CONVOLUTIONAL GOPPA CODES DEFINED ON FIBRATIONS

J. I. IGLESIAS CURTO, J. M. MUÑOZ PORRAS, F. J. PLAZA MARTÍN
AND G. SERRANO SOTELO

ABSTRACT. We define a new class of Convolutional Codes in terms of fibrations of algebraic varieties generalizaing our previous constructions of Convolutional Goppa Codes ([1, 14]). Using this general construction we can give several examples of Maximum Distance Separable (MDS) Convolutional Codes.

1. INTRODUCTION

This paper offers a generalization of our algebro-geometric construction of Convolutional Goppa Codes (CGC) ([1, 2, 9, 10, 14]). Recall, that Algebraic Geometry has been successfully applied in Coding Theory during the last decades, first for block codes (e.g. [4, 5, 16, 20, 8]) and more recently for convolutional codes ([12, 17]), as a natural continuation of the algebraic constructions of convolutional codes already known for long (as for example [11, 15]). Our aim is to consider algebro-geometric properties of higher dimensional varieties in order to obtain Convolutional Goppa Codes with good properties, as it has been successfully done for block codes ([6, 21]).

CGC are constructed in terms of families of algebraic varieties, $X \to \mathbb{A}^1$, parametrized by an affine line $\mathbb{A}^1$. In the case of block codes, the generalization of Goppa Codes to higher-dimensional varieties has been successfully used.

The contents of this work are arranged in the following way. In §2 we summarize some notions and results on convolutional codes based on [3, 13]. In §3 we expose the construction of CGC defined by a family of algebraic varieties, $X \to \mathbb{A}^1$, parametrized by the affine line. This construction consists of evaluating sections of an invertible sheaf on sections of the fibration $X \to \mathbb{A}^1$. In §4 details are given for the construction when consider in the particular case of the trivial fibration $\mathbb{P}^2_{\mathbb{F}_q} \times \mathbb{A}^1 \to \mathbb{A}^1$. §5 provides some examples in order to illustrate the possibilities of our approach.

We use the standard notations of Algebraic Geometry as can be found in [7].

Key words and phrases. Convolutional codes, Goopa codes, MDS codes, finite fields.
MSC 14G50, 94B10 , 11T71, 94B27.

This research was supported by the Spanish DGESYC through research project MTM2009-11393 MICINN and by the "Junta de Castilla y León" through research project SA029A08.

2. Preliminaries on Convolutional Codes

Let $\mathbb{F}_q$ be a finite field of size $q = p^s$, with p a prime.

Recall that, opposed to the definition of block codes as vector subspaces, convolutional codes are (roughly) defined as submodules of $\mathbb{F}[z]^n$. Convolutional codewords are then polynomial vectors; indeed, the encoded sequence $(c_0, c_1, c_2, \ldots)$ (with $c_i \in \mathbb{F}^n$) is equivalently represented as the polynomial $c(z) = \sum_{i=0} c_i z^i$. Each codeword (encoded sequence) results of applying a polynomial generator matrix to an information word (or information sequence) $(u_0, u_1, u_2, \ldots)$, which will be analogously written as a polynomial $u(z) = \sum_{i=0} u_i z^i$. The fact that the entries of the generator matrix are polynomials implies that each encoded block c_i depends not only on u_i but also on the previous information blocks $u_{i-1}, \ldots$. This is the distinctive aspect between block and convolutional codes. The term "convolutional" is used since the output sequences can be regarded as the convolution of the input sequences with the sequences in the encoder, [3]. The control matrix (a.k.a. parity check matrix) and dual code for convolutional codes are defined exactly in the same way as for block codes.

More rigourously, an (n,k) *convolutional code* $\mathscr{C}$ over $\mathbb{F}_q$ is defined as a rank k submodule of $\mathbb{F}_q[z]^n$. The integers (n,k) are called, respectively, the *length* and *dimension* of the convolutional code. The quotient $\frac{k}{n}$ is called the *rate* of the code.

Every $k \times n$ matrix of maximal rank, G, with entries in $\mathbb{F}_q[z]$ defines an injective map

$$G\colon F[z]^k \hookrightarrow F[z]^n$$

Its image defines a (n,k) convolutional code $\mathscr{C}$ and, in this case, G will be called a *polynomial encoder* or *generator matrix* of $\mathscr{C}$, although not every generator matrix is equally suitable. We will prefer matrices which are basic; we say that G is *basic* if the g.c.d. of the minors of order k of G is equal to 1.

Any polynomial encoder G for $\mathscr{C}$ induces a injective $\mathbb{F}_q(z)$-linear map

$$G\colon \mathbb{F}_q(z)^k \hookrightarrow \mathbb{F}_q(z)^n .$$

Although this may allow us to generalize the notion of convolutional code as subspaces of $\mathbb{F}_q(z)^n$, one has to bear in mind that different associated encoders G generate submodules of $\mathbb{F}_q[z]^n$ which may be different. However, basic encoders always generate the same submodule ([2]). Therefore, in this sense we may consider that the notions of convolutional codes as submodules of $\mathbb{F}_q[z]^n$ or as vector subspaces of $\mathbb{F}_q(z)^n$ are equivalent.

Indeed, for a given convolutional code $\mathscr{C}$, the unimodular group $GL(k, \mathbb{F}_q[z])$ acts transitively on the set of basic encoders for $\mathscr{C}$ ([2]). Then, one can consider an invariant associated with the code, the *degree* of the code, δ, defined as (e.g. [13])

$$\delta := \text{maximum degree of the minors of order } k \text{ of a basic encoder for } \mathscr{C}$$

The *degree* of a polynomial encoder G, $\deg G$, is the sum of the degrees of its rows. Forney ([3]) proved that for each (n,k)-convolutional code of degree δ there exists at least one basic encoder G such that

$$\delta = \deg G \leq \deg G',$$

for all polynomial encoders G' of the convolutional code. These basic encoders G are called *minimal basic encoders* by Forney [3] or *canonical encoders* by McEliece [13].

As for block codes, there is a notion of distance that will characterize the error detection/correction capacity of convolutional codes the *free distance*, d_{free}. Let us define the overall Hamming weight of a polynomial vector $v(z) = \sum_{i=0} v_i z^i$ as $\mathrm{w}(v(z)) = \sum_{i=0} \mathrm{w}(v_i)$. Then the free distance of the code $\mathscr{C}$ is defined as

$$d_{free}(\mathscr{C}) := \min_{c \in \mathscr{C}} \mathrm{w}(c)\,. \tag{1}$$

The free distance is directly related to the other parameters of the code. However, the exact relationship is not known and different bounds are considered instead. One of the most usually considered is the generalized Singleton bound [19]

$$d_{free} \leq S(n,k,\delta) = (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1 \tag{2}$$

Convolutional codes attaining the generalized Singleton bound are called Maximum Distance Separable (MDS).

Convolutional codes do have one more parameter which do not have a counterpart in block codes, the *memory*. It is well known, e.g. [13], that the row degrees of a canonical generator matrix are, up to ordering, uniquely determined by the code. They are known as the *Forney indices* of the code. The largest of them is called the memory of the code and denoted m. The sum of the Forney indices, which is equal the maximal degree of the minors of any basic matrix, coincides the degree (also known as complexity) of the code. Roughly, the degree of the code measures the dependance of an encoded block with respect to the information blocks, while the memory counts on how many information blocks does every encoded block depend. Convolutional codes of degree 0 are precisely linear block codes.

3. General construction

Let X be a variety of dimension $m+1 \geq 2$, let $\mathbb{A}^1 = \operatorname{Spec} \mathbb{F}_q[z]$ denote the affine line and let us consider a flat and projective morphism $\pi : X \to \mathbb{A}^1$ whose fibers are smooth and geometrically irreducible algebraic varieties of dimension m. Recall that for $\dim X = 2$ the fibers are curves; this case has been studied in [1, 14]. For the basic facts on algebraic geometry that will be used here, we address the reader to [7].

Let us choose n different sections of π

$$p_i : \mathbb{A}^1 \to X \qquad \text{with } p_i \circ \pi = \mathrm{Id} \quad \forall i = 1, \dots, n$$

and, thus, $p_i(\mathbb{A}^1) \subset X$ is a curve isomorphic to $\mathbb{A}^1$. Consider the closed subscheme

$$D = p_1(\mathbb{A}^1) \cup \ldots \cup p_n(\mathbb{A}^1)$$

as well as the morphism p given by the composition

$$\begin{tikzcd} D \arrow[r, hook] \arrow[dr, "p"'] & X \arrow[d, "\pi"] \\ & \mathbb{A}^1 \end{tikzcd}$$

which is flat and finite of degree n.

Let us call $\mathscr{O}_D$ and $\mathscr{I}_D$ respectively the sheaves of rings and ideals of $D \hookrightarrow X$. We have an exact sequence

$$0 \to \mathscr{I}_D \to \mathscr{O}_X \to \mathscr{O}_D \to 0$$

Let $\mathscr{L}$ be an invertible sheaf over X. The tensor product of the sequence with $\mathscr{L}$ yields

$$0 \to \mathscr{L} \otimes \mathscr{I}_D \to \mathscr{L} \to \widetilde{\mathscr{O}_D} \to 0\,,$$

where $\widetilde{\mathscr{O}_D} = \mathscr{O}_D \underset{\mathscr{O}_X}{\otimes} \mathscr{L}$. Taking global sections we obtain the long exact sequence of $\mathbb{F}_q[z]$-modules

(3)

$$0 \to H^0(X, \mathscr{L} \otimes \mathscr{I}_D) \to H^0(X, \mathscr{L}) \to H^0(X, \widetilde{\mathscr{O}_D}) \to H^1(X, \mathscr{L} \otimes \mathscr{I}_D) \to H^1(X, \mathscr{L}) \to 0$$

Remark 3.1. Note that the flatness of $p : D \to \mathbb{A}^1$ implies the existence of isomorphisms $\phi : p_* \mathscr{O}_D \xrightarrow{\sim} \mathbb{F}_q[z]^n$, where $\mathbb{F}_q[z]$ also denotes its corresponding sheaf on $\mathbb{A}^1$. In general these isomorphisms are not canonical but, if the chosen sections p_i are disjoint, then there exists a canonical isomorphism $p_* \mathscr{O}_D \simeq \mathbb{F}_q[z]^n$ induced by p.

Since $\mathscr{L}$ restricted to the sections is trivial, then $\widetilde{\mathscr{O}_D} \simeq \mathscr{O}_D$, but such identification is not canonical. Thus, if we fix an isomorphism

$$\phi : H^0(X, \mathscr{O}_D) \xrightarrow{\sim} \mathbb{F}_q[z]^n\,,$$

as well as trivializations for each section p_i, we obtain induced isomorphisms $\widetilde{\mathscr{O}_D} \simeq \mathscr{O}_D$ and $\psi : H^0(X, \widetilde{\mathscr{O}_D}) \xrightarrow{\sim} \mathbb{F}_q[z]^n$.

Remark 3.2. If we take $\mathscr{L} \simeq \mathscr{O}_X(H)$, being H an effective divisor on X which is flat over $\mathbb{A}^1$, the trivializations $\mathscr{L}|_{p_i}$ and the isomorphism ψ are fixed.

Definition 3.3. The *convolutional Goppa code* $\mathscr{C}(\Gamma, D, \psi)$ determined by the sheaf $\mathscr{L}$, the subscheme D, the isomorphism ψ, and a submodule $\Gamma \subseteq H^0(X, \mathscr{L})$ is the submodule given by the image of the homomorphism f defined by

$$\begin{tikzcd} 0 \arrow[r] & H^0(X, \mathscr{L} \otimes \mathscr{I}_D) \arrow[r] & H^0(X, \mathscr{L}) \arrow[r] & H^0(X, \widetilde{\mathscr{O}_D}) \arrow[d, "\psi", "\wr"'] \\ & & \Gamma \arrow[u, hook] \arrow[r, dashed, "f"] & \mathbb{F}_q[z]^n \end{tikzcd}$$

By the very construction, the *length of the code* is given by the rank of $\mathscr{O}_D$ as an $\mathscr{O}_{\mathbb{A}^1}$-module, which is the number n of sections taken to define the code. The issue of constructing such sections is clearly related with the question of finding rational points in algebraic varieties over finite fileds.

The *dimension of the code* is equal to the rank of the submodule $\mathrm{Im}(f)$ which coincides with the rank of Γ if and only if $\Gamma \cap H^0(X, \mathscr{L} \otimes \mathscr{I}_D) = (0)$. Note that in the case of the complete linear series, $\Gamma = H^0(X, \mathscr{L})$, the additive property of the dimension applied to the exact sequence 3 yields

$$\mathrm{rk}\,\mathscr{C}(\Gamma, D, \psi) = h^0(\mathscr{L}) - h^0(\mathscr{L} \otimes \mathscr{I}_D) = h^0(\widetilde{\mathscr{O}_D}) - h^1(\mathscr{L} \otimes \mathscr{I}_D) + h^1(\mathscr{L})$$

Nevertheless, the explicit calculus of these numbers for the general case is a very hard problem in classical algebraic geometry based on the theory of syzygies.

For the approach in terms of subspaces of $\mathbb{F}_q(z)$, one considers the the generic point of $\mathbb{A}^1$, η, whose residue field is $\mathbb{F}_q(\eta) = \mathbb{F}_q(z)$. The fiber X_η is an m-dimensional variety over $\mathbb{F}_q(z)$, and $p_1(\eta), \dots, p_n(\eta)$ are n different $\mathbb{F}_q(z)$-rational points. Then we have $D_\eta = p_1(\eta) \cup \ldots \cup p_n(\eta)$, and an isomorphism

$$\psi_\eta : H^0(X_\eta, \widetilde{\mathscr{O}_{D_\eta}}) \xrightarrow{\sim} \mathbb{F}_q(z)^n .$$

Moreover, if $\mathscr{L} = \mathscr{O}_X(H)$ then ψ_η is canonical.

Definition 3.4. The *convolutional Goppa code* $\mathscr{C}(\Gamma, D_\eta, \psi_\eta)$ is the image of the homomorphism f_η defined by

$$\begin{tikzcd} 0 \arrow[r] & H^0(X_\eta, \mathscr{L}_\eta \otimes \mathscr{I}_{D_\eta}) \arrow[r] & H^0(X_\eta, \mathscr{L}_\eta) \arrow[r] & H^0(X_\eta, \widetilde{\mathscr{O}_{D_\eta}}) \arrow[d, "\psi_\eta", "\wr"'] \\ & & \Gamma \arrow[u, hook] \arrow[r, dashed, "f_\eta"] & \mathbb{F}_q(z)^n \end{tikzcd}$$

where Γ is a given subspace of $H^0(X_\eta, \mathscr{L}_\eta)$

The length and dimension of the code $\mathscr{C}(\Gamma, D_\eta, \psi_\eta)$ are computed as above.

In the rest of the paper we will continue with the submodule approach, but as we have just seen the shift to the subspace setting would be straightforward.

As it was already mentioned in the Introduction, the case when $\dim X = 2$ has been already studied in [1, 14], in particular for $X = \mathbb{P}^1 \times \mathbb{A}^1$. In the next Section we will illustrate in detail how the construction works for higher dimensional varieties by considering $X = \mathbb{P}^2_{\mathbb{F}_q} \times \mathbb{A}^1$.

4. Codes defined on the projective plane over $\mathbb{F}_q$

Let $\mathbb{P}^2_{\mathbb{F}_q} = \operatorname{Proj} \mathbb{F}_q[x_0, x_1, x_2]$ be the projective plane over $\mathbb{F}_q$, and let

$$X = \mathbb{P}^2_{\mathbb{F}_q} \times \mathbb{A}^1 \xrightarrow{\pi} \mathbb{A}^1 \,.$$

be the trivial fibration.

Let $H_\infty \subset \mathbb{P}^2_{\mathbb{F}_q}$ be the line defined by the equation $x_0 = 0$. Then, its complement is an affine plane, $\mathbb{P}^2_{\mathbb{F}_q} \setminus H_\infty = \mathbb{A}^2$.

We will choose the sections p_i $(1 \le i \le n)$ of π taking values in $\mathbb{A}^2 \times \mathbb{A}^1$. They are given by

$$\begin{aligned} \mathbb{A}^1 &\xrightarrow{p_i} \mathbb{A}^2 \times \mathbb{A}^1 \\ z &\mapsto p_i(z) = (\alpha_{i,1} z + \beta_{i,1}, \alpha_{i,2} z + \beta_{i,2}, z) \end{aligned}$$

where all $\alpha_{i,r}, \beta_{i,s} \in \mathbb{F}_q$. Observe that the length of the code is bounded by the number of different sections; that is, $n \le q^4$. However, this count includes also linear codes (e.g. $\alpha_{i,r} \equiv 0$ for all i, r) as well as codes defined with the fibration $\mathbb{P}^1_{\mathbb{F}_q} \times \mathbb{A}^1 \xrightarrow{\pi} \mathbb{A}^1$ (e.g. when the n sections are collinear).

Let us considerer the divisor $\pi_1^* H_\infty$, where $\pi_1 \colon X \to \mathbb{P}^2_{\mathbb{F}_q}$ is the projection onto the first factor, and the invertible sheaf given by

$$\mathscr{L} := \mathscr{O}_{\mathbb{P}^2_{\mathbb{F}_q[z]}} (\pi_1^* H_\infty)^{\otimes r} \simeq \pi_1^* \mathscr{O}(1)^{\otimes r} = \mathscr{O}(r) \underset{\mathbb{F}_q}{\otimes} \mathbb{F}_q[z]$$

where we write $\mathscr{O}(r) := \mathscr{O}_{\mathbb{P}^2_{\mathbb{F}_q}} (H_\infty)^{\otimes r}$ for simplicity.

Notice that, as it was pointed out in Remark 3.2, the trivializations of $\mathscr{L}$ on the sections p_i and the isomorphism $\psi \colon H^0(X, \widetilde{\mathscr{O}_D}) \xrightarrow{\sim} \mathbb{F}_q[z]^n$ are fixed.

If we denote $t = \frac{x_1}{x_0}$, $s = \frac{x_2}{x_0}$ the affine coordinates in the affine plane $\mathbb{A}^2$, the space of global sections is explicitly described as

$$H^0(\mathbb{P}^2_{\mathbb{F}_q}, \mathscr{O}(r)) \;=\; \langle t^i s^j \mid 0 \le i + j \le r \rangle$$

Hence, the evaluation of $t^i s^j$ at the points $p_1, \dots, p_n$ is given by

$$f(t^i s^j) = ((\alpha_{1,1} z + \beta_{1,1})^i \cdot (\alpha_{1,2} z + \beta_{1,2})^j, \dots, (\alpha_{n,1} z + \beta_{n,1})^i \cdot (\alpha_{n,2} z + \beta_{n,2})^j).$$

Since $H^1(X, \mathscr{L}) = 0$ and $H^0(X, \mathscr{L}) = H^0(\mathbb{P}^2_{\mathbb{F}_q}, \mathscr{O}(r)) \otimes_{\mathbb{F}_q} \mathbb{F}_q[z]$, the long exact sequence (3) reads now as follows

$$0 \longrightarrow H^0(X, \mathscr{L} \otimes \mathscr{I}_D) \longrightarrow H^0(\mathbb{P}^2_{\mathbb{F}_q}, \mathscr{O}(r)) \otimes_{\mathbb{F}_q} \mathbb{F}_q[z] \longrightarrow \mathbb{F}_q[z]^n \longrightarrow H^1(X, \mathscr{L} \otimes \mathscr{I}_D) \longrightarrow 0$$

Furthermore, let $\Gamma \subset H^0(X, \mathscr{L})$ be a submodule such that

$$\Gamma \cap H^0(X, \mathscr{L} \otimes \mathscr{I}_D) = (0)$$

then, f will be injective and a generator matrix of the code $\mathscr{C}(\Gamma, D)$ (Definition 3.3) can be obtained from the evaluation map

$$\Gamma \hookrightarrow \mathbb{F}_q[z]^n$$

The length n, dimension k, memory m and the degree δ of the convolutional Goppa codes defined in this section are bounded by

$$n \le q^4, \quad k \le h^0(\mathbb{P}^2_{\mathbb{F}_q}, \mathscr{O}(r)) = \frac{(r+1)(r+2)}{2}, \quad m \le r, \quad \delta \le \sum_{i=0}^{r} (i+1)i = \frac{1}{3} r(r+1)(r+2)$$

For illustrating this setup and exploring its possibilities, some examples will be provided in the following section.

5. Explicit Examples

We will write down explicit examples of the above given construction of convolutional codes. We will vary Γ and D so that codes of different lengths and dimensions will be obtained.

For the sake of clarity, all the examples will deal with a particular case of the situation exposed in §4. More precisely, let us take $q = 8$, $\mathbb{F}_8$ as base field and a a primitive element such that $a^3 + a^2 + 1 = 0$.

Recall that $X := \mathbb{P}^2_{\mathbb{F}_8[z]} = \mathbb{P}^2_{\mathbb{F}_8} \times \mathbb{A}^1$ and that x_0, x_1, x_2 denote the homogeneous coordinates in $\mathbb{P}^2$.

Set $\mathscr{L} = \mathscr{O}_{\mathbb{P}^2_{\mathbb{F}_8[z]}}(\pi_1^* H_\infty)^{\otimes 2}$, then

$$H^0(X, \mathscr{L}) = H^0(\mathbb{P}^2_{\mathbb{F}_8[z]}, \mathscr{O}_{\mathbb{P}^2_{\mathbb{F}_8[z]}}(\pi_1^* H_\infty)^{\otimes 2}) = < 1, t, s, t^2, ts, s^2 >$$

where $t = \frac{x_1}{x_0}$, $s = \frac{x_2}{x_0}$ are affine coordinates.

In the following examples will study the codes corresponding to certain choices of D and $\Gamma \subseteq H^0(X, \mathscr{L})$.

5.1. **Rate $1/3$ codes.** In this case we consider the restriction of the evaluation map to a submodule $\Gamma \subset H^0(X, \mathscr{L})$ generated by one section. Here we do not need to care about the properties of D and $\mathscr{L}$ in order to determine the kernel of the evaluation map; whenever the restriction of the evaluation map to Γ is non-zero, f is injective.

Let us consider the 1-dimensional convolutional Goppa code $\mathscr{C}(D, \Gamma, \psi)$, where $\Gamma \subset H^0(X, \mathscr{L})$ is the submodule generated by the section $t + s^2$, and D is consists of the points

$$p_i(z) := (a^{2^i} + a^{2^{i-1}} z, a^{2^{i+1}} + a^{2^i} z, z) \qquad i = 1, 2, 3 \tag{4}$$

Then, the map f have the following expression

$$G = \begin{pmatrix} a^6 + az + a^4 z^2 & a^5 + a^2 z + a z^2 & a^3 + a^4 z + a^2 z^2 \end{pmatrix}$$

which is a generator matrix of the code. A straightforward check shows that this generator matrix is canonical.

A control matrix is

$$\begin{pmatrix} a^5+a^2z+az^2 & a^6+az+a^4z^2 & 0 \\ a^3+a^4z+a^2z^2 & 0 & a^6+az+a^4z^2 \end{pmatrix}$$

This code has length 3, dimension 1, memory 2, degree 2 and free distance 9. Further, it attains the generalized Singleton bound (2) and is, thus, a MDS code.

5.2. **Rate** $2/3$ **codes.** Continuing with the idea of the previous example, let us consider the submodule $\Gamma \subset H^0(X, \mathscr{L})$ generated by the sections $\{t, s^2\}$ and the closed subscheme D given by the three section of equation (4). It will be seen that the restriction of the evaluation map to Γ is injective.

Then, the matrix associated to the restriction of the evaluation map is

$$G = \begin{pmatrix} a^2+az & a^4+a^2z & a+a^4z \\ a+a^4z^2 & a^2+az^2 & a^4+a^2z^2 \end{pmatrix}$$

and, since it is injective, it gives us a generator matrix of the code, which is canonical too.

A control matrix is given by the matrix

$$\begin{pmatrix} a^4+az^2+a^2z^3 & a+a^2z^2+a^4z^3 & a^2+a^4z^2+az^3 \end{pmatrix}$$

This code has length 3, dimension 2, memory 2, degree 3 and free distance 6 and it is, thus, a MDS code.

5.3. **Rate** $1/4$ **codes.** In order to increase the length of the code, four points will be considered. Indeed, D will be now the union of the following four points

$$p_i(z) := (a^i + a^{3i}z, a^{2i} + z, z) \qquad i = 1, \dots, 4 \tag{5}$$

and Γ the submodule generated by $t + s^2$.

Then, the restriction of the evaluation map to Γ yields a generator matrix of the code $\mathscr{C}(D, \Gamma, \psi)$

$$G = \begin{pmatrix} a^3+a^3z+z^2 & a^6+a^6z+z^2 & a^6+a^2z+z^2 & a^5+a^5z+z^2 \end{pmatrix}$$

and a control matrix is

$$\begin{pmatrix} a^6+a^6z+z^2 & a^3+a^3z+z^2 & 0 & 0 \\ a^6+a^2z+z^2 & 0 & a^3+a^3z+z^2 & 0 \\ a^5+a^5z+z^2 & 0 & 0 & a^3+a^3z+z^2 \end{pmatrix}$$

This code has length 4, dimension 1, memory 2, degree 2 and free distance 12 and it is, thus, a MDS code.

5.4. **Rate** $2/4$ **codes.** Finally, let us choose another submodule Γ and preserve the same D as above (equation (5)) in order to get a code of length 4 and dimension 2. Let Γ the submodule generated by $\{t, s^2\}$.

Then, the restriction of the evaluation map to Γ yields the following generator matrix of the code $\mathscr{C}(D, \Gamma, \psi)$

$$G = \begin{pmatrix} a+a^3z & a^2+a^6z & a^3+a^2z & a^4+a^5z \\ a^4+z^2 & a+z^2 & a^5+z^2 & a^2+z^2 \end{pmatrix}$$

and a control matrix is

$$\begin{pmatrix} a^6+az+z^2+az^3 & a^4+a^2z+a^4z^2+z^3 & a+az+a^6z^2+a^5z^3 & 0 \\ a^2+a^2z+a^5z^2+a^3z^3 & a^4+a^4z+a^3z^2+a^6z^3 & 0 & a+az+a^6z^2+a^5z^3 \end{pmatrix}$$

This code has length 4, dimension 2, memory 2, degree 3 and free distance 8 and it is, thus, a MDS code.

6. Conclusions and future work

The present work is embedded in the study of convolutional codes from an algebraic geometric point of view. It is in particular a further step in the construction of convolutional codes by means of algebraic geometric tools. The main contribution with respect to previous works is the generalization of the setting where codes are defined. We present in this paper the construction of convolutional codes on higher dimensional varieties using a rather small alphabet. In particular, the construction is detailed for the variety $\mathbb{P}^2_{\mathbb{F}_q} \times \mathbb{A}^1$. Although it is in general a hard task to compute the parameters of the codes obtained we are able to find different MDS convolutional codes, and to illustrate this fact examples of codes with different rates are also presented for the case of the projective plane over $\mathbb{F}_8$.

The results obtained confirm our belief that this is a promising research line. Future steps could be to determine conditions on the geometric elements to obtain good codes or to adapt decoding algorithms to decode them.

References

1. J. A. Domínguez Pérez, J. M. Muñoz Porras, and G. Serrano Sotelo, *Convolutional codes of Goppa type*, AAECC **15** (2004), 51–61.
2. J. A. Domínguez Pérez, J. M. Muñoz Porras, and G. Serrano Sotelo, *Algebraic geometry constructions of convolutional codes*, in Advances in algebraic geometry codes, pp. 365–391, World Scientific, May 2008.
3. G. D. Forney Jr., *Convolutional codes I: Algebraic structure*, IEEE Trans. Information Theory (1970).
4. V. D. Goppa, *Codes associated with divisors*, Probl. Peredachi Inform. **13** (1977), no. 1, 33–39, Translation: *Probl. Inform. Transmission*, vol. 13, pp. 22-26, 1977.
5. V. D. Goppa, *Codes on algebraic curves*, Dokl. Adad. Nauk SSSR **259** (1981), 1289–1290, Translation: *Soviet Math. Dokl.*, vol 24, pp. 170-172, 1981.
6. S. H. Hansen, *The geometry of Deligne-Lusztig varieties; higher-dimensional ag codes*, Ph.D. thesis, University of Aarhus, July 1999.

7. R. Hartshorne, *Algebraic geometry*, Grad. Texts in Math., vol. 52, Springer-Verlag, New York, 1977.
8. T. Høholdt, J.H. van Lint and R. Pellikaan, Algebraic Geometric Codes, in: *Handbook of Coding theory*, Ed. by V.S. Pless and W.C. Huffman (Elsevier, Amsterdam, 1998) 871–962.
9. J. I. Iglesias Curto, *AAECC 2009*, ch. On Elliptic Convolutional Goppa Codes, pp. 83–91.
10. J. I. Iglesias Curto, *Generalized AG convolutional codes*, Advances in Mathematics of Communications **3** (2009), no. 4, 317–328.
11. J. Justesen, *Algebraic construction of rate* $1/\nu$ *convolutional codes*, IEEE Trans. Inform. Theory **IT-21** (1975), 577–580.
12. V. Lomadze, *Convolutional codes and coherent sheaves*, Applicable Algebra in Engineering, Communication and Computing **12** (2001), 273–326.
13. R. J. McEliece, *The algebraic theory of convolutional codes*, Handbook of Coding Theory (V. Pless and W. Huffman, eds.), vol. 1, 1998, pp. 1065–1138.
14. J. M. Muñoz Porras, J. A. Dominguez Perez, J. I. Iglesias Curto, and G. Serrano Sotelo, *Convolutional Goppa codes*, IEEE Trans. Inform. Theory **52** (2006), no. 1, 340–344.
15. P. Piret, *Structure and constructions of cyclic convolutional codes*, IEEE Trans. Inform. Theory **IT-22** (1976), 147–155.
16. P. Piret, *Convolutional codes: An Algebraic Approach*. Cambridge, MA: 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 (1994), no. 34, 329–352.
18. J. Rosenthal, *Codes, systems and graphical models*, IMA, vol. 123, ch. Connections between linear systems and convolutional codes, pp. 39–66, Springer-Verlag, 2001.
19. J. Rosenthal and R. Smarandache, *Maximum distance separable convolutional codes*, AAECC **10** (1999), no. 1, 15–32.
20. J.H. van Lint and G. van der Geer, *Introduction to Coding Theory and Algebraic Geometry* DMV Seminar, vol. **12**, (Birkhäuser, Basel, 1998).
21. J. F. Voloch and M. Zarzar, *Algebraic geometric codes on surfaces*, Séminaires & Congrès (2009), no. 21, 211–216.

DEPARTAMENTO DE MATEMÁTICAS, UNIVERSIDAD DE SALAMANCA, PLAZA DE LA MERCED 1, 37008 SALAMANCA, SPAIN, TEL.: +34+923294500 EXT. 1553, FAX: +34+923294583,

E-mail address: `joseig@usal.es`
E-mail address: `jmp@usal.es`
E-mail address: `fplaza@usal.es`
E-mail address: `laina@usal.es`