A Class of One-Dimensional MDS Convolutional Codes

Heide Gluesing-Luerssen* and Barbara Langfeld†

April 25, 2005

Abstract

A class of one-dimensional convolutional codes will be presented. They are all MDS codes, i. e., have the largest distance among all one-dimensional codes of the same length n and overall constraint length δ. Furthermore, their extended row distances are computed, and they increase with slope at least $n - \delta$. In certain cases of the algebraic parameters, we will also derive parity check matrices of Vandermonde type for these codes. Finally, cyclicity in the convolutional sense of [8] will be discussed for our class of codes. It will turn out that they are cyclic if and only if the field element used in the generator matrix has order n. This can be regarded as a generalization of the block code case.

Keywords: Convolutional coding theory, generalized Singleton bound, cyclic convolutional codes.

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

1 Introduction

The main task of coding theory is the construction of powerful codes. This applies equally well to block codes and convolutional codes. In either case codes are required to have good error-correcting properties, i. e., a large distance, and an efficient decoding algorithm. In block coding theory this goal has been achieved best by the class of Reed-Solomon codes along with their efficient algebraic decoding algorithm. These codes are in particular MDS (maximum distance separable), meaning that they have the largest distance possible among all codes with the same length and dimension. On the other hand, despite their frequent and successful use in engineering practice, the mathematical theory of convolutional codes is still in its infancy. The algebraic theory of this class of codes was initiated with Forney's paper [2] and has seen a considerable development ever since.

*University of Groningen, Department of Mathematics, P. O. Box 800, 9700 AV Groningen, The Netherlands; gluesing@math.rug.nl

†Kombinatorische Geometrie (M9), Zentrum Mathematik, Technische Universität München, Boltzmannstr. 3, 85747 Garching bei München, Germany; langfeld@ma.tum.de

In particular, extensive efforts have been made in the area of constructing convolutional codes with large distance. The first group of the according papers appeared in the seventies of the last century. In [11, 14, 12] quasi-cyclic block codes have been used in order to construct convolutional codes with good distance. The relation between the weights of the block codewords and the convolutional codewords is made by the weight-retaining property. This topic has been resumed later on in [24] where the ideas have been used to construct MDS convolutional codes with (almost) arbitrary algebraic parameters. In the papers [22, 21, 9] system theoretic methods are used in order to analyze and design good convolutional codes. Other more recent attempts of constructing good convolutional codes try to impose additional algebraic structure on the convolutional codes themselves. In [1] methods from algebraic geometry are used in order to construct convolutional codes of Goppa type. In [18, 20, 8] convolutional codes with cyclic structure have been introduced and analyzed. We will explain the notion of cyclicity later in Section 4 of this paper.

In the present paper we will combine the main lines mentioned above. We will present a class of one-dimensional codes that are not only MDS but also have extended row distances increasing with slope at least $n - \delta$ (where n is the length of the code and δ the overall constraint length). We will also compare the required field size needed for the construction with the field sizes of other constructions known in the literature. It will turn out that our field sizes are smaller for many parameters than what has been used before. For one set of parameters the field size is even only one above the theoretic minimum. In addition to these distance computations and field size investigations, we will also discuss the algebraic structure of these codes. As it turns out, for certain algebraic parameters the presented codes are cyclic in the sense mentioned above. In this case the codes can in fact be regarded as a generalization of (one-dimensional) Reed-Solomon codes. They even have a polynomial parity check matrix of Vandermonde type and can also be understood as a special case of convolutional Goppa codes as introduced in [1].

We end this introduction with the basic notions of convolutional coding theory. Let $\mathbb{F}$ be any finite field. A *convolutional code* $\mathcal{C} \subseteq \mathbb{F}[z]^n$ with (algebraic) parameters (n, k, δ) is a submodule of the form $\mathcal{C} = \operatorname{im} G := \{uG \mid u \in \mathbb{F}[z]^k\}$, where $G \in \mathbb{F}[z]^{k\times n}$ is a right-invertible matrix, i. e., $G\tilde{G} = I_k$ for some matrix $\tilde{G} \in \mathbb{F}[z]^{n\times k}$, and such that $\delta = \max\{\deg \gamma \mid \gamma \text{ is a } k\text{-minor of } G\}$. We call G a *generator matrix* of the code. The number n is called the *length*, k is the *dimension*, and δ is called the *overall constraint length* of the code. A code with overall constraint length zero can be regarded as a block code. By resorting to the Smith normal form for polynomial matrices one can easily see that the right invertibility of G is equivalent to the submodule $\mathcal{C} = \operatorname{im} G$ being a direct summand of $\mathbb{F}[z]^n$. This in turn is equivalent to the existence of a matrix $H \in \mathbb{F}[z]^{(n-k)\times n}$ such that $\operatorname{im} G = \ker H^{\mathsf{T}} := \{v \in \mathbb{F}[z]^n \mid vH^{\mathsf{T}} = 0\}$. It is easily seen that we may assume H to be right-invertible as well. We call H a *parity check matrix* of $\mathcal{C}$. Obviously, the matrix H generates the *dual code*, i. e., $\operatorname{im} H = \mathcal{C}^{\perp} := \{w \in \mathbb{F}[z]^n \mid wv^{\mathsf{T}} = 0 \text{ for all } v \in \mathcal{C}\}$. It should be noted that generator and parity check matrix of a code are uniquely determined up to left multiplication by a unimodular matrix, i. e. by a matrix from $Gl_k(\mathbb{F}[z])$ or $Gl_{n-k}(\mathbb{F}[z])$, respectively.

The most important concept in coding theory is the distance. For a polynomial vector $v = \sum_{j=0}^{N} v_j z^j \in \mathbb{F}[z]^n$ the *weight* is defined as $\operatorname{wt}(v) = \sum_{j=0}^{N} \operatorname{wt}(v_j)$, where $\operatorname{wt}(v_j)$ denotes

the usual Hamming weight of $v_j \in \mathbb{F}^n$. Then the *(free) distance* of a code $\mathcal{C} \subseteq \mathbb{F}[z]^n$ is given as $\operatorname{dist}(\mathcal{C}) := \min\{\operatorname{wt}(v) \mid v \in \mathcal{C},\ v \neq 0\}$. In [23, Thm. 2.2] an upper bound for the distance has been derived, the *generalized Singleton bound*. It states that the distance d of a code with parameters (n, k, δ) over any field satisfies $d \leq S(n, k, \delta) := (n-k)(\lfloor \delta/k \rfloor + 1) + \delta + 1$. As a special case the well-known Singleton bound for block codes $S(n, k, 0) = n - k + 1$ appears. Observe also that for $k = 1$ the generalized Singleton bound $S(n, 1, \delta) = n(\delta + 1)$ is easily seen since in this case each generator matrix, being a codeword itself, obviously has weight at most $n(\delta+1)$. Like for block codes we call a code $\mathcal{C}$ with $\operatorname{dist}(\mathcal{C}) = S(n, k, \delta)$ an MDS code (maximum distance separable), see [23, Def. 2.5].

2 A class of one-dimensional MDS codes

In this section we present a construction of one-dimensional MDS convolutional codes. The distance will be computed straightforwardly. We will then compare our results with constructions known from the literature. Thereafter we will also study the extended row distances and derive that they are increasing with a slope of at least $n - \delta$.

Theorem 2.1 *Let $n \in \mathbb{N}$ be such that $n \leq |\mathbb{F}| - 1$ and let $0 \leq \delta \leq n - 1$. Choose an element $\alpha \in \mathbb{F}$ such that $\operatorname{ord}(\alpha) \geq n$. Define*

$$G := \sum_{\nu=0}^{\delta} z^\nu \begin{pmatrix} 1 & \alpha^\nu & \alpha^{2\nu} & \dots & \alpha^{(n-1)\nu} \end{pmatrix} \in \mathbb{F}[z]^{1\times n} \tag{2.1}$$

and let $\mathcal{C} := \operatorname{im} G \subseteq \mathbb{F}[z]^n$. Then G is right invertible, i. e., the submodule $\mathcal{C}$ is a convolutional code, and $\operatorname{dist}(\mathcal{C}) = n(\delta + 1)$. In other words, $\mathcal{C}$ is an MDS code with parameters $(n, 1, \delta)$.

Notice that for $\delta = 0$ the code is simply the n-fold repetition (block) code over $\mathbb{F}$ and the assertions are obvious.

Proof: In order to show that G is right invertible, we have to prove that the entries $\sum_{\nu=0}^{\delta}(\alpha^j z)^\nu$, $j = 0, \dots, n-1$, of the matrix G are coprime, that is, that they do not have a common root in any extension field $\hat{\mathbb{F}}$ of $\mathbb{F}$. But this is clear since if $\beta \in \hat{\mathbb{F}}$ was such a common root then the assumptions imply that $\beta, \alpha\beta, \dots, \alpha^{n-1}\beta$ are more than δ pairwise different roots of $\sum_{\nu=0}^{\delta} z^\nu$.

Next we will prove that $\operatorname{dist}(\mathcal{C}) = n(\delta+1)$. To this end put $G_\nu := (1,\ \alpha^\nu,\ \alpha^{2\nu},\ \dots, \alpha^{(n-1)\nu})$ for $\nu = 0, \dots, \delta$. Let $u = \sum_{i=0}^{t} u_i z^i \in \mathbb{F}[z]$, where $t \geq 0$ and $u_0 \neq 0 \neq u_t$, and put $uG =: v = \sum_{i=0}^{\delta+t} v_i z^i$. Defining $G_\nu := 0$ for $\nu < 0$ and $\nu > \delta$, we have

$$v_\nu = (u_0, \dots, u_t)\tilde{G}_\nu, \text{ where } \tilde{G}_\nu = \begin{pmatrix} G_\nu \\ G_{\nu-1} \\ \vdots \\ G_{\nu-t} \end{pmatrix} \tag{2.2}$$

for $\nu = 0, \ldots, \delta + t$. Notice that for $\nu \leq \delta$ the first row of $\tilde{G}_\nu$ is nonzero while for $\nu \geq t$ the last row is nonzero. Since $u_0 \neq 0 \neq u_t$ this will provide us with a good estimate of the weight of v_ν for these indices. In order to see this, note that for each index ν the nonzero rows of $\tilde{G}_\nu$ are consecutive and form a matrix of the type

$$R := \begin{pmatrix} 1 & \alpha^{s+r} & \alpha^{2(s+r)} & \ldots & \alpha^{(n-1)(s+r)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{s+1} & \alpha^{2(s+1)} & \ldots & \alpha^{(n-1)(s+1)} \\ 1 & \alpha^{s} & \alpha^{2s} & \ldots & \alpha^{(n-1)s} \end{pmatrix}$$

where $0 \leq s \leq s + r \leq \delta$. Since $\operatorname{ord}(\alpha) \geq n > \delta$, the block code $\operatorname{im} R \subseteq \mathbb{F}^n$ is MDS, that is,

$$\operatorname{dist}(\operatorname{im} R) = n - r. \tag{2.3}$$

This will now be used for counting the weight of the vectors v_ν for $\nu \in \{0, \ldots, \delta, t, \ldots, \delta + t\}$.
1. case: $t > \delta$
In this case the indices $0, \ldots, \delta, t, \ldots, \delta + t$ are all different and we have

$$\tilde{G}_\nu = \begin{pmatrix} G_\nu \\ G_{\nu-1} \\ \vdots \\ G_0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \text{ for } \nu = 0, \ldots, \delta \text{ and } \tilde{G}_\mu = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ G_\delta \\ G_{\delta-1} \\ \vdots \\ G_{\mu-t} \end{pmatrix} \text{ for } \mu = t, \ldots, \delta + t \tag{2.4}$$

and all displayed rows G_ℓ are nonzero. Thus, using (2.3),

$$\operatorname{wt}(v_\nu) \geq n - \nu \text{ for } \nu = 0, \ldots, \delta \text{ and } \operatorname{wt}(v_\mu) \geq n - (\delta + t - \mu) \text{ for } \mu = t, \ldots, \delta + t, \tag{2.5}$$

and therefore

$$\operatorname{wt}(v) \geq 2\big(n + (n-1) + \ldots + (n-\delta)\big) = 2n(\delta+1) - \delta(\delta+1) \geq n(\delta+1) \tag{2.6}$$

where the last inequality follows from $\delta < n$.
2. case: $t \leq \delta$
In this case we consider the indices $0, \ldots, \delta, \delta + 1, \ldots, \delta + t$. For $\nu = 0, \ldots, t$ and for $\mu = \delta + 1, \ldots, \delta + t$ the matrices $\tilde{G}_\nu$ and $\tilde{G}_\mu$ are as in (2.4), while for $\nu = t + 1, \ldots, \delta$ the matrix $\tilde{G}_\nu$ is as in (2.2) and all its rows are nonzero. From this and (2.3) we obtain

$$\begin{aligned} \operatorname{wt}(v) &\geq \big(n + (n-1) + \ldots + (n-t)\big) + (\delta - t)(n-t) + \big((n-t+1) + (n-t+2) + \ldots + n\big) \\ &= 2\Big(tn - \sum_{i=0}^{t-1} i\Big) + (\delta - t + 1)(n-t) = n(\delta+1) + t(n-\delta) \geq n(\delta+1). \end{aligned} \tag{2.7}$$

This concludes the proof. □

The proof above also shows that uG with $u \in \mathbb{F} \backslash \{0\}$, i. e., the nonzero constant multiples of G, are the only codewords having weight $n(\delta + 1)$. Indeed, the inequality in (2.6) is always strict and the last inequality in (2.7) is strict for all $t > 0$.

Remark 2.2 It is not hard to see that the matrix G in (2.1) is also right-invertible for all $\delta \geq n$ for which $\mathrm{ord}(\alpha) \nmid \delta + 1$. Examples show that these codes often have a large distance, too, but are not MDS in general. We cannot provide a general result in this case.

Remark 2.3 The codes given in Theorem 2.1 can be regarded as convolutional Goppa codes (CGC, for short) in the sense of [1]. Indeed, they can be described as the polynomial part of the $\mathbb{F}(z)$-vector space $C(T, D)$ with divisors $D = \sum_{i=0}^{n-1} \left[1 : \sum_{\nu=0}^{\delta} \alpha^{i\nu} z^{\nu}\right]$ and $T = [0 : 1] - [1 : 0]$ on the projective line $\mathbb{P}^1_{\mathbb{F}(z)}$ and where $C(T, G)$ is defined as in [1, p. 52]. Unfortunately, this insight does not provide any further information concerning the distance of the code. In [17] it is shown that the dual of a CGC is a CGC again, and a rational basis with Goppa code structure is derived for the dual code, considered over the field $\mathbb{F}(z)$. In the next section we will restrict to a special case of codes as in Theorem 2.1 and compute (polynomial) parity check matrices of Vandermonde type showing once more that these codes and their duals are CGC's.

We would like to comment on the field size required for the construction of the MDS codes in Theorem 2.1. In [12, Lemma 1] and [6, Thm. 3.7] it has been shown that if $\mathcal{C}$ is an $(n, 1, \delta)$-MDS code over $\mathbb{F}_q$ then $q \geq \delta + 1$. In Theorem 2.1 the field size q satisfies $q \geq n + 1 \geq \delta + 2$. Thus, in the case $n = \mathrm{ord}(\alpha) = q - 1$ and $\delta = n - 1$ our field size is just one above the lower bound mentioned before. As to our knowledge it is not known in general whether there exist $(n, 1, n-1)$-MDS codes over $\mathbb{F}_n$ (in the case where n is a prime power). We also would like to compare our results with previous constructions of MDS codes. In [12] MDS codes with parameters $(n, 1, \delta)$ for certain combinations have been constructed. However, these combinations are different from ours. For instance, the result in [12, Thm. p. 580] does not contain the case of $(q-1, 1, q-2)$-MDS codes over $\mathbb{F}_q$ and no $(q-1, 1, q-3)$-MDS codes over $\mathbb{F}_q$ where $q > 5$. On the other hand, the construction of that theorem allows the construction of a $(17, 1, 20)$-MDS code over $\mathbb{F}_{32}$ which is not part of our Theorem 2.1. In [25] a construction of $(n, 1, \delta)$-MDS codes is given over fields $\mathbb{F}_q$ where $q > \delta n + 1$. Except for the case $\delta = 1$ this is a considerably bigger field size than ours where $q \geq n + 1$. However, the construction in [25] works for all δ and not just for $\delta < n$. Another construction of MDS codes is given in [24]. Therein, MDS codes with (almost) arbitrary parameters (n, k, δ) are constructed over fields $\mathbb{F}_q$ of size $q \geq \frac{\delta n^2}{k(n-k)} + 2$. The construction is based on cyclic block codes with large distance. In the case $k = 1$ this again amounts to a considerably bigger field than in our construction.

We want to go into more details about the weight distribution of these codes and therefore give also lower bounds for the extended row distances. These parameters have been introduced in [13, p. 541] and are very closely related to the trellis structure of the code and thus to its performance. Details on the importance of these parameters can be found in [13]. The jth extended row distance amounts to the minimum weight of all paths through the state diagram starting at the zero state and which reach the zero state for the first time after exactly j steps. In [16] a codeword corresponding to such a path is called *atomic* of length j. It has degree $j - 1$. The details are also explained in [10, Sec. 3.10] and [4]. In our case where the codes are one-dimensional, the atomic codewords are easily described. Indeed, for a right-invertible matrix $G \in \mathbb{F}[z]^{1\times n}$ with overall constraint

length δ and for a message $u \in \mathbb{F}[z]$ one has

$$uG \text{ is atomic} \iff u \text{ does not have } \delta \text{ consecutive zero coefficients.} \tag{2.8}$$

This follows readily from the fact that the last δ coefficients of the message make up the current state in the state diagram. For detailed notions and proofs see also [4, Sec. 3].

Having this in mind, the jth extended row distance of the one-dimensional code $\mathcal{C} = \operatorname{im} G$ can be defined as

$$\hat{d}_j^r := \min\left\{ \operatorname{wt}(uG) \;\middle|\; \begin{array}{l} u \in \mathbb{F}[z],\ u_0 \neq 0,\ \deg u = j-\delta-1, \\ \text{no } \delta \text{ consecutive coefficients of } u \text{ are zero} \end{array} \right\} \text{ for all } j \geq \delta+1.$$

Notice that $\deg(u) = j-\delta-1$ implies $\deg(uG) = j-1$ and thus the associated path has length j. As for the index notation we diverge somewhat from [13] where the index j equals the degree of the associated codewords while in our case it reflects the length.

Proposition 2.4 *Let $\mathcal{C} = \operatorname{im} G \subseteq \mathbb{F}[z]^n$ be the code described in Theorem 2.1. Then*

$$\hat{d}_j^r \geq (n-\delta)j + \delta(\delta+1) \text{ for all } j \geq \delta+1.$$

Hence the extended row distances, regarded as a function of the length j, are bounded from below by a linear function with slope $n-\delta$.

Before we prove this result we wish to mention that, in a certain sense, this result is the best one can expect. As Equation (2.9) below shows, the "middle" coefficients of a codeword are contained in an $(n, \delta+1)$-block code. The distance of this code is therefore a lower bound for the slope. In our case this code is MDS, hence optimal. However, in specific cases certain constellations of consecutive coefficients of the generator matrix might even allow a better row distance. After the proof we will present examples for both cases, the estimate in Proposition 2.4 being an identity and being a strict inequality.

PROOF: Let $u \in \mathbb{F}[z]$ and $\deg u = j-\delta-1 \geq 0$. Then $uG =: v = \sum_{i=0}^{j-1} v_i z^i$ has degree $j-1$ and length j.
If $j-\delta-1 \leq \delta$, then (2.7) shows $\operatorname{wt}(v) \geq n(\delta+1) + (j-\delta-1)(n-\delta) = \delta(\delta+1) + j(n-\delta)$.
Let now $j-\delta-1 > \delta$. From (2.5) we have $\operatorname{wt}\Big(\sum_{i=0}^{\delta} v_i z^i + \sum_{i=j-\delta-1}^{j-1} v_i z^i\Big) \geq (2n-\delta)(\delta+1)$.
Thus it remains to consider the coefficients v_i where $i = \delta+1, \ldots, j-\delta-2$. Since

$$v_i = \sum_{l=0}^{\delta} u_{i-l} G_l = (u_i, u_{i-1}, \ldots, u_{i-\delta}) \begin{pmatrix} G_0 \\ G_1 \\ \vdots \\ G_\delta \end{pmatrix} \tag{2.9}$$

and v is atomic, the vector $(u_i, u_{i-1}, \ldots, u_{i-\delta})$ is nonzero by (2.8). Thus $\operatorname{wt}(v_i) \geq n-\delta$ by (2.3) and $\operatorname{wt}(v) \geq (2n-\delta)(\delta+1) + (j-2\delta-2)(n-\delta) = (n-\delta)j + \delta(\delta+1)$. □

In the following examples we consider a few cases of the parameters n and δ in Theorem 2.1. We computed the exact weight distribution $A(W, L)$ of the codes using Maple. For the precise definition and the computation see [4, Sec. 3].

Example 2.5 (1) Let $\delta = 1$, $\mathrm{char}(\mathbb{F}) = 2$ and n be arbitrary. Then it is easy to see that $\mathrm{wt}\big((\sum_{i=0}^{j-2} z^i)G\big) = 2 + j(n-1)$ for each $j \geq 2$, hence the estimate in Proposition 2.4 is an identity.

(2) Let $\delta = 2$, $n = 3$ and $\mathbb{F} = \mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ where $\alpha^2 = \alpha + 1$. Then G as defined in Theorem 2.1 is given by

$$G = \begin{pmatrix} 1 + z + z^2 & 1 + \alpha z + \alpha^2 z^2 & 1 + \alpha^2 z + \alpha z^2 \end{pmatrix}.$$

In this case one can show that the weight distribution is given by

$$\begin{aligned} A(L, W) &= 3W^9L^3(1 + 2LW - 2LW^3)/(6L^3W^8 - 6L^3W^6 - 3L^2W^5 - 2LW^3 - LW + 1) \\ &= 3W^9L^3 + 9W^{10}L^4 + (9W^{11} + 18W^{13} + 9W^{14})L^5 + O(L^6), \end{aligned}$$

meaning, for instance, that there are 36 atomic codewords of length five, 9 of which have weight 11 and 14, respectively, and 18 have weight 13. Using induction it is easy to see that in the series expansion for each $j \geq 3$ the coefficient of L^j is divisible by W^{6+j} but not by W^{7+j}. Hence, $\hat{d}_j^r = 6 + j$, and, like in (1), the estimate in Proposition 2.4 is an equality. Again, in this case one has $\mathrm{wt}\big((\sum_{i=0}^{j-3} z^i)G\big) = 6 + j$ for each $j \geq 3$.

(3) In general however, the inequality for the jth extended row distance is not an identity and the growth rate can even be better. This happens for instance for $n = 3$, $\delta = 2$ and $\mathbb{F} = \mathbb{F}_8$ with, of course, $\mathrm{ord}(\alpha) = 7$. In this case the lower bound for $\hat{d}_j^r$ is given by $(n - \delta)j + \delta(\delta + 1) = j + 6$. One can show that the weight distribution of the code in Theorem 2.1 is of the form $A(L, W) = 7W^9L^3 + (21W^{10} + 28W^{12})L^4 + (14W^{12} + 126W^{13} + 147W^{14} + 105W^{15})L^5 + \sum_{j=6}^{\infty} A_j(W)L^j$ where $A_j \in \mathbb{Q}[W]$ is divisible by $W^{j+8+\lfloor \frac{j-6}{9} \rfloor}$ for all $j \geq 6$. Thus, $\lim_{j\to\infty} \big(\hat{d}_j^r - (j+6)\big) = \infty$, showing that asymptotically the growth rate is even infinitely better than the lower bound given in Proposition 2.4.

3 Parity check matrices with Vandermonde structure

In this section we will restrict to the case where $\mathrm{ord}(\alpha) = n = \delta + 1$ and derive two types of parity check matrices for the codes of Theorem 2.1, one of them being minimal in the sense of [3, p. 459]. Both reveal a type of Vandermonde structure for these codes.

Theorem 3.1 *Let* $\mathrm{ord}(\alpha) = n$ *and consider the matrix*

$$H := \begin{pmatrix} z - \alpha^n & z - \alpha^{n-1} & \cdots & z - \alpha^2 & z - \alpha \\ (z - \alpha^n)^2 & (z - \alpha^{n-1})^2 & \cdots & (z - \alpha^2)^2 & (z - \alpha)^2 \\ \vdots & \vdots & & \vdots & \vdots \\ (z - \alpha^n)^{n-1} & (z - \alpha^{n-1})^{n-1} & \cdots & (z - \alpha^2)^{n-1} & (z - \alpha)^{n-1} \end{pmatrix} \in \mathbb{F}[z]^{(n-1)\times n}.$$

Then H *is right-invertible and* $GH^{\mathsf{T}} = 0$ *where* $G = \sum_{\nu=0}^{n-1} z^\nu \begin{pmatrix} 1 & \alpha^\nu & \alpha^{2\nu} & \ldots & \alpha^{(n-1)\nu} \end{pmatrix}$. *Hence, if* $\mathrm{ord}(\alpha) = n = \delta + 1$, *then the code given in Theorem 2.1 has parity check matrix* H.

PROOF: For $j = 1, \ldots, n$ let $H^{(j)} \in \mathbb{F}[z]^{(n-1)\times(n-1)}$ be the submatrix of H obtained by omitting the jth column. Then, due to the Vandermonde structure of H, we obtain

$$\det H^{(j)} = \prod_{\substack{\nu=1\\ \nu\neq n-j+1}}^{n} (z-\alpha^\nu) \prod_{\substack{\nu=1\\ \nu\neq n-j+1}}^{n} \prod_{\substack{\mu=\nu+1\\ \mu\neq n-j+1}}^{n} (z-\alpha^\mu - z + \alpha^\nu) = \prod_{\substack{\nu=1\\ \nu\neq n-j+1}}^{n} (z-\alpha^\nu) \prod_{\substack{1\leq\nu<\mu\leq n\\ \nu,\mu\neq n-j+1}} (\alpha^\nu - \alpha^\mu).$$

Since $\mathrm{ord}(\alpha) = n$, the last factor is nonzero for each j. But then the first factors show the coprimeness of the maximal minors of H, and thus H is right-invertible [15, Thm. A.1]. Let G be given as above. Then for $j = 1, \ldots, n$ the jth entry G_j is of the form

$$G_j = \sum_{\nu=0}^{n-1} \left(\alpha^{j-1} z\right)^\nu = \frac{(\alpha^{j-1}z)^n - 1}{\alpha^{j-1}z - 1} = \frac{z^n-1}{\alpha^{j-1}z-1} = \alpha^{n-j+1}\frac{z^n-1}{z-\alpha^{n-j+1}},$$

where for the last two identities we used $\mathrm{ord}(\alpha) = n$. Thus,

$$G = \Big(\alpha^n \frac{z^n-1}{z-\alpha^n},\, \alpha^{n-1}\frac{z^n-1}{z-\alpha^{n-1}}, \ldots, \alpha\frac{z^n-1}{z-\alpha}\Big). \tag{3.1}$$

Now we can prove $GH^{\mathsf{T}} = 0$. For easier indexing we will write down the sums of the matrix product backwards. Then we have to show that $\sum_{\nu=1}^{n} \alpha^\nu \frac{z^n-1}{z-\alpha^\nu} \cdot (z-\alpha^\nu)^j = 0$ for $j = 1, \ldots, n-1$. This is equivalent to

$$\sum_{\nu=1}^{n} \alpha^\nu (z-\alpha^\nu)^j = 0 \text{ for } j = 0, \ldots, n-2. \tag{3.2}$$

In order to see this, compute

$$\sum_{\nu=1}^{n} \alpha^\nu (z-\alpha^\nu)^j = \sum_{\nu=1}^{n} \alpha^\nu \sum_{\mu=0}^{j} \binom{j}{\mu} z^{j-\mu}(-1)^\mu \alpha^{\nu\mu} = \sum_{\mu=0}^{j} z^{j-\mu}\binom{j}{\mu}(-1)^\mu \sum_{\nu=1}^{n} \alpha^{\nu(\mu+1)}.$$

Notice that for fixed $\mu = 0, \ldots, j \leq n-2$ we have $\alpha^{\mu+1} \neq 1$ due to $\mathrm{ord}(\alpha) = n$. Therefore,

$$\sum_{\nu=1}^{n} \alpha^{\nu(\mu+1)} = \sum_{\nu=0}^{n-1} \alpha^{\nu(\mu+1)} = \frac{\alpha^{(\mu+1)n}-1}{\alpha^{\mu+1}-1} = 0 \text{ for all } \mu = 0, \ldots, j. \tag{3.3}$$

This proves Equations (3.2) and thus $GH^{\mathsf{T}} = 0$. □

One should notice that the parity check matrix H is highly non-minimal, i. e., it is not a minimal basis for the dual code $\mathcal{C}^\perp$ (for the notion of minimal basis see [3, p. 459] or [10, Sec. 2.5]). Obviously the leading coefficient matrix is the all-1-matrix and thus has rank 1 only. This implies non-minimality of H by [3, Main Thm.]. A minimal parity check matrix will be presented at the end of this section.

The reader will have noticed that we did not make use of the Vandermonde parity check matrix H when computing the distances of the codes in the last section. As to our knowledge no theoretical result is known yet about the distances of convolutional codes with Vandermonde generator or parity check matrices. As an indication that such a relation

is not obvious, we would like to mention that codes generated by H as in Theorem 3.1 are in general not MDS codes. In general, they don't even meet the Griesmer bound ([10, Thm. 3.22] or [6, Thm. 3.4]). On the other hand, in [1, Exa. 4.1] a few examples of MDS convolutional Goppa codes with generator matrix similar to H above have been presented. A deeper understanding as to whether there is a relation between the distance of the codes $\ker H^{\mathsf{T}}$ or $\operatorname{im} H$ and the Vandermonde structure of H must be considered as one of the main tasks in algebraic convolutional coding theory. It might also have impact on the possibility of algebraic decoding of these codes.

Remark 3.2 With completely different methods it is possible to prove that also in the general case $0 \leq \delta < n = \operatorname{ord}(\alpha)$, the codes from Theorem 2.1 have a parity check matrix of a (somewhat modified) Vandermonde type. Indeed, in that case such a matrix is given by

$$H := \begin{pmatrix} 1 & \alpha & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha^{n-\delta-1} & \cdots & \alpha^{(n-\delta-1)(n-1)} \\ z-\alpha^n & z-\alpha^{n-1} & \cdots & z-\alpha \\ (z-\alpha^n)^2 & (z-\alpha^{n-1})^2 & \cdots & (z-\alpha)^2 \\ \vdots & \vdots & & \vdots \\ (z-\alpha^n)^\delta & (z-\alpha^{n-1})^\delta & \cdots & (z-\alpha)^\delta \end{pmatrix} \in \mathbb{F}[z]^{(n-1)\times n}.$$

Hence H is right invertible and satisfies $GH^{\mathsf{T}} = 0$. The proof of this statement needs detailed methods from the theory of cyclic convolutional codes as derived in [8] and will be omitted. It will appear in a forthcoming paper on Vandermonde parity check matrices of doubly-cyclic codes in the sense of [7].

At the end of this section we will return to the case where $\delta = n-1$ and present a minimal parity check matrix, i. e., a right-invertible matrix with minimal row degrees in the sense of [3, p. 459] or [10, Sec. 2.5]. It shows that the dual code of $\operatorname{im} G$ has Forney index 1 (counted $(n-1)$ times)[1] and thus is a compact code in the sense of [15, Cor. 4.3].

Theorem 3.3 *Let again* $\operatorname{ord}(\alpha) = n$ *and define*

$$H_{min} := \left((\alpha^{n-\nu+1})^{j-1} z - (\alpha^{n-\nu+1})^j\right)_{\substack{j=1,\ldots,n-1 \\ \nu=1,\ldots,n}} \in \mathbb{F}[z]^{(n-1)\times n}.$$

Then H_{min} *is minimal and right-invertible and* $G\,H_{min}^{\mathsf{T}} = 0$, *where* G *is again as in Theorem 3.1. Hence in the case where* $\operatorname{ord}(\alpha) = n = \delta + 1$ *the matrix* H_{min} *is a parity check matrix of the code given in Theorem 2.1.*

Proof: 1) Notice that H_{min} is of the form $H_{min} = H_1 z - H_0$ where both H_1 and H_0 have Vandermonde structure and full row rank. Thus the matrix H_{min} has full row rank and the overall constraint length of $\operatorname{im} H_{min}$ is $n-1$, the sum of its row degrees, see [3,

[1] The Forney indices of a code are defined to be the row degrees of a minimal generator matrix, see [15, p. 1081].

p. 495]. As a consequence, H_{min} is minimal.
2) As for the product $G\,H_{min}^{\mathsf{T}}$ we use again the representation (3.1) for the matrix G. Writing down the sums of the product GH_{min}^{T} backwards we obtain

$$\sum_{\nu=1}^{n} \alpha^{\nu} \frac{z^n-1}{z-\alpha^{\nu}} \big((\alpha^{\nu})^{j-1} z - (\alpha^{\nu})^j \big) = (z^n-1) \sum_{\nu=0}^{n-1} (\alpha^j)^{\nu}.$$

But the last expression is zero for all $j = 1, \ldots, n-1$ as we have shown in (3.3). From this we obtain that $\operatorname{im} H_{min} \subseteq \ker G^{\mathsf{T}} = (\operatorname{im} G)^{\perp}$. Hence $H_{min} = B\hat{H}$, where $\hat{H}$ is a generator matrix of the code $(\operatorname{im} G)^{\perp}$, hence $\hat{H}$ is right invertible, and B is some polynomial matrix. By [3, Thm. 3] the overall constraint length of $\operatorname{im} \hat{H}$ is $n-1$, too. But then Part 1) of this proof implies $\det(B) \in \mathbb{F}\backslash\{0\}$ and thus H_{min} is right-invertible, too. □

We wish to point out the slight similarity of the matrix H_{min} with a construction in [19, pp. 445]. Therein, MDS codes with parity check matrices of the form $H_1 z + H_0$, where H_0, H_1 are Vandermonde matrices, are presented. However, in that construction the codes have large dimension $k > \frac{n}{2}$ while in our case $k = 1$.

4 Cyclicity

In this section we will show that for positive overall constraint length the codes given in Theorem 2.1 are cyclic if and only if $\operatorname{ord}(\alpha) = n$. Cyclic convolutional codes have been introduced in [18] and [20] and were studied in detail in [8]. We will introduce the notion of cyclicity as needed for our puroposes and refer to the papers [18, 20, 8, 5] for a motivation and the details.

Just like for cyclic block codes we assume from now on that the length n and the field size $|\mathbb{F}|$ are coprime. Moreover, we will use the standard identification

$$\mathfrak{p} : \mathbb{F}^n \longrightarrow A := \mathbb{F}[x]/\langle x^n - 1 \rangle, \quad (v_0, \ldots, v_{n-1}) \longmapsto \sum_{i=0}^{n-1} v_i x^i \tag{4.1}$$

of $\mathbb{F}^n$ with the ring of polynomials modulo $x^n - 1$. Then we can identify $\mathbb{F}[z]^n = \{\sum_{\nu=0}^{N} z^{\nu} v_{\nu} \mid N \in \mathbb{N}_0,\, v_{\nu} \in \mathbb{F}^n\}$ with the polynomial ring

$$A[z] := \Big\{ \sum_{\nu=0}^{N} z^{\nu} a_{\nu} \,\Big|\, N \in \mathbb{N}_0,\, a_{\nu} \in A \Big\}$$

by extending the mapping $\mathfrak{p}$ above coefficientwise. Following the theory of cyclic block codes one would like to declare a convolutional code $\mathcal{C} \subseteq \mathbb{F}[z]^n$ cyclic if it is invariant under the cyclic shift acting on $\mathbb{F}[z]^n$, or, equivalently, if its image in $A[z]$ is an ideal. However, it has been shown in [18, 20, 8] that this does not lead to any codes other than cyclic block codes. Due to this result a more general notion of cyclicity has been introduced and discussed in the papers mentioned above. This concept is based on some automorphism of the $\mathbb{F}$-algebra A. Thus, let $\operatorname{Aut}_{\mathbb{F}}(A)$ be the group of all $\mathbb{F}$-automorphisms on A. It is

clear that each automorphism $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$ is uniquely determined by the single value $\sigma(x) \in A$, but not every choice for $\sigma(x)$ determines an automorphism on A.

Fixing an arbitrary automorphism $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$ we define a new multiplication on the $\mathbb{F}[z]$-module $A[z]$ via

$$az = z\sigma(a) \text{ for all } a \in A. \tag{4.2}$$

Along with associativity and distributivity and where multiplication inside A is defined as usual, this turns $A[z]$ into a ring which is denoted by $A[z;\sigma]$. Notice that $A[z;\sigma]$ is non-commutative unless σ is the identity. Moreover, the mapping

$$\mathfrak{p} : \mathbb{F}[z]^n \longrightarrow A[z;\sigma], \quad \sum_{\nu=0}^{N} z^\nu v_\nu \longmapsto \sum_{\nu=0}^{N} z^\nu \mathfrak{p}(v_\nu)$$

where $\mathfrak{p} : \mathbb{F}^n \to A$ is as in (4.1), is an isomorphism of left $\mathbb{F}[z]$-modules. Now we declare a submodule $\mathcal{C} \subseteq \mathbb{F}[z]^n$ to be *σ-cyclic* if $\mathfrak{p}(\mathcal{C})$ is a left ideal in $A[z;\sigma]$. The latter is equivalent to saying that the $\mathbb{F}[z]$-submodule $\mathfrak{p}(\mathcal{C})$ is closed under left multiplication by x. In the papers [18, 8, 6, 5] the algebraic properties of these codes have been investigated in detail and plenty of cyclic convolutional codes, all optimal with respect to their free distance, have been presented.

In order to investigate the codes given in Theorem 2.1 with respect to cyclicity we need some more details about $A[z;\sigma]$. By coprimeness of the length n and $\mathrm{char}(\mathbb{F})$ there exists a prime factorization

$$x^n - 1 = \pi_1 \cdot \ldots \cdot \pi_r, \tag{4.3}$$

where $\pi_1, \ldots, \pi_r \in \mathbb{F}[x]$ are irreducible, monic, and pairwise different. We will always assume that $\pi_1 = x - 1$. As a consequence, the ring A contains a unique list of primitive and pairwise orthogonal idempotents given by

$$\varepsilon^{(j)} = \gamma_j \prod_{\substack{i=1 \\ i \neq j}}^{r} \pi_i \text{ for some } \gamma_j \in \mathbb{F}^*, \quad j = 1, \ldots, r, \tag{4.4}$$

where γ_j is such that $\varepsilon^{(j)} \mathrm{mod}\ \pi_i = \delta_{ij}$ for all $i, j = 1, \ldots, r$. This implies in particular $\gamma_1 = \frac{1}{n}$, thus

$$\varepsilon^{(1)} = \frac{1}{n} \sum_{i=0}^{n-1} x^i. \tag{4.5}$$

Now we can prove the main result of this section. We will make heavy use of the results derived in [8].

Theorem 4.1 *Let $n \in \mathbb{N}$ be coprime with $|\mathbb{F}|$ and let $\alpha \in \mathbb{F}$ be such that $\mathrm{ord}(\alpha) \geq n$. Moreover, let $\delta \in \mathbb{N}$ and put G as in (2.1). Define the submodule $\mathcal{C} := \mathrm{im}\, G$. Then $\mathcal{C}$ is σ-cyclic for some $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$ if and only if $\mathrm{ord}(\alpha) = n$. In this case $\mathcal{C}$ is σ-cyclic for the automorphism σ defined via $\sigma(x) = \alpha x$.*

Remember that only for specific values of δ these submodules are actually convolutional codes, see also Remark 2.2. Recall also from the last section that in the case $\mathrm{ord}(\alpha) = n > \delta$ the codes can be described by a certain Vandermonde parity check matrix. Therefore, in this case the codes have a very rich structure.

PROOF: "If-part": First of all, since $(\alpha x)^i, i = 0, \ldots, n-1$, are linearly independent over $\mathbb{F}$ and $(\alpha x)^n = 1$, the mapping σ defined via $\sigma(x) = \alpha x$ is indeed an automorphism on A. We have to prove that $\mathfrak{p}(\mathcal{C})$ is closed with respect to left multiplication by x. Thus, consider the image of G under the mapping $\mathfrak{p}$, i. e., define

$$g := \mathfrak{p}(G) = \sum_{\nu=0}^{\delta} z^\nu \sum_{i=0}^{n-1} \alpha^{\nu i} x^i \in A[z;\sigma]. \tag{4.6}$$

Using $\sigma^\nu(x) = \alpha^\nu x$ one calculates $\sigma^\nu(x) \sum_{i=0}^{n-1} \alpha^{\nu i} x^i = \sum_{i=0}^{n-1} \alpha^{\nu(i+1)} x^{i+1} = \sum_{i=0}^{n-1} \alpha^{\nu i} x^i$. By virtue of (4.2) this yields $xg = g$. Making use of the $\mathbb{F}[z]$-linearity of $\mathfrak{p}$ it is now straightforward to see that $x\mathfrak{p}(uG) \in \mathfrak{p}(\mathcal{C})$ for each $u \in \mathbb{F}[z]$, proving the desired result.
"Only-if-part": We will make use of the notation introduced in (4.3) – (4.5). Let $\mathcal{C}$ be σ-cyclic for some $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$. By assumption $\mathrm{ord}(\alpha) \geq n$ and we have to show that $\mathrm{ord}(\alpha) = n$. By assumption and $\mathbb{F}[z]$-linearity of $\mathfrak{p}$ the set $\mathfrak{p}(\mathcal{C})$ is the left ideal generated by g as given in (4.6), see also [8, Prop. 6.8]. Since $\mathrm{rank}\, \mathcal{C} = 1$, the generator matrix G is unique up to a nonzero constant in $\mathbb{F}$. Thus, the generator of the left ideal is also unique up to a constant factor and, along with [8, Cor. 4.13 and Thm. 4.15(b)], this shows that the polynomial g is reduced in the sense of [8, Def. 4.9(b)]. Moreover, since the code is one-dimensional we obtain from [8, Thm. 7.13] that $g = \varepsilon^{(k)} g$ for some $k = 1, \ldots, r$ such that $\deg \pi_k = 1$. In particular we have $g_0 = \varepsilon^{(k)} g_0$ for the constant coefficient g_0 of g. Since (4.6) and (4.5) yield $g_0 = n\varepsilon^{(1)}$ and $\varepsilon^{(k)}\varepsilon^{(1)} = 0$ for $k > 1$, we conclude $k = 1$, thus $g = \varepsilon^{(1)} g$. Therefore,

$$g_0 + zg_1 + z^2 g_2 + \ldots + z^\delta g_\delta = \varepsilon^{(1)} g_0 + z\sigma(\varepsilon^{(1)}) g_1 + z^2 \sigma^2(\varepsilon^{(1)}) g_2 + \ldots + z^\delta \sigma^\delta(\varepsilon^{(1)}) g_\delta$$

where g_ν is the coefficient of z^ν in g. Hence, $g_\nu = \sigma^\nu(\varepsilon^{(1)}) g_\nu$ for all $\nu = 0, \ldots, \delta$. Moreover, since $\delta > 0$ we have $\sigma(\varepsilon^{(1)}) \neq \varepsilon^{(1)}$ for otherwise the code would have overall constraint length zero, see [5, Lemma 3.4]. Consider now the coefficient $g_1 = \sum_{i=0}^{n-1} (\alpha x)^i$. The equation $g_1 = \sigma(\varepsilon^{(1)}) g_1$ along with the orthogonality of the idempotents implies $\varepsilon^{(1)} g_1 = 0$. Substituting $x = 1$, we obtain $\sum_{i=0}^{n-1} \alpha^i = 0$. But then $\sum_{i=0}^{n-1} \alpha^i(\alpha - 1) = \alpha^n - 1 = 0$ which along with the assumption $\mathrm{ord}(\alpha) \geq n$ implies $\mathrm{ord}(\alpha) = n$. □

We want to close the paper with yet another representation of the cyclic codes considered so far. In [8, Prop. 7.10] it has been shown that a polynomial $g \in A[z;\sigma]$ with the property $g = \varepsilon^{(k)} g$ for some $k = 1, \ldots, r$ generates an ideal that is a convolutional code, i. e., a direct summand in the left $\mathbb{F}[z]$-module $A[z;\sigma]$, if and only if $g = \varepsilon^{(k)} u$ for some unit $u \in A[z;\sigma]$. More details about this can be found in [5]. In the situation of Theorem 2.1 we can easily derive how such a unit looks like. The same kind of arguments also provide us with yet another representation of these codes.

Proposition 4.2 *Let* $\mathrm{ord}(\alpha) = n$ *and let* $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$ *be defined via* $\sigma(x) = \alpha x$. *Let* $x^n - 1$ *be factored as in* (4.3) *where now* $r = n$ *and* $\pi_i = x - \alpha^{i-1}$ *for* $i = 1, \ldots, n$.

Furthermore, let $1 \leq \delta \leq n-1$ *and let* G *and* $\mathcal{C}$ *be as in Theorem 2.1. Finally, let* $g = \mathfrak{p}(G)$. *Then*

(a) $g = \varepsilon^{(1)}u$ *where* $u = n(1 + z\varepsilon^{(n)})(1 + z\varepsilon^{(n-1)}) \cdot \ldots \cdot (1 + z\varepsilon^{(n-\delta+1)})$ *and* u *is a unit in* $A[z;\sigma]$.

(b) The ideal $\mathfrak{p}(\mathcal{C})$ *in* $A[z;\sigma]$ *is the left ideal generated by* $\prod_{i=1}^{n-1}(x-\alpha^i)\sum_{\nu=0}^{\delta} z^\nu$.

Because of (b) we call these codes one-dimensional Reed-Solomon convolutional codes.

PROOF: (a) Let us first investigate the action of σ on the primitive idempotents. Using $\mathrm{ord}(\alpha) = n$ and (4.4), we have $\varepsilon^{(j)} = \gamma_j \prod_{i\in\{0,\ldots,n-1\}\setminus\{j-1\}}(x-\alpha^i)$ and

$$\sigma(\varepsilon^{(j)}) = \varepsilon^{(j)}(\alpha x) = \gamma_j \prod_{\substack{i=0\\ i\neq j-1}}^{n-1} (\alpha x - \alpha^i) = \gamma_j \alpha^{n-1} \prod_{\substack{i=0\\ i\neq j-1}}^{n-1} (x - \alpha^{i-1}) = \gamma_j \alpha^{n-1} \prod_{\substack{i=0\\ i\neq j-2 \bmod n}}^{n-1} (x - \alpha^i).$$

Since $\sigma(\varepsilon^{(j)})$ is one of the idempotents again, see [8, (4.2)], it follows $\sigma(\varepsilon^{(j)}) = \varepsilon^{(j-1)}$ for $j = 2,\ldots,n$ and $\sigma(\varepsilon^{(1)}) = \varepsilon^{(n)}$. From this and the orthogonality of the idempotents we obtain $(1 + z\varepsilon^{(n-j)})(1 - z\varepsilon^{(n-j)}) = (1 - z\varepsilon^{(n-j)})(1 + z\varepsilon^{(n-j)}) = 1$ for $j = 0,\ldots,n-1$. Thus u is indeed a unit in $A[z;\sigma]$. Furthermore, one can show by induction on δ that

$$u = n\Big(1 + z \sum_{k=n-\delta+1}^{n} \varepsilon^{(k)} + z^2 \sum_{k=n-\delta+1}^{n-1} \varepsilon^{(k)} + \ldots + z^\delta \sum_{k=n-\delta+1}^{n-\delta+1} \varepsilon^{(k)}\Big) \text{ for } \delta = 1,\ldots,n-1,$$

where a sum is zero if the lower index is strictly bigger than the upper one. Using $\varepsilon^{(1)}z^\nu = z^\nu \sigma^\nu(\varepsilon^{(1)}) = z^\nu \varepsilon^{(n-\nu+1)}$ for $\nu = 1,\ldots,n$ we derive that

$$\varepsilon^{(1)}u = n\Big(\varepsilon^{(1)} + \sum_{\nu=1}^{\delta} z^\nu \varepsilon^{(n-\nu+1)} \sum_{k=n-\delta+1}^{n-\nu+1} \varepsilon^{(k)}\Big) = n\Big(\varepsilon^{(1)} + \sum_{\nu=1}^{\delta} z^\nu \varepsilon^{(n-\nu+1)}\Big) = n\varepsilon^{(1)} \sum_{\nu=0}^{\delta} z^\nu.$$

On the other hand, the identity $\sigma^\nu(x) = \alpha^\nu x$ yields $\sigma^\nu\big(\varepsilon^{(1)}\big) = \varepsilon^{(1)}(\alpha^\nu x) = \frac{1}{n}\sum_{i=0}^{n-1} \alpha^{\nu i} x^i$ and by virtue of (4.6) we get $g = n\varepsilon^{(1)}\sum_{\nu=0}^{\delta} z^\nu = \varepsilon^{(1)}u$.
Part (b) follows now from (4.4) and since the element $n \in \mathbb{F}$ is a unit in $A[z;\sigma]$ □

The representation of cyclic codes via units like in Proposition 4.2(a) has been proven useful in [5] in order to investigate as to which algebraic parameters (field size, dimension, overall constraint length, and Forney indices) can be realized by cyclic convolutional codes. In particular, a construction of certain compact cyclic convolutional codes (i. e., all Forney indices are the same) has been derived. In the paper [7] higher-dimensional Reed-Solomon convolutional codes are introduced and the presentation as in part (b) above was helpful in order to determine the distance of these codes.

Open Problems

We have presented a class of one-dimensional convolutional codes with maximum possible distance. The construction requires a field element α with order at least n, the length of

the code. In the specific case where $\mathrm{ord}(\alpha) = n$ these codes are cyclic and have a Vandermonde parity check matrix. Without using explicitly Vandermonde matrices, but highly the theory of cyclic convolutional codes, first attempts are currently under investigation of how to generalize the construction of cyclic convolutional codes with large distance to higher dimensions, see [7]. In general, we consider it most important to understand whether Vandermonde structure of a cyclic convolutional code can be exploited for distance computations and algebraic decoding algorithms. We think that the one-dimensional cyclic MDS codes with their rich structure as presented in this paper might be a good starting point in this regard.

References

[1] J. A. Domínguez Pérez, J. M. Muñoz Porras, and G. Serrano Sotelo. Convolutional codes of Goppa type. *Appl. Algebra Engrg. Comm. and Comput.*, 15:51–61, 2004.

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

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

[4] H. Gluesing-Luerssen. On the weight distribution of convolutional codes. Preprint 2005. Submitted. Available at http://front.math.ucdavis.edu/ with ID-number IT/0501016, 2005.

[5] H. Gluesing-Luerssen and B. Langfeld. On the algebraic parameters of convolutional codes with cyclic structure. Preprint 2003. Accepted for publication in Journal of Algebra and its Applications. Available at http://front.math.ucdavis.edu/ with ID-number RA/0312092.

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

[7] H. Gluesing-Luerssen and W. Schmale. On doubly-cyclic convolutional codes. Preprint 2004. Submitted. Available at http://front.math.ucdavis.edu/ with ID-number RA/0410317.

[8] H. Gluesing-Luerssen and W. Schmale. On cyclic convolutional codes. *Acta Applicandae Mathematicae*, 82:183–237, 2004.

[9] R. Hutchinson, J. Rosenthal, and R. Smarandache. Convolutional codes with maximum distance profile. Preprint 2003. To appear in Systems and Control Letters. Available at http://front.math.ucdavis.edu/ with ID-number OC/0307196.

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

[11] J. Justesen. New convolutional code constructions and a class of asymptotically good time-varying codes. *IEEE Trans. Inform. Theory*, IT-19:220–225, 1973.

[12] J. Justesen. Algebraic construction of rate $1/\nu$ convolutional codes. *IEEE Trans. Inform. Theory*, IT-21:577–580, 1975.

[13] J. Justesen, E. Paaske, and M. Ballan. Quasi-cyclic unit memory convolutional codes. *IEEE Trans. Inform. Theory*, IT-36:540–547, 1990.

[14] J. L. Massey, D. J. Costello, and J. Justesen. Polynomial weights and code constructions. *IEEE Trans. Inform. Theory*, IT-19:101–110, 1973.

[15] 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.

[16] R. J. McEliece. How to compute weight enumerators for convolutional codes. In M. Darnell and B. Honory, editors, *Communications and Coding (P. G. Farrell 60th birthday celebration)*, pages 121–141. Wiley, New York, 1998.

[17] J. M. Muñoz Porras, J. A. Domínguez Pérez, J. I. Iglesias Curto, and G. Serrano Sotelo. Convolutional Goppa codes. Preprint 2003. Available at http://front.math.ucdavis.edu/ with ID-number OC/0310149.

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

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

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

[21] 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.

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

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

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

[25] R. Smarandache and J. Rosenthal. A state space approach for constructing MDS rate $1/n$ convolutional codes. In *Proceedings of the 1998 IEEE Information Theory Workshop on Information Theory, Killarney, Ireland*, pages 116–117, 1998.