for instance *overall constraint length* [4, p. 721], [12, p. 55] (and many others papers), *constraint length* [13, p. 1616], *degree* [18, Def. 3.5], or *code degree* [10, p. 663]. The last two would easily lead to confusion in the course of our paper where different types of degree will naturally occur. Piret [20, Def. 2.7] defines *complexity* in a way equivalent to our definition and, e. g., to the one in [24, p. 1885]. It seems that the phrase complexity (or encoding complexity) best expresses the hardware meaning of this number. It reflects the complexness of the encoding process in the sense of the minimal number of memory elements needed. As for the other notions in the definition above, notice that each code has a generator and a parity check matrix. The parity check matrix always has rank $n-k$. We would like to point out the difference between a generator matrix and a generating matrix in the sense of Proposition 2.1: the latter one need not have full rank and therefore is not suitable as an encoder. However, we will need this notion, since certain square (singular) generating matrices naturally arise in our investigations of cyclic convolutional codes. Of course, one can always constructively obtain a (full rank) generator matrix out of these matrices by computing for instance the Hermite normal form. But in our specific context a better way to a generator matrix will be shown in Section 7.

Remark 2.4

(1) In Definition 2.3 we adopt the viewpoint that codewords and message words are finite sequences rather than infinite ones, the latter being slightly more common in convolutional coding theory; see [24] for a discussion of this subtle difference. The codewords and messages are therefore represented by polynomials rather than by Laurent series from $\mathbb{F}(\!(z)\!)$. But in any case, even if Laurent series are admitted, the encoders are always polynomial matrices exactly as in Definition 2.3, see, e. g., [4, 18]. Moreover, there is a one-one correspondence between CC's in the sense of Definition 2.3 and CC's as subspaces of $\mathbb{F}(\!(z)\!)^n$ with a polynomial generator matrix.

(2) It is well-known that the complexity does not depend on the choice of the encoder. Furthermore, from the theory of minimal bases (see [5]) it follows that a code has complexity zero if and only if it has a constant encoder. Thus, in this case the code behaves just like a block code.

Some of our investigations will hold under weaker assumptions, which are closely related to the following concepts of coding theory.

Definition 2.5
Let V be a submodule of $\mathbb{F}[z]^n$. Then

(a) V is called non-catastrophic if (2.3) *is satisfied for all $v \in \mathbb{F}[z]^n$ and all $\lambda \in \mathbb{F}[z]\backslash z\mathbb{F}[z]$.*

(b) V is called delay-free if (2.3) *is satisfied for all $v \in \mathbb{F}[z]^n$ and $\lambda = z$.*

A non-catastrophic and delay-free submodule is, by definition, a convolutional code, see Proposition 2.2(5).

A first indication for the quality of a code is given by its free distance defined as follows, for details see also [12, Ch. 3].

Definition 2.6

(a) The weight of the word $v = \sum_{\nu=0}^{N} v_\nu z^\nu \in \mathbb{F}[z]^n$ is defined as $\mathrm{wt}(v) := \sum_{\nu=0}^{N} \mathrm{wt}(v_\nu) \in \mathbb{N}_0$, where $\mathrm{wt}(v_\nu)$ denotes the Hamming weight of the constant vector $v_\nu \in \mathbb{F}^n$.

(b) The free distance of a code $\mathcal{C} \subseteq \mathbb{F}[z]^n$ is defined as $d_{\text{free}}(\mathcal{C}) := \min\{\mathrm{wt}(v) \mid v \in \mathcal{C}\backslash\{0\}\}$.

In our examples we will often state explicitly the free distance of the code under investigation. Although we do not investigate the free distance of a cyclic convolutional code in this paper, we think it worthwhile computing the distance in order to have a more complete picture of the codes in question. Most of these computations have been done with the help of MAPLE.

Now we turn to the notion of cyclicity. A block code $\mathcal{C} \subseteq \mathbb{F}^n$ is said to be cyclic if it is invariant under the cyclic shift, that is, if

$$(v_0, \ldots, v_{n-1}) \in \mathcal{C} \Longrightarrow (v_{n-1}, v_0, \ldots, v_{n-2}) \in \mathcal{C} \tag{2.4}$$

or, equivalently, if

$$\mathcal{C}S \subseteq \mathcal{C} \tag{2.5}$$

where

$$S = \begin{bmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ 1 & 0 & \cdots & 0 \end{bmatrix} \in \mathbb{F}^{n\times n}. \tag{2.6}$$

An important tool in the theory of cyclic block codes is the so-called polynomial representation. It is based on the $\mathbb{F}$-isomorphism

$$\mathfrak{p} : \mathbb{F}^n \longrightarrow A, \quad v = (v_0, \ldots, v_{n-1}) \longmapsto \mathfrak{p}(v) = \sum_{i=0}^{n-1} v_i x^i,$$

where $A := \mathbb{F}[x]/_{\langle x^n - 1\rangle}$ is displayed in the canonical way

$$A = \{f \in \mathbb{F}[x] \mid \deg f < n\} \text{ with multiplication modulo } x^n - 1.$$

The inverse of $\mathfrak{p}$ will be denoted by $\mathfrak{v}$. The map $\mathfrak{p}$ translates the cyclic shift into multiplication by x. As a consequence, a cyclic block code $\mathcal{C}$ can now be represented as an ideal $\mathfrak{p}(\mathcal{C})$ in A and vice versa; in other words,

$$\text{a block code } \mathcal{C} \text{ is cyclic if and only if } \big[\, a \in \mathfrak{p}(\mathcal{C}) \Longrightarrow\ xa \in \mathfrak{p}(\mathcal{C})\,\big]. \tag{2.7}$$

For later use we immediately extend $\mathfrak{p}$ to all of $\mathbb{F}[z]^n$ via

$$\mathfrak{p} : \mathbb{F}[z]^n \longrightarrow A[z], \quad \sum_{\nu\geq 0} z^\nu v_\nu \longmapsto \sum_{\nu\geq 0} z^\nu \mathfrak{p}(v_\nu). \tag{2.8}$$

The map $\mathfrak{p}$ is an isomorphism of left $\mathbb{F}[z]$-modules with inverse $\mathfrak{v} := \mathfrak{p}^{-1}$.

It would be quite natural to define cyclicity of convolutional codes just like for block codes, that is, by requiring invariance as in (2.4). But already in [19, Thm. 3.12] and [22, Thm.6] the following important observation has been made.

Proposition 2.7
Let $\mathcal{C} \subseteq \mathbb{F}[z]^n$ be a code satisfying (2.4) *for all* $(v_0, \ldots, v_{n-1}) \in \mathbb{F}[z]^n$. *Then $\mathcal{C}$ is a block code.*

This result will appear as a special case in Proposition 3.4. However, we include an independent and elementary linear algebraic proof at the end of this section.

The negative result of Proposition 2.7 has led Piret [19] to a more general and complex notion of cyclicity for convolutional codes. Instead of shift-invariance of $\mathcal{C}$ under the shift-matrix S from (2.6), which would require $\sum_{\nu=0}^{d} z^\nu v_\nu S \in \mathcal{C}$, whenever $\sum_{\nu=0}^{d} z^\nu v_\nu \in \mathcal{C}$, Piret introduced a kind of graded quasi-cyclicity. Precisely, he called a convolutional code $\mathcal{C}$ cyclic, if there exists some m, which is coprime to the length n of the code, such that

$$\sum z^\nu v_\nu \in \mathcal{C} \Longrightarrow \sum z^\nu v_\nu S^{(m^\nu)} \in \mathcal{C}. \tag{2.9}$$

In polynomial language, i. e. in the polynomial ring $A[z]$, this translates into

$$\sum z^\nu \mathfrak{p}(v_\nu) \in \mathfrak{p}(\mathcal{C}) \Longrightarrow \sum z^\nu x^{(m^\nu)} \mathfrak{p}(v_\nu) \in \mathfrak{p}(\mathcal{C}). \tag{2.10}$$

The coprimeness of the integers m and n guarantees not only that the minimal polynomial of S^m is the same as that of S, that is $x^n - 1$, but also that the map $x \longmapsto x^m$ induces an $\mathbb{F}$-automorphism of A. This allows to introduce an $\mathbb{F}$-algebra structure on the left $\mathbb{F}[z]$-module $A[z]$ which naturally extends the algebra A. The details of the construction will be explained below.

Piret's notion of cyclicity has been generalized by Roos [22] in a natural way to arbitrary $\mathbb{F}$-automorphisms σ of A. We propose the name *σ-cyclicity*, since later on different automorphisms will have to be considered simultaneously. In the following definition we introduce this notion for arbitrary submodules of $\mathbb{F}[z]^n$.

Definition 2.8
Let $\mathrm{Aut}_{\mathbb{F}}(A)$ denote the group of all $\mathbb{F}$-algebra automorphisms on A and let $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$. A submodule $\mathcal{C}$ of $\mathbb{F}[z]^n$ is called σ-cyclic if

$$g = \sum_{\nu=0}^{d} z^\nu g_\nu \in \mathfrak{p}(\mathcal{C}) \implies x *_\sigma g := \sum_{\nu=0}^{d} z^\nu \sigma^\nu(x) g_\nu \in \mathfrak{p}(\mathcal{C}). \tag{2.11}$$

Consequently, a σ-cyclic convolutional code (σ-CCC) is a σ-cyclic direct summand of $\mathbb{F}[z]^n$.

In [22], Equation (2.11) was extended to a left $\mathbb{F}[z]$-module structure on $A[z]$, which then was used to investigate in great detail the structure of σ-CCC's. Unfortunately, generator polynomials as constructed by Piret could not be incorporated in this setting. It seems to be more helpful to use $*_\sigma$ for a non-commutative ring structure on $A[z]$ as follows.

Definition 2.9
Let $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$. We define the product of $g = \sum_{\nu \geq 0} z^\nu g_\nu$ and $h = \sum_{\mu \geq 0} z^\mu h_\mu \in A[z]$ by

$$\Big(\sum_{\nu \geq 0} z^\nu g_\nu\Big) *_\sigma \Big(\sum_{\mu \geq 0} z^\mu h_\mu\Big) := \sum_{\lambda \geq 0} z^\lambda \sum_{\nu+\mu=\lambda} \sigma^\mu(g_\nu) h_\mu.$$

$A[z]$ equipped with the multiplication $*_\sigma$ will be denoted by $A[z;\sigma]$ and often be abbreviated by $\mathcal{R}$. We call $A[z;\sigma]$ a Piret algebra (with parameters $q = |\mathbb{F}|$, n, σ).

Observe that multiplication in $A[z;\sigma]$ is simply an extension of the (commutative) multiplication in A together with the rule

$$a *_\sigma z = z *_\sigma \sigma(a) \text{ for all } a \in A. \tag{2.12}$$

In particular we have

$$\lambda *_\sigma z = z *_\sigma \lambda \text{ for all } \lambda \in \mathbb{F}$$

and therefore we obtain the usual product whenever the left factor is in $\mathbb{F}[z]$; precisely,

$$\Big(\sum_{\nu \geq 0} z^\nu g_\nu\Big) *_\sigma \Big(\sum_{\mu \geq 0} z^\mu h_\mu\Big) = \sum_{\lambda \geq 0} z^\lambda \sum_{\nu+\mu=\lambda} g_\nu h_\mu \text{ for all } \sum_{\nu \geq 0} z^\nu g_\nu \in \mathbb{F}[z] \text{ and } \sum_{\mu \geq 0} z^\mu h_\mu \in A[z].$$

Notice that we put the z-coefficients always to the right of z. This is, of course, a matter of choice, but the explicit form of the non-commutative product $*_\sigma$ highly depends on it. Using the multiplication rule (2.12) the coefficients can always be shifted to the left of z if a suitable power of σ^{-1} is applied. One should always bear in mind that a monomial $z^\nu a$, $a \in A$, can also be read as $z^\nu *_\sigma a$.

The notation $A[z;\sigma]$ is common in the theory of skew polynomial rings over integral domains, see for instance [2, p. 438]. In our setting $A[z;\sigma]$ typically has many zero divisors and — as we will see later — many nonconstant units.

The discussion above leads directly to a nice skew polynomial representation for σ-cyclic submodules.

Observation 2.10

(a) *$A[z;\sigma]$ is an $\mathbb{F}$-algebra which, at the same time, carries a canonical left $\mathbb{F}[z]$-module structure. The algebra $A[z;\sigma]$ is non-commutative whenever the automorphism σ is not the identity on A.*

(b) *A submodule $\mathcal{C}$ of $\mathbb{F}[z]^n$ is σ-cyclic if and only if its polynomial version $\mathfrak{p}(\mathcal{C})$ is a left ideal in $A[z;\sigma]$.*

(c) *It is worthwhile noting that $A[z;\sigma]$ also carries a canonical right $\mathbb{F}[z]$-structure. This is even more obvious than the left $\mathbb{F}[z]$-module structure since in the multiplication $*_\sigma$ the automorphism σ acts only on the left factor.*

Example 2.11

Let $\mathbb{F} = \mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ and $n = 3$.

(1) We choose the automorphism σ given by $\sigma(x) = \alpha^2 x$ (it will be explained in Example 2.13 below that this indeed induces an automorphism on A). We wish to find the smallest σ-CCC $\mathcal{C}$ containing the codeword

$$v := (1 + z + z^2,\ \alpha + z + \alpha^2 z^2,\ \alpha^2 + z + \alpha z^2) \in \mathbb{F}[z]^3.$$

First of all, $\mathfrak{p}(\mathcal{C})$ has to contain the left ideal in $A[z;\sigma]$ generated by the polynomial

$$g := \mathfrak{p}(v) = 1 + \alpha x + \alpha^2 x^2 + z(1 + x + x^2) + z^2(1 + \alpha^2 x + \alpha x^2).$$

One calculates

$$x *_\sigma g = \alpha^2 + x + \alpha x^2 + z\alpha^2(1 + x + x^2) + z^2(\alpha^2 + \alpha x + x^2) = \alpha^2 g$$

and thus $x^2 *_\sigma g = \alpha g$. Furthermore, one easily checks that the matrix

$$G := \begin{bmatrix} 1 + z + z^2, & \alpha + z + \alpha^2 z^2, & \alpha^2 + z + \alpha z^2 \end{bmatrix}$$

is basic and therefore $\mathcal{C} = \operatorname{im} G$ is the smallest σ-CCC containing the word v above. This code happens to be quite a good one, since one can show that $d_{\text{free}}(\mathcal{C}) = 9$, which is the maximum value for the free distance of any one-dimensional code of length 3 and complexity 2, see [25, Thm. 2.2]. Hence $\mathcal{C}$ is an MDS-code in the sense of [25, Def. 2.5].

(2) Let us also consider the situation in (1) with the automorphism $\sigma = \mathrm{id}$. In this case multiplication by x simply corresponds to the usual cyclic shift and therefore the smallest σ-CCC $\mathcal{C}'$ containing v has to satisfy

$$\mathcal{C}' \supseteq \operatorname{im} G', \text{ where } G' := \begin{bmatrix} 1 + z + z^2 & \alpha + z + \alpha^2 z^2 & \alpha^2 + z + \alpha z^2 \\ \alpha^2 + z + \alpha z^2 & 1 + z + z^2 & \alpha + z + \alpha^2 z^2 \\ \alpha + z + \alpha^2 z^2 & \alpha^2 + z + \alpha z^2 & 1 + z + z^2 \end{bmatrix}.$$

Since $\det G' \neq 0$, the code $\mathcal{C}'$ is 3-dimensional and, by Proposition 2.2(7), it follows

$$\mathcal{C}' = \operatorname{im} I_3 = \mathbb{F}[z]^3.$$

Hence $\mathcal{C}'$ is a (trivial) block code and we encounter an example of the result in Proposition 2.7.

(3) In the paper [21] Piret gave a class of unit memory convolutional codes based on Reed-Solomon block codes. One can show that these codes are all σ-cyclic with respect to the automorphism given by $\sigma(x) = x^{n-1}$.

(4) Finally, we would like to mention the class of convolutional codes constructed in the paper [27]. Just like the codes in [21] they are based on cyclic block codes and, therefore, have a generator matrix with a type of row-wise cyclic shift structure. Yet, they are in general *not* σ-cyclic with respect to any automorphism σ. $\square$

As has been explained above, Definition 2.9 and Observation 2.10 basically go back to [19], with the only difference that in [19] only monomial automorphisms are considered, i. e. automorphisms σ, where $\sigma(x) = x^m$ for some $m \in \mathbb{N}$. It is easy to see that the set $\{m \mid 1 \leq m \leq n-1, \gcd(m,n) = 1\}$ leads to all monomial automorphisms. Note also that for every n, the choice $m = n-1$ produces the automorphism given by $\sigma(x) = x^{-1}$.

Remark 2.12
Definition 2.8 extends cyclicity of block codes in the sense of (2.7). One can also express σ-cyclicity solely in terms of vector polynomials, i. e., without resorting to the identifications $\mathfrak{p}$ and $\mathfrak{v}$. This yields a generalization of cyclic block codes in the sense of (2.4). Since this is more easily understood after some appropriate objects have been defined, we will postpone this description to Observation 7.1. At this point one should simply note that for $\sigma = \mathrm{id}$ one has

$$\mathfrak{v}\big(x *_\sigma \mathfrak{p}(v)\big) = vS \quad \text{for} \ \ v \in \mathbb{F}[z]^n$$

(the usual cyclic shift) and in this case the map $v \mapsto \mathfrak{v}\big(x *_\sigma \mathfrak{p}(v)\big)$ on $\mathbb{F}[z]^n$ is $\mathbb{F}[z]$-linear. For $\sigma \neq \mathrm{id}$ this is no longer true, due to non-commutativity of $A[z;\sigma]$.

Example 2.13
The above raises the question as to how the group $\mathrm{Aut}_{\mathbb{F}}(A)$ looks like. A very simple, but tedious way of finding all automorphisms is as follows. First of all, notice that any $\mathbb{F}$-algebra automorphism σ is fully determined by the value of $\sigma(x)$ in A. Secondly, since $x^n = 1$ and $1, x, \ldots, x^{n-1}$ are linearly independent over $\mathbb{F}$, the same has to be true for $a := \sigma(x) \in A$. Furthermore, it is easy to see that each element $a \in A$ such that $1, a, \ldots, a^{n-1}$ are linearly independent and $a^n = 1$ uniquely determines an automorphism $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$ via $\sigma(x) = a$. Of course, $a = x$ corresponds to $\sigma = \mathrm{id}$. Applying this for instance to the case $\mathbb{F} = \mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ and $n = 3$ leads to six automorphisms given by

$$a \in \{x, x^2, \alpha x, \alpha^2 x, \alpha x^2, \alpha^2 x^2\}.$$

In the next section a more sophisticated and detailed investigation of the group $\mathrm{Aut}_{\mathbb{F}}(A)$ will be presented.
For an example of the non-commutativity of $A[z;\sigma]$ take e. g. the isomorphism σ given by $\sigma(x) = \alpha x$. Then $x^2 *_\sigma z = z *_\sigma \sigma(x^2) = z *_\sigma \alpha^2 x^2$. $\square$

In the rest of this paper we will omit the symbol $*_\sigma$ in the skew multiplication of Definition 2.9. Precisely,

$$gh := g *_\sigma h \text{ for all } g,\, h \in A[z;\sigma]. \tag{2.13}$$

This won't cause any confusion since the Piret algebra under investigation will always be clear from the context.

Since we will often switch between σ-cyclic submodules of $\mathbb{F}[z]^n$ and their counterpart as left ideals in the Piret algebra, the following will be very convenient. Notice that we make use of the notation in (2.13).

Observation 2.14
Let $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$. A left ideal $\mathcal{J}$ of $A[z;\sigma]$ is called non-catastrophic (resp. delay-free) if $\mathfrak{v}(\mathcal{J})$ is a non-catastrophic (resp. delay-free) submodule of $\mathbb{F}[z]^n$. Since $\mathfrak{p}$ and $\mathfrak{v}$ are $\mathbb{F}[z]$-linear mappings, this is equivalent to
$\mathcal{J}$ *is non-catastrophic* $\Longleftrightarrow \big[\,\forall\, g \in A[z;\sigma]\ \forall\, \lambda \in \mathbb{F}[z] \setminus z\mathbb{F}[z] :\ \lambda g \in \mathcal{J} \Longrightarrow g \in \mathcal{J}\,\big]$,
$\mathcal{J}$ *is delay-free* $\Longleftrightarrow \big[\,\forall\, g \in A[z;\sigma]\ \forall\, k \geq 1 :\ z^k g \in \mathcal{J} \Longrightarrow g \in \mathcal{J}\,\big]$,
$\mathcal{J}$ *is a direct summand of* $A[z;\sigma] \Longleftrightarrow \big[\,\forall g \in A[z;\sigma]\ \forall\, \lambda \in \mathbb{F}[z]\backslash\{0\} :\ \lambda g \in \mathcal{J} \Longrightarrow g \in \mathcal{J}\,\big]$,
where a direct summand is understood in the context of left $\mathbb{F}[z]$-modules. Recall that $\mathcal{J}$ is a direct summand if and only if $\mathfrak{v}(\mathcal{J})$ is a convolutional code.
We will also need the corresponding notions for right ideals, in which case, of course, λg and $z^k g$ have to be replaced by $g\lambda$ and gz^k, respectively. In this case, one has to recall from Observation 2.10 that $A[z;\sigma]$ is also a right $\mathbb{F}[z]$-module.

We conclude this section with a direct proof of Proposition 2.7.

PROOF: By assumption $\mathcal{C}S \subseteq \mathcal{C}$, where S is as in (2.6). The minimal polynomial of S is given by $x^n - 1$. Let $x^n - 1 = \pi_1 \cdots \pi_r$ be the factorization into prime polynomials, which are, due to (2.1), pairwise different. Then we obtain the decomposition

$$\mathbb{F}[z]^n = \ker \pi_1(S) \oplus \cdots \oplus \ker \pi_r(S)$$

of $\mathbb{F}[z]^n$ into $\mathbb{F}[z]$-submodules which are minimal S-invariant direct summands. Since $\mathcal{C}$ itself is a direct summand, too, we similarly obtain

$$\mathcal{C} = \bigoplus_{i \in T} \ker \pi_i(S), \text{ where } T = \{i \mid \ker \pi_i(S) \cap \mathcal{C} \neq \{0\}\}.$$

Since $\mathbb{F}^n S = \mathbb{F}^n$, the $\mathbb{F}[z]$-submodules $\ker \pi_i(S)$ are generated by $\ker \pi_i(S) \cap \mathbb{F}^n$ and this leads directly to a constant generating matrix and thus to a constant encoder for $\mathcal{C}$. By Definition 2.3(4) the complexity is zero, i. e. $\mathcal{C}$ is a block code . □

3 Basic information on $\mathbb{F}$-automorphisms of $A[z;\sigma]$

As is clear from the last section, in order to get access to all σ-cyclic convolutional codes, it is necessary to have precise information on the group $\mathrm{Aut}_{\mathbb{F}}(A)$. In particular, it will be advantageous to describe the action on the components of $A = \mathbb{F}[x]/\langle x^n - 1\rangle$ when represented as a cartesian product of fields. We now give this information as far as absolutely necessary and for reasons of space only partially with proofs.

Under the assumption (2.1) we know that the normalized factors $\pi_i \in \mathbb{F}[x]$ of the prime factor decomposition

$$x^n - 1 = \pi_1 \cdot \ldots \cdot \pi_r \tag{3.1}$$

are pairwise different. We order the prime polynomials such that

$$\deg \pi_1 = \cdots = \deg \pi_{r_1} < \cdots\cdots < \deg \pi_{r_1+\cdots+r_{s-1}+1} = \cdots = \deg \pi_{r_1+\cdots+r_s}$$

where $r_1 + \cdots + r_s = r$.

The most natural and constructive way to represent and decompose the $\mathbb{F}$-algebra A is as follows. Let

$$A := \{f \in \mathbb{F}[x] \mid \deg f < n\} \text{ with multiplication modulo } x^n - 1 \tag{3.2}$$

and for $1 \leq k \leq r$ let

$$K_k := \{f \in \mathbb{F}[x] \mid \deg f < \deg \pi_k\} \text{ with multiplication modulo } \pi_k. \tag{3.3}$$

Then $K_k \cong \mathbb{F}[x]/\langle \pi_k \rangle$ is a finite Galois extension of $\mathbb{F}$ of dimension $[K_k : \mathbb{F}] = \deg \pi_k$. Denote by $\varrho_k(a) \in K_k$ the remainder of $a \in \mathbb{F}[x]$ when dividing by π_k. By means of the Chinese remainder theorem the map

$$\varrho : A \longrightarrow K_1 \times \cdots \times K_r, \quad a \longmapsto [\varrho_1(a), \cdots, \varrho_r(a)] \tag{3.4}$$

is an isomorphism of rings, where the cartesian product is endowed with component-wise addition and multiplication. The isomorphism ϱ can be computed easily and it induces an isomorphism of the respective automorphism groups. Therefore, in this section we assume from now on that

$$A = K_1 \times \ldots \times K_r. \tag{3.5}$$

The basic properties of the ring A which we will use in the following reflect the fact that A is a semi-simple ring. The canonical $\mathbb{F}$-basis vectors

$$\varepsilon^{(k)} = [\delta_{k,j}]_{1 \leq j \leq r} = [0, \ldots, 0, 1, 0, \ldots, 0], \text{ where the 1 is at the } k\text{-th position,} \tag{3.6}$$

are at the same time the uniquely determined primitive and pairwise orthogonal idempotents of A. Recall that an idempotent is called *primitive* if it cannot be written as a nontrivial sum of orthogonal idempotents. We call

$$K^{(k)} := \varepsilon^{(k)} A = 0 \times \cdots \times K_k \times \cdots \times 0 \tag{3.7}$$

the k-th component of A. Each component of A is a field, since of course $K^{(k)} \cong K_k$. In particular one has for all a, $b \in A$ the rule

$$a\varepsilon^{(k)} b = 0 \Longrightarrow a\varepsilon^{(k)} = 0 \text{ or } \varepsilon^{(k)} b = 0. \tag{3.8}$$

Any ideal of A is readily seen to be of the type

$$\sum_{k=1}^{r} U_k \text{ where } U_k \in \{\{0\}, K^{(k)}\} \text{ for } 1 \leq k \leq r.$$

Two components $K^{(k)}$ and $K^{(l)}$ are isomorphic if and only if $\deg \pi_k = \deg \pi_l$. Therefore up to a further, usually non-unique, automorphism we can even assume from now on that

$$A = \underbrace{L_1 \times \cdots \times L_1}_{r_1} \times \cdots\cdots \times \underbrace{L_s \times \cdots \times L_s}_{r_s} = L_1^{r_1} \times \cdots \times L_s^{r_s} \tag{3.9}$$

where the field L_j is isomorphic to $K_{\sum_{k=1}^{j-1} r_k+1} \cong \cdots \cong K_{\sum_{k=1}^{j} r_k}$ and, as a consequence, $L_1, \ldots, L_s$ are pairwise non-isomorphic. In particular $\sum_{k=1}^{s} r_k = r$.

Let us now consider the $\mathbb{F}$-automorphisms of A. One first observes that for an automorphism $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$ necessarily $\sigma(K^{(k)}) = K^{(l)}$ for some l. Thus σ acts as a permutation on the set $\mathcal{K} = \{K^{(1)}, \ldots, K^{(r)}\}$ of components of A and $\mathcal{K}$ is the disjoint union of cycles determined by σ. All fields in one cycle must have the same degree over $\mathbb{F}$ and therefore are isomorphic. Therefore σ can only permute those components of A which correspond to one of the fields L_j for a fixed j in the decomposition (3.9). On the other hand, any such type of permutation together with automorphisms of the components induces an $\mathbb{F}$-automorphism of A and it can be shown that there are no further automorphisms. This is the main information of the following fundamental theorem.

Theorem 3.1
For $1 \le j \le s$ let $G_j := \mathrm{Aut}_{\mathbb{F}}(L_j)$. Let furthermore $S_{r_1,\ldots,r_s}$ be the subgroup of the group S_r of permutations of $\{1, \ldots, r\}$, which leaves all sets

$$\{1, \ldots, r_1\}\ , \ldots\ ,\ \{\textstyle\sum_{k=1}^{s-1} r_k + 1, \ldots, \underbrace{\textstyle\sum_{k=1}^{s} r_k}_{=r}\}$$

invariant. Then

$$\mathrm{Aut}_{\mathbb{F}}(A) \cong (G_1^{r_1} \times \cdots \times G_s^{r_s}) \circ (S_{r_1,\ldots,r_s}), \tag{3.10}$$

where $\circ$ is defined as

$$\big((\gamma_1, \ldots, \gamma_r) \circ \beta\big)[a_1, \ldots, a_r] = \big[\gamma_1(a_{\beta(1)}), \ldots,\ \gamma_r(a_{\beta(r)})\big]$$

for all $[a_1, \ldots, a_r] \in L_1^{r_1} \times \cdots \times L_s^{r_s}$.

Note that the group on the right hand side of (3.10) is the automorphism group of A in the representation (3.9). Of course, one has to incorporate the various isomorphisms in order to obtain the automorphism group of A in the description of (3.5) or (3.2). We will describe this translation in detail via an example below. The representation in (3.10) is an instance of the wreath product. In [28] one can find in a more general situation a result (without proof) from which Theorem 3.1 could be deduced. For our purposes a direct proof of the Theorem is preferable and not very difficult in the concrete context as developed before Theorem 3.1. However, we skip the proof for the sake of brevity. As an immediate consequence we obtain a formula for the number of automorphisms on A.

Corollary 3.2
Let the data be as in (3.1) and (3.9). Define $l_1 := 1$ and $l_i := r_1 + \ldots + r_{i-1} + 1$ for $i = 2, \ldots, s$. Then $|\mathrm{Aut}_{\mathbb{F}}(A)| = (\deg \pi_{l_1})^{r_1} \cdots (\deg \pi_{l_s})^{r_s} r_1! \cdots r_s!$.

The advantage of Theorem 3.1 is that it provides us with a very systematic and well-organized list of the automorphisms on A in the representation (3.9). However, for the investigations of cyclic codes in Section 6 and thereafter, we will need the $\mathbb{F}$-automorphisms for the ring A as given in (3.2), i. e. for $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$ we will need to know the value $\sigma(x) \in A$, which completely determines σ. In order to find this representation of σ one has to incorporate an isomorphism leading from (3.2) to (3.9). This is illustrated in Example 3.3(b) below.

Example 3.3

(a) Let $\mathbb{F} = \mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ and $n = 3$. Then we compute $x^n - 1 = \pi_1\pi_2\pi_3$ where $\pi_1 = x+1$, $\pi_2 = x+\alpha$ and $\pi_3 = x+\alpha^2$. In this case $s = 1$, $r_1 = 3$, and $L_1 = \mathbb{F}$. Thus Corollary 3.2 gives us $r_1! = 6$ automorphisms, which are also given in Example 2.13. They all arise from pure permutations of the components.

(b) Let $\mathbb{F} = \mathbb{F}_4$ as before and $n = 5$. In this case

$$x^5 - 1 = (x+1)(x^2 + \alpha x + 1)(x^2 + \alpha^2 x + 1)$$

and we find $s = 2$, $r_1 = 1$, $r_2 = 2$, $L_1 = \mathbb{F}$, $L_2 \cong \mathbb{F}_{16}$. Furthermore

$$K_1 = \mathbb{F}[x]/\langle x+1\rangle, \quad K_2 = \mathbb{F}[x]/\langle x^2+\alpha x+1\rangle, \quad K_3 = \mathbb{F}[x]/\langle x^2+\alpha^2 x+1\rangle. \tag{3.11}$$

Corollary 3.2 now says, that there are $1^1 2^2 1!\,2! = 8$ automorphisms. Once given the only nontrivial $\mathbb{F}$-automorphism λ of L_2 they can be listed systematically according to Theorem 3.1. We want to present these automorphisms with respect to the various descriptions of A as in (3.2), (3.5), and (3.9). In order to do so we first notice that λ is given by the Frobenius homomorphism, i. e. $\lambda(a) = a^4$ for all $a \in L_2$. Secondly, we need an $\mathbb{F}$-isomorphism between the two fields K_2 and K_3. The list given below is based on the isomorphism

$$\Psi : \mathbb{F}[x]/\langle x^2+\alpha x+1\rangle \longrightarrow \mathbb{F}[x]/\langle x^2+\alpha^2 x+1\rangle, \quad \text{where } \Psi(x) = \alpha^2 x + 1, \tag{3.12}$$

with inverse given by $\Psi^{-1}(x) = \alpha x + \alpha$. Going through all the necessary isomorphisms one obtains the descriptions for the automorphisms on A as given in the table below. In the first column of the list we use the standard notation $\big(\rho(1), \rho(2), \rho(3)\big)$ for a permutation $\rho \in S_3$. In the second (resp. third) column the image of $[1, x, x]$ (resp. x) under the corresponding automorphism is given. Recall that this fully determines the $\mathbb{F}$-automorphism. For instance, the second column of the seventh row is obtained as follows (in suggestive notation)

$$\begin{aligned}\big((\mathrm{id}, \lambda, \mathrm{id}) \circ (1,3,2)\big)[1,\ x,\ x] &= (\mathrm{id}, \lambda, \mathrm{id})[1,\ \Psi^{-1}(x),\ \Psi(x)]\\ &= (\mathrm{id}, \lambda, \mathrm{id})[1,\ \alpha x + \alpha,\ \alpha^2 x + 1]\\ &= [1,\ (\alpha x+\alpha)^4 \bmod (x^2+\alpha x+1),\ \alpha^2 x + 1].\end{aligned}$$

Hence this automorphism maps $[a, b, c]$ onto $[a, \Psi^{-1}(c)^4, \Psi(b)]$. The relation between the third and second column is given by the Chinese Remainder Theorem, see (3.4).

$\mathbb{F} \times \mathbb{F}_{16}^2$	$\mathbb{F}[x]/_{\langle x+1\rangle} \times \mathbb{F}[x]/_{\langle x^2+\alpha x+1\rangle} \times \mathbb{F}[x]/_{\langle x^2+\alpha^2 x+1\rangle}$	$\mathbb{F}[x]/_{\langle x^5-1\rangle}$
$(\mathrm{id}, \mathrm{id}, \mathrm{id}) \circ (1,2,3)$	$[1, x, x]$	x
$(\mathrm{id}, \mathrm{id}, \lambda) \circ (1,2,3)$	$[1, x, x^4] = [1, x, x+\alpha^2]$	$\alpha x^4 + x^3 + x^2 + \alpha^2 x$
$(\mathrm{id}, \lambda, \mathrm{id}) \circ (1,2,3)$	$[1, x^4, x] = [1, x+\alpha, x]$	$\alpha^2 x^4 + x^3 + x^2 + \alpha x$
$(\mathrm{id}, \lambda, \lambda) \circ (1,2,3)$	$[1, x+\alpha, x+\alpha^2]$	x^4
$(\mathrm{id}, \mathrm{id}, \mathrm{id}) \circ (1,3,2)$	$[1, \alpha x+\alpha, \alpha^2 x+1]$	$x^4 + \alpha x^3 + \alpha^2 x^2 + x$
$(\mathrm{id}, \mathrm{id}, \lambda) \circ (1,3,2)$	$[1, \alpha x+\alpha, (\alpha^2 x+1)^4] = [1, \alpha x+\alpha, \alpha^2 x+\alpha^2]$	x^3
$(\mathrm{id}, \lambda, \mathrm{id}) \circ (1,3,2)$	$[1, (\alpha x+\alpha)^4, \alpha^2 x+1] = [1, \alpha x+1, \alpha^2 x+1]$	x^2
$(\mathrm{id}, \lambda, \lambda) \circ (1,3,2)$	$[1, \alpha x+1, \alpha^2 x+\alpha^2]$	$x^4 + \alpha^2 x^3 + \alpha x^2 + x$

In the examples of the next two sections about the left ideals in $A[z;\sigma]$, we will mainly use a representation as displayed in the second column above. Only thereafter, when dealing with cyclic codes, we will need computations mod $(x^n - 1)$ as in the third column.

In the foregoing example (b) the first four automorphisms do not permute the components of A. In such a case there exist no non-trivial σ-CCC's as we will see in part (a) of the following result, which also can be regarded as an extension of Proposition 2.7. The if-part of this statement can also be found at [22, Thm. 8], a special case also occurs in [19, Thm. 3.12]. Part (b) below is also in [22, Thm. 6].

Proposition 3.4

(a) Let $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$ and $K^{(k)}$ be as in (3.7). Then every σ-CCC is a block code iff $\sigma(K^{(k)}) = K^{(k)}$ for all $1 \le k \le r$.

(b) Let $\mathcal{C}$ be σ-CCC, $\mathcal{J} = \mathfrak{p}(\mathcal{C})$ be the corresponding ideal in $\mathcal{R}$ and $\mathcal{J}_0 := \{c \in A \mid \exists\, g \in \mathcal{J} : g_0 = c\}$, where g_0 denotes the z-free term of g. If $\sigma(\mathcal{J}_0) = \mathcal{J}_0$, then $\mathcal{C}$ is a block code.

It is possible to give a direct proof of the result at this point. Since we don't need the proposition, it is most efficient to postpone the proof to the end of Section 7.

The proposition demonstrates that an essential ingredient of a nontrivial σ-CCC is the way of how σ properly permutes the components of A. This in turn determines to a large extent the structure of the algebra $\mathcal{R} = A[z;\sigma]$. To give an idea of this we mention without proofs the following facts (which won't be used in the paper):

(1) Let $\bigcup_{j=1}^{s} Z_j$ be a partition of $\mathcal{K} := \{K^{(1)}, \ldots, K^{(r)}\}$ which is invariant under σ, i. e. $\sigma(Z_j) = Z_j$ for all $1 \le j \le s$. Then $\mathcal{R}$ is a direct sum of subalgebras $\mathcal{R} = \bigoplus_{j=1}^{s} \mathcal{R}^{(Z_j)}$, where $\mathcal{R}^{(Z_j)} = \sum_{K^{(i)} \in Z_j} \varepsilon^{(i)}\mathcal{R}$.

(2) Whenever Z_j contains exactly one field $K^{(i)}$, then $\mathcal{R}^{(Z_j)} = \varepsilon^{(i)}\mathcal{R}$ is a classical skew-polynomial domain.

4 Generators for left ideals in $A[z;\sigma]$

As a first fundamental property we note that $\mathcal{R} = A[z;\sigma]$ inherits from $\mathbb{F}[z]^n$ the property 'left Noetherian' by means of the left $\mathbb{F}[z]$-isomorphism $\mathfrak{p}$ from (2.8). This is also a straightforward consequence of results in Section 6, where $\mathcal{R}$ will appear as the image of $\mathbb{F}[z,x]$ under a left $\mathbb{F}[z]$-homomorphism (see the discussion following Theorem 6.9). In a similar way or by an anti-isomorphism as given below in Observation 4.16 one can see that $\mathcal{R}$ is also right Noetherian.
The central theme in Piret's fundamental article [19] is the detailed construction of a generator polynomial for an irreducible σ-CCC, resp. left ideal in $\mathcal{R}$. This is done for an automorphism σ which maps x onto a power of x. The constructions are displayed in terms of involved matrix manipulations. But at the same time central arguments rely heavily on the decomposition of A into components as introduced in the foregoing section. Maybe this is the reason why the small step in [14] for obtaining a single generator polynomial for *reducible* CCC's is not done in [19]. In this section we will first show by quite different, rather short and purely algebraic arguments and for an arbitrary automorphism σ that any delay-free left ideal in $\mathcal{R}$ is in fact a principal left ideal (Theorem 4.5). This result is not constructive. The development of an algorithmic procedure is postponed to the next section.

In [19, 14] uniqueness of generator polynomials is not addressed. The key to our uniqueness result in Theorem 4.15 is a reduction procedure which resembles the one in Gröbner basis theory but which has to take into account that $A[z;\sigma]$ usually has many zero divisors and is not commutative. It turns out that reduced generators are essentially unique. At the same time reduced generators behave well for explicitly writing down a generator matrix for the corresponding code (see Section 7). They also will lead directly to minimal generator matrices for CCC's. We conclude the section with some information on right ideals which will be of later use, too.

In this section any isomorphic representation of A as a direct product of fields with the corresponding unique set of pairwise orthogonal primitive idempotents $\varepsilon^{(1)},\ldots,\varepsilon^{(r)}$ will do. A canonical way of displaying the algebra has been described in (3.1) – (3.5). However, in any case we obtain the fields (see also (3.7) for the canonical representation)

$$K^{(k)} := \varepsilon^{(k)}A \text{ for } k = 1,\ldots,r.$$

The primitive idempotents will play a central role in the arguments of this and the next section. Notice that $\sum_{k=1}^{r}\varepsilon^{(k)}$ is the identity in A, and thus also in $\mathcal{R}$, and therefore,

$$f = \varepsilon^{(1)}f + \cdots + \varepsilon^{(r)}f \text{ for all } f \in \mathcal{R}. \tag{4.1}$$

Before we proceed let us introduce the following useful notation.

Notation 4.1
(1) For $f \in \mathcal{R}$ and $k = 1,\ldots,r$ put $f^{(k)} := \varepsilon^{(k)}f$. We call $f^{(k)}$ the k-th component of f. Furthermore, we call $T_f := \{k \mid f^{(k)} \neq 0\}$ the support of f. If $f = f^{(k)}$ for some $k = 1,\ldots,r$, then we call f simply a component.

(2) For a polynomial $f = \sum_{\nu=0}^{d} z^\nu f_\nu$, where $f_\nu \in A$ and $f_d \neq 0$, we call $\deg_z f := d$ the z-degree, f_d the leading z-coefficient, and f_0 the z-free term of f.

(3) The left (resp. right) ideal in $\mathcal{R}$ generated by a set $M \subseteq \mathcal{R}$ will be denoted by ${}^{\bullet}\langle\, M \,\rangle$ (resp. $\langle\, M \,\rangle^{\bullet}$).

From (4.1) we immediately obtain the following.

Observation 4.2
Let $f_1, \ldots, f_t \in \mathcal{R}$ and put $f_i^{(k)} := \varepsilon^{(k)} f_i$ for $i = 1, \ldots, t$ and $k = 1, \ldots, r$. Then

$$ {}^{\bullet}\langle\, f_1, \ldots, f_t \,\rangle = {}^{\bullet}\langle\, f_1^{(1)}, \ldots, f_1^{(r)}, \ldots\ldots, f_t^{(1)}, \ldots, f_t^{(r)} \,\rangle. $$

It is an elementary, but crucial fact that each automorphism $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$ induces a permutation on the set of primitive idempotents, i. e.

$$ \{\varepsilon^{(1)}, \ldots, \varepsilon^{(r)}\} = \{\sigma(\varepsilon^{(1)}), \ldots, \sigma(\varepsilon^{(r)})\}. \tag{4.2} $$

This implies that for a given polynomial $g = \sum_{\nu \geq 0} z^\nu g_\nu \in \mathcal{R}$ the z-coefficients of the components

$$ \varepsilon^{(k)} g = \sum_{\nu=0}^{d} z^\nu \sigma^\nu(\varepsilon^{(k)}) g_\nu \tag{4.3} $$

are in general not in $K^{(k)}$ but rather move around according to the permutation (4.2). In particular, for each $\nu \geq 0$ and each $k \in \{1, \ldots, r\}$ there exists a unique $l \in \{1, \ldots, r\}$ such that $\sigma^\nu(\varepsilon^{(k)}) g_\nu \in K^{(l)}$, see also Example 4.4 below.

The following lemma will be of frequent use.

Lemma 4.3

(a) The element x is a unit (i.e. invertible) in A and $a \in A$ is a unit in A if and only if $\varepsilon^{(k)} a \neq 0$ for all $k \in \{1, \ldots, r\}$.

(b) Let $g = \sum_{\nu=0}^{d} z^\nu g_\nu \in \mathcal{R}$ and suppose that for some $\mu \in \{0, \ldots, d\}$ the coefficient g_μ is nonzero. Then there is a unit $a \in A$ such that $ag = \sum_{\nu=0}^{d} z^\nu (ag)_\nu = \sum_{\nu=0}^{d} z^\nu \sigma^\nu(a) g_\nu$, satisfies for all $1 \leq k \leq r$

$$ \varepsilon^{(k)} g_\mu \neq 0 \implies \varepsilon^{(k)} (ag)_\mu = \varepsilon^{(k)}. $$

(c) Let $g \in \mathcal{R}$ be a nonzero polynomial. Then there exists a unit $a \in A$, such that for all $1 \leq k \leq r$

$$ k \in T_g \Longrightarrow \text{ the leading } z\text{-coefficient of } (ag)^{(k)} \text{ is a primitive idempotent.} $$

We say that the polynomial ag is normalized.

(d) Let $f, g \in \mathcal{R}$ and $1 \leq k \leq r$, then

$$ f\varepsilon^{(k)} g = 0 \implies f\varepsilon^{(k)} = 0 \text{ or } \varepsilon^{(k)} g = 0. $$

Notice that, since A is commutative, $(ag)^{(k)} = ag^{(k)}$ for all $a \in A$ and $g \in \mathcal{R}$.

PROOF: (a) is obvious.
(b) Since $K^{(k)} = \varepsilon^{(k)}A$ is a field, we can find $b_k \in A$ such that $\varepsilon^{(k)}b_k g_\mu = \varepsilon^{(k)}$ whenever $\varepsilon^{(k)}g_\mu \neq 0$. Now

$$a := \sigma^{-\mu}\Big(\sum_{k\in T_{g_\mu}} \varepsilon^{(k)}b_k + \sum_{k\notin T_{g_\mu}} \varepsilon^{(k)}\Big).$$

has the desired properties. Invertibility follows from (a).
(c) By the previous part we can find for each $k \in T_g$ units $a_k \in A$ such that $a_k g^{(k)}$ has a primitive idempotent as leading z-coefficient. Let

$$a := \sum_{k\in T_g} a_k\varepsilon^{(k)} + \sum_{k\notin T_g} \varepsilon^{(k)}.$$

Then one easily verifies that a is a unit in A and $ag^{(k)} = a_k g^{(k)}$ yields the desired property.
(d) If $f\varepsilon^{(k)} \neq 0 \neq \varepsilon^{(k)}g$, then the leading z-terms of $f\varepsilon^{(k)}$ and $\varepsilon^{(k)}g$ are of the form $z^\nu a\varepsilon^{(k)} \neq 0$ and $\varepsilon^{(k)}bz^\mu \neq 0$, respectively, for some a, $b \in A$. But then the leading z-term of $f\varepsilon^{(k)}g$ is $z^\nu a\varepsilon^{(k)}bz^\mu$, which is nonzero by (3.8). □

Note that part (d) above extends (3.8).

Example 4.4
Let us consider the case $\mathbb{F} = \mathbb{F}_4$ and $n = 5$. The ring A and its automorphisms have been described in detail in Example 3.3(b). We now choose the automorphism σ given by $\sigma(x) = x^2$. The effect of normalization is best visualized when representing the elements in A as triples in $K_1 \times K_2 \times K_3$, where the fields K_i are as in (3.11), see also the list in Example 3.3(b). In this description we have $\sigma([u, v, w]) = [u, \Psi^{-1}(w)^4, \Psi(v)]$, where Ψ is as in (3.12). The primitive idempotents $\varepsilon^{(1)} = [1, 0, 0]$, $\varepsilon^{(2)} = [0, 1, 0]$, and $\varepsilon^{(3)} = [0, 0, 1]$ satisfy $\sigma(\varepsilon^{(1)}) = \varepsilon^{(1)}$, $\sigma(\varepsilon^{(2)}) = \varepsilon^{(3)}$, and $\sigma(\varepsilon^{(3)}) = \varepsilon^{(2)}$. Consider now the element

$$g = [0, z(\alpha^2x + \alpha^2), \alpha x + 1].$$

Then one easily verifies that $\varepsilon^{(1)}g = \varepsilon^{(2)}g = 0$ and $\varepsilon^{(3)}g = g$. We want to normalize g. Since $(\alpha^2x + \alpha^2)^{-1} = x + \alpha^2$ in the field K_2, we put $a := \sigma^{-1}([1, x + \alpha^2, 1])$, see the proof of part (b) above. Since $\sigma^{-1}(x) = x^3$, or, in the current representation, $\sigma^{-1}([u, v, w]) = [u, \Psi^{-1}(w), \Psi(v)^4]$, we calculate $a = [1, 1, \alpha^2x]$. Now one checks that

$$ag = z[0, 1, 0] + [0, 0, 1] = [0, z, 1].$$

In this case normalization of the leading z-coefficient led to a normalization of the z-free term, too. □

We can now proceed to our algebraic (generalized and completed) version of Piret's result on ideal generators for σ-CCC's, see [19, Thm. 3.10].

Theorem 4.5
Let $\mathcal{C}$ be an $\mathbb{F}[z]$-submodule of $\mathbb{F}[z]^n$ and $\mathcal{J} = \mathfrak{p}(\mathcal{C})$ its image in $\mathcal{R}$. Then the following properties are equivalent.

(a) $\mathcal{C}$ is σ-cyclic and delay-free.

(b) $\mathcal{J} = {}^{\bullet}\langle\, g\,\rangle$ for some polynomial $g \in \mathcal{R}$ satisfying $T_g = T_{g_0}$, precisely

$$\varepsilon^{(k)} g \neq 0 \Longleftrightarrow \varepsilon^{(k)} g_0 \neq 0 \text{ for all } 1 \leq k \leq r. \tag{4.4}$$

Here T_g denotes the support and g_0 the z-free term of g, see 4.1.
In particular, every delay-free left ideal of $\mathcal{R}$ is principal.

Proof: For any polynomial $f \in \mathcal{R}$ we will use the notation f_0 for its z-free term.
"(a) $\Rightarrow$ (b)" Without loss of generality we may assume $\mathcal{C} \neq \{0\}$, thus $\mathcal{J} \neq \{0\}$. Recall from Observation 2.10(b) that $\mathcal{J}$ is a left ideal. Thus it remains to show that $\mathcal{J}$ has a principal generator satisfying (4.4). For $k \in \{1, \ldots, r\}$ define $g^{(k)} := 0$ if $\big(\varepsilon^{(k)}\mathcal{J}\big)_0 := \big\{f_0 \mid f \in \varepsilon^{(k)}\mathcal{J}\big\} = \{0\}$ and let otherwise $g^{(k)}$ be a polynomial of minimal z-degree in $\big\{f \in \varepsilon^{(k)}\mathcal{J} \mid f_0 \neq 0\big\}$. By delay-freeness not all $g^{(k)}$ are zero. Multiplying by an appropriate unit in A according to Lemma 4.3(b), we can assume that $g_0^{(k)} = \varepsilon^{(k)}$ whenever $g^{(k)} \neq 0$. Then for each $k \in \{1, \ldots, r\}$ either $g^{(k)} = 0$ or $g^{(k)} = \varepsilon^{(k)} + \sum_{i=1}^{d_k} z^i g_{k,i}$ for some $d_k \geq 0$, $g_{k,i} \in A$, and $g_{k,d_k} \neq 0$. Put

$$g := \sum_{k=1}^{r} g^{(k)}. \tag{4.5}$$

Obviously, $g^{(k)} = \varepsilon^{(k)} g$ and the notation matches with 4.1(1). By construction we have ${}^{\bullet}\langle\, g\,\rangle \subseteq \mathcal{J}$ as well as property (4.4). Hence it remains to show that $\mathcal{J} \subseteq {}^{\bullet}\langle\, g\,\rangle$. In order to do so, define the length of an arbitrary polynomial $f = \sum_{i=i_0}^{i_0+d} z^i f_i \in \mathcal{R}$ with $f_{i_0} \neq 0 \neq f_{i_0+d}$ as $l(f) := d + 1$ and put $l(0) := 0$. Suppose now that $\mathcal{J} \setminus {}^{\bullet}\langle\, g\,\rangle \neq \varnothing$ and let f be a polynomial of minimal length in $\mathcal{J} \setminus {}^{\bullet}\langle\, g\,\rangle$. We have $f = z^{i_0}\overline{f}$ and $l(f) = l(\overline{f})$ for some $\overline{f} \in \mathcal{R}$ such that $\overline{f}_0 \neq 0$. Delay-freeness of $\mathcal{J}$, see Observation 2.14, implies $\overline{f} \in \mathcal{J}$, too. Since $\overline{f} \notin {}^{\bullet}\langle\, g\,\rangle$ we can assume without restriction $\overline{f} = f$, i. e. $f_0 \neq 0$. Now let $f' := f - f_0 g$. Then $f' \in \mathcal{J} \setminus {}^{\bullet}\langle\, g\,\rangle$. Moreover, we obtain for each $k \in T_g$ the identity

$$\varepsilon^{(k)} f' = \varepsilon^{(k)} f - \varepsilon^{(k)} f_0 g = \varepsilon^{(k)} f - f_0 g^{(k)}.$$

Since $g_0^{(k)} = \varepsilon^{(k)}$ we conclude $(\varepsilon^{(k)} f')_0 = 0$. If $k \notin T_g$, then $g^{(k)} = 0$, which means that $(\varepsilon^{(k)}\mathcal{J})_0 = \{0\}$, and thus $(\varepsilon^{(k)} f')_0 = 0$, too. Hence $f'_0 = 0$ and, by the choice of the polynomials $g^{(k)}$, one has $\deg_z f' \leq \deg_z f$. This together implies $l(f') < l(f)$, which contradicts the choice of f. This proves $\mathcal{J} = {}^{\bullet}\langle\, g\,\rangle$.
"(b) $\Rightarrow$ (a)" Let $\mathcal{J} = {}^{\bullet}\langle\, g\,\rangle$ be a principal left ideal and g satisfy (4.4). Since by Observation 2.10 $\mathcal{C} = \mathfrak{v}(\mathcal{J})$ is σ-cyclic, it remains to show that $\mathcal{J}$ is delay-free, see also Observation 2.14. In order to do so, we may assume by Lemma 4.3(b) and (4.4) that for all $1 \leq k \leq r$ either $g_0^{(k)} = \varepsilon^{(k)}$ or $g^{(k)} = 0$. Let now $f = ug \in \mathcal{J}$ where $u = \sum_{\mu=0}^{\delta} z^\mu u_\mu$ and assume $f_0 = 0$. Then $f = zf'$ for some $f' \in \mathcal{R}$ and we have to show that $f' \in \mathcal{J}$. From the equation

$$0 = f_0 = u_0 g_0 = u_0 \sum_{k=1}^{r} g_0^{(k)} = \sum_{k=1}^{r} u_0 \varepsilon^{(k)} g_0^{(k)} = \sum_{k \in T_g} u_0^{(k)}$$

we get $u_0^{(k)} = 0$ for all $k \in T_g$. This in turn implies $u_0 g = \sum_{k=1}^{r} u_0 \varepsilon^{(k)} g = 0$ and thus $f = u'g$ for $u' := u - u_0$. But $u' = zu''$ and we finally conclude that $f' = u''g \in \mathcal{J}$, showing that $\mathcal{J}$ is delay-free. □

The next example shows that not all left ideals in $\mathcal{J}$ are principal and that not every generator g of a delay-free principal left ideal fulfills (4.4).

Example 4.6

(a) Let $\mathbb{F} = \mathbb{F}_4$ and $n = 3$ be as in Example 2.11. In Example 3.3(a) we saw that up to an isomorphism $A = K_1 \times K_2 \times K_3$, where $K_i = \mathbb{F}[x]/\langle \pi_i \rangle$. We choose the automorphism σ which corresponds to the permutation $(1, 3, 2)$. In the representation $A \cong \mathbb{F}[x]/\langle x^3 - 1 \rangle$ this corresponds to the automorphism which maps x onto $\alpha^2 x$. Now let $f_1 = z[1, 1, 1]$, $f_2 = [0, 1, 0]$ and assume that ${}^{\bullet}\langle f_1, f_2 \rangle = {}^{\bullet}\langle g \rangle$ for some $g \in \mathcal{R}$. Then the z-free term of g is of the form $[0, a, 0]$ for some $a \in A\backslash\{0\}$ and comparing z-coefficients in an equation $f_1 = ug$, $u \in \mathcal{R}$, leads to a contradiction. Thus the left ideal ${}^{\bullet}\langle f_1, f_2 \rangle$ is not principal. The same example works, mutatis mutandis, for any automorphism $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$ satisfying $\sigma(\varepsilon^{(2)}) = \varepsilon^{(3)}$ and for any n and $\mathbb{F}$ where, as usual, $\mathrm{char}(\mathbb{F}) \nmid n$.

(b) Let now A be arbitrary and $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$ such that $\sigma(\varepsilon^{(1)}) = \varepsilon^{(2)}$. Let $g = (z+1)\varepsilon^{(2)}$. Then $\sigma(\varepsilon^{(2)}) \neq \varepsilon^{(2)}$ and the left ideal ${}^{\bullet}\langle g \rangle = {}^{\bullet}\langle \varepsilon^{(2)} \rangle$ is delay-free, but $\varepsilon^{(1)} g = z\varepsilon^{(2)} \neq 0$ and $\varepsilon^{(1)} g_0 = 0$. □

The proof of Theorem 4.5 is not constructive as long as there is no finite procedure to determine the minimal polynomials $g^{(k)} \in \varepsilon^{(k)}\mathcal{J}$ starting from a finite generating family of $\mathcal{J}$. In the next section such a procedure will be developed. But before we go into the computational issues we will investigate, as to what extent a generator of a principal left ideal is unique. The key to our uniqueness result is a reduction procedure based on a monomial ordering which we introduce now.

Definition 4.7

(a) *For $\mu \geq 0$ and $1 \leq k \leq r$ the polynomials $z^{\mu}\varepsilon^{(k)}$ are called the (left-) monomials of $\mathcal{R}$.*

(b) *Given two monomials $z^{\mu}\varepsilon^{(k)}, z^{\nu}\varepsilon^{(l)}$ we define*

$$z^{\mu}\varepsilon^{(k)} < z^{\nu}\varepsilon^{(l)} :\Longleftrightarrow \mu < \nu \text{ or } \mu = \nu \text{ and } k < l.$$

(c) *Let $f = \sum_{\mu=0}^{d} z^{\mu} f_{\mu} \in \mathcal{R}$ be nonzero and have the following component expansion*

$$f = \left(\varepsilon^{(1)} f_0 + \cdots + \varepsilon^{(r)} f_0\right) + z\left(\varepsilon^{(1)} f_1 + \cdots + \varepsilon^{(r)} f_1\right) + \cdots + z^d\left(\varepsilon^{(1)} f_d + \cdots + \varepsilon^{(r)} f_d\right).$$

Then the individual summands $z^{\mu}\varepsilon^{(k)} f_{\mu}$ are called the terms of f. The (left-) leading monomial, denoted by $\mathrm{LM}(f)$, is the largest monomial $z^{\mu}\varepsilon^{(k)}$ (with respect to $<$) such that $\varepsilon^{(k)} f_{\mu} \neq 0$. The associated term is called the leading term of f.

Observe that in the canonical representation of A as given in (3.5), (3.6) the monomials are of the form

$$z^{\mu}\varepsilon^{(k)} = [0, \ldots, 0, z^{\mu}, 0, \ldots, 0] \text{ where } z^{\mu} \text{ is at the } k\text{-th position.}$$

In the context of ordinary Gröbner basis theory (i.e. commutative and no zero-divisors) one would like to call such an ordering a TOP-monomial ordering (Term Over Position) and in fact one readily verifies that (b) defines a well-ordering on the set of all monomials which respects left-multiplication by monomials as far as the result is nonzero. As will soon become clear our results actually will not depend on the way the components are ordered in the representation of A (see also the paragraph after the proof of Corollary 4.13).

Since we won't make use of any right monomials we will call left monomials simply monomials. The following rules will be very useful.

Lemma 4.8

(a) *For all possible μ, ν, k, l and all $a \in A$ such that $a^{(l)} \neq 0$ one has:*
$z^\mu \varepsilon^{(k)}$ is a right divisor of $z^\nu \varepsilon^{(l)} a \Longleftrightarrow \mu \leq \nu$ and $k = l$.

(b) *Let g, $g' \in \mathcal{R}$ and $k, l \in \{1, \ldots, r\}$ such that $\varepsilon^{(k)} g \neq 0 \neq \varepsilon^{(l)} g'$ and $\mathrm{LM}(\varepsilon^{(k)} g) = z^\alpha \mathrm{LM}(\varepsilon^{(l)} g')$ for some $\alpha \in \mathbb{N}_0$. Then $\varepsilon^{(l)} = \sigma^\alpha(\varepsilon^{(k)})$.*

Proof: Part (a) is obvious. As for (b), let $\deg_z(\varepsilon^{(k)} g) = d$ and $\deg_z(\varepsilon^{(l)} g') = d'$. Then $\mathrm{LM}(\varepsilon^{(k)} g) = z^d \sigma^d(\varepsilon^{(k)})$ and $\mathrm{LM}(\varepsilon^{(l)} g') = z^{d'} \sigma^{d'}(\varepsilon^{(l)})$. Now the assumption implies $d = \alpha + d'$ and $\sigma^{\alpha + d'}(\varepsilon^{(k)}) = \sigma^d(\varepsilon^{(k)}) = \sigma^{d'}(\varepsilon^{(l)})$, from which the assertion follows. $\square$

Now we turn to the notion of reducedness.

Definition 4.9

(a) *Let $f_1, \ldots, f_s$ be any family of polynomials from $\mathcal{R}$. The family is called (left-) reduced if for all $1 \leq k, l \leq s$ such that $k \neq l$ and $f_k \neq 0 \neq f_l$ no nonzero term of f_k is right divisible by $\mathrm{LM}(f_l)$.*

(b) *A single polynomial $g \in \mathcal{R}$ is called (left-) reduced if the family $\varepsilon^{(1)} g, \ldots, \varepsilon^{(r)} g$ is left-reduced.*

Again, we will usually skip the qualifier 'left'. Note that a reduced family might contain one or more zero polynomials, but, of course, no other polynomial appears more than once. We wish to emphasize that, according to our definition, a single polynomial always forms a reduced family, but not necessarily a reduced polynomial. This slight inconsistency will not cause any confusion since reducedness in the generality of (a) will be dealt with only in Proposition 4.10 below. Thereafter, a family of polynomials will always consist of components, i. e. the family is in $\bigcup_{k=1}^r \varepsilon^{(k)} \mathcal{R}$. In that case the definitions are consistent since a component is always reduced in the sense of (b) above. Finally, let us also mention that constants in A are always reduced polynomials.

The following result describes the basic reduction process which will lead us to unique ideal generators. They will later on turn out to have further nice properties. For the process we will need so-called 'elementary operations' on a family $f_1, \ldots, f_s$, by which we mean the replacement of some f_k by

$$f'_k := f_k - z^\mu a f_l, \text{ for any } l \neq k, \mu \in \mathbb{N}_0 \text{ and } a \in A. \tag{4.6}$$

Proposition 4.10
Any finite family $f_1, \ldots, f_s$ from $\mathcal{R}$ can be transformed by finitely many elementary operations into a reduced family $g_1, \ldots, g_s$ such that for the respective left ideals one has

$$^{\bullet}\langle f_1, \ldots, f_s \rangle = {}^{\bullet}\langle g_1, \ldots, g_s \rangle.$$

Proof: First of all, it is clear that elementary operations leave the corresponding left ideal invariant. As for the reduction assume now that the leading term of some f_k is given by $z^\nu b$ and is right divisible by $\mathrm{LM}(f_l)$ for some $l \neq k$, say

$$z^\nu b = z^\mu \hat{a} \mathrm{LM}(f_l) \text{ for some } \hat{a} \in A,\ \mu \in \mathbb{N}_0. \tag{4.7}$$

Define

$$f'_k := f_k - z^\mu a f_l, \tag{4.8}$$

where $a \in A$ is such that (4.7) holds true when we replace $\hat{a}$ by a and $\mathrm{LM}(f_l)$ by the leading term of f_l (a does indeed exists, since the coefficients in (4.7) are in a field). Then either $f'_k = 0$ or $\mathrm{LM}(f'_k) < \mathrm{LM}(f_k)$. Observe also that $\deg_z(f'_k) \leq \deg_z(f_k)$ and equality is possible. Proceed now with the family $f_1, \ldots, f'_k, \ldots, f_s$. Since $<$ is a well-ordering, we get after finitely many steps a family $\hat{f}_1, \ldots, \hat{f}_s$, where no leading term is right divisible by any other.
As a second and final step we now autoreduce the family $\hat{f}_1, \ldots, \hat{f}_s$. Assuming that a nonzero term of $\hat{f}_k$, say $z^\nu b$, is right divisible by $\mathrm{LM}(f_l)$ for some $l \neq k$, we proceed as in (4.7) and (4.8). Since these operations do not affect the higher terms of $\hat{f}_k$ we arrive after finitely many steps at the desired family. □

The following case of the reduction step will be of specific importance.

Observation 4.11
If in (4.7) and (4.8) $f_k \in \varepsilon^{(k)}\mathcal{R}$ and $f_l \in \varepsilon^{(l)}\mathcal{R}$, then $f'_k \in \varepsilon^{(k)}\mathcal{R}$, too. This follows from the fact that $z^\nu b$ is a term of $f_k = \varepsilon^{(k)} f_k$ and hence $\varepsilon^{(k)} z^\nu = z^\mu \mathrm{LM}(f_l)$ by (4.7). Using Lemma 4.8(b), this implies $\varepsilon^{(l)} = \sigma^\mu(\varepsilon^{(k)})$ and as a consequence $f'_k = f_k - z^\mu a f_l = \varepsilon^{(k)} f_k - z^\mu a \varepsilon^{(l)} f_l = \varepsilon^{(k)}(f_k - z^\mu a f_l) \in \varepsilon^{(k)}\mathcal{R}$.

Example 4.12
Let us again consider the case $\mathbb{F} = \mathbb{F}_4$ and $n = 5$ as described in Example 3.3(b). Just like in Example 4.4 we will represent the elements as triples in $K_1 \times K_2 \times K_3$, where the fields K_i are as in (3.11). We now choose the automorphism σ given by $\sigma([u, v, w]) = [u, \Psi^{-1}(w), \Psi(v)^4]$, where Ψ is as in (3.12), see the sixth line of the list n 3.3(b). The primitive idempotents satisfy $\sigma(\varepsilon^{(1)}) = \varepsilon^{(1)}$, $\sigma(\varepsilon^{(2)}) = \varepsilon^{(3)}$, and $\sigma(\varepsilon^{(3)}) = \varepsilon^{(2)}$. Consider the family $f_1, \ldots, f_6$, where

$$\begin{aligned}
f_1 &= z\varepsilon^{(1)} = z[1,0,0],\\
f_2 &= z\varepsilon^{(3)}(\alpha x + \alpha) + \varepsilon^{(2)}\alpha^2 x = z[0,0,\alpha x + \alpha] + [0, \alpha^2 x, 0],\\
f_3 &= z\varepsilon^{(1)} + \varepsilon^{(1)} = z[1,0,0] + [1,0,0],\\
f_4 &= z^2\varepsilon^{(1)}\alpha + z\varepsilon^{(1)}\alpha^2 + \varepsilon^{(1)} = z^2[\alpha,0,0] + z[\alpha^2,0,0] + [1,0,0],\\
f_5 &= z\varepsilon^{(3)}(\alpha x + 1) + \varepsilon^{(2)}(\alpha^2 x + \alpha^2) = z[0,0,\alpha x + 1] + [0, \alpha^2 x + \alpha^2, 0],\\
f_6 &= z^2\varepsilon^{(3)}(\alpha^2 x + \alpha^2) + z\varepsilon^{(2)} x = z^2[0,0,\alpha^2 x + \alpha^2] + z[0,x,0].
\end{aligned}$$

Note that in each case the first term is the leading term. The family is not reduced and we perform the following steps.

(1) $f_3' := f_3 - f_1 = \varepsilon^{(1)}$.

(2) $f_1' := f_1 - zf_3' = 0$.

(3) $f_4' := f_4 - z^2\alpha f_3' = z\varepsilon^{(1)}\alpha^2 + \varepsilon^{(1)}$.

(4) $f_4'' := f_4' - z\alpha^2 f_3' = \varepsilon^{(1)}$.

(5) $f_4''' := f_4'' - f_3' = 0$.

(6) $f_5' := f_5 - af_2$, where $a \in A$ is such that $z\varepsilon^{(3)}(\alpha x + 1) = az\varepsilon^{(3)}(\alpha x + \alpha)$. Hence $a = \sigma^{-1}[0, 0, c]$, where $c = (\alpha x + 1)(\alpha x + \alpha)^{-1} = \alpha^2 x \in K_3$, and we get $a = [0, \Psi^{-1}(\alpha^2 x)^4, 0] = [0, x + \alpha^2, 0] = \varepsilon^{(2)}(x + \alpha^2)$. Then we compute $f_5' = \varepsilon^{(2)}(\alpha^2 x + \alpha^2) - \varepsilon^{(2)}(x + \alpha^2)\varepsilon^{(2)}\alpha^2 x = 0$.

(7) $f_6' := f_6 - z\alpha f_2 = 0$.

Now the family

$$\hat{f}_1 = 0, \quad \hat{f}_2 = f_2 = z\varepsilon^{(3)}(\alpha x + \alpha) + \varepsilon^{(2)}\alpha^2 x, \quad \hat{f}_3 = \varepsilon^{(1)}, \quad \hat{f}_4 = 0, \quad \hat{f}_5 = 0, \quad \hat{f}_6 = 0$$

is reduced. We know that ${}^{\bullet}\langle f_1, \ldots, f_6 \rangle = {}^{\bullet}\langle \hat{f}_2, \hat{f}_3 \rangle$. Applying Lemma 4.3(c), we can even normalize the generators and obtain (after changing the ordering and omitting zero polynomials)

$$g_1 := \varepsilon^{(1)}, \quad g_2 := \sigma^{-1}[1, 1, (\alpha x + \alpha)^{-1}]\hat{f}_2 = [1, \alpha x + \alpha^2, 1]\hat{f}_2 = z\varepsilon^{(3)} + \varepsilon^{(2)}.$$

Since $g_k \in \varepsilon^{(k)}\mathcal{R}$ for $k = 1, 2$ we know from Observation 4.2 that ${}^{\bullet}\langle f_1, \ldots, f_6 \rangle = {}^{\bullet}\langle g \rangle$, where $g := g_1 + g_2 = z[0, 0, 1] + [1, 1, 0] \in \mathcal{R}$. Thus we have found a reduced and normalized generator of the left ideal generated by $f_1, \ldots, f_6$. □

On first sight, the example appears somewhat specific in the sense that all given generator polynomials are components, precisely $f_1, f_3, f_4 \in \varepsilon^{(1)}\mathcal{R}$, $f_2, f_5 \in \varepsilon^{(2)}\mathcal{R}$, and $f_6 \in \varepsilon^{(3)}\mathcal{R}$. However, by virtue of Observation 4.2 each ideal has a generating set consisting of components only.

Corollary 4.13

(a) For every $f \in \mathcal{R}$ there exists a unit $u \in \mathcal{R}$, i. e. $u\overline{u} = \overline{u}u = 1$ for some $\overline{u} \in \mathcal{R}$, such that the polynomial uf is reduced. In particular, every principal left ideal has a reduced generator.

(b) Every delay-free principal left ideal has a reduced generator satisfying property (4.4).

PROOF: (a) Only the first statement needs to be proven. Define

$$f_k := \varepsilon^{(k)} f = f^{(k)} \text{ for } 1 \le k \le r. \tag{4.9}$$

Then $f_k \in \varepsilon^{(k)}\mathcal{R}$ and by definition the polynomial f is reduced if and only if the family $f_1, \ldots, f_r$ is reduced. In order to prove the corollary we will analyze the effect of the reduction process on the polynomial f. It suffices to consider a single reduction step as in (4.7) and (4.8), the result of which is the family $f_1, \ldots, f_k', \ldots, f_r$. We will prove that

(i) $f_k' \in \varepsilon^{(k)}\mathcal{R}$,
(ii) $u := 1 - z^\mu a\varepsilon^{(l)}$ is a unit in $\mathcal{R}$,
(iii) $f' := f_k' + \sum_{j\neq k} f_j$ satisfies $f' = uf$.
Part (i) is in Observation 4.11. As a consequence, one also has

$$z^\mu a f_l \in \varepsilon^{(k)}\mathcal{R}. \tag{4.10}$$

As for (ii), one easily derives from (4.10) that $u\overline{u} = \overline{u}u = 1$ for $\overline{u} := 1 + z^\mu a\varepsilon^{(l)}$. Finally, (iii) is established once we have shown that $\varepsilon^{(j)}f' = \varepsilon^{(j)}uf$ for all $j = 1,\ldots,r$. Using again (4.10) and the orthogonality of the idempotents we obtain for $j = k$ the identity $\varepsilon^{(k)}uf = f_k - \varepsilon^{(k)}z^\mu a f_l = f_k' = \varepsilon^{(k)}f'$ while for $j \neq k$ we have $\varepsilon^{(j)}uf = f_j - \varepsilon^{(j)}z^\mu a f_l = f_j = \varepsilon^{(j)}f'$. This completes the proof of (a).
(b) By Theorem 4.5 we may assume that $\mathcal{J} = {}^\bullet\!\langle\, f\,\rangle$, where $f \in \mathcal{R}$ satisfies (4.4). Again, it suffices to show that a single reduction step (4.8) respects this property. But this is clear since ${f'}^{(j)} = f^{(j)}$ for all $j \neq k$ and (4.10) shows that (4.8) occurs only for $\mu > 0$ and in this case ${f'}_0^{(k)} = f_0^{(k)}$. □

In the proof we made use of the monomial ordering for the case where the family consists of the components $f^{(1)},\ldots,f^{(r)}$ of a single polynomial $f \in \mathcal{R}$. In this case the leading term of each component is uniquely determined by the z-degree only and the arbitrarily prescribed ordering of the idempotents $\varepsilon^{(1)},\ldots,\varepsilon^{(r)}$ has no effect on the reducedness. It simply determines the ordering of the family $f^{(1)},\ldots,f^{(r)}$.

One should notice that in (ii) of the proof above we encounter one of the many units of the ring $\mathcal{R}$ which are not constant polynomials.

The following basic properties of reduced families of components will be of essential use in the sequel.

Lemma 4.14
(a) Let $g = g^{(k)} \in \varepsilon^{(k)}\mathcal{R}$ and $u \in \mathcal{R}$ such that $ug \neq 0$. Then

$$\mathrm{LM}(ug) = z^\alpha \mathrm{LM}(g) \text{ for some } \alpha \geq 0.$$

(b) Let G be a finite reduced subset of $\mathcal{R}$ such that $G \subseteq \bigcup_{k=1}^r \varepsilon^{(k)}\mathcal{R}$, in other words, each element of G is a component. Let furthermore $f \in \mathcal{R}\backslash\{0\}$. Then

$$f \in {}^\bullet\!\langle\, G\,\rangle \Longrightarrow \mathrm{LM}(f) = z^\alpha \mathrm{LM}(g) \text{ for some } g \in G \text{ and some } \alpha \in \mathbb{N}_0.$$

(c) Let $g \in \mathcal{R}$ be a nonzero reduced polynomial and $u_1,\ldots,u_r \in \mathcal{R}$. Then

$$\sum_{k=1}^r u_k g^{(k)} = 0 \Longrightarrow u_k g^{(k)} = 0 \text{ for all } k = 1,\ldots,r.$$

Proof: (a) Let $u = \sum_{\nu=0}^\delta z^\nu u_\nu$ and $g = \varepsilon^{(k)}g = \sum_{\mu=0}^d z^\mu \sigma^\mu(\varepsilon^{(k)})g_\mu$, where $\sigma^d(\varepsilon^{(k)})g_d \neq 0$. Then $ug = \sum_{\nu=0}^\delta z^\nu u_\nu g$ and if for some ν we find $u_\nu g \neq 0$, then also $u_\nu\varepsilon^{(k)} \neq 0$ and thus

$$\mathrm{LM}(u_\nu g) = \mathrm{LM}\Big(\sum_{\mu=0}^d z^\mu \sigma^\mu(u_\nu\varepsilon^{(k)})g_\mu\Big) = \mathrm{LM}(g)$$

since $\sigma^d(u_\nu\varepsilon^{(k)}) \neq 0$ and by (3.8) also $\sigma^d(u_\nu\varepsilon^{(k)})g_d \neq 0$. In order to find the leading monomial of ug we thus only have to pick the maximal power z^α such that $u_\alpha g \neq 0$ and then

$$\mathrm{LM}(ug) = \mathrm{LM}(z^\alpha u_\alpha g) = z^\alpha \mathrm{LM}(g).$$

(b) Suppose $G^{(k)} := \varepsilon^{(k)}G = \{g_1^{(k)}, \dots, g_{m_k}^{(k)}\}$, where $m_k = 0$ if $G^{(k)} = \varnothing$ and let

$$f = \sum_{k=1}^{r}\sum_{j=1}^{m_k} u_{kj}g_j^{(k)} = \sum_{k=1}^{r}\sum_{j=1}^{m_k} \underbrace{\left(u_{kj}\varepsilon^{(k)}\right) g_j^{(k)}}_{=:f_{kj}} \text{ for some } u_{kj} \in \mathcal{R}.$$

By part (a) we have

$$\mathrm{LM}(f_{kj}) = z^{\beta_{kj}}\mathrm{LM}(g_j^{(k)}) \text{ for some } \beta_{kj} \in \mathbb{N}_0 \text{ if } f_{kj} \neq 0.$$

Consider now the leading monomials of the polynomials f_{kj} of maximal z-degree. By reducedness of G these monomials are all different and this proves the assertion.
(c) Let $\sum_{k=1}^r u_k g^{(k)} = 0$. By part (a) we know already that $\mathrm{LM}(u_k g^{(k)}) = z^{\alpha_k}\mathrm{LM}(g^{(k)})$ for some $\alpha_k \geq 0$ whenever $u_k g^{(k)} \neq 0$. If there are nonzero products $u_k g^{(k)}$ at all, then there must be some cancellation of the maximal leading monomials which contradicts reducedness. $\square$

We can now apply these techniques in order to obtain uniqueness of generators of left ideals if we also assume normalization in the sense of Lemma 4.3(c).

Theorem 4.15
(a) Every left ideal in $\mathcal{R}$ has a unique finite left-reduced generating family, each element of which is a nonzero and normalized component.
(b) Every principal left ideal in $\mathcal{R}$ has a unique left-reduced and normalized generator.

Proof: Part (b) is a consequence of (a) and Corollary 4.13.
As for (a) notice that, by virtue of Observation 4.2, each left ideal has a generating family consisting only of polynomials in the components $\varepsilon^{(1)}\mathcal{R}, \dots, \varepsilon^{(r)}\mathcal{R}$. Using Observation 4.11 this property is preserved when reducing the family. Normalizing each element then proves the existence of the desired generating family. As for uniqueness, assume

$$\mathcal{J} = {}^\bullet\langle\, g_1^{(k_1)}, \dots, g_s^{(k_s)}\,\rangle = {}^\bullet\langle\, g_1'^{(l_1)}, \dots, g_t'^{(l_t)}\,\rangle$$

where $g_i^{(k_i)} \in \varepsilon^{(k_i)}\mathcal{R}$ and $g_i'^{(l_i)} \in \varepsilon^{(l_i)}\mathcal{R}$, where all polynomials are normalized, and both families are reduced. Let $i \in \{1, \dots, s\}$. By Lemmata 4.14(b), 4.8(b) one has

$$\mathrm{LM}(g_i^{(k_i)}) = z^\alpha\mathrm{LM}(g_j'^{(l_j)}) \text{ for some } \alpha \in \mathbb{N}_0 \text{ and } j \text{ such that } \varepsilon^{(l_j)} = \sigma^\alpha(\varepsilon^{(k_i)}),$$
$$\mathrm{LM}(g_j'^{(l_j)}) = z^\beta\mathrm{LM}(g_m^{(k_m)}) \text{ for some } \beta \in \mathbb{N}_0 \text{ and } m \text{ such that } \varepsilon^{(k_m)} = \sigma^\beta(\varepsilon^{(l_j)}).$$

Combining these two equations we first obtain $\mathrm{LM}(g_i^{(k_i)}) = z^{\alpha+\beta}\mathrm{LM}(g_m^{(k_m)})$. Then by reducedness of the family $g_1^{(k_1)}, \dots, g_s^{(k_s)}$ we conclude successively $\alpha = \beta = 0$, $i = m$,

$k_i = k_m = l_j$. Hence each leading monomial of the family $g_1^{(k_1)}, \ldots, g_s^{(k_s)}$ occurs as leading monomial of the other family. Symmetry and the fact that the leading monomials of a reduced family are pairwise different, shows that $s = t$ and, after reordering,

$$k_i = l_i \;\text{ and }\; \mathrm{LM}(g_i^{(k_i)}) = \mathrm{LM}(g_i'^{(k_i)}) \text{ for all } i = 1, \ldots, s.$$

Suppose now that for some i we have $g_i^{(k_i)} \neq g_i'^{(k_i)}$, or equivalently $f := g_i^{(k_i)} - g_i'^{(k_i)} \neq 0$. By normalization the leading terms of $g_i^{(k_i)}$ and $g_i'^{(k_i)}$ are equal and thus cancel. Therefore any nonzero term of f comes from a non leading term of $g_i^{(k_i)}$ or $g_i'^{(k_i)}$ or is a difference of such terms. Since $f \in \mathcal{J}$, by Lemma 4.14(b) the leading term of f must be right divisible by some $\mathrm{LM}(g_j^{(k_j)})$, $j \neq i$. This contradicts reducedness. Thus $f = 0$ and both reduced and normalized families must coincide. □

In the same way as σ-CCC's are linked to left ideals, their duals will turn out to be linked to certain right ideals in $\mathcal{R}$. Our results on left ideals can be translated to right ideals by means of the following anti-isomorphism.

Observation 4.16
For any $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$ the map $\widetilde{\ }: A[z;\sigma] \longrightarrow A[z;\sigma^{-1}]$ defined by

$$g = \sum_{\nu \geq 0} z^\nu g_\nu \longmapsto \widetilde{g} := \sum_{\nu \geq 0} g_\nu z^\nu = \sum_{\nu \geq 0} z^\nu \sigma^{-\nu}(g_\nu) \tag{4.11}$$

is an $\mathbb{F}$-algebra anti-isomorphism.

Theorem 4.5 immediately implies

Corollary 4.17
Any delay-free right ideal $\mathcal{J}$ in $A[z;\sigma]$ is a principal right ideal.

In the next section the results will be complemented by a computational procedure, which checks whether a finitely generated left ideal is delay-free or principal and, if so, computes the unique generator polynomial.

5 On the computation of principal generators of left ideals

While establishing uniqueness of a generator polynomial has been (typically) somewhat more cumbersome, the computation — starting from a finite set of generators of a delay-free left ideal $\mathcal{J}$ — can be achieved by a rather straightforward and systematic procedure. Remembering the proof of Theorem 4.5 it will be sufficient to compute minimal z-degree polynomials with nonzero z-free term in each component $\varepsilon^{(k)}\mathcal{J}$, $1 \leq k \leq r$, in order to obtain a single generating polynomial. Thereafter, reduction and normalization will lead to uniqueness according to Theorem 4.15 and Theorem 4.5. As we will show in Theorem 5.1 below, we obtain such minimal polynomials if we pick any finite set of generators of the ideal, decompose it into its components, and apply the reduction procedure to the family of components. Furthermore, the algorithm even provides a test whether the ideal under consideration is principal and/or delay-free. The details are as follows.

Let $f_1, \ldots, f_s \in \mathcal{R} = A[z;\sigma]$ be any finite family and define

$$F^{(k)} := \{f_1^{(k)}, \ldots, f_s^{(k)}\} \text{ for } k = 1, \ldots, r \text{ and } F := \bigcup_{k=1}^{r} F^{(k)}. \tag{5.1}$$

By Observation 4.2

$$\mathcal{J} := {}^{\bullet}\!\langle f_1, \ldots, f_s \rangle = {}^{\bullet}\!\langle F \rangle. \tag{5.2}$$

Note that some of the sets $F^{(k)} \subseteq \varepsilon^{(k)}\mathcal{J}$ may just contain the zero polynomial but typically they also contain nonzero polynomials. It is quite surprising that just reducing the set F leads us, after normalization, to the unique reduced and normalized generator polynomial. The important observation here is, that when reducing some polynomial $f_i^{(k)} \in F^{(k)}$ by some other $f_j^{(l)} \in F^{(l)}$, the result $f_i^{(k)} - z^t a f_j^{(l)}$ is necessarily again in $F^{(k)} \subseteq \varepsilon^{(k)}\mathcal{J}$. Therefore, the reduction process respects the partition $F = \bigcup_{k=1}^{r} F^{(k)}$, and only the contents of the individual sets $F^{(k)}$ changes. The following theorem describes what can be obtained by reducing F.

Theorem 5.1
Let F and $\mathcal{J}$ be as in (5.1) *and* (5.2). *Furthermore, let F be transformed via finitely many elementary operations into the reduced family G. Define $G^{(k)} := \varepsilon^{(k)}G$ for $k = 1, \ldots, r$ and let*

$$T := \big\{k \in \{1, \ldots, r\} \,\big|\, G^{(k)} \neq \{0\}\big\}.$$

Then

(a) $G = \bigcup_{k=1}^{r} G^{(k)}$ and $\mathcal{J} = {}^{\bullet}\!\langle G \rangle$.

(b) $\mathcal{J}$ is principal if and only if for each $k \in T$ the set $G^{(k)}$ contains exactly one nonzero polynomial. Furthermore, if $\mathcal{J}$ is principal then $\mathcal{J} = {}^{\bullet}\!\langle g \rangle$ where $g = \sum_{k \in T} g^{(k)}$ and $g^{(k)}$ is the unique nonzero polynomial in $G^{(k)}$. In particular, the polynomial g is reduced.

(c) $\mathcal{J}$ is delay-free if and only if $\mathcal{J}$ is principal and the polynomial g of part (b) satisfies (4.4).

(d) Let $\mathcal{J}$ be delay-free and g as in part (b). Then for each $k \in T$ one has $\deg_z g^{(k)} \leq \deg_z f$ for all $f \in \varepsilon^{(k)}\mathcal{J}$ with nonzero z-free term.

Proof: (a) follows from Observations 4.11 and 4.2.
(b) "$\Leftarrow$" and the second statement are consequences of Observation 4.2. "$\Rightarrow$" Note that if $\mathcal{J} = {}^{\bullet}\!\langle f \rangle$, then according to Observation 4.11, the reduction of the family $f^{(1)}, \ldots, f^{(r)}$ leads to at most one polynomial in each component $\varepsilon^{(k)}\mathcal{R}$, and therefore the assertion is a consequence of the uniqueness in Theorem 4.15.
(c) "$\Leftarrow$" is in Theorem 4.5 while "$\Rightarrow$" is a combination of Corollary 4.13(b) and Theorem 4.15.
(d) Suppose that for some $k \in T$ there exists a polynomial $f \in \varepsilon^{(k)}\mathcal{J}$ satisfying $\deg_z f < \deg_z g^{(k)}$ and having nonzero z-free term. Then there is a constant $c \in A$ and a polynomial

$\overline{f} \in \mathcal{R}$ such that $g^{(k)} - cf = z\overline{f}$. By delay-freeness we have $\overline{f} \in \mathcal{J}$ and Lemma 4.14(b) implies

$$\mathrm{LM}(g^{(k)}) = z\mathrm{LM}(\overline{f}) = z^{1+\alpha}\mathrm{LM}(g^{(l)}) \text{ for some } l \in \{1, \dots, r\} \text{ and } \alpha \geq 0, \tag{5.3}$$

contradicting reducedness of G. □

Based on the forgoing proposition we have the following simple algorithmic procedure for the computation of the unique reduced and normalized generator g of a given delay-free ideal $\mathcal{J} \subseteq \mathcal{R}$.

Algorithm 5.2
Input: A finite set $f_1, \dots, f_s$ of generators of the left ideal $\mathcal{J}$.

Step 1: For all $1 \leq k \leq r$ calculate $\varepsilon^{(k)} f_l$, $1 \leq l \leq s$ and form the sets $F^{(k)}$.

Step 2: Reduce the set $F = \bigcup_{k=1}^{r} F^{(k)}$ to obtain the reduced sets $G^{(k)}$ and G.

Step 3: Evaluation of results:

Case 1: If $G^{(k)}$ contains more than one nonzero polynomial for some $k = 1, \dots, r$, then $\mathcal{J}$ is not principal and thus not delay-free.

Case 2: If each set $G^{(k)}$ contains at most one nonzero polynomial, denoted by $g^{(k)}$, put $g := \sum g^{(k)}$ and normalize g according to Lemma 4.3(c). Then $\mathcal{J} = {}^{\bullet}\langle\, g \,\rangle$ is principal and g is its unique reduced and normalized generator. Furthermore, $\mathcal{J}$ is delay-free if and only if g satisfies (4.4).

We close this section by an example.

Example 5.3
Consider again the situation of Example 4.12 with the automorphism given therein. Furthermore, let $\mathcal{J} = {}^{\bullet}\langle\, h_1, h_2, h_3 \,\rangle$, where

$$\begin{aligned}
h_1 &:= z\varepsilon^{(1)} + \varepsilon^{(2)}\alpha^2 x + z\varepsilon^{(3)}(\alpha x + \alpha),\\
h_2 &:= z\varepsilon^{(1)} + \varepsilon^{(1)} + \varepsilon^{(2)}\alpha^2 x + z\varepsilon^{(3)}(\alpha x + \alpha),\\
h_3 &:= z^2\varepsilon^{(1)}\alpha + z^2\varepsilon^{(3)}(\alpha^2 x + \alpha^2) + z\varepsilon^{(1)}\alpha^2 + z\varepsilon^{(2)}x + z\varepsilon^{(3)}(\alpha x + 1) + \varepsilon^{(1)} + \varepsilon^{(2)}(\alpha^2 x + \alpha^2).
\end{aligned}$$

As a first step we have to compute the components of these polynomials. They are, not counting the zero components, just given by the polynomials in Example 4.12, precisely

$$\begin{aligned}
&\{h_1^{(1)},\, h_2^{(1)},\, h_3^{(1)}\} = \{f_1,\, f_3,\, f_4\}, \quad \{h_1^{(2)},\, h_2^{(2)},\, h_3^{(2)}\} = \{f_2,\, f_2,\, f_5\},\\
&\{h_1^{(3)},\, h_2^{(3)},\, h_3^{(3)}\} = \{0,\, 0,\, f_6\}.
\end{aligned}$$

Thus, $\mathcal{J} = {}^{\bullet}\langle\, f_1, \dots, f_6 \,\rangle = {}^{\bullet}\langle\, h \,\rangle$, where the reduced and normalized generator

$$h = z\varepsilon^{(3)} + \varepsilon^{(1)} + \varepsilon^{(2)}$$

has already been calculated in Example 4.12. □

6 σ-circulant matrices

While in the last sections we have concentrated on σ-CCC's as left ideals in $A[z;\sigma]$ we now focus on the description of these codes as submodules of $\mathbb{F}[z]^n$. More precisely, we introduce σ-circulant matrices as a counterpart of a generator polynomial of a principal left ideal. These matrices show close resemblance to classical circulants which are common in the theory of cyclic block codes. As a guideline through this section we first recall some basic facts about classical circulant matrices over finite fields. Many of these properties can then be generalized appropriately to σ-circulants. The consequences for σ-CCC's will then be discussed in the next section.

Throughout this section we use the representation of the ring $A \cong \mathbb{F}[x]/\langle x^n - 1\rangle$ as in (3.2). No direct decomposition into fields is needed. Since more than one automorphism appear simultaneously we do not use the abbreviation $\mathcal{R}$ for $A[z;\sigma]$. It will be convenient in the following to index the rows and columns of an $n \times n$-matrix as well as the entries of n-vectors from 0 to $n-1$.

We begin with classical circulants. Recall the notation $\mathfrak{p}$ and $\mathfrak{v} = \mathfrak{p}^{-1}$ from (2.8).

Definition 6.1
For $g = \sum_{i=0}^{n-1} g_i x^i \in A$ define

$$M_g := \begin{bmatrix} g_0 & g_1 & \cdots & g_{n-2} & g_{n-1} \\ g_{n-1} & g_0 & \cdots & g_{n-3} & g_{n-2} \\ \vdots & \vdots & & \vdots & \vdots \\ g_2 & g_3 & \cdots & g_0 & g_1 \\ g_1 & g_2 & \cdots & g_{n-1} & g_0 \end{bmatrix} = \begin{bmatrix} \mathfrak{v}(g) \\ \mathfrak{v}(xg) \\ \vdots \\ \mathfrak{v}(x^{n-2}g) \\ \mathfrak{v}(x^{n-1}g) \end{bmatrix} = \big[g_{(j-i) \bmod n}\big]_{i,j=0,\ldots,n-1} \in \mathbb{F}^{n\times n}.$$

We call M_g the circulant matrix associated with g.

The following properties of circulant matrices are either trivial or well-known in the theory of block codes, see e. g. [15, p. 501], but also [3] for a general reference on circulant matrix theory.

Lemma 6.2
(a) The mapping $A \longrightarrow \mathbb{F}^{n\times n},\ g \longmapsto M_g$ is $\mathbb{F}$-linear and injective.
(b) For $g,h \in A$ we have $M_{gh} = M_g M_h = M_h M_g$.
(c) $\operatorname{rank} M_g = \deg \frac{x^n-1}{\gcd(g,x^n-1)} =: k$ (where the quotient is evaluated in $\mathbb{F}[x]$) and every set of k consecutive rows (resp. columns) of M_g is linearly independent.
(d) Let $g = \sum_{i=0}^{n-1} g_i x^i$ and put $\widehat{g} := g(x^{n-1}) = g_0 + g_{n-1}x + g_{n-2}x^2 + \ldots + g_1 x^{n-1}$. Then

$$^{\mathsf{t}}M_g = M_{\widehat{g}}.$$

The map $\theta : A \longrightarrow A,\ g \longmapsto \widehat{g}$ is an involutive $\mathbb{F}$-algebra automorphism of A.

(e) A matrix $M \in \mathbb{F}^{n\times n}$ is the circulant matrix associated with some polynomial $g \in A$ if and only if $SM = MS$ where

$$S := M_x = \begin{bmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ 1 & 0 & \cdots & 0 \end{bmatrix}. \tag{6.1}$$

(f) $M_g = g(S)$ for all $g \in A$.

(g) $\mathfrak{v}(ab) = \mathfrak{v}(a)b(S)$ for all $a, b \in A$.

(h) S is the matrix of the linear map $a \longmapsto ax$ for $a \in A$ with respect to the basis $1, x, \ldots, x^{n-1}$ of the $\mathbb{F}$-vector space A and, as a consequence, $M_g = g(S)$ is the matrix of the map $a \longmapsto ag$.

The equation in Lemma 6.2(f) can also be used as an alternative, but less intuitive definition of circulant matrices. Many of the properties above are easily proved on the basis of this identity, as there are linearity, commutativity, and multiplicativity as well as the transposition rule, where the latter is a direct consequence of the rule ${}^{\mathsf{t}}S = S^{-1}$. One also obtains the well known fact that all circulant matrices can be simultaneously diagonalized over an extension field of $\mathbb{F}$ that contains a primitive n-th root of unity.

Also for later use we note that the set of all $n \times n$-circulant matrices over $\mathbb{F}$ is just $\mathbb{F}[S]$ and thus is a commutative subring of $\mathbb{F}^{n\times n}$ which is isomorphic to A.

The main additional ingredient for our generalized σ-circulants will be the following.

Definition 6.3
For $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$ we define

$$P_\sigma := \begin{bmatrix} \mathfrak{v}(1) \\ \mathfrak{v}(\sigma(x)) \\ \vdots \\ \mathfrak{v}(\sigma(x^{n-2})) \\ \mathfrak{v}(\sigma(x^{n-1})) \end{bmatrix}.$$

One should observe that P_σ is the matrix with respect to the basis $1, x, \ldots, x^{n-1}$ associated with the $\mathbb{F}$-linear map which is induced by the automorphism σ, i. e. we have

$$vP_\sigma = \mathfrak{v}\big(\sigma(\mathfrak{p}(v))\big) \text{ for all } v \in \mathbb{F}^n. \tag{6.2}$$

We will need the following properties.

Lemma 6.4
Let σ, $\tau \in \mathrm{Aut}_{\mathbb{F}}(A)$ and g, $h \in A$. Then

(1) $P_{\mathrm{id}} = I_n$ and $P_{\sigma\tau} = P_\tau P_\sigma$. Furthermore $P_\sigma \in Gl_n(\mathbb{F})$ and ${P_\sigma}^{-1} = P_{\sigma^{-1}}$.

(2) $P_\sigma^{-1} M_g P_\sigma = M_{\sigma(g)}$.

(3) For $v \in \mathbb{F}^n$ one has $\mathfrak{p}(vP_\sigma M_g) = \sigma(\mathfrak{p}(v))g$.

PROOF: (1) is a direct consequence of the fact that P_σ, P_τ are just the matrices which are associated with σ and τ when considered as $\mathbb{F}$-linear maps. The most important property (2) can be obtained as follows. For $v \in \mathbb{F}^n$ let $\mathfrak{p}(v) =: f$ and suppose $\sigma(x) = a$. Using Lemma 6.2(f), (g) and (h) as well as (6.2) we compute

$$vSP_\sigma = \mathfrak{v}(\sigma(fx)) = \mathfrak{v}(\sigma(f)\sigma(x)) = \mathfrak{v}(\sigma(f))a(S) = vP_\sigma M_{\sigma(x)}.$$

Part (3) is a direct consequence of the fact that P_σ and M_g are matrix representations of the $\mathbb{F}$-linear maps σ and multiplication with g. $\square$

Notice that (2) of the lemma above shows that the automorphisms on A appear as inner automorphisms $M_g \mapsto M_{\sigma(g)} = P_\sigma^{-1} M_g P_\sigma$ on $\mathbb{F}[S]$, where $\mathbb{F}[S] \cong A$ as noted above. This observation leads to

Lemma 6.5
Let $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$ and assume that

$$Q^{-1} M_x Q = P_\sigma{}^{-1} M_x P_\sigma$$

for some invertible matrix $Q \in \mathbb{F}^{n\times n}$. Then $Q = P_\sigma M_u$ for some unit $u \in A$.

PROOF: By Lemma 6.2(e), the identity $M_x\big(QP_\sigma{}^{-1}\big) = \big(QP_\sigma{}^{-1}\big)M_x$ is possible only if QP_σ^{-1} is a circulant. Hence $QP_\sigma^{-1} = M_{u'}$ for some $u' \in A$ which, by invertibility of Q, has to be a unit in A. Using Lemma 6.4(2) we obtain $Q = P_\sigma M_{\sigma(u')}$ and $u := \sigma(u')$ is a unit in A, too. $\square$

Now we can define polynomial circulant matrices.

Definition 6.6
Let $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$. For $g = \sum_{\nu\geq 0} z^\nu g_\nu \in A[z;\sigma]$ we define

$$\mathcal{M}^\sigma(g) := \sum_{\nu\geq 0} z^\nu P_\sigma{}^\nu M_{g_\nu} \in \mathbb{F}[z]^{n\times n}.$$

We call $\mathcal{M}^\sigma(g)$ the σ-circulant (matrix) for g.

Let us first present an

Example 6.7
Consider again the situation of Example 2.11(1) where σ is the automorphism given by $\sigma(x) = \alpha^2 x$ and

$$g := (1 + \alpha x + \alpha^2 x^2) + z(1 + x + x^2) + z^2(1 + \alpha^2 x + \alpha x^2).$$

Then

$$P_{\sigma^0} = I_3,\ P_\sigma = \begin{bmatrix} 1 & & \\ & \alpha^2 & \\ & & \alpha \end{bmatrix},\ P_{\sigma^2} = \begin{bmatrix} 1 & & \\ & \alpha & \\ & & \alpha^2 \end{bmatrix}$$

and thus

$$\mathcal{M}^\sigma(g) = \begin{bmatrix} 1 & \alpha & \alpha^2 \\ \alpha^2 & 1 & \alpha \\ \alpha & \alpha^2 & 1 \end{bmatrix} + zP_\sigma \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} + z^2 P_{\sigma^2} \begin{bmatrix} 1 & \alpha^2 & \alpha \\ \alpha & 1 & \alpha^2 \\ \alpha^2 & \alpha & 1 \end{bmatrix}$$
$$= \begin{bmatrix} 1+z+z^2 & \alpha+z+\alpha^2z^2 & \alpha^2+z+\alpha z^2 \\ \alpha^2+\alpha^2z+\alpha^2z^2 & 1+\alpha^2z+\alpha z^2 & \alpha+\alpha^2z+z^2 \\ \alpha+\alpha z+\alpha z^2 & \alpha^2+\alpha z+z^2 & 1+\alpha z+\alpha^2z^2 \end{bmatrix}.$$

It is easy to see that $\mathcal{M}^\sigma(g)$ has rank 1 and from Example 2.11(1) we conclude that the matrix is basic. It generates the 1-dimensional code $\mathcal{C} := \operatorname{im}\mathcal{M}^\sigma(g) = \operatorname{im}[1+z+z^2,\ \alpha+z+\alpha^2z^2,\ \alpha^2+z+\alpha z^2] \subseteq \mathbb{F}^3$. As noted in 2.11(1) the free distance is 9. $\square$

Notice that $\mathcal{M}^\sigma(g) = M_g$ whenever $g \in A$. Hence σ-circulants form a generalization of classical circulant matrices. This will be even more obvious from part (a) of the next proposition. Just like classical circulants provide a direct link between ideal generators and generator matrices for cyclic block codes we obtain a similar link for σ-circulants and σ-CCC's in part (b) below. This will be exploited extensively in Section 7 where the correspondences between left principal ideals, σ-circulants and σ-CCC's will be investigated in detail.

Proposition 6.8
In the situation of Definition 6.6 one has
(a)

$$\mathcal{M}^\sigma(g) = \begin{bmatrix} \mathfrak{v}(g) \\ \mathfrak{v}(xg) \\ \vdots \\ \mathfrak{v}(x^{n-1}g) \end{bmatrix}.$$

(b) $\mathfrak{p}\big(u\mathcal{M}^\sigma(g)\big) = \mathfrak{p}(u)g$ *for all* $u \in \mathbb{F}[z]^n$. *In particular,* $\mathfrak{p}\big((1,0,\ldots,0)\mathcal{M}^\sigma(g)\big) = g$.

Note that the foregoing rules are equally valid for classical circulants.

Proof: (a) Let $g = \sum_{\nu\geq 0} z^\nu g_\nu$. The i-th canonical basis vector in $\mathbb{F}[z]^n$ is $e_i := \mathfrak{v}(x^i)$. It is sufficient to show that $\mathfrak{p}(e_i\mathcal{M}^\sigma(g)) = x^i g$ for $1 \leq i \leq n$. For this one computes

$$\mathfrak{p}(e_i\mathcal{M}^\sigma(g)) = \mathfrak{p}(\sum_{\nu\geq 0} z^\nu e_i {P_\sigma}^\nu M_{g_\nu}) = \sum_{\nu\geq 0} z^\nu \mathfrak{p}(e_i P_{\sigma^\nu} M_{g_\nu}) = \sum_{\nu\geq 0} z^\nu \sigma^\nu(x^i) g_\nu = x^i g,$$

where we used the $\mathbb{F}[z]$-linearity of $\mathfrak{p}$ and Lemma 6.4(3) in the second and third equation, respectively.
(b) Using (a) and $\mathbb{F}[z]$-linearity of $\mathfrak{v}$ and $\mathfrak{p}$ we obtain for $u = (u_0,\ldots,u_{n-1}) \in \mathbb{F}[z]^n$ the identities

$$\mathfrak{p}\big(u\mathcal{M}^\sigma(g)\big) = \mathfrak{p}\big(\mathfrak{v}\big(\textstyle\sum_{i=0}^{n-1} u_i x^i g\big)\big) = \mathfrak{p}(u)g. \qquad \square$$

The following generalizes Lemma 6.2(a) and (b) to σ-circulants.

Theorem 6.9
Let $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$ and $g,\ h \in A[z;\sigma]$.
(a) The mapping $\mathcal{M}^\sigma : A[z;\sigma] \longrightarrow \mathbb{F}[z]^{n\times n}$ is $\mathbb{F}$-linear and injective.
(b) $\mathcal{M}^\sigma(g)\mathcal{M}^\sigma(h) = \mathcal{M}^\sigma(gh)$.
As a consequence, the Piret algebra $A[z;\sigma]$ and the ring $\mathcal{M}^\sigma\big(A[z;\sigma]\big)$ of all σ-circulants are isomorphic as $\mathbb{F}$-algebras.

Proof: (a) is a consequence of the definition of $\mathcal{M}^\sigma$, the invertibility of P_σ and the injectivity of the mapping $g \mapsto M_g$.
(b) By virtue of Proposition 6.8(b) and the isomorphism $\mathfrak{p}$ we have for each $u \in \mathbb{F}[z]^n$

$$\mathfrak{p}\big(u\mathcal{M}^\sigma(g)\mathcal{M}^\sigma(h)\big) = \mathfrak{p}\big(u\mathcal{M}^\sigma(g)\big)\,h = \mathfrak{p}(u)gh = \mathfrak{p}\big(u\mathcal{M}^\sigma(gh)\big),$$

leading to the desired result. □

Part (b) above has the interesting consequence, that each left inverse of a polynomial f in $A[z;\sigma]$ is also a right inverse of f, since this is the case for the ring $\mathbb{F}[z]^{n\times n}$.

One should observe that the isomorphism $g \mapsto \mathcal{M}^\sigma(g)$ induces a left $\mathbb{F}[z]$-module structure on the set $\mathcal{M}^\sigma\big(A[z;\sigma]\big)$ which is different from the canonical left $\mathbb{F}[z]$-module structure induced by $\mathbb{F}[z]^{n\times n}$. Furthermore, by Definition 6.6 and Lemma 6.2(f) we see that

$$\mathcal{M}^\sigma(g) = g(zP_\sigma, S) \text{ for } g(z,x) = \sum_{\nu\geq 0} z^\nu \sum_{i=0}^{n-1} g_{i\nu}x^i \in A[z;\sigma].$$

Therefore the isomorphism between $A[z;\sigma]$ and $\mathcal{M}^\sigma\big(A[z;\sigma]\big)$ can also be understood as an evaluation homomorphism whose image is just $\mathbb{F}[zP_\sigma, S]$, a subring of $\mathbb{F}[z]^{n\times n}$.

Next we turn to transposes of σ-circulants which will occur later on in our investigation of the dual of a σ-CCC. For this purpose the description of σ-circulants in Proposition 6.8(a), although very natural, is not helpful. Instead we have to resort to Definition 6.6. It will turn out that the transposes are in general not σ-circulant, but rather $\widehat{\sigma}$-circulant, where $\widehat{\sigma} \in \mathrm{Aut}_{\mathbb{F}}(A)$ is such that $P_{\widehat{\sigma}} = {}^{\mathsf{t}}P_\sigma$. Let us begin with an example.

Example 6.10
Consider the case $\mathbb{F} = \mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ and $n = 5$. Let $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$ be given by $\sigma(x) = x^2$. Then it is easy to see that ${}^{\mathsf{t}}P_\sigma = P_{\widehat{\sigma}}$ where $\widehat{\sigma} \in \mathrm{Aut}_{\mathbb{F}}(A)$ is given by $\widehat{\sigma}(x) = x^3$. Consider now the polynomial

$$g := 1 + \alpha^2 x + \alpha^2 x^2 + x^3 + z(1 + x + \alpha^2 x^2 + \alpha^2 x^4) \in A[z;\sigma]$$

with associated σ-circulant

$$\mathcal{M}^\sigma(g) = \begin{bmatrix} 1+z & \alpha^2+z & \alpha^2+z\alpha^2 & 1 & z\alpha^2 \\ 0 & 1+z\alpha^2 & \alpha^2+z & \alpha^2+z & 1+z\alpha^2 \\ 1+z & z\alpha^2 & 1 & \alpha^2+z\alpha^2 & \alpha^2+z \\ \alpha^2+z\alpha^2 & 1+z & z & 1+z\alpha^2 & \alpha^2 \\ \alpha^2+z\alpha^2 & \alpha^2 & 1+z\alpha^2 & z & 1+z \end{bmatrix}.$$

It is clear that if ${}^{\mathsf{t}}\mathcal{M}^\sigma(g)$ is a circulant matrix at all, then it is defined by the polynomial given in the first column of $\mathcal{M}^\sigma(g)$. Thus let

$$\widehat{g} := (1 + x^2 + \alpha^2 x^3 + \alpha^2 x^4) + z(1 + x^2 + \alpha^2 x^3 + \alpha^2 x^4) \in A[z;\sigma].$$

Then one verifies that $\mathcal{M}^\sigma(\widehat{g}) \neq {}^{\mathsf{t}}\mathcal{M}^\sigma(g)$ but rather $\mathcal{M}^{\widehat{\sigma}}(\widehat{g}) = {}^{\mathsf{t}}\mathcal{M}^\sigma(g)$.
We will come back to this example in the next sections where we translate this result into codes and their duals. □

In order to establish an identity of the type ${}^{\mathsf{t}}\mathcal{M}^\sigma(g) = \mathcal{M}^{\widehat{\sigma}}(\widehat{g})$ for any automorphism σ, we need the existence of an automorphism $\widehat{\sigma} \in \mathrm{Aut}_{\mathbb{F}}(A)$ such that ${}^{\mathsf{t}}P_\sigma = P_{\widehat{\sigma}}$. In fact, this already implies the desired identity for the σ-circulants since for any $g = \sum_{\nu\geq 0} z^\nu g_\nu$ we obtain from Definition 6.6, Lemma 6.2(d) and Lemma 6.4(2)

$${}^{\mathsf{t}}\mathcal{M}^\sigma(g) = \sum_{\nu\geq 0} z^\nu M_{\widehat{g_\nu}} {}^{\mathsf{t}}P_\sigma{}^\nu = \sum_{\nu\geq 0} z^\nu M_{\widehat{g_\nu}} P_{\widehat{\sigma}}^\nu = \sum_{\nu\geq 0} z^\nu P_{\widehat{\sigma}}^\nu M_{\widehat{\sigma}^\nu(\widehat{g_\nu})} = \mathcal{M}^{\widehat{\sigma}}(\widehat{g}^\sigma), \tag{6.3}$$

where $\widehat{g}^\sigma = \sum_{\nu\geq 0} z^\nu \widehat{\sigma}^\nu(\widehat{g_\nu})$. In order to show the existence of $\widehat{\sigma}$, we will make use of the involution θ given in Lemma 6.2(d). Notice that by Lemma 6.4(2) and Lemma 6.2(d) we have

$${}^{\mathsf{t}}P_\sigma^{-1} M_x {}^{\mathsf{t}}P_\sigma = {}^{\mathsf{t}}(P_\sigma M_{\widehat{x}} P_{\sigma^{-1}}) = {}^{\mathsf{t}}M_{\sigma^{-1}(\widehat{x})} = M_{\widehat{\sigma^{-1}(\widehat{x})}}.$$

Taking into account once more Lemma 6.4(2), this indicates how the desired automorphism $\widehat{\sigma}$ has to look like.

Theorem 6.11
Let $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$. Define $\widehat{\sigma} := \theta \circ \sigma^{-1} \circ \theta \in \mathrm{Aut}_{\mathbb{F}}(A)$, thus $\widehat{\sigma}(a) = \widehat{\sigma^{-1}(\widehat{a})}$ for all $a \in A$. Then $\widehat{\widehat{\sigma}} = \sigma$ and $\sigma \longmapsto \widehat{\sigma}$ defines an anti-automorphism on the group $\mathrm{Aut}_{\mathbb{F}}(A)$. Furthermore,

$${}^{\mathsf{t}}P_\sigma = P_{\widehat{\sigma}}.$$

Proof: Only the identity ${}^{\mathsf{t}}P_\sigma = P_{\widehat{\sigma}}$ needs proof. Applying several times Lemma 6.4(2) and Lemma 6.2(d) we obtain

$$P_{\widehat{\sigma}}^{-1} M_x P_{\widehat{\sigma}} = M_{\widehat{\sigma}(x)} = {}^{\mathsf{t}}M_{\widehat{\widehat{\sigma}(x)}} = {}^{\mathsf{t}}\big(P_\sigma M_{\sigma(\widehat{\widehat{\sigma}(x)})} P_\sigma^{-1}\big) = {}^{\mathsf{t}}P_\sigma^{-1} M_{\widehat{\sigma(\widehat{\widehat{\sigma}(x)})}} {}^{\mathsf{t}}P_\sigma = {}^{\mathsf{t}}P_\sigma^{-1} M_x {}^{\mathsf{t}}P_\sigma,$$

where the last equality follows from $\widehat{\sigma(\widehat{\widehat{\sigma}(x)})} = x$. Lemma 6.5 now yields

$${}^{\mathsf{t}}P_\sigma = P_{\widehat{\sigma}} M_u \text{ for some unit } u \in A. \tag{6.4}$$

We will show now that the matrix P_σ not only has zeros in the first row except for the very first entry (which is obvious by definition), but also in the first column. Then Equation (6.4) implies that the first row of M_u is of the form $(1, 0, \ldots, 0)$ and, being a circulant, $M_u = I_n$. This proves the theorem.
In order to establish the zero entries in the first column of P_σ let $\sigma(x) = a = \sum_{l=0}^{n-1} a_l x^l$. For the rest of the proof it will be convenient to use the notation $[f]_i$ for the coefficient of x^i in the polynomial $f \in A$. Then, according to Definition 6.3 we have to show

$[\sigma(x^i)]_0 = [a^i]_0 = 0$ for all $i > 0$. Since σ is an automorphism, the powers $1, a, \ldots, a^{n-1}$ are linearly independent over $\mathbb{F}$ and $a^n = 1$. Using linearity and multiplicativity of the circulants, this implies that the characteristic polynomial of M_a is given by $X^n - 1$ and we can conclude $0 = \mathrm{trace}(M_a) = n[a]_0$. But then also $[a]_0 = 0$ since $\gcd(n, \mathrm{char}(\mathbb{F})) = 1$. As for $[a^i]_0$, we wish to argue along the same lines. In order to determine the characteristic polynomial of $M_{a^i} = (M_a)^i$, let $X^n - 1 = \prod_{l=0}^{n-1}(X - \omega^l)$ for some primitive n-th root of unity ω in some extension field $\overline{\mathbb{F}}$ of $\mathbb{F}$. Furthermore assume $\gcd(i, n) = d$ and $n = d\tilde{n}$. Then ω^i is a primitive $\tilde{n}$-th root of unity and, since M_a is diagonalizable over $\overline{\mathbb{F}}$, the characteristic polynomial of M_{a^i} is given by

$$\prod_{l=0}^{n-1}(X - \omega^{il}) = \Big(\prod_{l=0}^{\tilde{n}-1}(X - \omega^{il})\Big)^d = (X^{\tilde{n}} - 1)^d.$$

As above we conclude $n[a^i]_0 = \mathrm{trace}(M_{a^i}) = 0$ for all $i > 0$ (in which case $\tilde{n} > 1$) and, again, $[a^i]_0 = 0$. □

In Example 6.10 above we had the specific situation that $\widehat{\sigma} = \sigma^{-1}$. This is not the case in general, see the remark below. However, the automorphisms of $A = \mathbb{F}_4[x]/\langle x^5 - 1\rangle$ as listed in Example 3.3(b) all satisfy either $\widehat{\sigma} = \sigma$ (in which case P_σ is symmetric) or $\widehat{\sigma} = \sigma^{-1}$ (which only occurs for $\sigma(x) = x^2$ and $\sigma(x) = x^3$). This too, is not true in general.

Remark 6.12
For the special class of automorphisms σ satisfying

$$\sigma(x) = \gamma x^r, \tag{6.5}$$

where $\gamma \in \mathbb{F}$, $r \in \{1, \ldots, n-1\}$, the associated $\widehat{\sigma}$ can be found easily. First notice that (6.5) induces an automorphism $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$ if and only if $\gamma^n = 1$ and $\gcd(r, n) = 1$. If these conditions are satisfied, then σ^{-1} and $\widehat{\sigma}$ are given by the equations

$$\sigma^{-1}(x) = \gamma^{-l}x^l \text{ and } \widehat{\sigma}(x) = \gamma^l x^l \text{ where } lr \equiv 1 \bmod n. \tag{6.6}$$

This can be verified remembering the definition of $\widehat{\sigma}$. The conditions in (6.6) lead to plenty of examples where the automorphisms σ, σ^{-1}, $\widehat{\sigma}$ are all different, e. g. for $A = \mathbb{F}_4[x]/\langle x^7 - 1\rangle$ and σ given by $\sigma(x) = \alpha x^4$.
We also wish to note that in [19] only automorphisms as in (6.5) with $\gamma = 1$ were considered. In this case one always has $\widehat{\sigma} = \sigma^{-1}$.

Now we can describe the transposes of σ-circulants. In part (a) below we obtain a direct generalization of Lemma 6.2(d). The anti-isomorphism in part (b) will be crucial in the next section when relating a parity check polynomial of a σ-cyclic code $\mathcal{C}$ to a generator polynomial of the $\widehat{\sigma}$-cyclic dual code $\mathcal{C}^\perp$.

Theorem 6.13
Let $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$ and $\widehat{\sigma}$ be defined as in Theorem 6.11. For any polynomial $g = \sum_{\nu\geq 0} z^\nu g_\nu \in A[z;\sigma]$ define

$$\widehat{g}^\sigma := \sum_{\nu\geq 0} \widehat{g_\nu} z^\nu = \sum_{\nu\geq 0} z^\nu \widehat{\sigma}^\nu(\widehat{g_\nu}) \;\in A[z;\widehat{\sigma}]. \tag{6.7}$$

Then

(a) ${}^{\mathsf{t}}\mathcal{M}^{\sigma}(g) = \mathcal{M}^{\widehat{\sigma}}(\widehat{g}^{\sigma})$.

(b) The map $\widehat{\ }^{\sigma} : A[z;\sigma] \longrightarrow A[z;\widehat{\sigma}],\ g \longmapsto \widehat{g}^{\sigma}$ *is an anti-isomorphism of the* $\mathbb{F}$*-algebras* $A[z;\sigma]$ *and* $A[z;\widehat{\sigma}]$*, that is,* $\widehat{\ }^{\sigma}$ *is* $\mathbb{F}$*-linear and satisfies* $\widehat{gh}^{\sigma} = \widehat{h}^{\sigma}\widehat{g}^{\sigma}$ *for all* $g, h \in A[z;\sigma]$*. The inverse map is given by* $\widehat{\ }^{\widehat{\sigma}} : A[z;\widehat{\sigma}] \longrightarrow A[z;\sigma],\ g \longmapsto \widehat{g}^{\widehat{\sigma}}$*.*

Proof: (a) has been shown in (6.3).
(b) $\mathbb{F}$-linearity and injectivity are obvious by (6.7). Anti-multiplicativity is a consequence of

$$\mathcal{M}^{\widehat{\sigma}}(\widehat{gh}^{\sigma}) = {}^{\mathsf{t}}\mathcal{M}^{\sigma}(gh) = {}^{\mathsf{t}}\mathcal{M}^{\sigma}(h){}^{\mathsf{t}}\mathcal{M}^{\sigma}(g) = \mathcal{M}^{\widehat{\sigma}}(\widehat{h}^{\sigma})\mathcal{M}^{\widehat{\sigma}}(\widehat{g}^{\sigma}) = \mathcal{M}^{\widehat{\sigma}}(\widehat{h}^{\sigma}\widehat{g}^{\sigma})$$

along with injectivity of the map $\mathcal{M}^{\widehat{\sigma}}$. Finally, the equation $\mathcal{M}^{\sigma}(g) = {}^{\mathsf{t}}\mathcal{M}^{\widehat{\sigma}}(\widehat{g}^{\sigma}) = \mathcal{M}^{\sigma}(\widehat{(\widehat{g}^{\sigma})}^{\widehat{\sigma}})$ shows that $\widehat{(\widehat{g}^{\sigma})}^{\widehat{\sigma}} = g$ for all $g \in A[z;\sigma]$, which completes the proof. □

As a simple consequence of Theorem 6.13 we obtain that each polynomial vector appears not only as a row but also as a column in some σ-circulant. Furthermore, as we will show next, the algebra of σ-circulants is saturated in the sense that if a multiple of a circulant within the ring $\mathbb{F}[z]^{n\times n}$ is a circulant again, then it is even a multiple within the algebra $\mathcal{M}^{\sigma}(A[z;\sigma])$. Also these results will be of use in the next section for generator and parity check matrices of σ-CCC's.

Corollary 6.14
Let $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$*. Then one has the implications*

(1) For each $v \in \mathbb{F}[z]^n$ *and* $g_1 = \mathfrak{p}(v) \in A[z;\sigma]$, $g_2 = \mathfrak{p}(v) \in A[z;\widehat{\sigma}]$ *and for each* $f \in A[z;\sigma]$ *one has*

$$v\mathcal{M}^{\sigma}(f) = 0 \iff \mathcal{M}^{\sigma}(g_1)\mathcal{M}^{\sigma}(f) = 0 \ \text{ and } \ \mathcal{M}^{\sigma}(f){}^{\mathsf{t}}v = 0 \iff \mathcal{M}^{\sigma}(f)\mathcal{M}^{\sigma}(\widehat{g_2}^{\widehat{\sigma}}) = 0.$$

(2) For all $f, g \in A[z;\sigma]$ *one has the two implications*

$$\exists\, Q \in \mathbb{F}[z]^{n\times n} : \mathcal{M}^{\sigma}(f) = Q\mathcal{M}^{\sigma}(g) \Longrightarrow \exists\, h \in A[z;\sigma] : \mathcal{M}^{\sigma}(f) = \mathcal{M}^{\sigma}(h)\mathcal{M}^{\sigma}(g),$$
$$\exists\, Q \in \mathbb{F}[z]^{n\times n} : \mathcal{M}^{\sigma}(f) = \mathcal{M}^{\sigma}(g)Q \Longrightarrow \exists\, h \in A[z;\sigma] : \mathcal{M}^{\sigma}(f) = \mathcal{M}^{\sigma}(g)\mathcal{M}^{\sigma}(h).$$

One should observe that part (2) above, applied to constant polynomials $f, g \in A$ leads to the analogous statements for classical circulants.

Proof: (1) The first equivalence can be obtained as follows with the help of Proposition 6.8(b):

$$v\mathcal{M}^{\sigma}(f) = 0 \iff g_1 f = 0 \iff \mathcal{M}^{\sigma}(g_1)\mathcal{M}^{\sigma}(f) = 0.$$

The second equivalence follows from the first one by transposition and Theorem 6.13.
(2) Let v be the first row of $\mathcal{M}^{\sigma}(f)$ and w be the first row of Q and $h = \mathfrak{p}(w)$. Then $\mathfrak{v}(f) = v$ and $v = w\mathcal{M}^{\sigma}(g)$. By Proposition 6.8(b) we obtain $f = hg$ which gives us $\mathcal{M}^{\sigma}(f) = \mathcal{M}^{\sigma}(h)\mathcal{M}^{\sigma}(g)$. The second statement follows as in (a) by transposition and Theorem 6.13. □

So far we have not discussed the rank of σ-circulants. As opposed to classical circulants (see Lemma 6.2(c)) there is no general simple rule telling the rank of $\mathcal{M}^{\sigma}(g)$ based on the polynomial g. Fortunately, if g is a reduced polynomial, a generalization of the classical result exists. This will be treated in Theorem 7.8.

7 Description of σ-cyclic codes and their duals

Now we are in a position to return to σ-CCC's in the sense of Definition 2.8 or Observation 2.10(b). In this section we introduce generator and parity check polynomials as well as (square circulant) generating and parity check matrices for σ-CCC's. We show that they behave just like those for block codes. Below we first summarize the relation between cyclic block codes and classical circulant matrices, as this shows exactly what we are after for convolutional codes. As a reference on cyclic block codes any (introductory) book on coding theory suffices, for instance [15] or [1].

Let $\mathcal{C} \in \mathbb{F}^n$ be a cyclic block code, then — in polynomial representation — we obtain a principal left ideal $\mathcal{J} = \mathfrak{p}(\mathcal{C}) = {}^{\bullet}\langle\, g \,\rangle$ for some $g \in A$. Once given a generator polynomial g, then the classical circulant M_g is a generating matrix for $\mathcal{C}$ in the sense of Proposition 2.1 and one has

$$\mathcal{C} := \mathfrak{v}(\mathcal{J}) = \operatorname{im} M_g = \ker M_h, \tag{7.1}$$

where $h \in A$ generates the annihilator ideal of $\mathcal{J}$ in A and M_h is its circulant.

Usually, M_g is not an encoder for $\mathcal{C}$, which must have full rank. Such an encoder is obtained by extracting the first k rows of M_g, where $k = \dim_{\mathbb{F}} \mathcal{C} = \operatorname{rank} M_g$. Of course, the generator polynomial g is not unique and can be modified by multiplying with units u from A. For the circulants this amounts to multiplying by M_u from either side since classical circulants commute. There are two natural ways of choosing a specific g by imposing one of the conditions

$$g \,\big|\, x^n - 1 \;\text{ in } \mathbb{F}[x] \text{ and the leading coefficient is } 1 \tag{7.2}$$

or

$$g \;\text{ is idempotent.} \tag{7.3}$$

The first condition is more widely used and the name 'generator polynomial' usually refers to this choice. If both, g and h of (7.1) satisfy (7.2) then $gh = x^n - 1$ and h is just the complementing factor for g and this is what usually is meant when calling h a 'parity check polynomial'.

In the situation of (7.1) the dual code $\mathcal{C}^\perp := \{w \in \mathbb{F}^n \mid w\,{}^{\mathsf{t}}v = 0 \text{ for all } v \in \mathcal{C}\}$ is given by

$$\mathcal{C}^\perp = \operatorname{im} {}^{\mathsf{t}}M_h = \ker {}^{\mathsf{t}}M_g = \ker M_{\widehat{g}} = \operatorname{im} M_{\widehat{h}}, \tag{7.4}$$

where $\widehat{g}$ and $\widehat{h}$ are defined as in Lemma 6.2(d). Normalizing according to (7.2) leads to the polynomials $h(0)^{-1}x^k\widehat{h}$ (resp. $g(0)^{-1}x^{n-k}\widehat{g}$), the generator (resp. parity check) polynomial of $\mathcal{C}^\perp$, see e.g. [15, p. 196]. Here $h(0)$ and $g(0)$ denote the constant terms of h and g.

In this section we will show, that with the help of σ-circulants and the generator polynomials from Section 4 and 5 the complete scenario generalizes nicely to σ-CCC's. In addition, the basic notions of convolutional coding theory, like non-catastrophicity, minimality, and complexity, can be incorporated successfully.

Throughout this section let $\sigma \in \operatorname{Aut}_{\mathbb{F}}(A)$ be a fixed automorphism and, as before, let $\mathcal{R} := A[z;\sigma]$.

Recall from Observation 2.10(b) that a submodule $\mathcal{C} \subseteq \mathbb{F}[z]^n$ is called σ-cyclic if $\mathfrak{p}(\mathcal{C})$ is a left ideal in $\mathcal{R}$. Using the calculus of σ-circulants, this can also be expressed in terms of vector polynomials. One simply has to translate multiplication by x in $\mathcal{R}$ via the isomorphism $\mathfrak{v}$ into a suitable mapping $\mathfrak{m}$ on $\mathbb{F}[z]^n$. Observe that, due to noncommutativity of $\mathcal{R}$, this mapping is $\mathbb{F}$-linear but not $\mathbb{F}[z]$-linear.

Observation 7.1
A submodule $\mathcal{C} \subseteq \mathbb{F}[z]^n$ is σ-cyclic iff $\mathfrak{m}(\mathcal{C}) \subseteq \mathcal{C}$, where

$$\mathfrak{m} : \mathbb{F}[z]^n \longrightarrow \mathbb{F}[z]^n, \quad \sum_{\nu \geq 0} z^\nu v_\nu \longmapsto \sum_{\nu \geq 0} z^\nu v_\nu M_{\sigma^\nu(x)} = \sum_{\nu \geq 0} z^\nu v_\nu {P_\sigma}^{-\nu} S {P_\sigma}^{\nu}$$

and $S = M_x$, as in (6.1). *This follows from the fact that $\mathfrak{m}(v) = \mathfrak{v}(x\mathfrak{p}(v))$ for all $v \in \mathcal{C}$, which itself is equivalent to $\mathfrak{p}(\mathfrak{m}(v)) = x\mathfrak{p}(v)$ and this is a direct consequence of Proposition 6.8(b) and Lemma 6.4(2).*

Observe that for $\sigma = \mathrm{id}$ one has $M_{\sigma^\nu(x)} = S$ and $P_\sigma = I_n$ so that in this case $\mathfrak{m}$ describes the classical cyclic shift. Furthermore, if $\sigma(x) = x^m$ for some m that is coprime with n, then $M_{\sigma^\nu(x)} = M_{x^{(m^\nu)}} = S^{(m^\nu)}$ and one obtains the graded shift (2.9).

By Theorem 4.5 each delay-free σ-cyclic submodule is a principal left ideal when considered in $A[z;\sigma]$. Using the correspondence of σ-circulants and principal left ideals as described in Proposition 6.8(b) this immediately leads to a circulant generating matrix. Precisely, one has

$$\mathfrak{v}\big({}^{\bullet}\langle\, g \,\rangle\big) = \operatorname{im} \mathcal{M}^\sigma(g) \text{ for all } g \in \mathcal{R}. \tag{7.5}$$

As a consequence, a delay-free submodule $\mathcal{C} \subseteq \mathbb{F}[z]^n$ is σ-cyclic if and only if $\mathcal{C} = \operatorname{im} \mathcal{M}^\sigma(g)$ for some $g \in A[z;\sigma]$, which, additionally, can be taken as a reduced and normalized polynomial satisfying (4.4), see Corollary 4.13.

In order to also get a description of σ-cyclic codes by parity check polynomials and parity check matrices we need the following.

Definition 7.2
Let $F \subseteq \mathcal{R}$ be any subset. Then
(1) $F^{\circ} := \{h \in \mathcal{R} \mid \forall\, f \in F : fh = 0\}$.
(2) ${}^{\circ}F := \{g \in \mathcal{R} \mid \forall\, f \in F : gf = 0\}$.
We call F° and ${}^{\circ}F$ the right and left annihilator of the set F, respectively. Obviously, $F^{\circ} = {}^{\bullet}\langle\, F \,\rangle^{\circ}$ and ${}^{\circ}F = {}^{\circ}\langle\, F \,\rangle^{\bullet}$ are the right and left annihilator of the left and right ideal generated by F, respectively.

Using Observation 2.14 and the fact that $\mathbb{F}[z]$ does not contain any zero divisors of $\mathcal{R}$, one verifies straightforwardly the following.

Observation 7.3
The annihilators ${}^{\circ}F$ and F° are direct summands of $\mathcal{R}$ as left resp. right $\mathbb{F}[z]$-modules. In particular, both ideals are delay-free and by Theorem 4.5 and Corollary 4.17 are principal left resp. right ideals.

Now we have the following

Lemma 7.4
Let $g,\, h \in \mathcal{R}$. Then
(1) ${}^{\bullet}\langle g \rangle^{\circ} = \langle h \rangle^{\bullet} \Longleftrightarrow \ker {}^{\mathsf{t}}\mathcal{M}^{\sigma}(g) = \operatorname{im} {}^{\mathsf{t}}\mathcal{M}^{\sigma}(h)$.
(2) ${}^{\bullet}\langle g \rangle = {}^{\circ}\langle h \rangle^{\bullet} \Longleftrightarrow \operatorname{im} \mathcal{M}^{\sigma}(g) = \ker \mathcal{M}^{\sigma}(h)$.
Furthermore, if the identities in equivalence in (1) (resp. (2)) are satisfied, then the matrix $\mathcal{M}^{\sigma}(h)$ (resp. $\mathcal{M}^{\sigma}(g)$) is basic.

PROOF: (1) can be established as follows.

$$\begin{aligned}
&{}^{\bullet}\langle g \rangle^{\circ} = \langle h \rangle^{\bullet} \\
&\quad \Longleftrightarrow gh = 0 \text{ and } [gf = 0 \Longrightarrow \exists\, a \in \mathcal{R} : f = ha] \\
&\quad \Longleftrightarrow \mathcal{M}^{\sigma}(g)\mathcal{M}^{\sigma}(h) = 0 \text{ and } [\mathcal{M}^{\sigma}(g)\mathcal{M}^{\sigma}(f) = 0 \Longrightarrow \exists\, a \in \mathcal{R} : \mathcal{M}^{\sigma}(f) = \mathcal{M}^{\sigma}(h)\mathcal{M}^{\sigma}(a)] \\
&\quad \Longleftrightarrow {}^{\mathsf{t}}\mathcal{M}^{\sigma}(h){}^{\mathsf{t}}\mathcal{M}^{\sigma}(g) = 0 \text{ and } [{}^{\mathsf{t}}\mathcal{M}^{\sigma}(f){}^{\mathsf{t}}\mathcal{M}^{\sigma}(g) = 0 \Rightarrow \exists\, a \in \mathcal{R} : {}^{\mathsf{t}}\mathcal{M}^{\sigma}(f) = {}^{\mathsf{t}}\mathcal{M}^{\sigma}(a){}^{\mathsf{t}}\mathcal{M}^{\sigma}(h)].
\end{aligned}$$

The last statement is satisfies if and only if $\ker {}^{\mathsf{t}}\mathcal{M}^{\sigma}(g) = \operatorname{im} {}^{\mathsf{t}}\mathcal{M}^{\sigma}(h)$, which can be seen as follows.
For the if-part only the implication in brackets needs proof. But this is obtained from Corollary 6.14(2) since ${}^{\mathsf{t}}\mathcal{M}^{\sigma}(f){}^{\mathsf{t}}\mathcal{M}^{\sigma}(g) = 0$ along with the assumption implies $\operatorname{im} {}^{\mathsf{t}}\mathcal{M}^{\sigma}(f) \subseteq \operatorname{im} {}^{\mathsf{t}}\mathcal{M}^{\sigma}(h)$, hence $\mathcal{M}^{\sigma}(f) = \mathcal{M}^{\sigma}(h)Q$ for some matrix Q and the corollary applies.
For the only-if-part we have to show that $\ker {}^{\mathsf{t}}\mathcal{M}^{\sigma}(g) \subseteq \operatorname{im} {}^{\mathsf{t}}\mathcal{M}^{\sigma}(h)$. Thus let $v\,{}^{\mathsf{t}}\mathcal{M}^{\sigma}(g) = 0$ for some $v \in \mathbb{F}[z]^n$. By Corollary 6.14(1) we obtain $\mathcal{M}^{\sigma}(g)\mathcal{M}^{\sigma}(\widehat{f}^{\widehat{\sigma}}) = 0$, where $f = \mathfrak{p}(v) \in A[z;\widehat{\sigma}]$. Then the assumption implies that $\mathcal{M}^{\widehat{\sigma}}(f) = {}^{\mathsf{t}}\mathcal{M}^{\sigma}(\widehat{f}^{\widehat{\sigma}}) = {}^{\mathsf{t}}\mathcal{M}^{\sigma}(a){}^{\mathsf{t}}\mathcal{M}^{\sigma}(h)$ for some $a \in A[z;\sigma]$ and hence $v \in \operatorname{im} {}^{\mathsf{t}}\mathcal{M}^{\sigma}(h)$.
(2) In this case the anti-isomorphism $\widehat{\ }^{\sigma}$ of Theorem 6.13(b) yields ${}^{\bullet}\langle g \rangle = {}^{\circ}\langle h \rangle^{\bullet}$ in $A[z;\sigma]$ if and only if $\langle \widehat{g}^{\sigma} \rangle^{\bullet} = {}^{\bullet}\langle \widehat{h}^{\sigma} \rangle^{\circ}$ in $A[z;\widehat{\sigma}]$. Thus, use of (1) and Theorem 6.13(a) leads to the desired result.
The additional assertion that the two given matrices are basic follows either from the equivalence of Proposition 2.2(6) and (3) or from the direct summand property as stated in Observation 7.3 together with 2.2(5). □

The following theorem collects the basic facts on σ-CCC's. Recall that transposes of σ-circulants are $\widehat{\sigma}$-circulants. Therefore, the dual code of a σ-CCC corresponds to a left ideal in the Piret algebra $A[z;\widehat{\sigma}]$. For simplicity, we use the notation ${}^{\bullet}\langle\ \ \rangle$ for left ideals in either Piret algebra; yet, in order to avoid confusion, we will make the corresponding algebra precise at each point. Recall also that the isomorphism $\mathfrak{p}$ in (2.8) does not depend on the multiplicative structure of the set $A[z]$ so that we may use it for either Piret algebra.

Theorem 7.5
Let $\mathcal{C} \subseteq \mathbb{F}[z]^n$ be a σ-cyclic code and let

$$\mathcal{C}^{\perp} := \left\{ w \in \mathbb{F}[z]^n \,\middle|\, w\,{}^{\mathsf{t}}v = 0 \textit{ for all } v \in \mathcal{C} \right\}$$

be its dual code. Furthermore, let $g,\, h \in A[z;\sigma]$ *be such that* $\mathfrak{p}(\mathcal{C}) = {}^{\bullet}\!\langle\, g\,\rangle$ *and* ${}^{\bullet}\!\langle\, g\,\rangle^{\circ} = \langle\, h\,\rangle^{\bullet}$*. Then*

(a) $\mathcal{M}^{\sigma}(g)$ *and* $\mathcal{M}^{\sigma}(h)$ *are both basic.*

(b) $\mathcal{C} = \operatorname{im}\mathcal{M}^{\sigma}(g) = \ker\mathcal{M}^{\sigma}(h)$.

(c) $\mathfrak{p}(\mathcal{C}) = {}^{\bullet}\!\langle\, g\,\rangle = {}^{\circ}\!\langle\, h\,\rangle^{\bullet}$ *in* $A[z;\sigma]$.

(d) $\mathcal{C}^{\perp} = \ker\mathcal{M}^{\widehat{\sigma}}(\widehat{g}^{\sigma}) = \operatorname{im}\mathcal{M}^{\widehat{\sigma}}(\widehat{h}^{\sigma})$.

(e) $\mathfrak{p}(\mathcal{C}^{\perp}) = {}^{\bullet}\!\langle\, \widehat{h}^{\sigma}\,\rangle = {}^{\circ}\!\langle\, \widehat{g}^{\sigma}\,\rangle^{\bullet}$ *in the Piret algebra* $A[z;\widehat{\sigma}]$*. Hence the dual of a* σ*-CCC is a* $\widehat{\sigma}$*-CCC.*

PROOF: (a) $\mathcal{M}^{\sigma}(g)$ is basic since it generates a code, see Proposition 2.2(3); $\mathcal{M}^{\sigma}(h)$ is basic by Lemma 7.4.
(b) $\mathcal{C} = \operatorname{im}\mathcal{M}^{\sigma}(g) \subseteq \ker\mathcal{M}^{\sigma}(h)$ follows from the choice of g and h, see also (7.5). Furthermore, by Lemma 7.4(1), $\ker{}^{\mathsf{t}}\mathcal{M}^{\sigma}(g) = \operatorname{im}{}^{\mathsf{t}}\mathcal{M}^{\sigma}(h)$ and thus $\operatorname{rank}\mathcal{M}^{\sigma}(h) = n - \operatorname{rank}\mathcal{M}^{\sigma}(g)$. But then Proposition 2.2(7) yields $\mathcal{C} = \ker\mathcal{M}^{\sigma}(h)$ since $\mathcal{C}$ is a direct summand.
(c) is a consequence of (b) along with Lemma 7.4(2).
(d) follows from the obvious fact that $\mathcal{C}^{\perp} = \ker{}^{\mathsf{t}}\mathcal{M}^{\sigma}(g) = \operatorname{im}{}^{\mathsf{t}}\mathcal{M}^{\sigma}(h)$.
(e) is a consequence of (d) along with Lemma 7.4(2). □

These results motivate the following definition.

Definition 7.6
Let $\mathcal{C} \subseteq \mathbb{F}[z]^n$ *be a* σ*-cyclic code and* $g,\, h \in \mathcal{R}$ *be such that* $\mathfrak{p}(\mathcal{C}) = {}^{\bullet}\!\langle\, g\,\rangle$ *and* $\mathfrak{p}(\mathcal{C})^{\circ} = \langle\, h\,\rangle^{\bullet}$*. Then we call* g *a generator polynomial and* h *a parity check polynomial of the code* $\mathcal{C}$*. Consequently, the polynomials* $\widehat{h}^{\sigma}$ *and* $\widehat{g}^{\sigma} \in A[z;\widehat{\sigma}]$ *are a generator and a parity check polynomial of the dual code* $\mathcal{C}^{\perp}$*, respectively.*

At this point there is no need to normalize generator and parity check polynomials. But there is a way to obtain uniqueness by requiring g and $\widehat{h}^{\sigma}$ to be left reduced and their z-free terms to be normalized according to (7.2) or (7.3).

Via the anti-isomorphism $\widehat{\ }^{\sigma} : A[z;\sigma] \longrightarrow A[z;\widehat{\sigma}],\ g \longmapsto \widehat{g}^{\sigma}$ from Theorem 6.13, one observes that the right annihilator $\langle\, h\,\rangle^{\bullet}$ of the code $\mathcal{C} = \mathfrak{v}({}^{\bullet}\!\langle\, g\,\rangle)$ is anti-isomorphic to the dual code $\mathcal{C}^{\perp} = \mathfrak{v}({}^{\bullet}\!\langle\, \widehat{h}^{\sigma}\,\rangle)$.

The following very detailed example is designed to shed some light on all aspects of our setting thus far.

Example 7.7
Consider again Example 6.10 where $\mathbb{F} = \mathbb{F}_4$, $n = 5$, and $\sigma(x) = x^2$. The circulant $\mathcal{M}^{\sigma}(g)$ associated with the polynomial

$$g := 1 + \alpha^2 x + \alpha^2 x^2 + x^3 + z(1 + x + \alpha^2 x^2 + \alpha^2 x^4) \in A[z;\sigma]$$

can be shown to be basic. Since $\operatorname{rank}\mathcal{M}^{\sigma}(g) = 2$, it defines a 2-dimensional σ-cyclic code $\mathcal{C} \subseteq \mathbb{F}[z]^5$. A parity check polynomial, i. e. a right annihilator of the left ideal ${}^{\bullet}\!\langle\, g\,\rangle \in A[z;\sigma]$ can be found as follows. First we compute a basis $w_1,\, w_2,\, w_3 \in \mathbb{F}[z]^5$ of the right kernel of $\mathcal{M}^\sigma(g)$, i. e. $\mathcal{M}^\sigma(g)\,{}^{\mathsf{t}}w_i = 0$ for $i = 1, 2, 3$. This can easily be achieved by use of a Smith-form of $\mathcal{M}^\sigma(g)$ and yields the basic matrix

$$H := \left[{}^{\mathsf{t}}w_1, {}^{\mathsf{t}}w_2, {}^{\mathsf{t}}w_3\right] = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1+z\alpha^2 & z\alpha^2 & \alpha+z\alpha+z^2 \\ \alpha+z & \alpha^2+z & 1+z+z^2\alpha \\ \alpha+z\alpha^2 & \alpha^2+z\alpha^2 & \alpha+z^2 \end{bmatrix}.$$

Then $\mathrm{im}\,{}^{\mathsf{t}}H = \ker \mathcal{M}^{\widehat{\sigma}}(\widehat{g}^{\sigma})$ and any parity check polynomial $h \in A[z;\sigma]$ of $\mathcal{C}$ satisfies $\mathrm{im}\,{}^{\mathsf{t}}H = \mathrm{im}\,{}^{\mathsf{t}}\mathcal{M}^\sigma(h) = \mathrm{im}\,\mathcal{M}^{\widehat{\sigma}}(h')$ where $h' := \widehat{h}^{\sigma}$. In the Piret algebra $A[z;\widehat{\sigma}]$ this reads as ${}^{\bullet}\langle\, \mathfrak{p}(w_1), \mathfrak{p}(w_2), \mathfrak{p}(w_3)\,\rangle = {}^{\bullet}\langle\, h'\,\rangle$ and thus we need to find a principal generator of this left ideal in $A[z;\widehat{\sigma}]$. Hence put

$$\begin{aligned} f_1 &:= \mathfrak{p}({}^{\mathsf{t}}w_1) = 1 + x^2 + \alpha x^3 + \alpha x^4 + z(\alpha^2x^2 + x^3 + \alpha^2x^4), \\ f_2 &:= \mathfrak{p}({}^{\mathsf{t}}w_2) = x + \alpha^2x^3 + \alpha^2x^4 + z(\alpha^2x^2 + x^3 + \alpha^2x^4), \\ f_3 &:= \mathfrak{p}({}^{\mathsf{t}}w_3) = \alpha x^2 + x^3 + \alpha x^4 + z(\alpha x^2 + x^3) + z^2(x^2 + \alpha x^3 + x^4). \end{aligned}$$

By Observation 7.3 we know that $\langle\, h\,\rangle^{\bullet}$ is delay-free, thus, using the anti-automorphism between $A[z;\sigma]$ and $A[z;\widehat{\sigma}]$, we get the delay-freeness of the left ideal ${}^{\bullet}\langle\, h'\,\rangle$ in $A[z;\widehat{\sigma}]$. As a consequence, application of Algorithm 5.2 to the family f_1, f_2, f_3 produces the desired principal generator $h' \in A[z;\widehat{\sigma}]$, even in reduced form. In order to actually perform these computation we first need to know the automorphism $\widehat{\sigma}$. Using Remark 6.12 we find $\widehat{\sigma}(x) = x^3$. Furthermore, the algorithm needs a decomposition of $A \cong \mathbb{F}[x]/\langle x^5 - 1\rangle$ into a direct sum of fields and the representation of the automorphism $\widehat{\sigma}$ as well as the given data in the according form. For this task we may use the list in Example 3.3(b). Switching to the notation of the second column therein we find $\widehat{\sigma}[a, b, c] = [a, \Psi^{-1}(c), \Psi(b)^4]$ where Ψ is as in (3.12). Furthermore, using the Chinese Remainder Theorem, precisely the map ϱ given in (3.4), the polynomials f_1, f_2, f_3 turn into

$$\begin{aligned} \varrho(f_1) = h_1 &:= \varepsilon^{(2)}\alpha^2x + z\varepsilon^{(1)} + z\varepsilon^{(3)}(\alpha x + \alpha), \\ \varrho(f_2) = h_2 &:= \varepsilon^{(1)} + \varepsilon^{(2)}\alpha^2x + z\varepsilon^{(1)} + z\varepsilon^{(3)}(\alpha x + \alpha), \\ \varrho(f_3) = h_3 &:= \varepsilon^{(1)} + \varepsilon^{(2)}(\alpha^2x + \alpha^2) + z\varepsilon^{(1)}\alpha^2 + z\varepsilon^{(2)}x + z\varepsilon^{(3)}(\alpha x + 1) \\ &\qquad + z^2\varepsilon^{(1)}\alpha + z^2\varepsilon^{(3)}(\alpha^2x + \alpha^2), \end{aligned}$$

where $\varepsilon^{(1)} = [1, 0, 0]$, $\varepsilon^{(2)} = [0, 1, 0]$, $\varepsilon^{(3)} = [0, 0, 1]$. Now we may run Algorithm 5.2 on the data h_1, h_2, h_3. Exactly this has been done in Example 5.3. Therein, a principal generator of the left ideal ${}^{\bullet}\langle\, h_1, h_2, h_3\,\rangle$ in $A[z;\widehat{\sigma}]$ was found to be the reduced and normalized polynomial

$$h'' := \varepsilon^{(1)} + \varepsilon^{(2)} + z\varepsilon^{(3)}. \tag{7.6}$$

Translating this back we obtain

$$h' := \varrho^{-1}(h'') = 1 + \alpha^2x + \alpha x^2 + \alpha x^3 + \alpha^2x^4 + z(\alpha^2x + \alpha x^2 + \alpha x^3 + \alpha^2x^4) \tag{7.7}$$

and finally the parity check polynomial

$$h = \widehat{h'}^{\widehat{\sigma}} = 1 + \alpha^2x + \alpha x^2 + \alpha x^3 + \alpha^2x^4 + z(\alpha x + \alpha^2x^2 + \alpha^2x^3 + \alpha x^4) \tag{7.8}$$

of the code $\mathcal{C}$ as well as the associated circulant parity check matrix

$$\mathcal{M}^{\sigma}(h) = \begin{bmatrix} 1 & \alpha^2+z\alpha & \alpha+z\alpha^2 & \alpha+z\alpha^2 & \alpha^2+z\alpha \\ \alpha^2+z\alpha^2 & 1+z\alpha & \alpha^2 & \alpha+z\alpha & \alpha+z\alpha^2 \\ \alpha+z\alpha & \alpha^2+z\alpha^2 & 1+z\alpha^2 & \alpha^2+z\alpha & \alpha \\ \alpha+z\alpha & \alpha & \alpha^2+z\alpha & 1+z\alpha^2 & \alpha^2+z\alpha^2 \\ \alpha^2+z\alpha^2 & \alpha+z\alpha^2 & \alpha+z\alpha & \alpha^2 & 1+z\alpha \end{bmatrix}. \tag{7.9}$$

Notice also that by Theorem 7.5 the polynomial $h' \in A[z;\widehat{\sigma}]$ is a generator polynomial of the dual code $\mathcal{C}^{\perp}$. A parity check polynomial of that code is easily computed as

$$g' := \widehat{g}^{\,\sigma} = 1 + x^2 + \alpha^2x^3 + \alpha^2x^4 + z(1 + x^2 + \alpha^2x^3 + \alpha^2x^4)$$

Altogether we have

$$\mathfrak{p}(\mathcal{C}) = {}^{\bullet}\langle\, g\,\rangle = {}^{\circ}\langle\, h\,\rangle^{\bullet} \subseteq A[z;\sigma], \quad \mathfrak{p}(\mathcal{C}^{\perp}) = {}^{\bullet}\langle\, h'\,\rangle = {}^{\circ}\langle\, g'\,\rangle^{\bullet} \subseteq A[z;\widehat{\sigma}].$$

It is worth mentioning that the code $\mathcal{C}$ has free distance equal to 8. This is optimal among all codes with the same parameters (length $n = 5$, dimension $k = 2$, complexity $\delta = 2$, memory $m = 1$, and field size $|\mathbb{F}| = q = 4$) according to the Heller bound (see [8, Thm. 3.4] or [12, p. 132] for the binary case)

$$d_{\text{free}} \le \min\left\{ \left\lfloor \frac{n(m+i)q^{k(m+i)-\delta-1}(q-1)}{q^{k(m+i)-\delta}-1} \right\rfloor \;\middle|\; i \in \mathbb{N} \right\}$$

(the memory is the largest row degree appearing in a minimal generator matrix in the sense of Definition 7.12 below). The free distance of the dual is 5, attained by the constant codeword $v := (\alpha,\alpha,\alpha,\alpha,\alpha) = (1,\alpha,1,0,0)^{\mathsf{t}}\mathcal{M}^{\sigma}(h)$. The dual code can also be regarded as optimal among all codes with the same parameters, since each code with complexity 2 and dimension 3 has to contain a constant codeword. This follows from the existence of minimal generator matrices in the sense of Definition 7.12 and the alternative characterizations given in [5, p. 495]. □

Next we will investigate the dimension of a σ-CCC, i. e. the rank of a σ-circulant, in terms of a given generator polynomial. For a classical circulant the rank of M_g can be read off from the polynomial $g \in A$ via the formula given in Lemma 6.2(d). Furthermore, the result shows how to cut out a rectangular generator matrix of full rank from the square singular circulant M_g. For σ-circulants these results are not true in this generality. For instance, the matrix $\mathcal{M}^{\sigma}(h)$ above is basic of rank 3, hence $\operatorname{im}\mathcal{M}^{\sigma}(h)$ is a 3-dimensional σ-CCC, but the first 3 rows do not form a generator matrix of that code, since one can show that $z^2 + z\alpha + \alpha$ is a common factor of the full size minors of that 3×5-matrix.

However, as we will show next, choosing a reduced generator g of the ideal $\mathfrak{p}(\mathcal{C})$ always leads to a rectangular full rank generator matrix of $\mathcal{C} = \operatorname{im}\mathcal{M}^{\sigma}(g)$ formed by the appropriate number of rows of the σ-circulant. In order to prove this result we have to combine the techniques of this section with the results and methods of the two foregoing sections. It is quite advantageous to give some technicalities beforehand. We will make use of the framework as in (3.1) – (3.7). In particular, let $x^n - 1 = \pi_1 \cdot \ldots \cdot \pi_r$ be the decomposition of $x^n - 1$ into its prime factors and for each $k = 1, \ldots, r$, let $\varepsilon^{(k)}$ be the irreducible idempotent associated with π_k, i. e. $\varepsilon^{(k)} A =: K^{(k)} \cong \mathbb{F}[x]/\langle \pi_k \rangle$. Then $\pi_k \varepsilon^{(k)} = 0$ when considered in A and

$$\pi_k \mid a \ \text{ in } \mathbb{F}[x] \iff a\varepsilon^{(k)} = 0 \tag{7.10}$$

for all $a \in A$. For each $g \in \mathcal{R}$ we define

$$\pi_{(g)} := \prod_{k \in T_g} \pi_k \in \mathbb{F}[x], \tag{7.11}$$

where, as before, T_g denotes the support of g, see Notation 4.1. Then $T_{\pi_{(g)}} \cap T_g = \varnothing$ and $T_{\pi_{(g)}} \cup T_g = \{1, \ldots, r\}$ by Equation (7.10) and thus

$$\pi_{(g)} g = 0 \text{ in } \mathcal{R}. \tag{7.12}$$

In the case where $T_g = T_{g_0}$ one can alternatively express $\pi_{(g)}$ as $\pi_{(g)} = \frac{x^n - 1}{\gcd(g_0, x^n - 1)}$.

Now we are in a position to show

Theorem 7.8
Let $g \in \mathcal{R}$ be a reduced and nonzero polynomial and let $\kappa := \deg_x \pi_{(g)}$. Then the family

$$g, xg, \ldots, x^{\kappa - 1} g \tag{7.13}$$

is a left $\mathbb{F}[z]$-basis of ${}^{\bullet}\langle\, g \,\rangle$. Equivalently, $\operatorname{rank} \mathcal{M}^{\sigma}(g) = \kappa$ *and the first κ rows of $\mathcal{M}^{\sigma}(g)$ form a full rank generator matrix $G \in \mathbb{F}[z]^{\kappa \times n}$ of the σ-cyclic submodule $\mathcal{C} := \mathfrak{v}\big({}^{\bullet}\langle\, g \,\rangle\big) \subseteq \mathbb{F}[z]^n$. Furthermore, if $\mathcal{C}$ is a code, i. e. the matrix $\mathcal{M}^{\sigma}(g)$ is basic, then G is basic, too.*

Proof: Only the first part needs proof. In order to establish left $\mathbb{F}[z]$-independence of the family in (7.13) let $u_i = \sum_{\nu=0}^{d_i} z^\nu u_{i\nu}$, where $u_{i\nu} \in \mathbb{F}$ and $i = 0, \ldots, \kappa - 1$, and suppose $\sum_{i=0}^{\kappa-1} u_i x^i g = 0$. Accepting possible zero-coefficients, we may assume $d_i = d$ for $0 \le i \le \kappa - 1$. Letting $f_\nu := \sum_{i=0}^{\kappa-1} u_{i\nu} x^i \in A$ and $f := \sum_{\nu=0}^{d} z^\nu f_\nu$ we obtain

$$0 = fg = fg^{(1)} + \cdots + fg^{(r)}$$

and by Lemma 4.14(c) and 4.3(d) we conclude that $f\varepsilon^{(k)} = 0$ for $k \in T_g$. The definition of f shows that then also $f_\nu \varepsilon^{(k)} = 0$ for all $0 \le \nu \le d$ and all $k \in T_g$. Using (7.10) we obtain $\pi_k \mid f_\nu$ in $\mathbb{F}[x]$ for all $k \in T_g$ and thus $\pi_{(g)} \mid f_\nu$ in $\mathbb{F}[x]$. Since $\deg_x(\pi_{(g)}) = \kappa > \deg_x f_\nu$, the latter implies $f_\nu = 0$ for all $\nu = 0, \ldots, d$. But then also $u_0 = \ldots = u_{\kappa-1} = 0$, showing the independence of the given family.
It remains to show that for $\kappa' \ge \kappa$ the polynomial $x^{\kappa'} g$ can be generated with coefficients from $\mathbb{F}[z]$ by the family (7.13). This is indeed the case (even with coefficients from $\mathbb{F}$) as can be deduced recursively from (7.12) by using the fact that the coefficients of $\pi_{(g)}$ are in $\mathbb{F}$ and thus commute with x. $\square$

One should observe that a constant polynomial, i. e. $g \in A$, is always reduced and in this case $\pi_{(g)} = \frac{x^n - 1}{\gcd(x^n - 1, g)}$, see (7.10). Hence Theorem 7.8 provides a generalization of the rank formula for classical circulants given in Lemma 6.2(d).

The last part of the proof above shows that even for non-reduced polynomials g the family in (7.13) is a generating system of the left $\mathbb{F}[z]$-module ${}^{\bullet}\langle\, g\,\rangle$. However, in this case the family need not be independent, or equivalently, κ might be strictly bigger than $\operatorname{rank}\mathcal{M}^{\sigma}(g)$. We will show an example below in part (3).

Example 7.9
Let us reconsider Example 7.7 along with the various representations.

(1) The polynomial g is reduced since $\varrho(g) = \varepsilon^{(3)}(\alpha x+1) + z\varepsilon^{(2)}(\alpha^2 x+\alpha^2) = \varepsilon^{(3)}\varrho(g)$. Normalization of this polynomial has been performed in Example 4.4. As stated in Example 7.7, the associated σ-circulant has rank 2 which is also in accordance with the theorem above since $\pi_{(g)} = \pi_3 = x^2+\alpha^2 x+1$. Furthermore, as stated in the theorem, the first two rows of $\mathcal{M}^{\sigma}(g)$ form a generator matrix of the code $\mathcal{C} = \mathfrak{v}\big({}^{\bullet}\langle\, g\,\rangle\big)$, which can also be checked directly.

(2) The dual code is given by $\mathcal{C}^{\perp} = \operatorname{im}\mathcal{M}^{\widehat{\sigma}}(h')$ where h' is as in (7.7). Since h' was the output of the reduction algorithm, it is reduced and thus Theorem 7.8 is applicable again. As can be seen from (7.6) we now have $\pi_{(h)} = \pi_1\pi_2$, thus $\kappa = 3$ telling us that the first three rows of $\mathcal{M}^{\widehat{\sigma}}(h')$ form a (basic) matrix of rank 3.

(3) Let us also consider the code $\mathcal{C}' := \operatorname{im}\mathcal{M}^{\sigma}(h) \subseteq \mathbb{F}[z]^n$, where h is as in (7.8). In this case the polynomial h is not reduced as one can see from $\varrho(h) = \varepsilon^{(2)} + \varepsilon^{(1)} + z\varepsilon^{(2)}$. The matrix $\mathcal{M}^{\sigma}(h)$ is basic of rank 3 (see Lemma 7.4) but the first three rows do not span the code $\mathcal{C}'$. Reduction of h leads to the polynomial $\tilde{h}$ where $\varrho(\tilde{h}) = \varepsilon^{(2)} + \varepsilon^{(1)}$. Since $\tilde{h} \in A$, we now get that $\mathcal{M}^{\sigma}(\tilde{h}) = M_{\tilde{h}}$ is a classical circulant and the code $\mathcal{C}'$ a 3-dimensional cyclic block code. Let us compare this with Theorem 7.8. Despite the non-reducedness of the polynomial we can calculate the polynomial $\pi_{(h)}$ and obtain $\pi_{(h)} = \pi_1\pi_2\pi_3 = x^5-1$. Thus $\kappa = 5 > \operatorname{rank}\mathcal{M}^{\sigma}(h)$ and the family in (7.13) is not $\mathbb{F}[z]$-linearly independent, but certainly an $\mathbb{F}[z]$-generating set of ${}^{\bullet}\langle\, h\,\rangle$. On the other hand, the reduced polynomial $\tilde{h}$ satisfies $\pi_{(\tilde{h})} = \pi_1\pi_2$, thus $\kappa = 3$ in accordance with $\operatorname{rank}\mathcal{M}^{\sigma}(h) = \operatorname{rank}\mathcal{M}^{\sigma}(\tilde{h}) = 3$. □

Now we are also in a position to characterize the reduced polynomials g which generate a code, in other words, for which $\mathcal{M}^{\sigma}(g)$ is basic.

Proposition 7.10
Let $g \in \mathcal{R}$ be a nonzero reduced polynomial with z-free term g_0. Then

$$\begin{aligned}
\mathcal{M}^{\sigma}(g) \text{ is basic } &\Longleftrightarrow {}^{\bullet}\langle\, \widehat{g}^{\,\sigma}\,\rangle = {}^{\bullet}\langle\, \widehat{g_0}\,\rangle \text{ in } A[z;\widehat{\sigma}]\\
&\Longleftrightarrow u\widehat{g}^{\,\sigma} = \widehat{g_0} \in A[z;\widehat{\sigma}] \text{ for some unit } u \text{ in } A[z;\widehat{\sigma}]\\
&\Longleftrightarrow gv = g_0 \text{ for some unit } v \text{ in } A[z;\sigma]\\
&\Longleftrightarrow \langle\, g\,\rangle^{\bullet} = \langle\, g_0\,\rangle^{\bullet}.
\end{aligned} \tag{7.14}$$

In other words, $\mathcal{M}^{\sigma}(g)$ is basic if and only if ${}^{\mathsf{t}}\mathcal{M}^{\sigma}(g)$ generates the cyclic block code $\operatorname{im}{}^{\mathsf{t}}M_{g_0}$.

One should note that the second equivalence says that $\widehat{g}^{\,\sigma}$ is left reducible to the constant $\widehat{g_0}$. It can be shown by examples, that the first equivalence is not true if g is not reduced.

Proof: Let $\pi = \pi_{(g)}$ be as in (7.11). Then $\mathcal{M}^{\sigma}(\pi)\mathcal{M}^{\sigma}(g) = M_{\pi}\mathcal{M}^{\sigma}(g) = 0$ and by Theorem 7.8 (see also Lemma 6.2(d)) we have $\operatorname{rank}\mathcal{M}^{\sigma}(g) = n - \operatorname{rank} M_{\pi}$. Therefore and upon using Proposition 2.2 and Lemma 7.4 we obtain

$$\mathcal{M}^{\sigma}(g) \text{ basic } \iff \operatorname{im}{}^{\mathsf{t}}\mathcal{M}^{\sigma}(g) = \ker{}^{\mathsf{t}}M_{\pi} \iff \operatorname{im}\mathcal{M}^{\widehat{\sigma}}(\widehat{g}^{\sigma}) = \ker M_{\widehat{\pi}} \iff {}^{\bullet}\langle\, \widehat{g}^{\sigma} \,\rangle = {}^{\circ}\langle\, \widehat{\pi} \,\rangle^{\bullet}\ .$$

Since $\widehat{\pi} \in A$ we have ${}^{\circ}\langle\, \widehat{\pi} \,\rangle^{\bullet} = {}^{\bullet}\langle\, \widehat{a} \,\rangle$ for $\widehat{a} = \frac{x^n-1}{\gcd(x^n-1,\widehat{\pi})} \in A$. Hence $\mathcal{M}^{\sigma}(g)$ is basic if and only if $\widehat{g}^{\sigma}$ can be left reduced to the constant $\widehat{a}$. By Corollary 4.13 this is equivalent to the existence of some unit $u \in A[z;\widehat{\sigma}]$ such that $u\widehat{g}^{\sigma} = \widehat{a}$. Since the z-free term u_0 of u is a unit in A and the z-free term of $\widehat{g}^{\sigma}$ is given by $\widehat{g_0}$, we obtain the identity $u_0\widehat{g_0} = \widehat{a}$ and without restriction we may assume $\widehat{a} = \widehat{g_0}$. This yields the desired result. □

It is straightforward to deduce from (7.14) that a σ-CCC always has a direct complement in $\mathbb{F}[z]^n$ that is σ-cyclic, too. In other words, a left ideal that is a direct summand of the left $\mathbb{F}[z]$-module $A[z;\sigma]$ is also a direct summand of the left $A[z;\sigma]$-module $A[z;\sigma]$, see [7, Thm. 2.9]. The proposition above has another interesting consequence.

Corollary 7.11
Let $g,\ h \in \mathcal{R}$ such that ${}^{\bullet}\langle\, g \,\rangle^{\circ} = \langle\, h \,\rangle^{\bullet}$ and $g \in A[z;\sigma]$ and $\widehat{h}^{\sigma} \in A[z;\widehat{\sigma}]$ are both left reduced, which can be assumed without restriction. Furthermore, assume that g generates a code, thus $\mathcal{M}^{\sigma}(g)$ is basic. Then $hg = 0$ and even

$${}^{\bullet}\langle\, h \,\rangle^{\circ} = \langle\, g \,\rangle^{\bullet}.$$

In particular, the identity $\mathcal{M}^{\sigma}(g)\mathcal{M}^{\sigma}(h) = 0$ implies that also $\mathcal{M}^{\sigma}(h)\mathcal{M}^{\sigma}(g) = 0$.

Again, the result is not true if any of the polynomials is not reduced.

Proof: First notice that $\mathcal{M}^{\sigma}(h)$ is basic by assumption, see Lemma 7.4. Thus, we may apply Proposition 7.10 to the polynomials g and $\widehat{h}^{\sigma}$ in their respective Piret algebras and obtain $gu = g_0$ and $\widehat{h}^{\sigma} v = \widehat{h_0}$ for some units $u \in A[z;\sigma]$ and $v \in A[z;\widehat{\sigma}]$. Then $gh = 0$ implies $0 = g_0h_0 = h_0g_0$, since A is commutative, and thus $0 = \widehat{v}^{\widehat{\sigma}}hgu$, after applying the anti-isomorphism $\widehat{\ }^{\widehat{\sigma}}$. Cancellation of the units yields $hg = 0$ and thus $\operatorname{im}\mathcal{M}^{\sigma}(h) \subseteq \ker\mathcal{M}^{\sigma}(g)$. Furthermore, from Lemma 7.4 we know that $\operatorname{rank}\mathcal{M}^{\sigma}(g) = n - \operatorname{rank}\mathcal{M}^{\sigma}(h)$ and since $\mathcal{M}^{\sigma}(h)$ is basic we may apply Proposition 2.2(7) in order to get $\operatorname{im}\mathcal{M}^{\sigma}(h) = \ker\mathcal{M}^{\sigma}(g)$. Then Lemma 7.4(2) completes the proof. □

As a by-product, Proposition 7.10 gives us an alternative proof of Proposition 2.7 since in the case where $\sigma = \mathrm{id}$, the ring $A[z;\sigma]$ is commutative and therefore (7.14) is the same as $vg = g_0$ so that, consequently, the corresponding left ideal has a constant generator.

Finally, it remains to discuss the important issue of minimal generator matrices. In convolutional coding theory one is mainly interested in minimal encoding matrices since they have, by definition, minimum possible row degrees, so that, as a consequence, their canonical linear shift realization needs the minimum number of memory elements; for details see [12, Sec. 2.7]. The row Hermite form of a polynomial matrix usually tends to have artificially high degrees in its entries and therefore is not minimal. The following definition is adapted to our purposes. More common but equivalent definitions can also be found e. g. in [5, p. 495].

Definition 7.12
Let $M \in \mathbb{F}[z]^{m\times n}$ be a matrix with rows $w_1,\dots,w_m \in \mathbb{F}[z]^n$ and $\operatorname{rank}_{\mathbb{F}[z]} M = m$. *The leading z-coefficient vector of w_i will be denoted by* $\mathrm{lc}_z(w_i) \in \mathbb{F}^n$. *The matrix M is called (row-) minimal if its (row-) leading coefficient matrix*

$$L(M) := \begin{bmatrix} \mathrm{lc}_z(w_1) \\ \mathrm{lc}_z(w_2) \\ \vdots \\ \mathrm{lc}_z(w_m) \end{bmatrix} \in \mathbb{F}^{m\times n}$$

satisfies $\operatorname{rank}_{\mathbb{F}} L(M) = m$.

It can easily be seen via some examples that the full rank generator matrix of a σ-CCC as constructed in Theorem 7.8 in general is not minimal. This is, for instance, the case for the matrix $\widehat{G}$ formed by the first three rows of $\mathcal{M}^{\widehat{\sigma}}(h') = {}^{\mathsf{t}}\mathcal{M}^{\sigma}(h)$ in Example 7.7. The matrix $\widehat{G}$ is a basic generator matrix of the dual code $\mathcal{C}^{\perp}$, but not minimal.

We will now show, how one can obtain a minimal generator matrix by extracting the appropriate number of first rows of the circulants associated with the components of a reduced generator polynomial.

Theorem 7.13
(a) *Let $g^{(k)} \in \varepsilon^{(k)}\mathcal{R}$ be non-zero and let π_k be the prime divisor of $x^n - 1$ corresponding to $\varepsilon^{(k)}$. Put $\kappa_k := \deg_x \pi_k$. Then the matrix*

$$G_k := \begin{bmatrix} \mathfrak{v}(g^{(k)}) \\ \mathfrak{v}(xg^{(k)}) \\ \vdots \\ \mathfrak{v}(x^{\kappa_k-1}g^{(k)}) \end{bmatrix} \in \mathbb{F}[z]^{\kappa_k\times n}$$

formed by the first κ_k rows of $\mathcal{M}^{\sigma}(g^{(k)})$ is a minimal generator matrix for the $\mathbb{F}[z]$-module $\mathfrak{v}\big({}^{\bullet}\langle\, g^{(k)}\,\rangle\big) \subseteq \mathbb{F}[z]^n$.

(b) *Let $g \in \mathcal{R}$ be non-zero and left reduced. Suppose $T_g = \{k_1,\dots,k_t\}$ and put $\kappa_{k_\nu} := \deg_x \pi_{k_\nu}$ for $1 \le \nu \le t$ and $\kappa := \sum_{\nu=1}^{t} \kappa_{k_\nu}$,*

$$G := \begin{bmatrix} G_{k_1} \\ \vdots \\ G_{k_t} \end{bmatrix} \in \mathbb{F}[z]^{\kappa\times n} \quad \text{and} \quad G_{k_\nu} := \begin{bmatrix} \mathfrak{v}(g^{(k_\nu)}) \\ \vdots \\ \mathfrak{v}(x^{\kappa_{k_\nu}-1}g^{(k_\nu)}) \end{bmatrix}.$$

Then G is a minimal generator matrix for the $\mathbb{F}[z]$-module $\mathfrak{v}\big({}^{\bullet}\langle\, g\,\rangle\big) \subseteq \mathbb{F}[z]^n$.

Proof: (a) Let $\deg_z g^{(k)} = d_k$ and denote the leading z-coefficient of $g^{(k)}$ by g_{d_k}, which then is nonzero. From Theorem 7.8 we know that $g^{(k)},\dots,x^{\kappa_k-1}g^{(k)}$ is a left $\mathbb{F}[z]$-basis for ${}^{\bullet}\langle\, g^{(k)}\,\rangle$ and that G_k is a full rank generator matrix of $\mathfrak{v}\big({}^{\bullet}\langle\, g^{(k)}\,\rangle\big)$. It remains to check minimality. Note that for all $i = 0, \dots, \kappa_k - 1$ the leading z-coefficient of the polynomial $x^i g^{(k)}$ is given by $\sigma^{d_k}(x^i) g_{d_k}$. Therefore, the leading coefficient matrix of G_k is

$$L(G_k) = \begin{bmatrix} \mathfrak{v}(g^{(k)}) \\ \mathfrak{v}(\sigma^{d_k}(x) g_{d_k}) \\ \vdots \\ \mathfrak{v}(\sigma^{d_k}(x^{\kappa_k - 1}) g_{d_k}) \end{bmatrix}$$

and we have to show that its rank is equal to κ_k. To this end suppose

$$\sum_{i=0}^{\kappa_k - 1} c_i \mathfrak{v}(\sigma^{d_k}(x^i) g_{d_k}) = 0 \text{ for some } c_0, \dots, c_{\kappa_k - 1} \in \mathbb{F}.$$

Then we compute

$$0 = \mathfrak{v}\Big(\sum_{i=0}^{\kappa_k - 1} c_i \sigma^{d_k}(x^i) g_{d_k} \Big) = \mathfrak{v}\bigg(\sigma^{d_k}\Big(\Big(\sum_{i=0}^{\kappa_k - 1} c_i x^i \Big) \sigma^{-d_k}(g_{d_k}) \Big) \bigg).$$

Since $\sigma^{-d_k}(g_{d_k})$ is from $\varepsilon^{(k)} A$ and, of course, also nonzero and since $\varepsilon^{(k)}$ is idempotent, we may use (3.8) and conclude

$$0 = \sum_{i=0}^{\kappa_k - 1} c_i \big(x \varepsilon^{(k)} \big)^i.$$

Since $c_i \in \mathbb{F}$, this equation takes place in the field $K^{(k)} = \varepsilon^{(k)} A$, and $\kappa_k \leq n$ implies $c_0 = \dots = c_{\kappa_k - 1} = 0$.
(b) By (a) we know that the family $g^{(k_\nu)}, \dots, x^{\kappa_{k_\nu} - 1} g^{(k_\nu)}$ generates ${}^{\bullet}\langle\, g^{(k_\nu)} \,\rangle$ for $1 \leq \nu \leq t$. Therefore the t families together generate the $\mathbb{F}[z]$-left module ${}^{\bullet}\langle\, g^{(k_1)}, \dots, g^{(k_t)} \,\rangle = {}^{\bullet}\langle\, g \,\rangle$. Reducedness of g and Theorem 7.8 imply that the $\mathbb{F}[z]$-rank of ${}^{\bullet}\langle\, g \,\rangle$ is κ. Recalling that $x g^{(k_\nu)} = (xg)^{(k_\nu)}$ we therefore see, that the entire family $\big(x^i g^{(k_\nu)} \big)_{0 \leq i \leq \kappa_{k_\nu} - 1,\, 1 \leq \nu \leq t}$ is $\mathbb{F}[z]$-linearly independent. This guarantees that G has full rank and it remains to consider the leading coefficient matrix $L(G)$. This time we have

$$L(G) = \begin{bmatrix} \mathfrak{v}(g_{d_1}) \\ \vdots \\ \mathfrak{v}(\sigma^{d_1}(x^{\kappa_{k_1} - 1}) g_{d_1}) \\ \vdots \\ \vdots \\ \mathfrak{v}(g_{d_t}) \\ \vdots \\ \mathfrak{v}(\sigma^{d_t}(x^{\kappa_{k_t} - 1}) g_{d_t}) \end{bmatrix},$$

where $d_\nu = \deg_z g^{(k_\nu)}$ and $g_{d_\nu} \neq 0$ is the leading z-coefficient of $g^{(k_\nu)}$. Suppose now $c\, L(G) = 0$ for some vector $c = (c_{10}, \dots, c_{1\, \kappa_{k_1} - 1}, \dots, c_{t0}, \dots, c_{t\, \kappa_{k_t} - 1}) \in \mathbb{F}^\kappa$. Then we conclude as in (a)

$$0 = \sum_{\nu=1}^{t} \sum_{i=0}^{\kappa_{k_\nu} - 1} c_{\nu i} \sigma^{d_\nu}(x^i) g_{d_\nu} = \sum_{\nu=1}^{t} \bigg(\sigma^{d_\nu}\Big(\sum_{i=0}^{\kappa_{k_\nu} - 1} c_{\nu i} \big(x \varepsilon^{(k_\nu)} \big)^i \Big) g_{d_\nu} \underbrace{\sigma^{d_\nu}(\varepsilon^{(k_\nu)})}_{\text{idempotent}} \bigg). \tag{7.15}$$

Since g is reduced, no two of the idempotents $\sigma^{d_1}(\varepsilon^{(k_1)}), \ldots, \sigma^{d_t}(\varepsilon^{(k_t)})$ can be equal. Therefore Equation (7.15) implies

$$\sum_{i=0}^{\kappa_{k_\nu}-1} c_{\nu i}(x\varepsilon^{(k_\nu)})^i = 0 \quad \text{for all} \quad 1 \le \nu \le t.$$

Just like in (a) we conclude $c = 0$ and the matrix $L(G)$ has full rank. □

Example 7.14
Consider again Example 7.7. In Example 7.9 we saw already that $\varrho(g) = \varepsilon^{(3)}\varrho(g)$ is reduced. According to the theorem above the first two rows of $\mathcal{M}^\sigma(g)$ form a minimal basic generator matrix of the code $\mathcal{C} = \mathfrak{v}(\overset{\bullet}{\langle} g \rangle)$, which can also be seen directly from the matrix given in Example 6.10. Furthermore, the first three rows of ${}^{\mathsf{t}}\mathcal{M}^\sigma(h) = \mathcal{M}^{\widehat{\sigma}}(h')$ form a basic generator matrix of the code $\mathcal{C}^\perp$. But as is easily seen, the matrix is not minimal. According to the theorem above and the representation (7.6) we have to combine the first row of $\mathcal{M}^{\widehat{\sigma}}\big(\varrho^{-1}(\varepsilon^{(1)}h')\big)$ and the first two rows of $\mathcal{M}^{\widehat{\sigma}}\big(\varrho^{-1}(\varepsilon^{(2)}h')\big)$ in order to get a minimal basic generator matrix of the code $\mathcal{C}^\perp$. This leads to the matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & \alpha^2 z + \alpha & \alpha z + \alpha^2 & \alpha z + \alpha^2 & \alpha + \alpha^2 z \\ \alpha z + \alpha & \alpha z & \alpha^2 z + \alpha & \alpha^2 & \alpha^2 z + \alpha^2 \end{bmatrix}. \qquad \square$$

The last theorem allows for a formula for the complexity of a σ-cyclic code in terms of a reduced generator. The key point is that the complexity, as defined in Definition 2.3(4), can be computed much easier if a minimal generator matrix is available. Indeed, it is known from [5, p. 495], see also [18, Sect. 3], that if $\mathcal{C} = \operatorname{im} G$ where $G \in \mathbb{F}[z]^{k\times n}$ is a minimal matrix with rows $G_1, \ldots, G_k$, then the complexity is given by $\delta = \sum_{i=1}^k \deg_z G_i$. Using Theorem 7.13(b), this immediately implies

Corollary 7.15
Let $g \in \mathcal{R}$ be a reduced polynomial such that $\mathcal{M}^\sigma(g)$ is basic and let $\mathcal{C} := \operatorname{im} \mathcal{M}^\sigma(g)$ be the σ-cyclic code generated by g. Then the complexity of $\mathcal{C}$ is given by

$$\delta = \sum_{i \in T_g} \deg_x \pi_i \deg_z g^{(i)},$$

where, again, π_i is the prime divisor of $x^n - 1$ corresponding to $\varepsilon^{(i)}$.

With the results of this section we now have a detailed picture of the algebraic theory of CCC's. It comprises a complete translation from left ideals in the Piret algebra to submodules in $\mathbb{F}[z]^n$, which also takes into account the parameters and other relevant notions of convolutional codes. We are confident that this should form a solid base for investigating the class of CCC's with respect to coding properties. Some more ideas in this direction will be presented in the last section.

At this point it only remains to append the

Proof of Proposition 3.4: (a) "$\Rightarrow$": Let $\sigma(\varepsilon^{(k)}) = \varepsilon^{(l)} \neq \varepsilon^{(k)}$ and put $g := z\varepsilon^{(l)} + \varepsilon^{(k)}$. Note that $g = \varepsilon^{(k)}g$. We claim that g generates a left ideal $\mathcal{J} = {}^{\bullet}\langle\, g \,\rangle$ corresponding to a σ-CCC, which cannot be generated by a constant matrix. In order to prove this it suffices to show that, firstly, $\mathcal{J}$ has no constant generator and that, secondly, $\mathcal{J}$ is a direct summand as a left $\mathbb{F}[z]$-submodule of $\mathcal{R}$, see Observation 2.14. A constant generator necessarily would be $\varepsilon^{(k)}$ up to a unit from A. Hence assume $\varepsilon^{(k)} = vg$ for some $v \in \mathcal{R}$. Comparing like powers of z in the equation $\varepsilon^{(k)} = vg = v\varepsilon^{(k)}(z+1)$ shows that this is not possible since the leading coefficient of $z+1$ is a unit in A. Therefore $\mathcal{J}$ has no constant generator. As for the direct summand property, we will use Observation 2.14. Assume $fu = vg \in {}^{\bullet}\langle\, g \,\rangle = \mathcal{J}$ for some $f \in \mathbb{F}[z]\backslash\{0\}$ and $u, v \in \mathcal{R}$. But then also $vg\varepsilon^{(k)} = v\varepsilon^{(k)} = fu\varepsilon^{(k)}$ and thus $fu = vg = v\varepsilon^{(k)}g = fu\varepsilon^{(k)}g$. But the latter implies $u \in \mathcal{J}$, since $f \in \mathbb{F}[z]\backslash\{0\}$, not being a zero divisor in $\mathcal{R} = A[z;\sigma]$, can be cancelled. Hence $\mathcal{J}$ is a direct summand of $\mathcal{R}$.
"$\Leftarrow$": The assumption $\sigma(K^{(k)}) = K^{(k)}$ for $1 \leq k \leq r$ can be rephrased as $\sigma(\varepsilon^{(k)}) = \varepsilon^{(k)}$ for $1 \leq k \leq r$. This in turn implies that all idempotents are lying in the center of $\mathcal{R}$ i.e. $\varepsilon^{(k)}g = g\varepsilon^{(k)}$ for all $1 \leq k \leq r$ and all $g \in \mathcal{R}$. Now let $\mathcal{C}$ be a σ-CCC and $\mathcal{J} = \mathfrak{p}(\mathcal{C})$ be the corresponding left ideal. We have to show that $\mathcal{J}$ has a constant generator polynomial. Since $\mathcal{C}$ is delay-free we know from Corollary 4.13 that $\mathcal{J} = {}^{\bullet}\langle\, g \,\rangle$ for some reduced polynomial $g \in \mathcal{R}$ which also satisfies (4.4). Define now $\varepsilon := \sum_{k\in T_g} \varepsilon^{(k)}$. Then $\varepsilon g = g = g\varepsilon$ and as a consequence $\mathcal{J} = {}^{\bullet}\langle\, g \,\rangle \subseteq {}^{\bullet}\langle\, \varepsilon \,\rangle$. The polynomials g and ε are both reduced and satisfy $T_g = T_\varepsilon$. Therefore Theorem 7.8 yields that $\mathcal{J}$ and ${}^{\bullet}\langle\, \varepsilon \,\rangle$ have the same rank as $\mathbb{F}[z]$-submodules of $\mathcal{R}$. Since $\mathcal{J} = \mathfrak{p}(\mathcal{C})$ is a direct summand it follows $\mathcal{J} = {}^{\bullet}\langle\, \varepsilon \,\rangle$, see Proposition 2.2(7), showing that $\mathcal{J}$ has a constant generator.
(b) can be shown with exactly the same line of arguments as in "$\Leftarrow$"of (a). $\square$

8 Future research topics

In this paper we made an effort to broaden the mathematical basis for a thorough investigation of σ-cyclic convolutional codes and their potential for coding. Yet, many important questions of coding theory still have to be answered. We hope that our contribution might serve as a basis for further investigations in this direction and close the paper with a brief list of issues to be addressed in the future. (a) In the paper [9] we presented an infinite series of 1-dimensional codes of length 2 over $\mathbb{F}_3$ with increasing complexity. We also showed that the first codes in this series have a pretty good distance. It would be worth knowing whether the free distance of these codes tends to infinity for increasing complexity. More generally, one might ask whether it is possible to construct families of σ-cyclic codes with constant dimension and length over a fixed field and with arbitrary large distance. In [8] many CCC's of various sizes are given all of which have optimal distance. These examples indicate that the class of CCC's does indeed contain plenty of excellent codes. (b) Any convolutional code allows for other representations besides those via generator and parity check matrices, see for instance [18, p. 1071] or [24], where a shift realization is translated into a description of the code as a first order discrete-time dynamical system over the field $\mathbb{F}$. Is it possible to recover cyclic structure in this description? If so, can such a description be used for the construction of good cyclic codes? (c) One of the strengths of cyclic block codes is the relation between the zeros of the generator polynomial and the distance of the code, leading to the design of powerful codes like BCH-codes. The central issue of the theory of CCC's is certainly the investigation of the distance of these codes in terms of a generator or parity check polynomial or other data determining the code. Any algebraic result in this direction would improve the theory of CCC's. (d) The other main advantage of cyclic block codes is their potential for decoding. Does the additional structure of CCC's, beyond the $\mathbb{F}[z]$-module structure, also allow for an algebraic decoding algorithm, that is, an algorithm where decoding is not obtained via a search algorithm but rather via an algebraic computation based on the received word? A positive answer would certainly be a breakthrough in the theory of convolutional codes.

Acknowledgement

We wish to thank Barbara Langfeld and the anonymous referee for pointing out several typos in the first version of the paper.

References

[1] A. Betten and other. *Codierungstheorie: Konstruktion und Anwendung linearer Codes*. Springer, Berlin, 1998.

[2] P. M. Cohn. *Algebra*, volume 2. Wiley, London, 1977.

[3] P. J. Davis. *Circulant Matrices*. A Wiley-Interscience Publication, New York, 1979.

[4] G. D. Forney Jr. Convolutional codes I: Algebraic structure. *IEEE Trans. Inform. Theory*, 16:720–738, 1970. (see also corrections in *IEEE Trans. Inf. Theory*, vol. 17,1971, p. 360).

[5] G. D. Forney Jr. Minimal bases of rational vector spaces, with applications to multivariable linear systems. *SIAM J. on Contr.*, 13:493–520, 1975.

[6] F. R. Gantmacher. *The Theory of Matrices*, volume 1. Chelsea, New York, 1977.

[7] H. Gluesing-Luerssen and B. Langfeld. On the parameters of convolutional codes with cyclic structure. Preprint 2003. Submitted. Available at http://front.math.ucdavis.edu/ with ID-number RA/0312092.

[8] H. Gluesing-Luerssen and W. Schmale. Distance bounds for convolutional codes and some optimal codes. Preprint 2003. Submitted. Available at http://front.math.ucdavis.edu/ with ID-number RA/0305135.

[9] H. Gluesing-Luerssen, W. Schmale, and M. Striha. Some small cyclic convolutional codes. In *Electronic Proceedings of the 15th International Symposium on the Mathematical Theory of Networks and Systems*, Notre Dame, IN (USA), 2002. (8 pages).

[10] K. J. Hole. On classes of convolutional codes that are not asymptotically catastrophic. *IEEE Trans. Inform. Theory*, 46:663–669, 2000.

[11] N. Jacobson. *Basic Algebra I.* W. H. Freeman, New York, 2. edition, 1985.

[12] R. Johannesson and K. S. Zigangirov. *Fundamentals of Convolutional Coding.* IEEE Press, New York, 1999.

[13] J. Justesen. Bounded distance decoding of unit memory codes. *IEEE Trans. Inform. Theory*, IT-39:1616–1627, 1993.

[14] Kaenel, P. A. von. Generators of principal left ideals in a noncommutative algebra. *Rocky Mountain Journal of Mathematics*, 11:27–30, 1981.

[15] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes.* North-Holland, 1977.

[16] J. L. Massey and M. K. Sain. Codes, automata, and continuous systems: Explicit interconnections. *IEEE Trans. Aut. Contr.*, AC-12:644–650, 1967.

[17] J. L. Massey and M. K. Sain. Inverses of linear sequential circuits. *IEEE Trans. Comput.*, C-17:330–337, 1968.

[18] R. J. McEliece. The algebraic theory of convolutional codes. In V. Pless and W. Huffman, editors, *Handbook of Coding Theory, Vol. 1*, pages 1065–1138. Elsevier, Amsterdam, 1998.

[19] P. Piret. Structure and constructions of cyclic convolutional codes. *IEEE Trans. Inform. Theory*, 22:147–155, 1976.

[20] P. Piret. *Convolutional Codes; An Algebraic Approach.* MIT Press, Cambridge, MA, 1988.

[21] P. Piret. A convolutional equivalent to Reed-Solomon codes. *Philips J. Res.*, 43:441–458, 1988.

[22] C. Roos. On the structure of convolutional and cyclic convolutional codes. *IEEE Trans. Inform. Theory*, 25:676–683, 1979.

[23] J. Rosenthal. Connections between linear systems and convolutional codes. In B. Marcus and J. Rosenthal, editors, *Codes, Systems, and Graphical Models*, pages 39–66. Springer, Berlin, 2001.

[24] J. Rosenthal, J. M. Schumacher, and E. V. York. On behaviors and convolutional codes. *IEEE Trans. Inform. Theory*, 42:1881–1891, 1996.

[25] J. Rosenthal and R. Smarandache. Maximum distance separable convolutional codes. *Appl. Algebra Engrg. Comm. Comput.*, 10:15–32, 1999.

[26] J. Rosenthal and E. V. York. BCH convolutional codes. *IEEE Trans. Inform. Theory*, IT-45:1833–1844, 1999.

[27] R. Smarandache, H. Gluesing-Luerssen, and J. Rosenthal. Constructions of MDS-convolutional codes. *IEEE Trans. Inform. Theory*, 47(5):2045–2049, 2001.

[28] M. Ventou. Automorphisms and isometries of some modular algebras. In *Algebraic algorithms and error-correcting codes; Proc. 3rd International Conf. AAECC-3*, pages 202–210. Springer Lecture Notes in Computer Science 229, 1985.