On the Construction of 1-D MDS Convolutional Goppa Codes

Francisco J. Plaza-Martín, José I. Iglesias-Curto, and Gloria Serrano-Sotelo

***Abstract*—We show that the free distance, as a function on a space parameterizing a family of convolutional codes, is a lower semicontinuous function and that, therefore, the property of being maximum distance separable (MDS) is an open condition. For a class of convolutional codes, an algorithm is offered to compute the free distance. The behavior of the free distance by enlargements of the alphabet and by increasing the length is also studied. As an application, the algebraic equations characterizing the subfamily of MDS codes are explicitly computed for families of 1-D convolutional Goppa codes.**

***Index Terms*—Algebro-geometric codes, coding theory, convolutional codes, families of codes, free distance, maximum distance separable (MDS) codes.**

I. Introduction

When constructing convolutional codes, two basic requirements are demanded: usability and high error-correction capability. With regard to the first feature, note that the smaller the alphabet (i.e., the base field), the easier the implementation. With respect to the second one, the so-called maximum distance separable (MDS) codes are the most significant [9, Th. 3.3], since they have the largest possible distance between codewords [18]. It is possible that both properties might not be optimized simultaneously since, for instance, the existence of certain MDS codes has only been proved over large enough fields [10], [18, Th. 2.10]. Indeed, it is hard to find references with explicit general methods for constructing MDS convolutional codes [2], [6].

In this paper, we report a detailed study of the free distance. More precisely, we provide an algorithm for computing the free distance, a proof of its lower semicontinuity, and its preservation by enlargements of the alphabet. As applications, we offer examples of families of MDS convolutional Goppa codes (CGC, see, e.g., [3], [14]), where the size of the base field has been kept as small as possible, as well as a method to produce MDS CGC of greater length.

Our techniques are based on algebraic tools, as in the pioneering work of Forney [4]. Similar approaches have been used fruitfully in the study of convolutional codes [11], [15], [17] and have provided good insight into their structure, such as a generalization of the singleton bound [18, Th. 2.2].

Manuscript received August 12, 2011; revised March 05, 2012; accepted March 01, 2013. Date of current version June 12, 2013. This work was supported by the Spanish Ministry of Science and Innovation under Project MTM2012-32342.

The authors are with the Department of Mathematics and IUFFyM, University of Salamanca, 37008 Salamanca, Spain (e-mail: fplaza@usal.es; joseig@usal.es; laina@usal.es).

Communicated by A. Ashikhmin, Associate Editor for Coding Techniques.

Digital Object Identifier 10.1109/TIT.2013.2251926

This paper is organized and its main results are presented as follows. After some preliminaries (see Section II), a case study is given in Section III-A. This *toy model* clearly exhibits the type of problems we are concerned with.

The computation of the free distance $\mathrm{d}_{\mathrm{free}}$ is a hard task for arbitrary codes. In order to estimate or compute $\mathrm{d}_{\mathrm{free}}$, in some cases, it is possible to use the well-known fact that the sequence of row distances converges to $\mathrm{d}_{\mathrm{free}}$ [9, Th. 3.5]. Nevertheless, the explicit computation normally requires *ad hoc* methods for each particular situation. The relation between the sequences of row distances, column distances, and active distances and $\mathrm{d}_{\mathrm{free}}$ is a highly interesting problem when designing convolutional codes (recall, for instance, the notions of maximum distance profile and strongly MDS, see, e.g., [7] and [8]). In this paper, for the first time, we are able to bound the stage at which the sequence of row distances has reached the free distance (see Theorem III.1).

The second issue in this section consists of showing that the free distance is preserved when the alphabet is enlarged (see Theorem III.3).

Section III continues with the study of convolutional codes depending on parameters, i.e., families of codes defined over a parameter space. In this situation, we prove that the free distance, which can be understood as a function from the parameter space to $\mathbb{Z}$, is lower semicontinuous (see Theorem III.6). Accordingly, the subset of the parameter space corresponding to MDS codes is open (Corollary III.8) or, tantamount to this, the closed subset of non-MDS codes is defined by finitely many algebraic relations in the parameters. This result improves that of [18, Sec. 5], which claims that the subset of MDS convolutional codes contains an open subset.

Applications of these results are to be found in Section IV. First, for the case of 1-D CGC [2], we offer systematic constructions of families as well as the explicit equations characterizing the locus of non-MDS codes as a subset of the parameter space. By demonstrating examples of MDS codes over small fields, we improve the result of [18] concerning the existence of MDS codes (see Corollary III.9), which requires that the field must have sufficiently many elements. Second, we offer a procedure that enables us to increase the length of a CGC, preserving the condition of being MDS (see Section IV-B).

The paper ends with some conclusions and possible directions for future work (see Section V).

II. Preliminaries

A. Convolutional Codes

We set an arbitrary q-ary alphabet where q is a power of a prime number p. That is, we work on a finite field, $\mathbb{F}$, with q elements and characteristic p. Let us now recall some basic facts

on convolutional codes following the classical references [4], [9], [12], [16].

A convolutional code is defined to be a $\mathbb{F}(z)$-subspace of $\mathbb{F}(z)^n$. The *length* of the code is the number n and the *dimension* of the code is its dimension as a $\mathbb{F}(z)$-vector space.

However, let us briefly comment the approach in terms of $\mathbb{F}[z]$-modules, which will be more suitable for our study. Note that each $\mathbb{F}[z]$-submodule of $\mathbb{F}[z]^n$, C, canonically yields a convolutional code $C \otimes_{\mathbb{F}[z]} \mathbb{F}(z)$. Since every convolutional code arises in this way, there is a bijective correspondence between convolutional codes and the equivalence classes of $\mathbb{F}[z]$-submodules, where C and C' are defined to be equivalent if $C \otimes_{\mathbb{F}[z]} \mathbb{F}(z) = C' \otimes_{\mathbb{F}[z]} \mathbb{F}(z)$ as subspaces of $\mathbb{F}(z)^n$.

Observe that for $G(z)$ a $k \times n$-matrix with entries in $\mathbb{F}[z]$, we may consider ϕ to be the $\mathbb{F}[z]^n$-linear map defined by it

$$\phi : \mathbb{F}[z]^k \hookrightarrow \mathbb{F}[z]^n \tag{1}$$

as well as its image, $C := \mathrm{Im}\phi$, which is the $\mathbb{F}[z]$-submodule generated by the rows of $G(z)$. In this setup, $G(z)$ is called the *generator matrix* of the convolutional code defined by C. It is known that each convolutional code has a generator matrix whose entries are polynomials [4].

Recall from commutative algebra that the following three conditions are equivalent: 1) the maximal minors of $G(z)$ are coprime (as polynomials in z); 2) $\mathrm{Coker}\phi$ is locally free; and, 3) C is a direct summand of $\mathbb{F}[z]^n$. If condition 1) is satisfied, we say that $G(z)$ is a basic generator matrix for (the convolutional code associated with) C. If it is not possible to reduce the row degrees of the generator matrix by elemental row operations, the matrix is called *reduced*. If it is both basic and reduced, we say that it is *canonical*.

Furthermore, for each convolutional code, there exists a representative of the associated equivalence class, $C \subset \mathbb{F}[z]^n$, such that C is a direct summand of $\mathbb{F}[z]^n$. In other words, every convolutional code admits a basic generator matrix. Consequently, every convolutional code admits a canonical generator matrix [12].

Henceforth, and for the sake of brevity, instead of "the convolutional code corresponding to the equivalence class of a $\mathbb{F}[z]$-submodule C," we shall simply say "the convolutional code defined by C".

The row degrees of a canonical generator matrix are invariants of the code (up to their order) and are known as the *Forney indices* of the code $\nu_1, \ldots, \nu_k$. The maximum of the Forney indices is called the *memory* of the code m, and their sum is the *degree* (or complexity) of the code δ, and this coincides with the highest degree of the maximal minors of the matrix.

Similarly to the case of block codes, there is a notion of distance that determines the error-correction capability of the convolutional code (see, e.g., [9, Th. 3.3]). Let us first recall that the weight of a polynomial vector is the number of the nonzero coefficients, that is, for a word $c = (a_{10} + \cdots + a_{1r_1} z^{r_1}, \ldots, a_{n0} + \cdots + a_{nr_n} z^{r_n})$, its weight is

$$\mathrm{w}(c) := \#\{a_{ij} | a_{ij} \neq 0\}.$$

Thus, the free distance between two codewords is the weight of their difference, and the *free distance* of the convolutional code $\mathrm{d}_{\mathrm{free}}$ is the minimum free distance between two different codewords. It is therefore natural to look for codes with the largest possible free distance. Accordingly, Rosenthal and Smarandache [18] studied the free distance of an arbitrary convolutional code and proved that it satisfies

$$\mathrm{d}_{\mathrm{free}} \leq (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1. \tag{2}$$

This bound is called the generalized singleton bound, since for codes of degree 0, i.e., block codes, it gives the classical singleton bound on the minimum distance. Consequently, MDS convolutional codes are defined as those whose free distance achieves the generalized singleton bound. Note that for the case of 1-D codes, the generalized singleton bound acquires a simpler form

$$\mathrm{d}_{\mathrm{free}} \leq n(\delta + 1). \tag{3}$$

B. Classification of Convolutional Codes

In [15], a classifying space for convolutional codes was introduced, providing valuable information about the structure of convolutional codes. Before briefly recalling a couple of results of that paper, let us first introduce some definitions that have no counterpart in the theory of block codes.

The ith *column index* of a code C is the maximum of the degrees of the entries of the ith column of a matrix $G(z)$ as $G(z)$ varies among the set of canonical generator matrices for C. Let $\{n_i\}_{i=1}^n$ denote the sequence of column indices. It is known [15, Th. 4.9] that there is an injective morphism

$$\left\{ \begin{array}{c} \text{convolutional codes of type } [n,k,\delta;m] \\ \text{with column indices } \{n_i\}_{i=1}^n \end{array} \right\} \hookrightarrow Gr(\kappa,\mu)$$

where $\kappa = k(m+1) - \delta, \mu = \sum_{i=1}^n (n_i + 1)$ and $Gr(\kappa,\mu)$ denotes the Grassmannian variety of κ-dimensional subspaces of a given μ-dimensional vector space.

Theorem II.1 [15, Th. 4.13]: Convolutional codes of type $[n,k,\delta;m]$ that have different Forney indices, i.e., $\delta < km$, are represented by an open subset of a closed subset of the Grassmannian $Gr(\kappa,\mu)$.

Convolutional codes of type $[n,k,\delta;m]$ that have all their Forney indices equal, i.e., $\delta = km$, are represented by an open subset of the Grassmannian $Gr(\kappa,\mu)$.

C. Zariski Topology

Since this paper deals with the study of some algebraic properties as certain parameters vary, it is natural to consider the Zariski topology. Indeed, *open* and *closed* in the statement of Theorem II.1 refer to the Zariski topology. Although this topology can be introduced for very general spaces (e.g., schemes), the case of the affine space will suffice for our purposes [1]. The reason for this assumption relies on the two aforementioned results and on the fact that Grassmannian varieties are covered by affine spaces.

A subset Z of the affine space $\mathbb{F}^{r+1}$ is called *Zariski closed* if it is defined by a finite number of algebraic relations, that is, there exist polynomials $p_i(\lambda_0, \ldots, \lambda_r) \in \mathbb{F}[\lambda_0, \ldots, \lambda_r]$ for

$i = 1, \ldots, s$ such that Z consists of the common zeroes of $p_1, \ldots, p_s$

$$Z = \{(\alpha_0, \ldots, \alpha_r) \in \mathbb{F}^{r+1} | p_i(\alpha_0, \ldots, \alpha_r) = 0, 1 \leq i \leq s\}.$$

Accordingly, a subset $U \subseteq \mathbb{F}^{r+1}$ is called *Zariski open* if and only if its complement, $\mathbb{F}^{r+1} \setminus U$, is Zariski closed.

Moreover, for any field extension $\mathbb{F} \hookrightarrow \mathbb{F}'$, there is a bijective correspondence between the set of $\mathbb{F}'$-valued points of Z

$$Z(\mathbb{F}') := \left\{(\alpha_0, \ldots, \alpha_r) \in (\mathbb{F}')^{r+1} | p_i(\alpha_0, \ldots, \alpha_r) = 0, 1 \leq i \leq s\right\}$$

and the set of maps of $\mathbb{F}$-algebras

$$\mathbb{F}[\lambda_0, \ldots, \lambda_r]/(p_1, \ldots, p_s) \rightarrow \mathbb{F}'.$$

More explicitly, the map associated with $(\alpha_0, \ldots, \alpha_r)$ sends λ_i to α_i for all i.

Similarly, one defines the set of $\mathbb{F}'$-valued points of an open subset U. It will be denoted by $U(\mathbb{F}')$.

A well-known criterion for a subset to be closed, which will be used in the proof of Theorem III.6, is that a subset $Z \subseteq \mathbb{F}^{r+1}$ is closed if and only if for every local and integral $\mathbb{F}$-algebra A and every morphism $\mathbb{F}[\lambda_0, \ldots, \lambda_r] \rightarrow A$ the following condition holds: if the composition $\mathbb{F}[\lambda_0, \ldots, \lambda_r] \rightarrow A \rightarrow A_{(0)}$ defines a point of Z, then the composition $\mathbb{F}[\lambda_0, \ldots, \lambda_r] \rightarrow A \rightarrow A/\mathfrak{m}$ also defines a point of Z. Here, $A_{(0)}$ denotes the function field of A and $\mathfrak{m}$ the maximal ideal of A.

III. Free Distance

Let us begin this section with an example of a convolutional code depending on a parameter. The study of its structure unveils some of its most relevant properties. Indeed, these properties do hold for general codes, as will be proved rigorously in the following sections.

A. Case Study

Let us work on the 2^r-ary alphabet, that is, on the base field $\mathbb{F}_{2^r}$. We consider the matrix

$$\begin{pmatrix} \lambda + z & \lambda + 1 + z & \lambda z & 1 + (\lambda + 1)z \\ \lambda^2 + (\lambda+1)z & 1 + z & \lambda + (\lambda+1)z & (\lambda+1)^2 + \lambda z \end{pmatrix}$$

and let C_λ be its image. After some computation, we see that this matrix is a basic generator matrix of C_λ, for λ an arbitrary element of $\mathbb{F}_{2^r} \setminus \{0\}$. In this case, C_λ has length $n = 4$, rank $k = 2$, degree 2, memory 1 and, consequently, the generalized singleton bound is 7 (see (2)).

Let us choose a particular case; namely, let $r = 3$ and let $\lambda \in \mathbb{F}_8 = \mathbb{F}_{2^3}$ be an element satisfying $\lambda^3 + \lambda + 1 = 0$. After some computations, one has that the sequence of row distances of C_λ (see, e.g., [9, Ch. 3]) is the constant sequence $7, 7, 7, \ldots$, such that the free distance of C_λ is 7, and therefore, it is MDS.

Let us now discuss the general situation, i.e., $r \geq 3$ and λ arbitrary. First, let us express the aforementioned generator matrix as $G(z) = G_0 + zG_1$, with G_0, G_1 matrices over $\mathbb{F}_{2^r}[\lambda]$. In this example, we observe that the determinant of $\binom{G_0}{G_1}$ appears in the list of 2×2-minors of $(G_0 \mid G_1)$, and therefore, it can be checked that C_λ is MDS if and only if the matrix $(G_0 \mid G_1)$ generates an MDS block code; i.e., all the 2×2-minors of $(G_0 \mid G_1)$ are nonzero. Summing up, C_λ fails to be MDS if λ satisfies any of the following equations:

$$\lambda + 1 = 0$$
$$\lambda^2 + \lambda + 1 = 0$$
$$\lambda^3 + \lambda^2 + 1 = 0.$$

We also observe that the number of values of λ for which C_λ fails to be MDS is finite.

Summing up, we have observed the following three phenomena.

1) Although we know that the sequence of row distances converges to the free distance, there is no estimation for the stage in which the sequence reaches $\mathrm{d}_{\mathrm{free}}(C_\lambda)$;
2) If C_λ is MDS for $\lambda \in \mathbb{F}_{2^r}$ and $\mathbb{F}_{2^r} \hookrightarrow \mathbb{F}'$, then the code generated by C_λ over $\mathbb{F}'$ is also MDS; or, in simpler words, the property of being MDS depends only on λ and not on the base field;
3) In a family of codes depending on parameters, the subset of the parameter space consisting of those values for which the code fails to be MDS is defined by a finite number of algebraic relations.

The three following sections are devoted to an in-depth study of these issues.

B. Computation of the Free Distance

Let us consider a convolutional code C of dimension k, length n, and degree δ, with a canonical generator matrix $G(z)$ decomposing as

$$G(z) = G_0 + G_1 z + \cdots + G_\delta z^\delta$$

where G_i are $k \times n$ matrices with entries in $\mathbb{F}$. In this case, G_0 has maximal rank, and therefore, the linear map defined by the $k(l+1) \times n(\delta + l + 1)$ matrix

$$\begin{pmatrix} G_0 & \ldots & G_\delta & 0 & \ldots & 0 \\ 0 & G_0 & \ldots & G_\delta & \ddots & \vdots \\ \vdots & \ddots & \ddots & & \ddots & 0 \\ 0 & \ldots & 0 & G_0 & \ldots & G_\delta \end{pmatrix} : \mathbb{F}^{k(l+1)} \rightarrow \mathbb{F}^{n(\delta+l+1)} \tag{4}$$

is injective for $l \geq 0$. Let C_l be the linear code defined by the image of this map and let d_l^r denote the distance of C_l. In [9, Ch. 3], d_l^r is called the lth *row distances*. Since any basic encoder is noncatastrophic [13], it follows from [9, Ch. 3] that starting with a basic encoder $G(z)$, the sequence $\{d_l^r\}$ is nonincreasing and eventually converges to the free distance of the convolutional code, i.e.,

$$\mathrm{d}_{\mathrm{free}}(C) = \min_{l \geq 0} \{d_l^r\}. \tag{5}$$

However, an explicit description of the step in which the sequence of row distances reaches the free distance has not been given. Our next result tackles this problem.

Theorem III.1: Let C be a convolutional code as earlier. Let C^0 be the linear code defined by the image of the map

$$\begin{pmatrix} G_\delta \\ G_{\delta-1} \\ \vdots \\ G_0 \end{pmatrix} : \mathbb{F}^{k(\delta+1)} \rightarrow \mathbb{F}^n \tag{6}$$

and let ν and μ be the dimension and the distance of C^0.

If ν is maximal, i.e., $k(\delta+1)=\nu$, then

$$\mathrm{d}_{\mathrm{free}}(C) \;=\; d^r_{\mathrm{l}(C)}$$

where

$$\mathrm{l}(C) \;:=\; \left\lfloor \frac{1}{\mu}\Big((n-k)\Big(\left\lfloor\frac{\delta}{k}\right\rfloor+1\Big)+\delta+1\Big)\right\rfloor \;-(\delta+1). \quad (7)$$

Proof: Let us consider a nonzero polynomial vector of degree $l \geq \delta, \alpha(z) = \sum_{i=0}^{l}\alpha_i z^i \in \mathbb{F}[z]^k$, and the codeword given by it

$$\begin{aligned}\alpha(z)G(z)=&(\alpha_0,\ldots,\alpha_l)\begin{pmatrix}G_0\\0\\\vdots\\0\end{pmatrix}+(\alpha_0,\ldots,\alpha_l)\begin{pmatrix}G_1\\G_0\\0\\\vdots\\0\end{pmatrix}z+\cdots\\ &+(\alpha_0,\ldots,\alpha_l)\begin{pmatrix}G_\delta\\\vdots\\G_0\\0\\\vdots\\0\end{pmatrix}z^\delta+\cdots+(\alpha_0,\ldots,\alpha_l)\begin{pmatrix}0\\\vdots\\0\\G_\delta\\\vdots\\G_0\end{pmatrix}z^l+\\ &+\cdots+(\alpha_0,\ldots,\alpha_l)\begin{pmatrix}0\\\vdots\\0\\G_\delta\end{pmatrix}z^{\delta+l}. \quad (8)\end{aligned}$$

Our task consists of finding a lower bound for the weight of this codeword.

Suppose that there exists j, with $\delta \leq j \leq l$, such that the coefficient of z^j vanishes. The hypothesis $k(\delta+1)=\nu$ implies that $\alpha_{j-\delta}=\alpha_{j-\delta+1}=\cdots=\alpha_j=0$. In that case, we would have

$$(\sum_{i=0}^{l}\alpha_i z^i)G(z)=(\sum_{i=0}^{j-\delta-1}\alpha_i z^i)G(z)+z^{j+1}(\sum_{i=j+1}^{l}\alpha_i z^{i-(j+1)})G(z).$$

Noting that the coefficients of the second term on the right-hand side (RHS) cannot cancel the coefficients of the first term, one has that

$$\begin{aligned}\mathrm{w}\big((\sum_{i=0}^{l}\alpha_i z^i)\cdot G(z)\big) \;\geq\; \mathrm{w}\big((\sum_{i=0}^{j-\delta-1}\alpha_i z^i)\cdot G(z)\big) \;\geq\\ \geq\; d^r_{j-\delta-1} \;\geq\; d^r_l \;\geq\; \mathrm{d}_{\mathrm{free}}(C).\end{aligned}$$

Therefore, when bounding the minimum weight of codewords from below, we can leave aside those words with $\alpha_{j-\delta}=\alpha_{j-\delta+1}=\cdots=\alpha_j=0$ for certain $\delta \leq j \leq l$. Let us define

$$m_l \;:=\; \min\big\{\mathrm{w}\big((\sum_{i=0}^{l}\alpha_i z^i)G(z)\big) : \alpha_0\neq 0, \alpha_l\neq 0\big\}$$

for $l<\delta$, and

$$m_l := \min\left\{\begin{array}{c}\mathrm{w}\big((\sum_{i=0}^{l}\alpha_i z^i)G(z)\big) \text{ such that } \alpha_0\neq 0,\alpha_l\neq 0\\ \text{and } \nexists j\in\{\delta,\ldots,l\} \text{ with } \alpha_{j-\delta}=\ldots=\alpha_j=0\end{array}\right\}$$

for $l \geq \delta$.

The previous discussion shows that

$$d^r_l \;=\; \mathrm{d}(C_l) \;=\; \min\{m_0,\ldots,m_l\}. \quad (9)$$

Let us bound m_l from below. First, let us consider $l<\delta$. The hypothesis $k(\delta+1)=\nu$ shows that $k(j+1)=\mathrm{rk}\begin{pmatrix}G_j\\\vdots\\G_0\end{pmatrix}$ for all $j \leq l$. In particular, if $\alpha_0 \neq 0$, then the coefficients of $z^0, z, \ldots, z^\delta$ cannot vanish. Similarly, $\alpha_l \neq 0$ implies that the coefficients of $z^l,\ldots,z^{\delta+l}$ do not vanish either. Consequently

$$m_l \;\geq\; (l+\delta+1)\mu \qquad \forall l<\delta.$$

Second, let $l \geq \delta$. The aforementioned arguments imply that the coefficients of $z^0, z, \ldots, z^{l+\delta}$ do not vanish and thus

$$m_l \;\geq\; (l+\delta+1)\mu \qquad \forall l \geq \delta.$$

Having in mind (5) and (9), we know that there exists l_0 such that $\mathrm{d}_{\mathrm{free}}(C)=m_{l_0}$. Recalling the singleton bound for C (2), we derive the following chain of inequalities:

$$(n-k)\Big(\left\lfloor\frac{\delta}{k}\right\rfloor+1\Big)+\delta+1 \geq \mathrm{d}_{\mathrm{free}}(C)=m_{l_0} \geq (l_0+\delta+1)\mu$$

and thus

$$l_0 \;\leq\; \frac{1}{\mu}\Big((n-k)\Big(\left\lfloor\frac{\delta}{k}\right\rfloor+1\Big)+\delta+1\Big) \;-(\delta+1)$$

and the conclusion follows. ■

It is worth pointing out that the previous result provides a method to compute the free distance of a convolutional code in terms of the distance of a linear code. More precisely, we have the following.

Algorithm III.2: For a convolutional code with a canonical generator matrix $G(z)$, its free distance is given by the following procedure:

1) compute the dimension and the distance of C^0, that is, ν and μ respectively;
2) check if $k(\delta+1)=\nu$; if yes, continue;
3) compute $\mathrm{l}(C)$ by (7);
4) $\mathrm{d}_{\mathrm{free}}(C)$ is given by the distance of the linear code $C_{\mathrm{l}(C)}$ (see (4)).

C. Preservation of $\mathrm{d}_{\mathrm{free}}$ By Enlargements of the Alphabet

Similarly to the relation between BCH and RS codes, we begin by studying whether the free distance changes when the alphabet is enlarged or, equivalently, when the base field $\mathbb{F}$ is replaced by a finite extension of it, say $\mathbb{F}'$. Indeed, if $G(z)$ is a matrix with entries in $\mathbb{F}[z]$ generating a convolutional code C, then the words of C are $\mathbb{F}[z]$-linear combinations of the rows of $G(z)$. Hence, for a finite extension $\mathbb{F}\hookrightarrow\mathbb{F}'$, and considering

$\mathbb{F}'[z]$-linear combinations of the rows of $G(z)$, we obtain another convolutional code C' that is related to C by the identity $C' := C \otimes_{\mathbb{F}} \mathbb{F}'$.

Theorem III.3: The free distance is preserved by enlargements of the alphabet.

Proof: With the previous notations, the following equation must be proved:

$$\mathrm{d}_{\mathrm{free}}(C) = \mathrm{d}_{\mathrm{free}}(C').$$

Since $\mathbb{F} \hookrightarrow \mathbb{F}'$, every word of C can also be understood as a word of C'. Thus, $\mathrm{d}_{\mathrm{free}}(C) \geq \mathrm{d}_{\mathrm{free}}(C')$.

Let us now check the opposite inequality. Let $G(z)$ be a generator matrix for C. It is therefore also a generator matrix for C'. Let us choose a nonzero codeword of C' of minimal weight, which will be of the type

$$\Big(\sum_j \alpha_{1,j} z^j, \ldots, \sum_j \alpha_{n,j} z^j\Big) = \Big(\sum_j \beta_{1,j} z^j, \ldots, \sum_j \beta_{k,j} z^j\Big) \cdot G(z) \quad (10)$$

where $\beta_{i,j} \in \mathbb{F}'$. Let us consider $\mathbb{F}'' := \mathbb{F}(\{\beta_{i,j}\}_{i,j})$, which is a finite extension of $\mathbb{F}$. Let $\omega : \mathbb{F}'' \to \mathbb{F}$ be a $\mathbb{F}$-linear form. Since the following identity holds:

$$\Big(\sum_j \omega(\alpha_{1,j}) z^j, \ldots, \sum_j \omega(\alpha_{n,j}) z^j\Big) = \Big(\sum_j \omega(\beta_{1,j}) z^j, \ldots, \sum_j \omega(\beta_{k,j}) z^j\Big) \cdot G(z) \quad (11)$$

it follows that its left-hand side is a codeword of C. Thus, if there exists ω and i, j such that $\omega(\beta_{i,j}) \neq 0$, then it follows that the weight of the codeword (11) is nonzero and equal to or smaller than the weight of the codeword (10), and therefore, $\mathrm{d}_{\mathrm{free}}(C) \leq \mathrm{d}_{\mathrm{free}}(C')$. On the other hand, let us assume that $\omega(\beta_{i,j}) = 0$ for all ω and all i, j. Since $\mathbb{F}''$ is a finite-dimensional $\mathbb{F}$-vector space, it follows that $\beta_{i,j} = 0$ for all i, j, and hence, the codeword (10) is zero, which contradicts our hypothesis. ∎

D. Variation of $\mathrm{d}_{\mathrm{free}}$ Along a Family

Our second result concerning the free distance is related to its variation along the members of a family of convolutional codes. In particular, we are interested in how the condition of being MDS behaves.

Inspired by the definition of a convolutional code (see Section II-A), let us introduce the notion of a family of convolutional codes, that is, a convolutional code depending on parameters $(\lambda_0, \ldots, \lambda_r)$, where λ_i takes values in $\mathbb{F}$.

Definition III.4: A family of convolutional codes of length n and rank k defined over an open subset U of $\mathbb{F}^{r+1}$ consists of a locally free $\mathbb{F}[\lambda_0, \ldots, \lambda_r][z]$-submodule $\mathcal{C}$ of $\mathbb{F}[\lambda_0, \ldots, \lambda_r][z]^n$ such that the restriction of $\mathbb{F}[\lambda_0, \ldots, \lambda_r][z]^n/\mathcal{C}$ to U is locally free of rank $n - k$. U will be called the *parameter space* of the family.

For the sake of clarity, let us interpret this definition in terms of matrices. First, note that we are replacing our field $\mathbb{F}$ by the $\mathbb{F}$-algebra $R := \mathbb{F}[\lambda_0, \ldots, \lambda_r]$ and, in particular, that the elements of $R[z]$ are polynomials in z whose coefficients are polynomials in $\lambda_0, \ldots, \lambda_r$. Now let $\mathcal{G}(z)$ be a $k \times n$-matrix with entries in $R[z]$. Therefore, for each point $(\alpha_0, \ldots, \alpha_r)$ of the affine space $\mathbb{F}^{r+1}$, we evaluate the entries of $\mathcal{G}(z)$ at $\lambda_i = \alpha_i$ for $i = 0, \ldots, r$ and obtain a $k \times n$-matrix, say $\mathcal{G}_\alpha(z)$, with entries in $\mathbb{F}[z]$. Now, let Z be the subset of points $\alpha \in \mathbb{F}^{r+1}$ such that $\mathcal{G}_\alpha(z)$ has rank smaller than k. Let V be the set of points $\alpha \in \mathbb{F}^{r+1}$ such that there exists a neighborhood of α in which $R[z]^n/\mathcal{C}$ is free. Observe that Z is closed and V is open. Therefore, the submodule $\mathrm{Im}(\mathcal{G}(z))$ defines a family of convolutional codes of length n and rank k over the open subset $U := V \setminus Z$.

Recall that, if a generator matrix is given, V consists of those points of the parameter space where the minors of maximal rank of the generator matrix are coprime and, consequently, the generator matrix yields a canonical generator matrix of $\mathcal{C}|_V$.

From now on, calligraphic letters (such as $\mathcal{C}, \mathcal{G}, \ldots$) will refer to families, while roman letters (i.e., $C, G, \ldots$) will be used for the case of a convolutional code over a field.

Remark III.5: For $r = 0$, one has that $R[z] = \mathbb{F}[\lambda_0, z]$, and hence, the entries of the generator matrix of a family over $\mathbb{F}$ are polynomials in two variables, namely, λ_0 and z. Therefore, 2-D convolutional codes [5] are instances of 1-parameter families of convolutional codes. Similarly, convolutional codes depending on several variables might be considered as families in the sense of Definition III.4.

Accordingly, if $\mathcal{C}$ is a family of convolutional codes over the parameter space $U \subseteq \mathbb{F}^{r+1}$, we may consider the map of sets

$$\begin{aligned} \mathrm{d}_{\mathrm{free}} : U &\longrightarrow \mathbb{Z} \\ \alpha = (\alpha_0, \ldots, \alpha_r) &\longmapsto \mathrm{d}_{\mathrm{free}}(\mathcal{C}_\alpha). \end{aligned} \quad (12)$$

However, the previous section shows that $\mathrm{d}_{\mathrm{free}}(\mathcal{C}_\alpha)$ is well defined, disregarding whether $(\alpha_0, \ldots, \alpha_r)$ is considered as a point with coordinates in $\mathbb{F}$ or in an extension $\mathbb{F} \hookrightarrow \mathbb{F}'$. Consequently, $\mathrm{d}_{\mathrm{free}}$ is really a function when U is endowed with the Zariski topology; i.e., the topology inherited from $\mathbb{F}^{r+1}$. Before proving an important property of it, let us recall that a function $f : X \to \mathbb{Z}$ is called lower semicontinuous if and only if

$$f^{-1}\big((N, +\infty)\big) := \{x \in X \mid f(\alpha) > N\}$$

is Zariski open for every $N \in \mathbb{Z}$. Here, $(N, +\infty) \subset \mathbb{Z}$ denotes the open interval.

Theorem III.6: Let $\mathcal{C}$ be a family of convolutional codes over the parameter space $U \subseteq \mathbb{F}^{r+1}$.

The function $\mathrm{d}_{\mathrm{free}} : U \to \mathbb{Z}$ of (12) is lower semicontinuous.

Proof: We shall use the criterion given at the end of Section II-C in order to prove that the subset

$$\{\alpha = (\alpha_0, \ldots, \alpha_r) \in U \mid \mathrm{d}_{\mathrm{free}}(\mathcal{C}_\alpha) \leq N\}$$

is a Zariski closed subset of U. Let A be a local and integral $\mathbb{F}$-algebra and let $\mathfrak{m}$ be its maximal ideal. It suffices to consider the case where the family of convolutional codes $\mathcal{C}$ is defined over A (i.e., all entries of the matrices belong to A). We must prove that the free distance of the code $\mathcal{C}_{(0)} := \mathcal{C} \otimes_A A_{(0)}$ is equal to or greater than that of the code $\mathcal{C}_{\mathfrak{m}} := \mathcal{C} \otimes_A A/\mathfrak{m}$.

Since A is local, it follows that $\mathcal{C}$ is a free submodule of $A[z]^n$ and has a generator matrix $\mathcal{G}(z)$. Observe that the codewords of $\mathcal{C}_{(0)}$ are $A_{(0)}$-linear combinations of the rows of $\mathcal{G}(z)$.

Now, let $c' = (\sum_j \beta'_{1,j} z^j, \ldots, \sum_j \beta'_{k,j} z^j) \cdot \mathcal{G}(z)$ be a nonzero codeword of $\mathcal{C}_{(0)}$ of minimal weight. Since there is a finite number of nonzero coefficients, and since $A_{(0)}$ consists of quotients $\frac{a}{b}$ with $a, b \in A$ and $b \neq 0$, there exists $b \in A$ such that $c := b \cdot c' = (\sum_j \beta_{1,j} z^j, \ldots, \sum_j \beta_{k,j} z^j) \cdot \mathcal{G}(z)$, which is another codeword of the same weight, belongs to $\mathcal{C}$. Taking the class of $\beta_{i,j}$ modulo $\mathfrak{m}$, say $\bar{\beta}_{i,j} \in A/\mathfrak{m}$, we obtain a codeword $\bar{c} \in \mathcal{C}_{\mathfrak{m}}$.

It is now straightforward to see that $\mathrm{d}_{\mathrm{free}}(\mathcal{C}_{(0)})$, which coincides with the weight of c', is equal to or greater than the weight of $\bar{c}$ and, therefore, equal to or greater than $\mathrm{d}_{\mathrm{free}}(\mathcal{C}_{\mathfrak{m}})$. ■

Remark III.7: For a family of convolutional codes $\mathcal{C}$ over the parameter space $U \subseteq \mathbb{F}^{r+1}$, the length and the dimension are constant for all codes of the family. However, the degree, the memory, and the column indices may vary. To illustrate how the degree changes, let us consider the degree as a function

$$\begin{aligned} \delta : U &\longrightarrow \mathbb{Z} \\ \alpha = (\alpha_0, \ldots, \alpha_r) &\longmapsto \delta(\mathcal{C}_\alpha) := \text{ degree of } \mathcal{C}_\alpha. \end{aligned}$$

It follows straightforwardly that δ is a lower semicontinuous function. Analogous statements can be proved for the memory and the column indices of the family.

In [18, Sec. 5], it was shown that the subset of the set of all convolutional codes consisting of those that are MDS contains a Zariski open subset. Our previous theorem now allows us to strengthen that claim.

Corollary III.8: The subset of MDS convolutional codes is a Zariski open subset of the set of all convolutional codes.

Proof: Recall from Theorem II.1 that the set of convolutional codes $\mathfrak{C}$ can be understood as a subset of a Grassmannian, and thus, it inherits the Zariski topology. Let $\mathfrak{M}$ denote the subset of $\mathfrak{C}$ consisting of those points corresponding to MDS convolutional codes. Thus, $\mathfrak{M}$ will be an open subset of $\mathfrak{C}$ if and only if there is a covering of the Grassmannian by Zariski open subsets $\{V_i\}$ such that $\mathfrak{M} \cap V_i$ is open in $\mathfrak{C} \cap V_i$ for all i.

Bearing in mind that Grassmannian are covered by affine spaces or, equivalently, that V_i can be assumed to be isomorphic to $\mathbb{F}^{r+1}$ for some r, it suffices to prove the following statement: let $\mathcal{C}$ be a family of convolutional codes over the parameter space U where U is a subset of $\mathbb{F}^{r+1}$; accordingly, the subset $\{\alpha \in U | \mathcal{C}_\alpha \text{is MDS}\}$ is Zariski open in U.

Furthermore, since we are dealing with a single Grassmannian of the type $Gr(\kappa, \mu)$, and hence connected, it may be assumed that the degree, the memory, and the sum of the column indices are constant along the family $\mathcal{C}$. Theorem II.1 implies that there is a well-defined map

$$\begin{aligned} U &\to \psi\mathfrak{C} \subset Gr(\kappa, \mu) \\ (\alpha_0, \ldots, \alpha_r) &\longmapsto \mathcal{C}_\alpha \end{aligned}$$

and, in particular, that the singleton bound (2) is the same constant, say N, for each code of the family corresponding to points of U.

Now, the subset of U consisting of MDS convolutional codes is precisely

$$\begin{aligned} \{\alpha \in U \mid \mathcal{C}_\alpha \text{ is MDS}\} &= U \cap \psi^{-1}(\mathfrak{M}) \\ &= \mathrm{d}_{\mathrm{free}}^{-1}\big((N-1, +\infty)\big) \cap U \end{aligned}$$

($\mathrm{d}_{\mathrm{free}} : U \to \mathbb{Z}$ being as above), which is Zariski open in U by Theorem III.6. ■

Corollary III.9: Let $\mathcal{C}$ be a family of convolutional codes over a parameter space U, where U is a nonempty open subset of $\mathbb{F}$.

For a finite extension $\mathbb{F} \hookrightarrow \mathbb{F}'$, let us define

$$N(\mathbb{F}') := \#\left\{ \begin{array}{c} \alpha \in U(\mathbb{F}') \text{ such that} \\ (\mathcal{C} \otimes_{\mathbb{F}} \mathbb{F}')_\alpha \text{ is non-MDS} \end{array} \right\}$$

where $U(\mathbb{F}')$ is the set of $\mathbb{F}'$-valued points of U (see Section II-C).

If $N(\mathbb{F}) > 0$, then there exists $N \in \mathbb{N}$, depending only on $\mathcal{C}$, such that

$$N(\mathbb{F}') \leq N$$

for any finite extension $\mathbb{F} \hookrightarrow \mathbb{F}'$.

Proof: Let $\bar{\mathbb{F}}$ denote the algebraic closure of $\mathbb{F}$. Recall that $\mathcal{C}$ is a submodule of $\mathbb{F}[\lambda_0][z]^n$ and thus $(\mathcal{C} \otimes_{\mathbb{F}} \bar{\mathbb{F}})$ is a submodule of $\bar{\mathbb{F}}[\lambda_0][z]^n$. For each $\alpha \in \bar{\mathbb{F}}$, evaluating λ_0 at α, one obtains a convolutional code $(\mathcal{C} \otimes_{\mathbb{F}} \bar{\mathbb{F}})_\alpha$.

Let V_1 be the set of $\alpha \in \bar{\mathbb{F}}$ such that $(\mathcal{C} \otimes_{\mathbb{F}} \bar{\mathbb{F}})_\alpha$ is locally free of rank k. Let V_2 be the maximal subset of $\bar{\mathbb{F}}$ where $\bar{\mathbb{F}}[\lambda_0][z]^n/(\mathcal{C} \otimes_{\mathbb{F}} \bar{\mathbb{F}})$ is locally free. It is easy to check that both V_1 and V_2 are open; $\mathcal{C} \otimes_{\mathbb{F}} \bar{\mathbb{F}}$ defines a family of convolutional codes over $V_1 \cap V_2$, and $V_1 \cap V_2$ contains $U(\mathbb{F}')$ for any extension $\mathbb{F}'$. Corollary III.8 shows that

$$W := \{\alpha \in V_1 \cap V_2 \mid (\mathcal{C} \otimes_{\mathbb{F}} \bar{\mathbb{F}})_\alpha \text{ is MDS}\}$$

is an open subset of $\bar{\mathbb{F}}$, which is nonempty by hypothesis.

Since nontrivial closed subsets of $\bar{\mathbb{F}}$ are finite sets, it follows that $N(\bar{\mathbb{F}})$ is finite and coincides with the number of points of the complement of W. Bearing in mind that $N(\mathbb{F}') \leq N(\bar{\mathbb{F}})$ for any finite extension $\mathbb{F} \hookrightarrow \mathbb{F}'$, the claim is proved. ■

IV. Applications to 1-D MDS CGC

This section applies the previous results for the study of MDS CGCs. In particular, it is worth noticing that these computations are carried out on small fields and consequently that there is no need to consider fields with sufficiently many elements in order to prove that the set of 1-D MDS CGC is nonempty. Recall that the nonemptiness of the set of MDS convolutional codes was proved in [18] under the assumption that the field was large enough.

For simplicity, we shall restrict ourselves to the case of 1-D codes constructed on the projective line [2]. Interested readers can check the general construction of higher dimensional CGC on arbitrary curves in [3] and [14]. Observe that if a 1-D convolutional code is MDS, then its column indices are all equal to the degree. Hence, we also assume that $n_i = \delta$ for all $i \leq n$.

Let us briefly recall the construction of CGC. Let $\mathbb{P}^1$ be the projective line over the field $\mathbb{F}(z)$. Fix a point at infinity p_∞ and an affine coordinate t in $\mathbb{A}^1 = \mathbb{P}^1 \backslash p_\infty$.

Let us consider n different points p_i with affine coordinates $\{a_i z + b_i\}_{1 \leq i \leq n}$ such that $a_i \neq 0$. Let $G = \delta p_\infty$ with $0 \leq \delta < n$, $L(G) = \langle 1, t, \ldots, t^\delta \rangle$ be the associated linear series and let $s(t) = \sum_{i=0}^{\delta} \lambda_i t^i \in L(G)$ be a rational function.

Now, consider $\bar{\mathcal{C}}$ the submodule given by the image of the evaluation of $s(t)$ at the points p_i

$$\begin{aligned} \langle s(t) = \lambda_0 + \lambda_1 t + \cdots + \lambda_\delta t^\delta \rangle &\to \mathbb{F}[\lambda_0, \ldots, \lambda_\delta][z]^n \\ s(t) &\mapsto (s(p_1), \ldots, s(p_n)) \end{aligned}$$

as a family of submodules parameterized by $\lambda = (\lambda_0, \ldots, \lambda_\delta) \in \mathbb{P}^\delta$. Let us prove that the restrictions of $\bar{\mathcal{C}}$ and $\mathbb{F}[\lambda_0, \ldots, \lambda_n][z]^n / \bar{\mathcal{C}}$ to the open subset

$$V := \bigcap_{1 \leq i < j \leq \delta} \left\{ \begin{array}{c} (\lambda_0, \ldots, \lambda_\delta) \text{ such that} \\ \sum_{k=0}^{\delta} \lambda_k (b_j - b_i)^k (a_i - a_j)^{\delta - k} \neq 0 \end{array} \right\} \quad (13)$$

are locally free.

Note that a matrix associated with the evaluation map above is given by

$$\mathcal{G}(z) = \left(\sum_{i=0}^{\delta} \lambda_i (a_1 z + b_1)^i \quad \ldots \quad \sum_{i=0}^{\delta} \lambda_i (a_n z + b_n)^i \right)$$

and that $\mathbb{F}[\lambda_0, \ldots, \lambda_n][z]^n / \bar{\mathcal{C}}$ fails to be locally free whenever these entries have a common root as polynomials in z. Let α be a common root; hence, $a_i \alpha + b_i$ is a root of $s(t) = \sum_{k=0}^{\delta} \lambda_k t^k$ for all i. Since $s(t)$ has degree δ and $\delta < n$, there exist i, j, with $1 \leq i < j \leq n$, such that

$$a_i \alpha + b_i = a_j \alpha + b_j.$$

For these indices, it must hold that $a_i \neq a_j$ since, otherwise, this equation implies that $b_i = b_j$ and, hence, $p_i = p_j$ which contradicts the hypothesis. Observe that $s(\frac{b_j - b_i}{a_i - a_j}) = s(\alpha) = 0$ implies that $\sum_{k=0}^{\delta} \lambda_k (b_j - b_i)^k (a_i - a_j)^{\delta - k} = 0$.

Hence, $\mathcal{C} := \{\mathcal{C}_\lambda\}_{\lambda \in V}$ defines a family of 1-D length n CGC with parameter space given by (13), canonical generator matrix equal to $\mathcal{G}(z)$, and degree given by the degree of $s(t)$. $\mathcal{G}(z)$ admits a polynomial decomposition as follows:

$$\mathcal{G}(z) = G_0 + G_1 z + \cdots + G_\delta z^\delta$$

with

$$\begin{aligned} G_j &= \left(\sum_{r=j}^{\delta} \lambda_r \binom{r}{j} a_1^j b_1^{r-j} \quad \ldots \quad \sum_{r=j}^{\delta} \lambda_r \binom{r}{j} a_n^j b_n^{r-j} \right) = \\ &= \left(a_1^j s_\lambda^{(j)}(b_1) \quad \ldots \quad a_n^j s_\lambda^{(j)}(b_n) \right) \end{aligned} \quad (14)$$

where, for the sake of notation, we have introduced the functions $s^{(j)} : \mathbb{F}^{\delta+1} \times \mathbb{F} \to \mathbb{F}$ defined by

$$s_\lambda^{(j)}(t) = \sum_{r=j}^{\delta} \binom{r}{j} \lambda_r t^{r-j}, \quad 0 \leq j \leq \delta, \ \lambda = (\lambda_0, \ldots, \lambda_\delta).$$

A. Family of MDS CGC

Let us now consider a family of CGC and let us compute the algebraic equations of the subset of the parameter space corresponding to non-MDS codes explicitly. These results are indeed consequences of Section III-D.

Let us consider n pairwise different points $\{p_i = a_i z + b\}_{1 \leq i \leq n}$ such that $a_i \neq 0$ and the rational function $s(t) = \sum_{i=0}^{\delta} \lambda_i t^i$ (where $\delta < n$). Observe that, in this situation, the open subset defined by (13) is the projective space, i.e., $V = \mathbb{P}^\delta$.

In this situation, the family of CGC defined previously, $\mathcal{C} = \{\mathcal{C}_\lambda\}_{\lambda \in \mathbb{P}^\delta}$, is of type $[n, 1, \delta]$, and furthermore, the generator matrix $\mathcal{G}$ is canonical.

Under these assumptions, Theorem 1.11 of [2] can be strengthened as follows.

Lemma IV.1: The previously defined code $\mathcal{C}_\lambda$ (i.e., constructed over points $p_i = a_i z + b$ for a_i nonzero and pairwise different) is MDS if and only if $s_\lambda^{(j)}(b) \neq 0$ for $0 \leq j \leq \delta$.

Proof: Observe that the code has a generator matrix $\mathcal{G}(z) = G_0 + G_1 z + \cdots + G_\delta z^\delta$, with G_i as in (14) and $b_i = b$ for all $i = 1, \ldots, n$.

Let us assume that $\mathcal{C}_\lambda$ is MDS. Then, the linear block codes G_j are MDS for all j. Otherwise, if one of them, say G_j, is not MDS, there exists a degree 0 information word that is encoded by it into a codeword of weight $< n$. Consequently, such an information word is encoded into a convolutional codeword of weight strictly lower than $n(\delta+1)$, contradicting the hypothesis of $\mathcal{C}$ being MDS (see (3)).

Note that the linear block code G_j is MDS if and only if its Hamming distance is n, that is, all entries in G_j are nonzero. Recalling the explicit expression of these entries (see (14)), one concludes.

Let us prove the converse. Note that the linear codes $\begin{pmatrix} G_u \\ \vdots \\ G_v \end{pmatrix}$ are MDS since all their maximal order minors have the form

$$\begin{vmatrix} a_i^u & \ldots & a_m^u \\ & \ddots & \\ a_i^v & \ldots & a_m^v \end{vmatrix} s_\lambda^{(u)}(b) \cdot \ldots \cdot s_\lambda^{(v)}(b)$$

and are nonzero by the assumptions. By [2, Th. 1.11], the CGC is of type $[n, 1, \delta]$ and MDS, and one concludes. ■

Theorem IV.2: Let $\mathcal{C} = \{\mathcal{C}_\lambda\}_{\lambda \in \mathbb{P}^\delta}$ be the family of CGC of type $[n, 1, \delta]$ defined previously.

Then, the subset of $\mathbb{P}^\delta$ consisting of the points associated with MDS CGC's is a nonempty open subset. More precisely, we have

$$\{\lambda \in \mathbb{P}^\delta \mid \mathcal{C}_\lambda \text{ is MDS } \} = \{\lambda \in \mathbb{P}^\delta \mid s_\lambda^{(j)}(b) \neq 0, \forall 0 \leq j \leq \delta\}.$$

Proof: By the previous lemma, it only remains to prove that the set in the statement is nonempty. This follows easily because this set can be identified with

$$\psi^{-1}\Big(\big\{x=(x_0,\dots,x_\delta)\in\mathbb{F}^{\delta+1}\,|\,x_i\neq 0,\ \text{for } 0\le i\le\delta\big\}\Big)$$

where ψ is the $\mathbb{F}$-linear map

$$\begin{aligned}\mathbb{F}^{\delta+1}&\to\psi\mathbb{F}^{\delta+1}\\ \lambda&\mapsto(s_\lambda^{(0)}(b),s_\lambda^{(1)}(b),\dots,s_\lambda^{(\delta)}(b))\end{aligned}$$

which is the isomorphism whose associated matrix is $\begin{pmatrix}1&*&\dots&*\\0&1&\dots&*\\\vdots&\ddots&\ddots&\vdots\\0&\dots&0&1\end{pmatrix}$. ■

Remark IV.3: If $b=0$, the equations of the non-MDS codes are $\lambda_i=0$ for $0\le i\le\delta$. Thus, the code corresponding to $\lambda=(1,\dots,1)\in\mathbb{P}^\delta$ is MDS. If, moreover, $a_j=a^{j-1}$ where a is an element of $\mathbb{F}$ with $\operatorname{order}(a)\ge n$, we obtain the class of 1-D MDS convolutional codes of type $[n,1,\delta]$ with generator matrix $\mathcal{G}(z)=\sum_{i=0}^{\delta}z^i\,(\,1\quad a^i\quad\dots\quad a^{(n-1)i}\,)$, constructed by Gluesing-Luerssen and Langfeld [6].

Example IV.4: Over the field extension $\mathbb{F}_4\simeq\mathbb{F}_2[\alpha]$ with α a root of x^2+x+1, let us fix pairwise different points $p_1=z+\alpha,p_2=\alpha z+\alpha,p_3=\alpha^2z+\alpha\in\mathbb{P}^1$ and let $s_\lambda(t)=1+\alpha t+t^2$, where $\lambda=(1,\alpha,1)$. We obtain the CGC of type $[n=3,1,\delta=2]$ generated by the canonical generator matrix

$$\mathcal{G}(z)=(\,z^2+\alpha z+1\quad\alpha^2z^2+\alpha^2z+1\quad\alpha z^2+z+1\,).$$

We have that $s_\lambda^{(0)}(\alpha)=1,s_\lambda^{(1)}(\alpha)=\alpha,s_\lambda^{(2)}(\alpha)=1$. Hence, from Theorem IV.2, the resulting code is MDS.

Example IV.5: Let us consider the projective line over $\mathbb{F}_5$, and let us fix the points $p_1=z+1,p_2=2z+1,p_3=3z+1,p_4=4z+1$, and $G=3p_\infty$. Any CGC of type $[n=4,1,\delta=3]$ with $s(t)=\lambda_0+\lambda_1t+\lambda_2t^2+\lambda_3t^3\in L(G)$ is generated by a matrix $\mathcal{G}(z)=G_0+zG_1+z^2G_2+z^3G_3$, where G_i are the matrices given by

$$\begin{aligned}G_0&=(\lambda_0+\lambda_1+\lambda_2+\lambda_3)\,(\,1\quad1\quad1\quad1\,)\\G_1&=(\lambda_1+2\lambda_2+3\lambda_3)\,(\,1\quad2\quad3\quad4\,)\\G_2&=(\lambda_2+3\lambda_3)\,(\,1\quad4\quad4\quad1\,)\\G_3&=\lambda_3\,(\,1\quad3\quad2\quad4\,).\end{aligned}$$

According to Theorem IV.2, the necessary and sufficient conditions for the above CGC to be MDS are

$$\begin{aligned}&\lambda_0+\lambda_1+\lambda_2+\lambda_3\neq0\\&\lambda_1+2\lambda_2+3\lambda_3\neq0\\&\lambda_2+3\lambda_3\neq0\\&\lambda_3\neq0.\end{aligned}$$

Example IV.6: Let us now consider the projective line over $\mathbb{F}_8\simeq\mathbb{F}_2[\alpha]$ with α a root of x^3+x+1, and let us fix points $\{p_i=a_iz+b\}_{1\le i\le7}$, as well as the divisor $G=2p_\infty$ and the rational function $s(t)=\lambda_0+\lambda_1t+\lambda_2t^2\in L(G)$ with $\lambda_2\neq0$. Thus, by Theorem IV.2, the above CGC, which is of type $[n=7,1,\delta=2]$, is MDS if and only if

$$\begin{aligned}&\lambda_0+\lambda_1b+\lambda_2b^2\neq0\\&\lambda_1\neq0\,.\end{aligned}$$

For instance, for $p_i=\alpha^{i-1}z+\alpha,i=1,\dots,7$, the code, which is a CGC of type $[n=7,1,\delta=2]$, is MDS if and only if

$$\begin{aligned}&\lambda_0+\lambda_1\alpha+\lambda_2\alpha^2\neq0\\&\lambda_1\neq0.\end{aligned}\tag{15}$$

In particular, the CGC generated by $G_0+zG_1+z^2G_2$ where

$$\begin{aligned}G_0&=(\,1\quad1\quad1\quad1\quad1\quad1\quad1\,)\\G_1&=(\,\alpha^2\quad\alpha^3\quad\alpha^4\quad\alpha^5\quad\alpha^6\quad1\quad\alpha\,)\\G_2&=(\,\alpha^2\quad\alpha^4\quad\alpha^6\quad\alpha\quad\alpha^3\quad\alpha^5\quad1\,)\end{aligned}$$

is MDS, since it is the code associated with $\lambda_0=\lambda_1=\lambda_2=\alpha^2$.

B. Increasing the Length of an MDS CGC

This section offers a constructive method for increasing the length of a given CGC. Using the results of Sections III-B and III-C, we show that it is possible to increase the length of the codes, preserving the property of being MDS.

More precisely, given a CGC of type $[n,1,2]$ with canonical generator matrix

$$\mathcal{G}(z):=\big(\mathcal{G}_1(z),\dots,\mathcal{G}_n(z)\big)$$

we shall add another point to the divisor $p_1+\cdots+p_n$ in order to obtain a CGC of type $[n+1,1,2]$.

Let $G=2p_\infty,p_i$ be the point with affine coordinate a_iz+b_i for $i=1,\dots,n$ where we assume that $a_i\neq0$ and $\delta=2<n$. Let $s(t)$ be the rational function $\lambda_0+\lambda_1t+\lambda_2t^2\in L(G)$. Let $p_{n+1}=az+b$ be the new point we wish to add. Let $\mathcal{F}(z)$ be the polynomial obtained by evaluating s at p_{n+1}, i.e.,

$$\begin{aligned}\mathcal{F}(z)&=F_0+F_1z+F_2z^2=s(p_{n+1})=\\&=\sum_{j=0}^{2}\lambda_j(az+b)^j=\sum_{j=0}^{2}s_\lambda^{(j)}(b)a^jz^j\,.\end{aligned}\tag{16}$$

We now consider $\widetilde{\mathcal{C}}$, a convolutional code of dimension 1 and length $n+1$, defined by the following generator matrix

$$\widetilde{\mathcal{G}}(z):=\big(\mathcal{G}_1(z),\dots,\mathcal{G}_n(z),\mathcal{F}(z)\big)\,.$$

Let us introduce $\mathcal{F}_k$ as the $(k+1)\times(k+3)$-matrix given by

$$\mathcal{F}_k=\begin{pmatrix}F_0&F_1&F_2&0&\dots&0\\0&F_0&F_1&F_2&\ddots&\vdots\\\vdots&\ddots&\ddots&&\ddots&0\\0&\dots&0&F_0&F_1&F_2\end{pmatrix}.\tag{17}$$

If no confusion arises and $\mathcal{F}_k$ is of maximal rank, we shall denote by $\mathcal{F}_k$ the linear code generated by the image of $\mathcal{F}_k:\mathbb{F}^{k+1}\to\mathbb{F}^{k+3}$, where we are identifying $\mathbb{F}^{k+1}\simeq\langle1,\dots,z^k\rangle$

and $\mathbb{F}^{k+3} \simeq \langle 1, \ldots, z^{k+2} \rangle$. With these notations, we have the following.

Lemma IV.7: Let $k_0 := \max\{\mathrm{l}(\widetilde{\mathcal{C}}), \mathrm{l}(\mathcal{C})\}$, where $\mathrm{l}(\mathcal{C})$ is given by (7). If $\mathcal{F}_{k_0}$ is of maximal rank, it holds that

$$\mathrm{d}_{\mathrm{free}}(\widetilde{\mathcal{C}}) \geq \mathrm{d}_{\mathrm{free}}(\mathcal{C}) + \mathrm{d}(\mathcal{F}_k) \qquad \forall k \geq k_0.$$

Proof: Let us introduce matrices G_i and $\widetilde{G}_i$. For $i = 0, 1, 2$, we use the polynomial decompositions of $\mathcal{G}(z)$ and $\widetilde{\mathcal{C}}$ as defining relations, i.e.,

$$\mathcal{G}(z) = G_0 + G_1 z + G_2 z^2$$
$$\widetilde{\mathcal{G}}(z) = \widetilde{G}_0 + \widetilde{G}_1 z + \widetilde{G}_2 z^2$$

while we set $G_i = F_i = 0$ for all $i < 0$ and $i > 2$. Observe that $\widetilde{G}_i$ is precisely the juxtaposition of the matrices G_i and F_i, which we denote by $(G_i|F_i)$.

A degree k information word $\alpha(z) = \alpha_0 + \alpha_1 z + \cdots + \alpha_k z^k$ is encoded as

$$\alpha(z)\widetilde{\mathcal{G}}(z) = \sum_{j=0}^{k+2} \begin{pmatrix} \alpha_0 & \ldots & \alpha_k \end{pmatrix} \begin{pmatrix} G_j & | & F_j \\ G_{j-1} & | & F_{j-1} \\ \vdots & & \vdots \\ G_{j-k} & | & F_{j-k} \end{pmatrix} \cdot z^j$$

or, equivalently, the juxtaposition of the polynomial words $\alpha(z)\mathcal{G}(z)$ and

$$\sum_{j=0}^{k+2} \begin{pmatrix} \alpha_0 & \ldots & \alpha_k \end{pmatrix} \begin{pmatrix} F_j \\ F_{j-1} \\ \vdots \\ F_{j-k} \end{pmatrix} \cdot z^j = \begin{pmatrix} \alpha_0 & \ldots & \alpha_k \end{pmatrix} \mathcal{F}_k \begin{pmatrix} z^0 \\ z^1 \\ \vdots \\ z^{k+2} \end{pmatrix}$$

where $\mathcal{F}_k$ is the matrix given in (17). Thus, the weight of $\alpha(z)\widetilde{\mathcal{G}}(z)$ can be computed as follows:

$$\mathrm{w}(\alpha(z)\widetilde{\mathcal{G}}(z)) = \mathrm{w}((\alpha(z)\mathcal{G}(z)) + \mathrm{w}((\alpha_0, \ldots, \alpha_k) \cdot \mathcal{F}_k).$$

Considering the distances as lower bounds of the terms on the RHS and bearing in mind Theorem III.1, we obtain

$$\mathrm{w}(\alpha(z)\widetilde{\mathcal{G}}(z)) \geq \mathrm{d}_{\mathrm{free}}(\mathcal{C}) + \min\{\mathrm{d}(\mathcal{F}_k) | k \geq 0\}$$

for all $\alpha \neq 0$ and $k \gg 0$. Noting that $\{\mathrm{d}(\mathcal{F}_k) | k \geq 0\}$ is a non-increasing sequence and allowing k to be larger than or equal to k_0, the statement follows. ∎

Example IV.8: Let us fix $\mathbb{F}_8 \simeq \mathbb{F}_2[\alpha]$, where α is a root of $x^3 + x + 1$, as the base field.

Let us consider the CGC corresponding to the point $\lambda = (1, 1, 1) \in \mathbb{P}^2$, i.e., the rational function $s(t) = 1 + t + t^2$, and the points $p_1 = z + \alpha, p_2 = \alpha z + \alpha, p_3 = \alpha^2 z + \alpha$.

We thus have a CGC of type $[n = 3, 1, \delta = 2]$ generated by

$$\mathcal{G}(z) = \begin{pmatrix} z^2 + z + \alpha^5 & \alpha^2 z^2 + \alpha z + \alpha^5 & \alpha^4 z^2 + \alpha^2 z + \alpha^5 \end{pmatrix}$$

which has free distance 9 and is therefore MDS.

Let us now consider $\tilde{\mathcal{C}}$, the CGC constructed from $\mathcal{G}(z)$ and the point $p_4 = \alpha^2 z + \alpha^4$ by the aforementioned procedure, that is, the code generated by

$$\tilde{\mathcal{G}}(z) = \begin{pmatrix} z^2 + z + \alpha^5 \\ \alpha^2 z^2 + \alpha z + \alpha^5 \\ \alpha^4 z^2 + \alpha^2 z + \alpha^5 \\ \alpha^4 z^2 + \alpha^2 z + \alpha^6 \end{pmatrix}^T.$$

We have that $s(p_4) = \alpha^4 z^2 + \alpha^2 z + \alpha^6$, i.e., $F_0 = \alpha^6, F_1 = \alpha^2, F_2 = \alpha^4$. Bearing in mind (7), one has that $\mathrm{l}(\mathcal{C}) = 6$ and $\mathrm{l}(\widetilde{\mathcal{C}}) = 3$ and also one easily checks that $d(\mathcal{F}_6) \geq 3$. Therefore, the lemma implies that $\widetilde{\mathcal{C}}$ is MDS and has free distance 12.

We are now ready to offer a way for increasing the length of a CGC.

Let us introduce the following notation. Let h_k be the kth complete symmetric function on the roots of $\mathcal{F}(z) = 0$.

Theorem IV.9: With the previous notations, let $\mathcal{C}$ be an MDS CGC of type $[n, 1, 2]$.

Assume that $\mathrm{d}\begin{pmatrix} G_2 \\ G_1 \\ G_0 \end{pmatrix} \geq 3$; $a \neq 0$; $s_\lambda^{(0)}(b) \neq 0$; $\lambda_2 \neq 0$; and, $h_k \neq 0$ for all $k \leq \mathrm{l}(\mathcal{C})$.

It then holds that 1) $\widetilde{\mathcal{C}}$ is an MDS CGC of type $[n + 1, 1, \delta = 2]$; 2) $\mathrm{d}\begin{pmatrix} G_2 & | & F_2 \\ G_1 & | & F_1 \\ G_0 & | & F_0 \end{pmatrix} \geq 3$; and 3) $\mathrm{l}(\widetilde{\mathcal{C}}) \leq \mathrm{l}(\mathcal{C}) + 1$.

Proof: First, note that 2) follows from the inequalities

$$\mathrm{d}\begin{pmatrix} G_2 & | & F_2 \\ G_1 & | & F_1 \\ G_0 & | & F_0 \end{pmatrix} \geq \mathrm{d}\begin{pmatrix} G_2 \\ G_1 \\ G_0 \end{pmatrix} \geq 3.$$

Let us now prove 3). Recall that $\mathcal{C}$ is of type $[n, 1, 2]$ and that $\mathrm{l}(\mathcal{C})$ is given by formula (7). Similarly, $\widetilde{\mathcal{C}}$ is of type $[n + 1, 1, 2]$ and in order to compute $\mathrm{l}(\widetilde{\mathcal{C}})$ by formula (7) we must juxtapose a new column given by the coefficients of $\mathcal{F}(z)$ to the matrix $\begin{pmatrix} G_2 \\ G_1 \\ G_0 \end{pmatrix}$. Part 2) yields

$$\mathrm{l}(\widetilde{\mathcal{C}}) \leq \left\lfloor 3(n+1)\mathrm{d}\begin{pmatrix} G_2 \\ G_1 \\ G_0 \end{pmatrix}^{-1} \right\rfloor - 3$$
$$\mathrm{l}(\mathcal{C}) = \left\lfloor 3n\mathrm{d}\begin{pmatrix} G_2 \\ G_1 \\ G_0 \end{pmatrix}^{-1} \right\rfloor - 3.$$

We have to show that $\mathrm{l}(\widetilde{\mathcal{C}}) - \mathrm{l}(\mathcal{C}) \leq 1$. The case $\mathrm{d}\begin{pmatrix} G_2 \\ G_1 \\ G_0 \end{pmatrix} = 3$ is easy. For $\mathrm{d}\begin{pmatrix} G_2 \\ G_1 \\ G_0 \end{pmatrix} \geq 4$, it is enough to note that

$$\mathrm{l}(\widetilde{\mathcal{C}}) \leq 3(n+1)\mathrm{d}\begin{pmatrix} G_2 \\ G_1 \\ G_0 \end{pmatrix}^{-1} - 3$$
$$\mathrm{l}(\mathcal{C}) \geq 3n\mathrm{d}\begin{pmatrix} G_2 \\ G_1 \\ G_0 \end{pmatrix}^{-1} - 4$$

and that $\left\lfloor 3\mathrm{d}\begin{pmatrix} G_2 \\ G_1 \\ G_0 \end{pmatrix}^{-1} \right\rfloor = 0$.

Finally, we prove the first item. Recalling the singleton bounds for block codes and for convolutional codes and Lemma IV.7, it will suffice to show that $\mathcal{F}_k$ is an MDS linear

code for $k = \mathrm{l}(\mathcal{C})$ (see Theorem III.1), that is, none of its maximal minors vanish.

Let us denote by d_k the determinant of the $(k+1)\times(k+1)$-matrix obtained by removing the first and last column of $\mathcal{F}_k$

$$d_k = \begin{vmatrix} F_1 & F_2 & 0 & \dots & 0 \\ F_0 & F_1 & \ddots & & \vdots \\ 0 & \ddots & & \ddots & 0 \\ \vdots & \ddots & \ddots & & F_2 \\ 0 & \dots & 0 & F_0 & F_1 \end{vmatrix}.$$

Bearing in mind (16), we note that $F_0 = s_\lambda^{(0)}(b)$ and that $F_2 = a^2\lambda_2$, and therefore, the minors of $\mathcal{F}_k$ are given by the following expressions:

$$F_0^{i-1}\cdot d_{j-i-1}\cdot F_2^{k+2-j} = \left(s_\lambda^{(0)}(b)\right)^{i-1}\cdot d_{j-i-1}\cdot\left(a^2\lambda_2\right)^{k+2-j}$$

for $1 \le i < j \le k+2$. It will suffice to show that $d_k \neq 0$ for all $k \le \mathrm{l}(\mathcal{C})+1$. Using the following recursion relation:

$$d_k = F_1 d_{k-1} - F_0 F_2 d_{k-2}$$

one has that $d_k = (-F_2)^{k+1}\sum_{i=0}^{k+1} r_1^i r_2^{k+1-i} = (-a^2\lambda_2)^{k+1}h_{k+1}$, where h_{k+1} is the $(k+1)$th complete symmetric function on the roots of $\mathcal{F}(z)=0$. ■

Remark IV.10: Let us comment on the $(k+1)$th complete symmetric function. First, note that h_{k+1} is explicitly given by $\sum_{i=0}^{k+1} r_1^i r_2^{k+1-i}$, where r_1, r_2 are the roots of $\mathcal{F}(z)=0$, and since it is symmetric in r_1, r_2, it belongs to the base field even if r_1, r_2 do not. Further, h_{k+1} can be expressed in terms of the coefficients of $\mathcal{F}(z)$ by the recursion relation $h_{k+1} = -h_k F_1/F_2 - h_{k-1}F_0/F_2$ with initial conditions $h_0 = 1, h_1 = F_1/F_2$.

Example IV.11: Let us consider Example IV.6. In particular, let $\mathcal{G}(z) = G_0 + zG_1 + z^2G_2$ be the generator matrix of the code CGC of type $[n=7,1,\delta=2]$, where $D = \sum_i^7 p_i, p_i = \alpha^{i-1}z + \alpha$ and $s(t) = \lambda_0 + \lambda_1 t + \lambda_2 t^2$ is the rational function verifying (15). We wish to extend this code to an MDS CGC of type $[8,1,2]$ by adding a point $p_8 = az + b \notin \{p_i\}_{i=1}^7$, with $a \neq 0$, to D.

Now, let $\mathcal{F}(z)$ be computed from (16) and let $\widetilde{\mathcal{G}} = (\mathcal{G}\,|\,\mathcal{F})$. Note that $\mathrm{d}\begin{pmatrix} G_2 \\ G_1 \\ G_0 \end{pmatrix} = 5$ while $s_\lambda^{(0)}(b) \neq 0$ and $\lambda_2 \neq 0$. Hence, $\widetilde{\mathcal{G}}$ generates an MDS code if $h_k \neq 0$ for all $k \le l(\mathcal{C})$. In fact $l(\widetilde{\mathcal{C}}) = l(\mathcal{C}) = 1$. Thus, the condition that we must check is equivalent to $d_1 \neq 0$, and

$$d_1 = \begin{vmatrix} F_1 & F_2 \\ F_0 & F_1 \end{vmatrix} = (\lambda_1 a)^2 + \lambda_2 a^2(\lambda_2 b^2 + \lambda_1 b + \lambda_0) = \\ = a^2(\lambda_1^2 + \lambda_2^2 b^2 + \lambda_2\lambda_1 b + \lambda_2\lambda_0).$$

Accordingly, the desired condition is $\lambda_1^2 + \lambda_2^2 b^2 + \lambda_2\lambda_1 b + \lambda_2\lambda_0 \neq 0$.

Remark IV.12: As a final remark, let us point out that Corollary III.8 also implies that, for a given rational function $s(t)$, the subset of eligible points:

$$\{p = az + b \in \mathbb{P}^1 \text{ such that } \widetilde{\mathcal{C}} \text{ is MDS}\}$$

is Zariski open in $\mathbb{P}^1$, i.e., *bad* points fulfill certain algebraic equations, and thus, we have plenty of choices for such p. For instance, let us consider Example IV.6 with $s(t) = 1 + t + t^2$, i.e., $\lambda_0 = \lambda_1 = \lambda_2 = 1$. Thus, the point $p_8 = az + b$ satisfies the condition that $\widetilde{\mathcal{C}}$ is indeed MDS if and only if $a \neq 0$ and $1 + (b^2 + b + 1) \neq 0$ or, equivalently, $a \neq 0$ and $b \neq 0, 1$.

V. Conclusion and Further Research

This work addresses several significant results with promising perspectives for future constructions of MDS convolutional codes. The results are related to the study of three properties of the free distance and the systematic construction of convolutional codes.

First, our study of the sequence of row distances for a class of codes has allowed us to bound the stage in which this sequence has achieved the free distance of the convolutional code. Thus, we have derived an explicit method for the calculation of the free distance.

Second, for the case of convolutional codes depending on parameters, the free distance has been studied as a function on the parameter space and it has been shown that it is lower semicontinuous. In particular, we conclude that the property of being MDS is an open condition, that is, the subset of the parameter space corresponding to non-MDS codes is defined by a finite number of algebraic equations.

The last property is that the free distance is preserved when the alphabet grows, i.e., it is invariant under extensions of the base field.

Finally, an illustration of our results is offered for the case of 1-D MDS CGCs. We compute the algebraic equations of the non-MDS locus in a number of examples. In particular, by exhibiting a number of examples on small fields, the existence of MDS convolutional codes is proved without requiring us to enlarge the base field. We finish with a procedure, given an MDS CGC, for producing a new MDS CGC of greater length.

As a continuation of our approach, we believe that some lines of research deserve further investigation. On the one hand, it would be desirable to obtain more general results about the relation between the sequence of row distances and the free distance. On the other, it would be interesting to explore different families of convolutional codes and to study the corresponding MDS locus.

Acknowledgment

The authors wish to express their gratitude to J. M. Muñoz Porras and the anonymous referees for their valuable comments and suggestions that have improved our work.

References

[1] S. M. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*. Reading, MA, USA: Addison-Wesley, 1969.

[2] J. A. Domínguez Pérez, J. M. Muñoz Porras, and G. Serrano Sotelo, One dimensional convolutional Goppa codes over the projective line 2011 [Online]. Available: arXiv:1107.2059

[3] J. A. Domínguez Pérez, J. M. Muñoz Porras, and G. Serrano Sotelo, "Convolutional codes of Goppa type," *Appl. Algebr. Eng., Commun. Comput.*, vol. 15, no. 1, pp. 51–61, 2004.

[4] G. D. Forney, Jr, "Convolutional codes I: Algebraic structure," *IEEE Trans. Inf. Theory*, vol. 16, no. 3, pp. 720–738, Nov. 1970.

[5] E. Fornasini and M. E. Valcher, "Algebraic aspects of two-dimensional convolutional codes," *IEEE Trans. Inf. Theory*, vol. 40, no. 4, pp. 1068–1082, Jul. 1994.
[6] H. Gluesing-Luerssen and B. Langfeld, "A class of one-dimensional MDS convolutional codes," *J. Algebr. Appl.*, vol. 5, pp. 505–520, 2006.
[7] H. Gluesing-Luerssen, J. Rosenthal, and R. Smarandache, "Strongly MDS convolutional codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 584–598, Feb. 2006.
[8] R. Hutchinson, J. Rosenthal, and R. Smarandache, "Convolutional codes with maximum distance profile," *Syst. Control Lett.*, vol. 54, no. 1, pp. 53–63, 2005.
[9] R. Johannesson and K. S. Zigangirov, *Fundamentals of Convolutional Coding*. New York, NY, USA: IEEE Press, 1999.
[10] J. Justesen, "An algebraic construction of rate $1/\nu$ convolutional codes," *IEEE Trans. Inf. Theory*, vol. IT-21, no. 1, pp. 577–580, Sep. 1975.
[11] V. Lomadze, "Convolutional codes and coherent sheaves," *Appl. Algebr. Eng., Commun. Comput.*, vol. 12, pp. 273–326, 2001.
[12] R. J. McEliece, "The algebraic theory of convolutional codes," in *Handbook of Coding Theory*, V. Pless and W. Huffman, Eds. New York, NY, USA: Elsevier, 1998, vol. 1, pp. 1065–1138.
[13] J. L. Massey and M. K. Sain, "Inverses of linear sequential circuits," *IEEE Trans. Comput.*, vol. C-17, no. 4, pp. 330–337, Apr. 1968.
[14] J. M. Muñoz Porras, J. A. Domínguez Pérez, J. I. Iglesias Curto, and G. Serrano Sotelo, "Convolutional Goppa codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 1, pp. 340–344, Jan. 2006.
[15] J. M. Muñoz Porras and J. I. Iglesias Curto, "Classification of convolutional codes," *Linear Algebr. Appl.*, vol. 432, no. 10, pp. 2701–2725, 2010.
[16] P. Piret, *Convolutional Codes: An Algebraic Approach*. Cambridge, MA, USA: MIT Press, 1988.
[17] M. S. Ravi and J. Rosenthal, "A smooth compactification of the space of transfer functions with fixed McMillan degree," *Acta Appl. Math.*, no. 34, pp. 329–352, 1994.
[18] J. Rosenthal and R. Smarandache, "Maximum distance separable convolutional codes," *Appl. Algebr. Eng., Commun. Comput.*, vol. 10, no. 1, pp. 15–32, 1999.

Francisco J. Plaza-Martín was born in Jaén, Spain, in 1970. He received the Ph. D. in Mathematics from University of Salamanca in 1997 where he is currently Assistant Professor of Geometry and Topology. His research topics are algebraic geometry and its applications to physics and information theory.

José I. Iglesias-Curto was born in Alba de Tormes, Spain. He received the B.S. degree in mathematics in 2000 and the Ph.D. degree in mathematics in 2008, both from the University of Salamanca, Spain. He was awarded the M.S. Prize and the Ph.D. Prize both at the University of Salamanca in 2002 and 2009 respectively. He has worked as a research fellow as well as with different academic positions at the Universities of Wuerzburg, Germany, and Salamanca, Spain, where he has been since 2008. His research interests include coding theory and applications to and from algebraic geometry and system theory.

Gloria Serrano-Sotelo was born in Oviedo, Spain, in 1954. She graduated in Mathematics from the University of Salamanca, Spain, in 1976. She is part-time Professor in the Department of Mathematics, University of Salamanca. Her research interests include coding theory.