AAECC
DOI 10.1007/s00200-012-0173-9

ORIGINAL PAPER

# Convolutional Goppa codes defined on fibrations

**J. I. Iglesias Curto · J. M. Muñoz Porras · F. J. Plaza Martín · G. Serrano Sotelo**

Received: 2 August 2010 / Revised: 11 October 2011 / Accepted: 25 July 2012


**Abstract** We define a new class of Convolutional Codes in terms of fibrations of algebraic varieties generalizing our previous constructions of Convolutional Goppa Codes (Domínguez Pérez et al. in AAECC 15:51–61, 2004 [1]; Muñoz Porras et al. in IEEE Trans. Inform. Theory 52(1):340–344, 2006; [16]). This general approach allow us to give convolutional codes with maximal error correction capability (Maximum Distance Separable).

**Keywords** Convolutional codes · Goopa codes · MDS codes · Finite fields

**Mathematics Subject Classification (2000)** 14G50 · 94B10 · 11T71 · 94B27

This research was supported by the Spanish DGESYC through research project MTM2009-11393 MICINN.

J. I. Iglesias Curto · J. M. Muñoz Porras · F. J. Plaza Martín (✉) · G. Serrano Sotelo
Departamento de Matemáticas, IUFFyM,
Universidad de Salamanca, Plaza de la Merced 1,
37008 Salamanca, Spain
e-mail: fplaza@usal.es

J. I. Iglesias Curto
e-mail: joseig@usal.es

J. M. Muñoz Porras
e-mail: jmp@usal.es

G. Serrano Sotelo
e-mail: laina@usal.es

Published online: 09 August 2012

## 1 Introduction

Algebraic tools have been utilized on Coding Theory to construct codes with certain desirable properties. In particular, different algebraic approaches have been used for long to obtain convolutional codes [13,17].

With the same purpose Algebraic Geometry has been successfully applied in Coding Theory during the last decades, first for block codes (e.g. [6,7,10,18,22]) and more recently for convolutional codes [14,19]. Particularly interesting results have been obtained by the authors by generalizing the initial idea of Goppa to the construction of Convolutional Goppa Codes (CGC) [1–3,11,12,16] from points lying on a curve.

Due to the success of this approach, and inspired by the previous experience of block codes [8,23], one is tempted to explore the case of higher dimensional varieties. Thus, this paper aims at constructing CGCs defined by a family of algebraic varieties parameterized by the affine line, $X \to \mathbb{A}^1$. The construction is offered in full generality and it consists of evaluating sections of an invertible sheaf on $X$ along sections of the fibration $X \to \mathbb{A}^1$. Then, some results concerning the parameters of these codes will be given and some cases will be written down in a very detailed way. It is remarkable that our construction includes more freedom on the choice of constructive ingredients and, thus, codes with parameters of a broader variety are obtained. Furthermore, this fact allows us to construct explicit Maximum Distance Separable (MDS) codes over small fields, which was not always possible using some previous constructions. In the development of our approach we use standard notations of Algebraic Geometry (see [9]).

The contents of this work are arranged in the following way. In Sect. 2 we summarize some notions and results on convolutional codes based on [5,15]. In Sect. 3 the general construction is developed. In Sect. 4 the construction is carried out in detail for the fibration $\mathbb{P}^2_{\mathbb{F}_q} \times \mathbb{A}^1 \to \mathbb{A}^1$, permitting a more explicit use of the geometric construction for the study of the codes obtained. The construction is illustrated with a number of cases in Sect. 4.1. In Sect. 5 the construction is detailed for $X$ the trivial ruled surface, that, in addition, shows a connection with 2D convolutional codes.

Finally, we thank the referees for their valuable comments and suggestions that have helped us to improve the paper.

## 2 Preliminaries on convolutional codes

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

Opposed to the definition of block codes as $\mathbb{F}_q$-vector subspaces, an $(n, k)$ *convolutional code* $\mathcal{C}$ over $\mathbb{F}_q$ is defined as a rank $k$ submodule of $\mathbb{F}_q[z]^n$ such that $\mathbb{F}_q[z]^n/\mathcal{C}$ is locally free. 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.

Convolutional codewords are thus polynomial vectors that don't represent just a single piece of the transmission but rather the whole sequence.

Equivalently, a $(n, k)$ convolutional code $\mathcal{C}$ maybe regarded as the image of a $\mathbb{F}_q[z]$-linear injective map

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

represented by a $k \times n$ polynomial matrix of maximal rank, $G$, such that the g.c.d. of its minors of order $k$ is equal to 1. Such matrix $G$ will be called a *basic polynomial encoder* or *basic generator matrix* of $\mathcal{C}$. It has been proved [5] that every code has at least one basic generator matrix, although it is not unique. In fact, for a given convolutional code $\mathcal{C}$, the unimodular group $GL(k, \mathbb{F}_q[z])$ acts transitively on the set of basic encoders for $\mathcal{C}$ [2].

We say that $G$ is a *reduced* generator matrix if it is not possible to reduce any row degree by elementary row operations. A basic generator matrix which is reduced is called a *minimal basic encoder* by Forney [5] or a *canonical generator matrix* by McEliece [15].

The control matrix (a.k.a. parity check matrix) and the dual code for convolutional codes are defined in an analogous way as for convolutional Goppa codes [1,16].

*Remark 1* As it has been shown in [20] it is equivalent to define convolutional codes as $\mathbb{F}_q(z)$-vector subspaces, as they appear for instance in [5,15]. In fact note that any $k \times n$ basic polynomial encoder $G$ for $\mathcal{C}$ induces an injective $\mathbb{F}_q(z)$-linear map

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

In this setting it is proved that every code has a polynomial encoder. Hence the previous definitions regarding encoders are suitable in this context.

The *degree* of a convolutional code, $\delta$, defined as (e.g. [15])

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

is a significant invariant of the code and has no counterpart in block codes. Indeed, convolutional codes of degree 0 correspond exactly to block codes.

The *degree* of a polynomial encoder $G$, $\deg G$, is the sum of the degrees of its rows. A canonical encoder $G$ satisfies that

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

for all polynomial encoders $G'$ of the convolutional code.

A second important parameter of a convolutional code, which has no counterpart in block codes, is the *memory*. It is well known, e.g. [15], 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 will be denoted by $m$. The sum of the Forney indices, which is equal the maximal degree of the minors of any basic generator matrix, coincides with the degree (also known as complexity) of the code. Both the degree and the memory are used to compute the dependency of an encoded block with respect to the information blocks.

As for block codes, there is a notion of distance that will characterize the error detection/correction capability 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 $\mathcal{C}$ is defined as

$$d_{free}(\mathcal{C}) := \min_{c \in \mathcal{C} - \{0\}} \mathrm{w}(c). \tag{1}$$

The free distance is upperbounded in terms of the other parameters of the code. Although several bounds are known, the generalized Singleton bound [21]

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

is the most often considered. Those convolutional codes attaining the generalized Singleton bound are called MDS and, thus, are those with optimal error correction capability. The known proofs of existence of MDS convolutional codes (e.g. [21]) require the field to have many elements, although for practical purposes this might not be the case. Therefore, finding explicit constructions of MDS convolutional codes over small fields is a highly relevant task.

## 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 [1,16]. For the basic facts on algebraic geometry that will be used here, we address the reader to [9].

Let us choose $n$ different sections of $\pi$

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

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

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

and denote by $\mathcal{O}_D$ and $\mathcal{I}_D$ respectively the sheaves of rings and ideals of $D \hookrightarrow X$.

Let $p$ denote the composition $D \hookrightarrow X \xrightarrow{\pi} \mathbb{A}^1$ and observe that it is flat and finite of degree $n$. Then, the flatness implies the existence of isomorphisms $\phi : p_* \mathcal{O}_D \xrightarrow{\sim} \mathbb{F}_q[z]^n$, 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 $p_* \mathcal{O}_D \simeq \mathbb{F}_q[z]^n$ induced by $p$.

Let $\mathcal{L}$ be an invertible sheaf over $X$. We have an exact sequence

$$0 \to \mathcal{L} \otimes \mathcal{I}_D \to \mathcal{L} \to \widetilde{\mathcal{O}_D} := \mathcal{O}_D \underset{\mathcal{O}_X}{\otimes} \mathcal{L} \to 0,$$

and considering cohomology, we obtain the long exact sequence of $\mathbb{F}_q[z]$-modules

$$0 \to H^0(X, \mathcal{L} \otimes \mathcal{I}_D) \to H^0(X, \mathcal{L}) \to H^0(X, \widetilde{\mathcal{O}_D}) \to H^1(X, \mathcal{L} \otimes \mathcal{I}_D) \to H^1(X, \mathcal{L}) \to 0 \tag{3}$$

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

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

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

*Remark 2* If we take $\mathcal{L} \simeq \mathcal{O}_X(H)$, $H$ being an effective divisor on $X$ flat over $\mathbb{A}^1$, then it follows that there exists a canonical isomorphism $\widetilde{\mathcal{O}_D} \simeq \mathcal{O}_D$. On the other hand, if $p_i(\mathbb{A}^1) \cap p_j(\mathbb{A}^1) = \emptyset$ for all $i \neq j$, then the above isomorphism $\phi$ can also be chosen canonically. Thus, if both hypotheses are fulfilled, then there is a canonical isomorphism $\psi$.

**Definition 1** The *convolutional Goppa code* $\mathcal{C}(D, \Gamma, \psi)$ determined by the sheaf $\mathcal{L}$, the subscheme $D$, the isomorphism $\psi$, and a submodule $\Gamma \subseteq H^0(X, \mathcal{L})$ is the submodule given by the image of the homomorphism $f$ defined by

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^0(X, \mathcal{L} \otimes \mathcal{I}_D) & \longrightarrow & H^0(X, \mathcal{L}) & \longrightarrow & H^0(X, \widetilde{\mathcal{O}_D}) \\ & & & & \uparrow & & \downarrow \wr \psi \\ & & & & \Gamma & \xrightarrow{f} & \mathbb{F}_q[z]^n \end{array} \tag{4}$$

The parameters of the above defined code are given by the following

**Theorem 1** 1. *The length of* $\mathcal{C}(D, \Gamma, \psi)$ *is given by the number of sections* $p_1, \ldots, p_n$.
2. $\dim \mathcal{C}(D, \Gamma, \psi) = \operatorname{rk} \operatorname{Im}(f)$.
3. $\dim \mathcal{C}(D, \Gamma, \psi) = \operatorname{rk} \Gamma$ *if and only if* $\Gamma \cap H^0(X, \mathcal{L} \otimes \mathcal{I}_D) = (0)$.
4. $\dim \mathcal{C}(D, \Gamma, \psi) = h^0(\mathcal{L}) - h^0(\mathcal{L} \otimes \mathcal{I}_D) = h^0(\widetilde{\mathcal{O}_D}) - h^1(\mathcal{L} \otimes \mathcal{I}_D) + h^1(\mathcal{L})$ *for the case of the complete linear series,* $\Gamma = H^0(X, \mathcal{L})$.

*Proof* By the very construction, the *length of the code* is given by the rank of $\mathcal{O}_D$ as an $\mathcal{O}_{\mathbb{A}^1}$-module, which is the number $n$ of sections taken to define the code.

The second item follows trivially from the very definition of dimension. Having in mind that $\ker(f) = \Gamma \cap H^0(X, \mathcal{L} \otimes \mathcal{I}_D)$ and diagram (4), one concludes the third claim.

The fourth statement is a straightforward consequence of the additive property of the dimension applied to the exact sequence (3).

*Remark 3* The explicit computation of the dimension for the general case is a very hard problem in classical algebraic geometry based on the theory of syzygies.

Let us briefly sketch how CGC can be alternatively introduced in terms of subspaces of $\mathbb{F}_q(z)$. For this goal, one considers the generic point of $\mathbb{A}^1$, $\eta$, whose residue field is $\mathbb{F}_q(\eta) = \mathbb{F}_q(z)$. The fiber $X_\eta$ is an $m$-dimensional variety over $\mathbb{F}_q(z)$, and $p_1(\eta), \ldots, p_n(\eta)$ 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

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

Moreover, if $\mathcal{L} = \mathcal{O}_X(H)$ then $\psi_\eta$ can be canonically chosen.

**Definition 2** The *convolutional Goppa code* $\mathcal{C}(D_\eta, \Gamma, \psi_\eta)$ is the image of the homomorphism $f_\eta$ defined by

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^0(X_\eta, \mathcal{L}_\eta \otimes \mathcal{I}_{D_\eta}) & \longrightarrow & H^0(X_\eta, \mathcal{L}_\eta) & \longrightarrow & H^0(X_\eta, \widetilde{\mathcal{O}_{D_\eta}}) \\ & & & & \uparrow & & \downarrow \psi_\eta \wr \\ & & & & \Gamma & \xrightarrow{f_\eta} & \mathbb{F}_q(z)^n \end{array}$$

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

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

In the rest of the paper, unless otherwise stated, we will continue with the submodule approach, although the translation to the subspace setting would be straightforward as we have just seen.

As it was already mentioned in the Introduction, the case when $\dim X = 2$ has been already studied in [1,16], in particular for $X = \mathbb{P}^1 \times \mathbb{A}^1$. In the next two sections we will illustrate in detail how the construction works for fibrations of surfaces.

## 4 Codes defined on the projective plane

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 $x_0 = 0$. We consider the line bundle, $\mathcal{L}$, defined by $\pi_1^* \mathcal{O}(1)^{\otimes r} = \mathcal{O}(r) \underset{\mathbb{F}_q}{\otimes} \mathbb{F}_q[z]$, where $\pi_1 \colon X \to \mathbb{P}^2_{\mathbb{F}_q}$ is the projection onto the first factor.

The parameters of the codes obtained from this fibration should fulfill some constraints, as it is shown in the following

**Theorem 2** *Let $\Gamma$ be a submodule of $H^0(\mathbb{P}^2_{\mathbb{F}_q[z]}, \pi_1^*\mathcal{O}(1)^{\otimes r})$. Let $D$ be the divisor given by the closure of* $\mathrm{Im}(p_i)$ *where*

$$\begin{aligned} \mathbb{A}^1 &\xrightarrow{p_i} \mathbb{A}^2 \times \mathbb{A}^1 = (\mathbb{P}^2_{\mathbb{F}_q} - H_\infty) \times \mathbb{A}^1 \\ z &\mapsto p_i(z) = (\alpha_{i,1}z + \beta_{i,1}, \alpha_{i,2}z + \beta_{i,2}, z) \end{aligned}$$

*with $\alpha_{i,r}, \beta_{i,s} \in \mathbb{F}_q$ and $p_i(\mathbb{A}^1) \cap p_j(\mathbb{A}^1) = \emptyset$ for $i \neq j$ and $1 \leq i \leq n$. Finally, let $\psi$ be the trivialization of $\mathcal{L}$ along $D$ given by Remark 2.*

*Then, for the convolutional Goppa code $\mathcal{C}(D, \Gamma, \psi)$ the following hold:*

1. *the length of the code is at most $q^4$;*
2. $\mathrm{rk}\,\mathcal{C}(D, \Gamma, \psi) \leq \binom{r+2}{2}$*;*

*Proof* The first claim follows from the trivial observation that the number of different sections of the above type, $q^4$, is an upper bound for the length of the code, $n$.

Regarding the second statement, one has

$$k := \mathrm{rk}\,\mathrm{Im}\,\Gamma \leq \mathrm{rk}\,H^0(\mathbb{P}^2_{\mathbb{F}_q[z]}, \pi_1^*\mathcal{O}(1)^{\otimes r}) = h^0(\mathbb{P}^2_{\mathbb{F}_q}, \mathcal{O}(1)^{\otimes r}) = \binom{r+2}{2}$$

*Remark 4* It is worth pointing out that the above count of the number of different sections also includes block codes, which corresponds to the case $\alpha_{i,r} \equiv 0$ for all $i, r$, as well as codes defined with the fibration $\mathbb{P}^1_{\mathbb{F}_q} \times \mathbb{A}^1 \xrightarrow{\pi} \mathbb{A}^1$, when the $n$ sections are collinear. Note that the constraint on the length for this class of codes allows to obtain longer codes than with the usual construction over curves of genus 0. Furthermore, if codes of length greater than $q^4$ are needed, then one could consider more general sections; namely, those of the type $z \mapsto (\alpha(z), \beta(z), z)$ where $\alpha$ and $\beta$ are polynomials. However, this choice increases the memory of the code.

**Theorem 3** *With the above hypothesis and assuming that*

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

*it then holds that:*

1. $m \leq \deg \mathcal{L}$*, where $m$ is the memory:*
2. $\delta \leq \frac{1}{3}r(r+1)(r+2)$*, where $\delta$ is the degree.*

*Proof* The constraint on $\Gamma$ means that the evaluation map $f$ [see Diagram (4), is injective and that the evaluation map

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

yields a generator matrix of the code $\mathcal{C}(D, \Gamma, \psi)$ (Definition 1)].

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

$$H^0\left(\mathbb{P}^2_{\mathbb{F}_q}, \mathcal{O}(r)\right) = \langle t^i s^j \mid 0 \leq i + j \leq r \rangle$$

Hence, the evaluation of $t^i s^j$ at the sections $p_1, \ldots, p_n$, which are polynomials in $z$ of degree 1, is given by

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

where $f$ is as in diagram (4). That is, the evaluation of $t^i s^j$ at each section has degree $i + j$ and, therefore, the degree at each row of an encoder is upperbounded by $r$ and so is the memory $m$ of the code.

Following the previous arguments, the row of the encoder obtained by the evaluation of the function $t^i s^j$ has degree $i + j$. Hence, the degree of such encoder, i.e. the sum of its row degrees, is at most

$$\sum_{\substack{i,j \\ 0 \le i+j \le r}} i + j = \sum_{l=0}^{r} \sum_{\substack{i,j \\ i+j=l}} i + j = \sum_{l=0}^{r} (l+1)l = \frac{1}{3} r(r+1)(r+2)$$

Bearing in mind that the degree of the code $\delta$ is upperbounded by the degree of any of its encoders, the conclusion follows.

**Proposition 1** *If, furthermore, $\Gamma$ is generated by $P(t, s)$, a polynomial of total degree less than or equal to $r$, then the matrix associated to the evaluation map $f$*

$$\begin{pmatrix} P(\alpha_{1,1}z + \beta_{1,1}, \alpha_{1,2}z + \beta_{1,2}) & \ldots & P(\alpha_{n,1}z + \beta_{n,1}, \alpha_{n,2}z + \beta_{n,2}) \end{pmatrix}$$

*is a canonical basic encoder of the convolutional Goppa code $\mathcal{C}(D, \Gamma, \psi)$ if and only if the mcd of its entries (as polynomials in $z$) is* 1.

*Proof* In this case, the notion of canonical basic encoder is equivalent to say that the cokernel of $f$ is a free module, which can be expressed as the coprimality condition.

Note that varying the coefficients of the polynomial and the sections, the above Proposition might be used as a way to find good 1-dimensional codes.

### 4.1 Explicit constructions

We will illustrate this construction by explicitly obtaining a number of MDS codes with different parameters over small fields. With this purpose we will vary $\Gamma$ and $D$.

We want to emphasize that although existence of MDS codes has been proved [21], that proof is not constructive and requires the field to have sufficiently many elements. On the other hand, only few instances of MDS codes over small fields have been given. As stated next, we will construct our codes over the field with 8 elements. This, together with the known fact that the condition of being MDS is open [21], shows that the set of MDS convolutional codes over $\mathbb{F}_8$ is dense, i.e., almost every code is MDS, and our construction provides an effective way to find such codes.

Let us take $\mathbb{F}_8$ as the base field and $a$ a primitive element such that $a^3+a^2+1=0$. Then we have $X := \mathbb{P}^2_{\mathbb{F}_8[z]} = \mathbb{P}^2_{\mathbb{F}_8} \times \mathbb{A}^1$. Let $x_0, x_1, x_2$ denote the homogeneous coordinates in $\mathbb{P}^2$ and let $t = \frac{x_1}{x_0}$, $s = \frac{x_2}{x_0}$ be affine coordinates. Set $\mathcal{L} = \pi_1^* \mathcal{O}_{\mathbb{P}^2_{\mathbb{F}_8[z]}}(1)^{\otimes 2}$, then

$$H^0(X, \mathcal{L}) = H^0\left(\mathbb{P}^2_{\mathbb{F}_8[z]}, \pi_1^* \mathcal{O}_{\mathbb{P}^2_{\mathbb{F}_8[z]}}(1)^{\otimes 2}\right) = \langle 1, t, s, t^2, ts, s^2 \rangle.$$

For the sake of simplicity we will consider sections over the generic point $\eta$, i.e. $\mathbb{F}_q(z)$-rational points over $X_\eta = \mathbb{P}^2_{\mathbb{F}_8(z)}$. As it was pointed out before, it is possible to choose canonically the isomorphism $\psi_\eta$, and hence we remove it from the notation. Having in mind [20] (see also Remark 1) one could reformulate this subsection in terms of submodules.

For each case all the geometric elements used and the corresponding encoder, as well as a control matrix, will be explicitly written down. Recall that the control matrix is not unique and that it doesn't need to be canonical in order to check whether a vector is a codeword or not.

### *4.1.1 Codes of dimension 1*

Let us consider the restriction of the evaluation map to a submodule $\Gamma \subset H^0(X, \mathcal{L})$ generated by one section. Here we do not need to care about the properties of $D$ and $\mathcal{L}$ in order to determine the kernel of the evaluation map; whenever the restriction of the evaluation map to $\Gamma$ is non-zero, $f$ is injective.

Note also that in this case the generalized Singleton bound is given by

$$d_{free} \leq n(\delta + 1)$$

which implies that constant terms of the entries of a generator matrix of a MDS code must be different from zero.

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

$$p_i(z) := \left(a^{2^i} + a^{2^{i-1}} z, a^{2^{i+1}} + a^{2^i} z\right) \quad i = 1, 2, 3 \tag{5}$$

Then, the evaluation map $f$ is represented by the matrix

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

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

A control matrix is

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

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

Let us consider now a code of length four. $D$ will be now the union of the following four points

$$p_i(z) := \left(a^i + a^{3i}z, a^{2i} + z\right) \quad i = 1, \ldots, 4 \tag{6}$$

and as before $\Gamma$ the submodule generated by $t + s^2$.

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

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

having as control matrix

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

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

### *4.1.2 Codes of dimension 2*

Let us consider now the submodule $\Gamma \subset H^0(X, \mathcal{L})$ generated by the sections $\{t, s^2\}$ and $D$ the divisor defined by the three points of Eq. (5). It can be easily seen that the restriction of the evaluation map to $\Gamma$ 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. This matrix is, in addition, a canonical encoder.

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.

Again, in order to get a code of length 4 we keep $\Gamma$ the submodule generated by $\{t, s^2\}$ and choose $D$ defined by the points in Eq. (6).

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

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

which can be easily checked to be canonical. A control matrix is

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

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

## 5 Codes defined on a ruled surface

Let us consider the trivial ruled surface $\mathbb{P}^1_{\mathbb{F}_q} \times \mathbb{P}^1_{\mathbb{F}_q}$ and the natural projection

$$\pi : X = \mathbb{P}^1_{\mathbb{F}_q} \times \mathbb{P}^1_{\mathbb{F}_q} \times \mathbb{A}^1 \longrightarrow \mathbb{A}^1.$$

Let $P_\infty$ be the infinity point of $\mathbb{P}^1$ defined by the equation $x_0 = 0$. For each pair of positive integers $(r, l)$ we define the following invertible sheaf on $X$:

$$\mathcal{L}(r, l) = \pi_1^* \mathcal{O}_{\mathbb{P}^1}(r P_\infty) \otimes_{\mathbb{F}_q} \pi_2^* \mathcal{O}_{\mathbb{P}^1}(l P_\infty) \otimes_{\mathbb{F}_q} \mathbb{F}_q[z]$$

where $\pi_i : \mathbb{P}^1 \times \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ are the two natural projections.

One has then a natural isomorphism

$$\Gamma = H^0(\mathbb{P}^1 \times \mathbb{P}^1, \pi_1^* \mathcal{O}_{\mathbb{P}^1}(r P_\infty) \otimes_{\mathbb{F}_q} \pi_2^* \mathcal{O}_{\mathbb{P}^1}(l P_\infty)) \simeq$$
$$\simeq H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(r P_\infty)) \otimes_{\mathbb{F}_q} H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(l P_\infty)).$$

Let us denote by $t$ the affine coordinate of the first copy of $\mathbb{P}^1$ and $s$ the affine coordinate of the second copy of $\mathbb{P}^1$. Then, the space $\Gamma$ of global sections is explicitly described as

$$\Gamma = \langle t^i \otimes s^j \mid i \leq r, j \leq l \rangle$$

We can define the sections $p_i$ of $\pi$ by their equations in affine coordinates:

$$p_i(z) = (\alpha_{i,1} z + \beta_{i,1}, \alpha_{i,2} z + \beta_{i,2}, z)$$

where $\alpha_{i,j}, \beta_{i,j} \in \mathbb{F}_q$.

Let us observe that, though the affine equations of the sections are the same as in the case $X = \mathbb{P}^2_{\mathbb{F}_1} \times \mathbb{A}^1$ their global structures are different since $\mathbb{P}^2 \not\simeq \mathbb{P}^1 \times \mathbb{P}^1$.

Now, we have the evaluation map at the sections $p_1, \ldots, p_n$:

$$H^0(X, \mathcal{L}(r, l)) = \Gamma \otimes_{\mathbb{F}_q} \mathbb{F}_q[z] \xrightarrow{f} \mathbb{F}_q[z]^n$$

and the convolutional code $\mathcal{C}$ is defined as the image of this map. The evaluation of $t^i \otimes s^j$ at $p_1, \ldots, p_n$ is given by

$$f(t^i \otimes s^j) = ((\alpha_{11}z + \beta_{11})^i(\alpha_{12}z + \beta_{12})^j, \ldots, (\alpha_{n1}z + \beta_{n1})^i(\alpha_{n2}z + \beta_{n2})^j)$$

This evaluation map allows to obtain a CGC as explained in Sect. 3. By replacing $\mathbb{P}^1 \times \mathbb{P}^1$ by another arbitrary ruled surface we obtain other CGC in the same way.

In addition, this formalization allows to relate classical convolutional codes with 2D convolutional codes defined as in [4].

Let us observe that the projection $\pi : \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{A}^1 \longrightarrow \mathbb{A}^1$ can be factorized as the composition of two projections:

$$\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{A}^1 \xrightarrow{\pi_{23}} \mathbb{P}^1 \times \mathbb{A}^1 \xrightarrow{\pi_3} \mathbb{A}^1$$

Let us consider sections of $\pi_{23}$

$$\begin{aligned} q_i : \mathbb{P}^1 \times \mathbb{A}^1 &\longrightarrow \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{A}^1 \\ (s, z) &\longmapsto (\alpha_{i1}z + \beta_{i1} + s, s, z) \end{aligned}$$

($s$ being the affine coordinate of the second copy of $\mathbb{P}^1$, as before), and sections of $\pi_3$

$$\begin{aligned} \overline{q_i} : \mathbb{A}^1 &\longrightarrow \mathbb{P}^1 \times \mathbb{A}^1 \\ z &\longmapsto (\alpha_{i2}z + \beta_{i2}, z) \end{aligned}$$

Thus, the compositions $q_i \circ \overline{q_i} = \overline{p_i}$ are sections

$$\overline{p_i} : \mathbb{A}^1 \longrightarrow \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{A}^1$$

given by the equations

$$\overline{p_i}(z) = ((\alpha_{i1} + \alpha_{i2})z + \beta_{i1} + \beta_{i2}, \alpha_{i2}z + \beta_{i2}, z)$$

The evaluation of $H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(rP_\infty)) \otimes \mathbb{F}_q[s] \otimes \mathbb{F}_q[z]$ at the sections $q_1, \ldots, q_n$ is given by

$$t^i(q_1, \ldots, q_n) = ((\alpha_{i1}z + \beta_{i1} + s)^i, \ldots, (\alpha_{n1}z + \beta_{n1} + s)^i)$$

which defines a 2D convolutional code. But the evaluation at the sections $\overline{p_1}, \ldots, \overline{p_n}$ gives the kind of convolutional codes described before. We hope that deeper insight of the connections between these two classes of codes will help to understand the properties of 2D convolutional codes.

## 6 Conclusions and future work

We offer a natural generalization of convolutional Goppa codes with the help of fibrations of higher dimensional varieties. Our construction covers a wide variety of codes but it is still simple enough to apply at concrete cases, as it has been shown in two different scenarios.

This generalization also yields MDS codes, whose properties are written down in terms of the geometric elements used to construct them. It is remarkable that such MDS codes are defined over small fields and, thus, our approach overcomes known constraints; for instance, those regarding the length of the codes with respect to the size of the field.

The results obtained, including a new connection with 2D codes, confirm our belief that this is a promising research line. In fact, further steps can be taken in order to characterize good codes in terms of the geometric elements or to adapt decoding algorithms to this class of CGC.

## References


1. Domínguez Pérez, J.A., Muñoz Porras, J.M., Serrano Sotelo, G.: Convolutional codes of Goppa type. AAECC **15**, 51–61 (2004)
2. Domínguez Pérez, J.A., Muñoz Porras, J.M., Serrano Sotelo, G.: Algebraic geometry constructions of convolutional codes. In: Martínez-Moro, E., Munuera, C., Ruano, D., Advances in Algebraic Geometry Codes, Vol. **5**, pp. 391–417. Ser. Coding Theory Cryptol. World Sci. Publ., Hackensack (2008)
3. Domínguez Pérez, J.A., Muñoz Porras, J.M., Serrano Sotelo, G.: One Dimensional Convolutinal Goppa Codes Over the Projective Line. Preprint available at arXiv:1107.2059
4. Fornasini, E., Valcher, M.E.: Algebraic aspects of two-dimensional convolutional codes. IEEE Trans. Inf. Theory **40**(4), 1068–1082 (1994)
5. Forney, G.D. Jr.: Convolutional codes I: algebraic structure. IEEE Trans. Inf. Theory, IT **16**, 720–738 (1970)
6. Goppa, V.D.: Codes associated with divisors. Probl. Peredachi Inform. **13**(1), 33–39 (1977) (Trans: Probl. Inform. Transmission., vol. **13**, pp. 22–26, 1977)
7. Goppa, V.D.: Codes on algebraic curves. Dokl. Adad. Nauk SSSR **259**, 1289–1290 (1981) (Trans: Soviet Math. Dokl., vol. **24**, pp. 170–172, 1981)
8. Hansen, S.H.: The geometry of Deligne-Lusztig varieties; higher-dimensional ag codes. Ph.D. thesis, University of Aarhus, July (1999)
9. Hartshorne, R.: Algebraic Geometry. Grad. Texts in Math., vol. **52**. Springer, New York (1977)
10. Høholdt, T., van Lint, J.H., Pellikaan, R.: Algebraic geometric codes. In: Pless, V.S., Huffman, W.C. (eds.) Handbook of Coding Theory, pp. 871–962. Elsevier, Amsterdam (1998)
11. Iglesias Curto, J.I.: AAECC 2009, ch. On Elliptic Convolutional Goppa Codes, pp. 83–91
12. Iglesias Curto, J.I.: Generalized AG convolutional codes. Adv. Math. Commun. **3**(4), 317–328 (2009)
13. Justesen, J.: Algebraic construction of rate $1/\nu$ convolutional codes. IEEE Trans. Inform. Theory **IT-21**, 577–580 (1975)
14. Lomadze, V.: Convolutional codes and coherent sheaves. Appl. Algebra Eng. Commun. Comput. **12**, 273–326 (2001)
15. McEliece, R.J.: The algebraic theory of convolutional codes. In: Pless, V., Huffman, W. (eds.) Handbook of Coding Theory, vol. **1**, pp. 1065–1138. North Holland, Amsterdam (1998)
16. Muñoz Porras, J.M., Dominguez Perez, J.A., Iglesias Curto, J.I., Serrano Sotelo, G.: Convolutional Goppa codes. IEEE Trans. Inform. Theory **52**(1), 340–344 (2006)
17. Piret, P.: Structure and constructions of cyclic convolutional codes. IEEE Trans. Inform. Theory **IT-22**, 147–155 (1976)
18. Piret, P.: Convolutional Codes: An Algebraic Approach. MIT Press, Cambridge (1988)

19. Ravi, M.S., Rosenthal, J.: A smooth compactification of the space of transfer functions with fixed McMillan degree. Acta Appl. Math. **34**(3), 329–352 (1994)
20. Rosenthal, J.: Codes, systems and graphical models, IMA, vol. **123**, ch. Connections between linear systems and convolutional codes, pp. 39–66, Springer, Berlin (2001)
21. Rosenthal, J., Smarandache, R.: Maximum distance separable convolutional codes. AAECC **10**(1), 15–32 (1999)
22. van Lint, J.H., van der Geer, G.: Introduction to coding theory and algebraic geometry DMV seminar, vol. **12**. Birkhäuser, Basel (1998)
23. Voloch, J.F., Zarzar, M.: Algebraic geometric codes on surfaces. Séminaires Congrès **21**, 211–216 (2009)