AAECC 15, 51–61 (2004)
Digital Object Identifier (DOI) 10.1007/s00200-004-0151-y

AAECC
Applicable Algebra in Engineering, Communication and Computing

Convolutional Codes of Goppa Type*

J.A. Domínguez Pérez, J.M. Muñoz Porras, G. Serrano Sotelo

Departamento de Matemáticas, Universidad de Salamanca, Plaza de la Merced 1-4, 37008 Salamanca, Spain
(e-mail: jadoming,jmp,laina@usal.es)

Received: February 20, 2003; revised version: March 2, 2004
Published online: April 20, 2004 –

Abstract. A new kind of Convolutional Codes generalizing Goppa Codes is proposed. This provides a systematic method for constructing convolutional codes with prefixed properties. In particular, examples of Maximum-Distance Separable (MDS) convolutional codes are obtained.

Keywords: Convolutional Codes, Goppa Codes, MDS Codes, Algebraic Curves, Coherent Sheaves, Finite Fields

1 Introduction

The aim of this paper is to propose a definition of Convolutional Goppa Codes (CGC). This definition will provide an algebraic method for constructing Convolutional Codes with prescribed invariants.

We propose a definition of CGC in terms of families of curves $X \to \mathbb{A}^1$ parametrized by the affine line $\mathbb{A}^1 = \operatorname{Spec} \mathbb{F}_q[z]$ over a finite field $\mathbb{F}_q$. In this setting, the usual definition of a Goppa Code as the code obtained by evaluation of sections at several rational points, is translated as a code obtained by evaluation (of sections of some invertible sheaf over X) along several sections of the fibration $X \to \mathbb{A}^1$.

The paper is organized as follows.

In §2 we offer a summary on Goppa Codes following [5], [8], and using the standard notations of Algebraic Geometry [4].

§3 is devoted to giving the general definition of CGC and gives some general results.

In §4 we study the case of a trivial fibration of projective lines over $\mathbb{A}^1$ and we conclude giving some explicit examples of MDS convolutional codes.

* This research was partially supported by the Spanish DGI through research project BFM2003-00078 and by the "Junta de Castilla y León" through research projects SA071/04 and SA032/02.

We freely use the standard notations of abstract Algebraic Geometry as can be found in [4]. After the works of V. Lomadze [6], J. Rosenthal and R. Smarandache [10], [11], there is evidence that the use of methods of Algebraic Geometry can be relevant to the study of Convolutional Codes. This paper is a step in favor of that evidence.

Other algebraic methods for constructing Convolutional Codes have been recently proposed [2], [3].

2 Background on Algebraic Geometry and Goppa Codes

In this Section we summarize the basic definitions about Goppa Codes, constructed using methods of Algebraic Geometry (see [5], [8]).

Let X be a geometrically irreducible, smooth and projective curve over the finite field $\mathbb{F}_q$. Let $p_1, \dots, p_n$ be n different $\mathbb{F}_q$-rational points of X, and D the divisor $D = p_1 + \cdots + p_n$. Let G be another effective divisor with support disjoint from D. The Goppa code $C(G, D)$ defined by (G, D) is the linear code of length n over $\mathbb{F}_q$ defined as the image of the linear map

$$\begin{aligned} \alpha\colon L(G) &\to \mathbb{F}_q^n \\ f &\mapsto (f(p_1), \dots, f(p_n)), \end{aligned}$$

where $L(G)$ is the complete linear series defined by G. That is, let $\mathbb{F}_q(X)$ be the field of rational functions over the curve X,

$$L(G) = \left\{ f \in \mathbb{F}_q(X) \text{ such that } \operatorname{Div}(f) + G \geq 0 \right\}.$$

The Goppa code has dimension

$$k = \dim C(G, D) = \dim L(G) - \dim L(G - D).$$

Let g be the genus of X; if we assume the inequality $2g - 2 < \deg(G) < n$, then one has

$$k = \deg(G) - g + 1,$$

and the minimum distance d of $C(G, D)$ satisfies the inequality

$$d \geq n - \deg(G).$$

Let $\mathcal{O}_X(D)$ be the invertible sheaf on X defined by the divisor D. One has the following exact sequence of sheaves

$$0 \to \mathcal{O}_X(-D) \to \mathcal{O}_X \to \mathcal{O}_D \to 0,$$

where $\mathcal{O}_D \simeq \mathcal{O}_{p_1}/\mathfrak{m}_{p_1} \times \cdots \times \mathcal{O}_{p_n}/\mathfrak{m}_{p_n} \simeq \mathbb{F}_q \times \overset{n)}{\cdots} \times \mathbb{F}_q$. Tensoring the above exact sequence by $\mathcal{O}_X(G)$, one obtains

$$0 \to \mathcal{O}_X(G - D) \to \mathcal{O}_X(G) \to \mathcal{O}_D \to 0.$$

By taking global sections, we obtain an exact sequence of cohomology

$$\begin{aligned} 0 \to H^0(X, \mathcal{O}_X(G-D)) &\to H^0(X, \mathcal{O}_X(G)) \overset{\alpha}{\to} \mathcal{O}_D \to \\ & H^1(X, \mathcal{O}_X(G-D)) \to \\ & \to H^1(X, \mathcal{O}_X(G)) \to 0\,, \end{aligned}$$

where $L(G) = H^0(X, \mathcal{O}_X(G))$ and α is the evaluation map defined above. In the case $2g - 2 < \deg(G) < n$, one has the exact sequence

$$0 \to H^0(X, \mathcal{O}_X(G)) \overset{\alpha}{\to} \mathcal{O}_D \to H^1(X, \mathcal{O}_X(G-D)) \to 0\,. \tag{2.1}$$

Let ω_X be the dualizing sheaf of X, which is isomorphic to the sheaf of regular 1-forms over X; $H^0(X, \omega_X)$ is the $\mathbb{F}_q$-vector space of global regular 1-forms over X, which is of dimension g = genus of X.

By Serre's duality ([4]), there exist canonical isomorphisms of $\mathbb{F}_q$-vector spaces

$$H^1(X, \mathcal{L})^* \simeq H^0(X, \omega_X \otimes \mathcal{L}^{-1})$$

for every invertible sheaf $\mathcal{L}$ on X. Given a divisor D over X, we shall denote by $\Omega(D)$ the vector space $H^0(X, \omega_X \otimes \mathcal{O}_X(-D))$.

The dual Goppa code, $C^*(G, D)$, associated with the Goppa code $C(G, D)$ is defined as the linear code of length n over $\mathbb{F}_q$ given by the image of the linear map

$$\begin{aligned} \alpha^* \colon \Omega(G-D) &\to \mathbb{F}_q^n \\ \eta &\mapsto (\mathrm{Res}_{p_1}(\eta), \ldots, \mathrm{Res}_{p_n}(\eta))\,, \end{aligned}$$

Let us take duals in the exact sequence (2.1):

$$0 \to H^1(X, \mathcal{O}_X(G-D))^* \overset{\beta}{\to} \mathcal{O}_D^* \overset{\alpha^t}{\to} H^0(X, \mathcal{O}_X(G))^* \to 0\,.$$

By Serre's duality, one has isomorphisms

$$\begin{aligned} H^1(X, \mathcal{O}_X(G-D))^* &\simeq \Omega(G-D)\,, \\ H^0(X, \mathcal{O}_X(G))^* &\simeq H^1(X, \omega_X \otimes \mathcal{O}_X(-G))\,, \end{aligned}$$

and the above sequence is the cohomology sequence induced by the exact sequence of sheaves

$$0 \to \omega_X(-G) \to \omega_X(D-G) \to \omega_X(D-G) \otimes_{\mathcal{O}_X} \mathcal{O}_D \to 0\,,$$

where we denote $\omega_X(-G) = \omega_X \otimes \mathcal{O}_X(-G)$, and β is precisely the map α^* defining $C^*(G, D)$.

Given a linear series $\Gamma \subseteq H^0(X, \mathcal{O}_X(G))$, that is, a vector subspace defining a family of divisors linearly equivalent to G, we define the Goppa code $C(\Gamma, D)$ associated with Γ and D as the image of the homomorphism $\alpha_{|\Gamma}$:

$$\begin{array}{ccc} H^0(X, \mathcal{O}_X(G)) & \xrightarrow{\alpha} & \mathcal{O}_D \\ \bigcup\vert & \nearrow_{\alpha_{|\Gamma}} & \\ \Gamma & & \end{array}$$

When $\Gamma \subsetneqq H^0(X, \mathcal{O}_X(G))$, we shall say that $C(\Gamma, D)$ is a non-complete Goppa code.

3 Convolutional Goppa Codes

We shall contruct a kind of convolutional code that generalizes the notion of Goppa codes. These codes will be associated with families of algebraic curves.

Given an algebraic variety S over the field $\mathbb{F}_q$, a family of projective algebraic curves parametrized by S is a morphism of algebraic varieties $\pi : X \to S$, such that π is a projective and flat morphism whose fibres $X_s = \pi^{-1}(s)$ are smooth and geometrically irreducible curves over $\mathbb{F}_q(s)$ (the residue field of $s \in S$).

Let us consider a family of curves $X \xrightarrow{\pi} U$ parametrized by $U = \operatorname{Spec} \mathbb{F}_q[z] = \mathbb{A}^1$. Given a closed point $u \in U$ with residue field $\mathbb{F}_q(u)$, the fibre $X_u = \pi^{-1}(u)$ is a curve over the finite field $\mathbb{F}_q(u)$.

Let p_i, $1 \leq i \leq n$, be n different sections, $p_i : U \to X$, of the projection π. These sections define a Cartier divisor on X:

$$D = p_1(U) + \cdots + p_n(U)\,,$$

which is flat of degree n over the base U ([4]).

Note that given a coherent sheaf $\mathcal{F}$ on X, the cohomology groups $H^i(X, \mathcal{F})$ are finite $\mathbb{F}_q[z]$-modules and $H^i(X, \mathcal{F}) = 0$ for $i \geq 2$ (see [4] III).

Let $\mathcal{L}$ be an invertible sheaf over X. One has an exact sequence of sheaves on X

$$0 \to \mathcal{L}(-D) \to \mathcal{L} \to \mathcal{O}_D \to 0\,, \tag{3.1}$$

(where $\mathcal{L} \otimes \mathcal{O}_D \simeq \mathcal{O}_D$) which induces a long exact cohomology sequence

$$\begin{aligned} 0 &\to H^0(X, \mathcal{L}(-D)) \to H^0(X, \mathcal{L}) \xrightarrow{\alpha} H^0(X, \mathcal{O}_D) \to H^1(X, \mathcal{L}(-D)) \\ &\to H^1(X, \mathcal{L}) \to 0\,. \end{aligned} \tag{3.2}$$

Let r be the degree of $\mathcal{L}$ in each fibre of π (which is independent of the fibre) and let g be the genus of any fibre of π (also independent of the fibres).

Proposition 3.1 *Let us assume that* $2g-2 < r$. *Then, one has that* $H^1(X, \mathcal{L}) = 0$ *and* $H^0(X, \mathcal{L})$ *is a free* $\mathbb{F}_q[z]$*-module of rank* $r - g + 1$

Proof. Under the condition $2g - 2 < r$, one has that $H^1(X_u, \mathcal{L}_{|X_u}) = 0$ for every point $u \in U$. Note that $H^i(X, \mathcal{F})^\sim = R^i\pi_*\mathcal{F}$ for every coherent sheaf $\mathcal{F}$ on X ([4] III), and applying ([4] III Corollary 12.9) one concludes the proof. □

Under the hypothesis of Proposition 3.1, there exists an exact sequence of $\mathbb{F}_q[z]$-modules

$$0 \to H^0(X, \mathcal{L}(-D)) \to H^0(X, \mathcal{L}) \overset{\alpha}{\to} H^0(X, \mathcal{O}_D) \to H^1(X, \mathcal{L}(-D)) \to 0\,. \tag{3.3}$$

where $H^0(X, \mathcal{O}_D)$ is a free $\mathbb{F}_q[z]$-module of rank n.

Remark 3.2 Let $\eta \in U$ be the generic point of U, whose residue field is $\mathbb{F}_q(z)$; the fibre $X_\eta = \pi^{-1}(\eta)$ is a smooth, irreducible curve over $\mathbb{F}_q(z)$. Note that $p_1(\eta), \dots, p_n(\eta)$ are n different $\mathbb{F}_q(z)$-rational points of the curve X_η. One then has a canonical decomposition of $H^0(X, \mathcal{O}_D)_\eta$ as a $\mathbb{F}_q(z)$-algebra

$$H^0(X, \mathcal{O}_D)_\eta = \mathbb{F}_q(z) \times \overset{n)}{\dots} \times \mathbb{F}_q(z)\,.$$

Given a $\mathbb{F}_q[z]$-module M, let us denote by M_η the $\mathbb{F}_q(z)$-vector space

$$M_\eta = M \otimes_{\mathbb{F}_q[z]} \mathbb{F}_q(z)\,.$$

The sequence (3.3) induces an exact sequence of $\mathbb{F}_q(z)$-vector spaces

$$0 \to \; H^0(X, \mathcal{L}(-D))_\eta \to H^0(X, \mathcal{L})_\eta \overset{\alpha_\eta}{\to} H^0(X, \mathcal{O}_D)_\eta \to$$
$$H^1(X, \mathcal{L}(-D))_\eta \to 0\,. \tag{3.4}$$

Definition 3.3 *The complete convolutional Goppa code associated with $\mathcal{L}$ and D is the image of the homomorphism α_η*

$$\mathcal{C}(\mathcal{L}, D) = \mathcal{I}\mathrm{m}\left(H^0(X, \mathcal{L})_\eta \xrightarrow{\alpha_\eta} H^0(X, \mathcal{O}_D)_\eta \simeq \mathbb{F}_q(z)^n\right)\,.$$

Given a free submodule $\Gamma \subseteq H^0(X, \mathcal{L})$, the convolutional Goppa code associated with Γ and D is the image of $\alpha_{\eta_{|\Gamma_\eta}}$

$$\mathcal{C}(\Gamma, D) = \mathcal{I}\mathrm{m}\left(\Gamma_\eta \xrightarrow{\alpha_\eta} \mathbb{F}_q(z)^n\right)\,.$$

Remark 3.4 We use definition 2.4 of [7] as definition of convolutional codes. Any matrix defining α_η (respectively $\alpha_{\eta_{|\Gamma_\eta}}$) is a generator matrix of rational functions for the code $\mathcal{C}(\mathcal{L}, D)$ (resp. $\mathcal{C}(\Gamma, D)$).

The canonical decomposition $H^0(X, \mathcal{O}_D)_\eta \simeq \mathbb{F}_q(z)^n$ as $\mathbb{F}_q(z)$-algebras does not extend (in general) to a decomposition $H^0(X, \mathcal{O}_D) \simeq \mathbb{F}_q[z]^n$ as rings.

In fact, one has a canonical isomorphism of rings $H^0(X, \mathcal{O}_D) \overset{\phi}{\simeq} \mathbb{F}_q[z]^n$ only when $p_1(U), \dots, p_n(U)$ are disjoint sections. However, $H^0(X, \mathcal{O}_D)$ is a free $\mathbb{F}_q[z]$-module; then, there exist (non-canonical) isomorphisms of $\mathbb{F}_q[z]$-modules:

$$H^0(X, \mathcal{O}_D) \overset{\phi}{\simeq} \mathbb{F}_q[z] \oplus \overset{n)}{\cdots} \oplus \mathbb{F}_q[z]\,,$$

which are not (in general) isomorphism of rings.

This allows us to give another definition of convolutional Goppa codes, as submodules of a polynomial module [9].

Definition 3.5 *Given a trivialization* $\phi\colon H^0(X, \mathcal{O}_D) \simeq \mathbb{F}_q[z]^n$ *as* $\mathbb{F}_q[z]$*-modules, one defines the convolutional Goppa code* $\mathcal{C}(\mathcal{L}, D, \phi)$ *as the image of* $\phi \circ \alpha$

$$H^0(X, \mathcal{L}) \overset{\alpha}{\to} H^0(X, \mathcal{O}_D) \overset{\phi}{\simeq} \mathbb{F}_q[z]^n\,.$$

Analogously, one defines the convolutional Goppa code $\mathcal{C}(\Gamma, D, \phi)$.

Let us assume (for the rest of the paper) that the invariants (r, n, g) satisfy the inequality

$$2g - 2 < r < n\,.$$

Proposition 3.6 *Under the above conditions on* (r, n, g), $H^0(X, \mathcal{L}(-D)) = 0$ *and* $H^1(X, \mathcal{L}(-D))$ *is a free* $\mathbb{F}_q[z]$*-module. The following exact sequence is exact*

$$0 \to H^0(X, \mathcal{L}) \overset{\alpha}{\to} H^0(X, \mathcal{O}_D) \to H^1(X, \mathcal{L}(-D)) \to 0\,. \tag{3.5}$$

and remains exact when we take fibres over every point $u \in U$.

Proof. If $2g - 2 < r < n$, $H^0(X_u, \mathcal{L}(-D)_{|X_u}) = 0$ for every point $u \in U$; and applying ([4] III Corollary 12.9) one concludes. □

Corollary 3.7 *The convolutional code* $\mathcal{C}(\mathcal{L}, D, \phi)$ *has dimension* $k = r - g + 1$ *and length* n*. Every matrix defining* $\phi \circ \alpha$ *is a basic generator matrix [7] for* $\mathcal{C}(\mathcal{L}, D, \phi)$.

Proof. This is a direct consequence of the last statement of Proposition 3.6 and the characterization of basic generator matrices of [7]. □

Let us consider the convolutional Goppa code $\mathcal{C}(\Gamma, D, \phi)$ defined by a submodule $\Gamma \subseteq H^0(X, \mathcal{L})$ and a trivialization ϕ. With the above restrictions, one has:

Proposition 3.8 *Every matrix defining* $\phi \circ \alpha_{|_\Gamma}$ *is a basic generator matrix for the code* $\mathcal{C}(\Gamma, D, \phi)$ *if and only if* $H^0(X, \mathcal{L})/\,\Gamma$ *is a torsion-free* $\mathbb{F}_q[z]$*-module.*

Proof. The sequence (3.5) induces a diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & \Gamma & \xrightarrow{\alpha_{|\Gamma}} & H^0(X, \mathcal{O}_D) & \longrightarrow & H^1(X, \Gamma) & \longrightarrow & 0 \\
 & & \downarrow & & \| & & \downarrow & & \\
0 & \longrightarrow & H^0(X, \mathcal{L}) & \longrightarrow & H^0(X, \mathcal{O}_D) & \longrightarrow & H^1(X, \mathcal{L}(-D)) & \longrightarrow & 0 \\
 & & \downarrow & & & & \downarrow & & \\
 & & H^0(X, \mathcal{L})/\,\Gamma & & & & 0 & &
\end{array}$$

Then, the kernel of $H^1(X, \Gamma) \to H^1(X, \mathcal{L}(-D))$ is isomorphic to $H^0(X, \mathcal{L})/\,\Gamma$ and $H^1(X, \mathcal{L}(-D))$ is free. This implies that the torsion elements of $H^1(X, \Gamma)$ are contained in $H^0(X, \mathcal{L})/\,\Gamma$, from which one concludes the proof. □

The above results allow us to construct basic generator matrices for the codes $\mathcal{C}(\Gamma, D, \phi)$. If $p_1(U), \dots, p_n(U)$ are disjoint sections and ϕ the canonical trivialization, this gives us a basic generator matrix for $\mathcal{C}(\Gamma, D)$. However, in general the codes $\mathcal{C}(\Gamma, D)$ and $\mathcal{C}(\Gamma, D, \phi)$ are different.

Let us describe a geometric way to obtain a basic generator matrix for $\mathcal{C}(\mathcal{L}, D)$ and $\mathcal{C}(\Gamma, D)$.

Assume that the curves $p_1(U), \dots, p_n(U)$ meet transversally at some points, and let $\bar{X}$ be the blowing-up [4] of X at these points. One has morphisms

$$\begin{array}{ccc}
\bar{X} & \xrightarrow{\beta} & X \\
 & {\scriptstyle \bar{\pi}=\pi\circ\beta}\searrow & \downarrow{\scriptstyle \pi} \\
 & & U
\end{array}$$

such that the proper transform of D under π is a divisor $\bar{D} \subset \bar{X}$ satisfying

$$\bar{D} = p_1(U) \amalg \cdots \amalg p_n(U) \xrightarrow{\beta} D\,,$$

and one has a canonical homomorphism of rings

$$0 \to \mathcal{O}_D \to \beta_* \mathcal{O}_{\bar{D}}$$

which induces

$$0 \to \pi_* \mathcal{O}_D \xrightarrow{\beta} \bar{\pi}_* \mathcal{O}_{\bar{D}} \simeq \widetilde{\mathbb{F}_q[z]^n}\,,$$

where $\bar{\pi}_* \mathcal{O}_{\bar{D}} \simeq \widetilde{\mathbb{F}_q[z]^n}$ is the canonical isomorphism of sheaves of rings.

$\beta^* \mathcal{L}$ is an invertible sheaf on $\bar{X}$ and there exists a canonical homomorphism

$$\beta^* \mathcal{L} \to \mathcal{O}_{\bar{D}} \to 0\,,$$

whose kernel is $(\beta^* \mathcal{L})(-\bar{D})$. We have also an injective homomorphism

$$0 \to \mathcal{L} \to \beta_* \beta^* \mathcal{L}\,,$$

and taking global sections one obtains

$$0 \to H^0(X, \mathcal{L}) \xrightarrow{\gamma} H^0(X, \beta_* \beta^* \mathcal{L}) \xrightarrow{\mu} \mathbb{F}_q[z]^n \,.$$

The image of μ is precisely a free submodule of $\mathbb{F}_q[z]^n$ that defines a basic generator matrix for $\mathcal{C}(\mathcal{L}, D)$.

Let us consider the sequence of homomorphisms

$$0 \to H^0(X, \mathcal{L}) \xrightarrow{\alpha} H^0(X, \mathcal{O}_D) \overset{\beta}{\hookrightarrow} H^0(X, \mathcal{O}_{\bar{D}}) = \mathbb{F}_q[z]^n \,.$$

$\beta \circ \alpha$ is not in general a basic matrix, since $H^0(X, \mathcal{O}_{\bar{D}})/H^0(X, \mathcal{O}_D)$ has torsion. Let us define

$$\bar{H}^0(X, \mathcal{L}) = \{p \in \mathbb{F}_q[z]^n \text{ such that } \lambda p \in H^0(X, \mathcal{L}) \text{ for some } \lambda \in \mathbb{F}_q[z]\} \,.$$

$\bar{H}^0(X, \mathcal{L})/H^0(X, \mathcal{L})$ is a torsion module and $\mathbb{F}_q[z]^n/\bar{H}^0(X, \mathcal{L})$ is torsion-free. Then, every matrix defining the homomorphism $\bar{H}^0(X, \mathcal{L}) \hookrightarrow \mathbb{F}_q[z]^n$ is a basic generator matrix for $\mathcal{C}(\mathcal{L}, D)$.

This is an algebraic-geometric interpretation of Forney's construction of the basic matrices of a convolutional code [1].

4 Convolutional Goppa Codes associated with the projective line

Let $\mathbb{P}^1 = \operatorname{Proj} \mathbb{F}_q[x_0, x_1]$ be the projective line over $\mathbb{F}_q$, and

$$X = \mathbb{P}^1 \times U \xrightarrow{\pi} U = \operatorname{Spec} \mathbb{F}_q[z]$$

the trivial fibration. Let us denote by $t = x_1/x_0$ the affine coordinate in $\mathbb{P}^1$, and by p_∞ its infinity point. Let us consider the following n different sections of π

$$p_i \colon U \to \mathbb{P}^1 \times U$$

defined in the coordinates (t, z) by

$$p_i(z) = (\alpha_i z + \beta_i, z)\,, \; \alpha_i, \beta_i \in \mathbb{F}_q \,.$$

Let $D = p_1(U) + \cdots + p_n(U)$ and let $\mathcal{L}$ be the invertible sheaf on X

$$\mathcal{L} = \pi_1^* \mathcal{O}_{\mathbb{P}^1}(r p_\infty) \otimes_{\mathbb{F}_q} \mathcal{O}_U \,, \; r < n \,,$$

The exact sequence (3.5) is in this case:

$$\begin{array}{ccccccc} 0 \to H^0(X, \mathcal{L}) & \xrightarrow{\quad\alpha\quad} & H^0(X, \mathcal{O}_D) & \longrightarrow & H^1(X, \mathcal{L}(-D)) & \longrightarrow & 0\,. \\ || & & || & & & & \\ H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(r p_\infty)) \otimes \mathbb{F}_q[z] & \xrightarrow{\quad\alpha\quad} & \mathbb{F}_q[z]^n & & & & \end{array}$$

Taking the fibres over the generic point η, and the canonical trivialization $(\pi_*\mathcal{O}_D)_\eta \simeq \mathbb{F}_q(z)^n$, the homomorphism α_η is the evaluation map at the points $p_1(\eta), \dots, p_n(\eta)$

$$\alpha_\eta \colon H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(rp_\infty)) \otimes_{\mathbb{F}_q} \mathbb{F}_q(z) \to \mathbb{F}_q(z)^n$$
$$\alpha_\eta(t^j) = \big(t^j(p_1(\eta)), \dots, t^j(p_n(\eta))\big) = \big((\alpha_1 z + \beta_1)^j, \dots, (\alpha_n z + \beta_n)^j\big),$$

where $\{1, t, \dots, t^r\}$ is the "canonical" basis of $H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(rp_\infty))$ in the affine coordinate t. The convolutional code $\mathcal{C}(\mathcal{L}, D)$ is a kind of *generalized Reed-Solomon (RS) code* (for $z = 0$ we obtain a classical RS-code).

Let $\Gamma \subseteq H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(rp_\infty))$ be the linear subspace generated by $\{t^s, \dots, t^r\}$. The convolutional Goppa code $\mathcal{C}(\Gamma, D)$ is the image of the homomorphism

$$\alpha_\eta \colon \Gamma \otimes_{\mathbb{F}_q} \mathbb{F}_q(z) \to \mathbb{F}_q(z)^n$$
$$t^j \longmapsto \alpha_\eta(t^j), \quad \text{for } s \le j \le r.$$

In this case $H^0(X, \mathcal{L})/\Gamma \simeq \big(H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(rp_\infty))/\Gamma\big) \otimes_{\mathbb{F}_q} \mathbb{F}_q[z]$ is torsion-free. Then, by Proposition 3.8 every matrix defining

$$\alpha \colon \Gamma \otimes_{\mathbb{F}_q} \mathbb{F}_q[z] \to H^0(X, \mathcal{O}_D)$$

is a basic generator matrix. To compute a matrix for α explicitly, we need to fix an isomorphism of $\mathbb{F}_q[z]$-modules

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

and this gives a generator matrix for $\mathcal{C}(\Gamma, D, \phi)$. However, it would be desirable to compute basic matrices for the codes $\mathcal{C}(\Gamma, D)$. We shall do this in general in a forthcoming paper. Here we shall offer some explicit examples.

Example 4.1 Let $a, b \in \mathbb{F}_q$ be two different non-zero elements, and

$$p_i(z) = (a^{i-1}z + b^{i-1}, z)\,, i = 1, \dots, n\,, \text{ with } n < q.$$

The evaluation map α_η over Γ is defined by the matrix

$$\begin{pmatrix} (z+1)^s & (az+b)^s & (a^2z+b^2)^s & \dots & (a^{n-1}z+b^{n-1})^s \\ (z+1)^{s+1} & (az+b)^{s+1} & (a^2z+b^2)^{s+1} & \dots & (a^{n-1}z+b^{n-1})^{s+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (z+1)^r & (az+b)^r & (a^2z+b^2)^r & \dots & (a^{n-1}z+b^{n-1})^r \end{pmatrix}. \tag{4.1}$$

This matrix is a generator matrix for the code $\mathcal{C}(\Gamma, D)$. Using this construction we can give concrete examples of CGC of dimension $k = r - s + 1$ that are Maximum-Distance Separable (MDS) convolutional codes, i.e., whose *free distance* d attains the generalized Singleton bound $d \le (n-k)(\lfloor \delta/k \rfloor + 1) + \delta + 1$, where δ is the degree of the code. ([10] Th. 2.2 and Definition 2.5).

- If $s = r$, the convolutional Goppa code $\mathcal{C}(\Gamma, D)$ has dimension 1, degree r, and (4.1) is a *canonical* (reduced and basic [7]) generator matrix. We can list a few examples, where k/n, δ and d are respectively the rate, the degree and the free distance of the code.

field	*canonical generator matrix*	k/n	δ	d
$\mathbb{F}_3 = \{0, 1, 2\}$	$\begin{pmatrix} z+1 & z+2 \end{pmatrix}$	1/2	1	4
$\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ where $\alpha^2 + \alpha + 1 = 0$	$\begin{pmatrix} z+1 & z+\alpha & z+\alpha^2 \end{pmatrix}$	1/3	1	6
$\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$	$\begin{pmatrix} (z+1)^2 & (z+2)^2 & (z+4)^2 \end{pmatrix}$	1/3	2	9

In these examples the sections $p_1, \dots, p_n$ are disjoint, such that $\mathcal{C}(\Gamma, D) = \mathcal{C}(\Gamma, D, \phi)$, where $\phi\colon H^0(X, \mathcal{O}_D) \stackrel{\sim}{\to} \mathbb{F}_q[z]^n$ is the corresponding canonical trivialization.

- If $s < r$, let us take $a \in \mathbb{F}_q$ as a primitive element.

  Now, the matrix (4.1) is reduced, since the matrix of highest-degree terms in each row is a Vandermonde matrix of rank k. The sections $p_1, \dots, p_n$ are not disjoint, but in some cases the matrix (4.1) is actually basic and we do not have to find an isomorphism of $\mathbb{F}_q[z]$-modules, $\phi\colon H^0(X, \mathcal{O}_D) \stackrel{\sim}{\to} \mathbb{F}_q[z]^n$, in order to compute a basic generator matrix for the code $\mathcal{C}(\Gamma, D)$.
  We present two examples of this situation.

field	*canonical generator matrix*	k/n	δ	d
$\mathbb{F}_4$	$\begin{pmatrix} 1 & 1 & 1 \\ z+1 & \alpha z+\alpha^2 & \alpha^2 z+\alpha \end{pmatrix}$	2/3	1	3
$\mathbb{F}_5$	$\begin{pmatrix} z+1 & 2z+3 & 4z+4 & 3z+2 \\ (z+1)^2 & (2z+3)^2 & (4z+4)^2 & (3z+2)^2 \end{pmatrix}$	1/2	3	8

Acknowledgments. We thank F.J. Plaza Martín and E. Gómez González for many enlightening comments, and J. Prada Blanco and J.I. Iglesias Curto for helpful questions that helped us to improve this paper.

References

1. Forney Jr., G.D.: Convolutional Codes I: Algebraic Structure. IEEE Trans. Inform. Theory **16**, 720–738 (1970)
2. Gluesing-Luerssen, H., Langfeld, B.: On the Parameters of Convolutional Codes with Cyclic Structure. Preprint arXiv: math.RA/0312092
3. Gluesing-Luerssen, H., Schmale, W.: On cyclic convolutional codes. Preprint arXiv: math.RA/0211040
4. Hartshorne, R.: Algebraic Geometry Grad. Texts in Math. vol. 52, Springer-Verlag, New York, 1977
5. Høholdt, T., van Lint, J.H., Pellikaan, R.: Algebraic Geometric Codes. In: Handbook of Coding theory, Ed. by V.S. Pless and W.C. Huffman, Elsevier, Amsterdam, 1998, pp. 871–962
6. Lomadze, V.: Convolutional Codes and Coherent Sheaves. AAECC **12**, 273–326 (2001)
7. McEliece, R.J.: The Algebraic Theory of Convolutional Codes. In: Handbook of Coding theory. Ed. by V.S. Pless and W.C. Huffman, Elsevier, Amsterdam, 1998, pp. 1065–1138
8. van Lint, J.H., van der Geer, G.: Introduction to Coding Theory and Algebraic Geometry DMV Seminar, vol. 12, Birkhäuser, Basel, 1998
9. Rosenthal, J., Schumacher, J.M., York, E.V.: On behaviors and convolutional codes. IEEE Trans. Inform. Theory **42**, 1881–1891 (1996)
10. Rosenthal, J., Smarandache, R.: Maximum Distance Separable Convolutional Codes. AAECC **10**, 15–32 (1999)
11. Smarandache, R., Gluesing-Luerssen, H., Rosenthal, J.: Constructions of MDS-Convolutional Codes. IEEE Trans. Inform. Theory **47**, 2045–2049 (2001)