21st International Symposium on
Mathematical Theory of Networks and Systems
July 7-11, 2014. Groningen, The Netherlands

Construction of arbitrary convolutional codes as evaluation codes over the projective line

José Ignacio Iglesias Curto, Ángel Luis Muñoz Castañeda,
José María Muñoz Porras and Gloria Serrano Sotelo

Abstract— **The introduction of Algebraic Geometry by Goppa as a tool for code construction resulted in a rich family of linear codes that also allowed to obtain already existing codes. This motivated the work of Pellikaan, Shen and van Wee about which linear codes could be obtained as algebraic geometric codes.**

Similar tools have been used to develop the convolutional counterpart of Goppa codes yielding some optimal constructions and, as in the linear case, some codes which were already known. Therefore it seems a natural question to determine which convolutional codes can be constructed using algebraic geometric tools. It has been shown by the authors that in fact any convolutional code can be given an algebraic structure, i.e. they can be obtained by evaluation of a certain subspace of rational functions, and they have given conditions so that it is defined by a complete linear system.

We present here such structure with explicit expressions considering the projective line as the curve over which the construction is carried out. That is to say, we expose how any convolutional code can be obtained as a convolutional Goppa code over the projective line. In addition we give the explicit conditions so that a code is defined by a complete linear system, i.e. the subspace of functions is the subspace of global sections of a certain divisor. Further, we consider the particular case of memory 0 codes, i.e. linear codes, which implies that our conclusions are of application to linear codes as well. In particular, considering linear codes as a class of convolutional codes allows to overcome the limitation on the number of rational points when working over a finite field.

I. Introduction

Convolutional Goppa codes (CGC) [1], [8] were introduced as a generalization for convolutional codes of the use of algebraic geometric elements to construct codes with a certain structure that could be used to study their properties and to decode them. It happens that, as it is also the case with block codes, some already existing codes have been shown to have that algebraic geometric structure.

Pellikaan et al. [10] studied which block codes were in fact algebraic geometric concluding that every code could be given an algebraic geometric structure, which they did explicitly considering for each code a curve of high genus in general.

José Ignacio Iglesias Curto, José María Muñoz Porras and Gloria Serrano Sotelo are with the Department of Mathematics and IUFFyM, Universidad de Salamanca, Plaza de la Merced 1, 37008 Salamanca, Spain (e-mail: joseig@usal.es; jmp@usal.es; laina@usal.es)

Ángel Luis Muñoz Castañeda is with the Institut für Mathematik, Freie Universität, Arnimallee 3, 14195 Berlin, Germany (e-mail: angel@math.fu-berlin.de)

This research was supported by the Spanish DGICT, Ministerio de Economía y Competitividad, through research project MTM2012-32342.

A different approach was considered in [6] to address the analogous question for convolutional codes. When considering convolutional Goppa codes, which are defined over a field $\mathbb{F}_q(z)$, the advantage of having curves with infinitely many rational points plays a fundamental role. As a result the authors concluded that any convolutional code, including block codes, could be constructed as CGC over any curve satisfying certain weak conditions, and in particular over the projective line.

In fact, note that curves of small genus are to be preferred when constructing algebraic geometric codes in order to have tighter bounds on the value of the minimum distance, respectively free distance, and on the error-correction capacity of decoding algorithms.

In this work we show that every convolutional code can be given a Goppa structure over the curve with lowest genus, the projective line. We will actually give the explicit procedure to construct any convolutional code in this way.

We will pay a particular attention to block codes, which are known to be convolutional codes of degree 0, and to which therefore all the results are of application.

Although this characterization may have apparently no immediate practical application it actually opens the door to the use of algebraic geometric tools for decoding any convolutional code. Further, the fact that the curve considered is the one with lowest genus and that, as it will be shown, one can do it over rather small fields, is expected to result in simpler and more effective procedures.

Our work has this structure. In Section II we expose the algebraic geometric tools that will be needed. In Section III we show how any code can be obtained as a convolutional Goppa code by evaluation of certain functions on a set of rational points of the projective line. In Section IV we address the question of which codes can be obtained as CGC defined by a complete linear system. In Section V we focus on the case of block codes.

II. Preliminaries

Convolutional Goppa codes are constructed making use of algebraic geometric tools. Before proceeding with our study, let us recall the main elements involved in the construction [5].

Let $\mathbb{F}_q$ be a finite field with q elements, where $q = p^s$ is the power of a prime and let $\mathbb{F}_q(z)$ be the field of rational functions over $\mathbb{F}_q$. Let us consider the projective line over the field $\mathbb{F}_q(z)$, $\mathbb{P}^1_{\mathbb{F}_q(z)} = \operatorname{Proj} \mathbb{F}_q(z)[x_0, x_1]$ and the affine line $\mathbb{A}^1_{\mathbb{F}_q(z)} = \mathbb{P}^1_{\mathbb{F}_q(z)} - \{p_\infty\}$ with affine coordinate $t = x_1/x_0$.

ISBN: 978-90-367-6321-9

A divisor D over a curve X, in our case the projective line, is a formal sum $D = \sum_{p\in X} n_p p$ where $n_p \in \mathbb{Z}$ and $n_p \neq 0$ only for finitely many points $p \in X$. The degree of D is defined as $\deg D = \sum n_p \deg(p)$, where $\deg(p)$ is the degree of the extension to the field where the point has its coordinates. Here we will be considering points p with coordinates in the ground field, i.e. rational points, and hence $\deg(p) = 1$. The support of the divisor D is the set $\{p \in X \mid n_p \neq 0\}$. Every rational function f over the curve defines a divisor $(f) = \sum n_i p_i - \sum n'_j q_j$, where p_i and q_j are the zeros of f with orders n_i, respectively its poles with orders n'_j.

Each divisor D can be associated to an invertible sheaf $\mathcal{O}_X(D)$ and therefore to the $\mathbb{F}_q(z)$-vector space of its global sections

$$H^0(X, \mathcal{O}_X(D)) = \{f \in \Sigma_X \mid (f) + D \geq 0\}\,.$$

A commonly used alternative notation for this space, that we will use for the sake of simplicity, is $L(D) \equiv H^0(X, \mathcal{O}_X(D))$.

An element with a central role in our study is the closed immersion defined by any very ample invertible sheaf $\mathcal{L}$

$$\begin{aligned} \varphi_{\mathcal{L}} : X &\hookrightarrow \mathbb{P}H^0(X,\mathcal{L})^* = \mathbb{P}^{n-1}_{\mathbb{F}_q(z)} \\ p &\longmapsto < \psi_p > \end{aligned} \tag{1}$$

where $\psi_p : H^0(X, \mathcal{L}) \longrightarrow \mathbb{F}_q(z)$ is the evaluation map $\psi_p(s) = s(p)$. Further, if $\{x_i\}_{i=0}^{n-1}$ is a basis of $H^0(X, \mathcal{L})^*$ then the global sections $\{\varphi^*_{\mathcal{L}}(x_i)\}_{i=0}^{n-1} \subset H^0(X, \mathcal{L})$ generate $\mathcal{L}$.

Here we will be mostly considering the invertible sheaf $\mathcal{L} = \mathcal{O}_{\mathbb{P}^1_{\mathbb{F}_q(z)}}(G)$ associated to the divisor $G = (n-1)p_\infty$ over the projective line. Bearing this in mind we can give an explicit expression of the closed immersion $\varphi_{\mathcal{L}}$ (1).

Note that that $L(G) = \langle 1, t, \ldots, t^{n-1}\rangle$. Any rational point $p \in \mathbb{A}^1_{\mathbb{F}_q(z)}$ with affine coordinate $\alpha \in \mathbb{F}_q(z)$ defines a valuation map $\psi_p \in L(G)^*$

$$\begin{aligned} \psi_p : L(G) &\to \mathbb{F}_q(z) \\ t^j &\mapsto t^j(p) = \alpha^j \end{aligned} \tag{2}$$

Let $\{w_1, \ldots, w_n\}$ be the dual basis of $\{1, t, \ldots, t^{n-1}\}$ in $L(G)^*$ then $\psi_p = 1w_1 + \alpha w_2 + \ldots + \alpha^{n-1}w_n$ and $\varphi_{\mathcal{L}}$ is given by

$$\begin{aligned} \varphi_{\mathcal{L}} : \mathbb{P}^1_{\mathbb{F}_q(z)} &\hookrightarrow \mathbb{P}L(G)^* = \mathbb{P}^{n-1}_{\mathbb{F}_q(z)} \\ p &\mapsto [1; \alpha; \ldots; \alpha^{n-1}] \end{aligned}\,. \tag{3}$$

This explicit expression allows us to prove the following crucial result.

Lemma 2.1: The images by $\varphi_{\mathcal{L}}$ of any n different rational points $p_1, \ldots, p_n \in \mathbb{A}^1_{\mathbb{F}_q(z)}$ are in general position in $\mathbb{P}L(G)^*$.

Proof: Let us consider n different rational points with affine coordinates $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q(z)$. Their images by $\varphi_{\mathcal{L}}$ are in general position if there is no hyperplane containing them. That means by (3) that they are in general position if and only if the vectors $(1, \alpha_i, \ldots, \alpha_i^{n-1})$, $i = 1, \ldots, n$, generate the whole $L(G)^*$, if and only if

$$\begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \ldots & \alpha_2^{n-1} \\ \vdots & & & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \ldots & \alpha_n^{n-1} \end{vmatrix} = \prod_{1\leq i<j\leq n} (\alpha_j - \alpha_i) \neq 0$$

which is obviously the case since the points are different. ■

III. Convolutional codes are CGC over $\mathbb{P}^1_{\mathbb{F}_q(z)}$

Let us recall some basic facts on convolutional Goppa codes assuming they are constructed over the projective line. The general construction in detail and proofs of their properties can be found in [6], [8].

CGC are constructed over a curve X, in our work we will restrict ourselves to $X = \mathbb{P}^1_{\mathbb{F}_q(z)}$ the projective line over $\mathbb{F}_q(z)$. Let $p_1, \ldots, p_n$ be a set of n different $\mathbb{F}_q(z)$-rational points of $\mathbb{P}^1_{\mathbb{F}_q(z)}$. Let us consider the divisor $D = p_1 + \cdots + p_n$ and let G be another divisor on $\mathbb{P}^1_{\mathbb{F}_q(z)}$ with support disjoint from D. It is possible to define an evaluation morphism

$$\begin{aligned} \alpha : L(G) &\to \mathbb{F}_q(z) \times \overset{n}{\cdots} \times \mathbb{F}_q(z) \\ s &\mapsto (s(p_1), \ldots, s(p_n)) \end{aligned}$$

Definition 3.1 ([8]): The convolutional Goppa code $\mathcal{C}(D, G)$ associated with the pair (D, G) is defined as the image of α. Analogously, given a subspace $\Gamma \subseteq L(G)$, one defines the convolutional Goppa code $\mathcal{C}(D, \Gamma)$ as the image of $\alpha|_\Gamma$.

By construction, $\mathcal{C}(D, G)$ is a convolutional code of length n and dimension

$$k \leq \dim L(G)\,.$$

Under the condition $2g - 2 < \deg G < n$, the evaluation map $\alpha\colon L(G) \hookrightarrow \mathbb{F}_q(z)^n$ is injective, and the dimension of $\mathcal{C}(D, G)$ is exactly

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

Considering the same divisors D, G there is a dual construction of convolutional Goppa codes which is based on taking residues at the support of D of a certain subspace of differentials determined by both divisors [8]. As in the block case, the resulting code is in fact the dual code $\mathcal{C}^\perp(D, G)$ to $\mathcal{C}(D, G)$.

Remark 3.2: Note that since we are considering the same divisors D, G in the construction of $\mathcal{C}^\perp(D, G)$ we conclude in particular that $\mathcal{C}$ is a Goppa code if and only if so is $\mathcal{C}^\perp$.

With these elements we can proceed to give an explicit description of how any convolutional code can be given a geometric structure over the projective line as presented in [6, §III.A].

Let $\mathcal{C}$ be a convolutional code of length n and dimension k generated by a matrix

$$\mathcal{G} = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \vdots \\ a_{k1} & \ldots & a_{kn} \end{pmatrix}, \qquad a_{ij} \in \mathbb{F}_q(z)\,. \tag{4}$$

We want to construct the code $\mathcal{C}$ as a convolutional Goppa code over $\mathbb{P}^1_{\mathbb{F}_q(z)}$, i.e. $g = 0$. For this we need n different rational points $p_1, \ldots, p_n \in \mathbb{A}^1_{\mathbb{F}_q(z)}$ and a k-dimensional $\mathbb{F}_q(z)$-vector subspace $\Gamma \subset L(G)$ for a certain divisor G such that $\mathrm{Im}\ \alpha|_\Gamma = \mathcal{C}$, $\alpha|_\Gamma$ being the restriction to Γ of the evaluation map α at $p_1, \ldots, p_n$.

Note that we can always take different rational points in the affine line $p_1, \ldots, p_n \in \mathbb{A}^1_{\mathbb{F}_q(z)}$ since $\mathbb{F}_q(z)$ has infinitely many elements. Let us fix $G = (n-1)p_\infty$. The sheaf $\mathcal{L} = \mathcal{O}_{\mathbb{P}^1_{\mathbb{F}_q(z)}}(G)$ defines a map $\varphi_\mathcal{L}$ (3) such that for any rational point $p \in \mathbb{P}^1_{\mathbb{F}_q(z)}$ $\varphi_\mathcal{L}(p) = \langle \psi_p \rangle \in \mathbb{P}L(G)^*$. By Lemma 2.1 their images by $\varphi_\mathcal{L}$ are in general position in $\mathbb{P}L(G)^*$ and hence $\langle \psi_{p_1}, \ldots, \psi_{p_n} \rangle = L(G)^*$.

Then we can define a linear map $\alpha = (\psi_{p_1}, \ldots, \psi_{p_n})$ by

$$\begin{aligned} \alpha : L(G) &\hookrightarrow \mathbb{F}_q(z)^n \\ s &\mapsto (\psi_{p_1}(s), \ldots, \psi_{p_n}(s)) = (s(p_1), \ldots, s(p_n)) \end{aligned} \tag{5}$$

Recall that we take t as affine coordinate in $\mathbb{A}^1_{\mathbb{F}_q(z)}$ and that $L(G) = \langle 1, t, \ldots, t^{n-1} \rangle$. Let $\{w_1, \ldots, w_n\}$ be the dual basis of $\{1, t, \ldots, t^{n-1}\}$ and let

$$V = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \ldots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \ldots & \alpha_n^{n-1} \end{pmatrix}$$

be the matrix of the change of basis linear map from $\{\psi_{p_i}\}$ to $\{w_i\}$. Let $\{\sigma_1, \ldots, \sigma_n\}$ be the dual basis of $\{\psi_{p_1}, \ldots, \psi_{p_n}\}$. The inverse of the dual to the basis change map is the basis change map from $\{\sigma_i\}$ to $\{t^i\}$, i. e. $\sigma_i = c_0^i + c_1^i t + \ldots + c_{n-1}^i t^{n-1}$, where $(c_o^i, \ldots, c_{n-1}^i)$ is the i-th row of the matrix $(V^t)^{-1}$. In order to give an explict expression of the coefficients of $\sigma_i(t) = c_0^i + c_1^i t + \ldots + c_{n-1}^i t^{n-1}$ note that the duality of the bases, $\sigma_i(\psi_{p_j}) = \delta_{ij}$, means $\sigma_i(\alpha_j) = 0$ if $i \neq j$, which implies

$$\sigma_i(t) = \lambda_i \prod_{j=1, i\neq j}^{n} (t - \alpha_j) \tag{6}$$

and $\sigma_i(\alpha_i) = 1$, which implies

$$\lambda_i = \frac{1}{\prod_{j=1, i\neq j}^{n} (\alpha_i - \alpha_j)}$$

Then the coefficients c_{n-r}^i, for all $r = 1, \ldots, n$, are

$$c_{n-r}^i = (-1)^r \lambda_i S_r(\alpha_1, \ldots, \hat{\alpha}_i, \ldots, \alpha_n)$$

with $S_r(\alpha_1, \ldots, \hat{\alpha}_i, \ldots, \alpha_n)$ the basic symmetric polynomial of degree r in $n-1$ variables that depends on all α_j, $j \leq n$, except α_i [7].

Let us consider $s_i \in L(G)$, $i = 1, \ldots, k$ with

$$\begin{aligned} s_1 &= a_{11}\sigma_1 + \ldots + a_{1n}\sigma_n \\ &\vdots \\ s_k &= a_{k1}\sigma_1 + \ldots + a_{kn}\sigma_n \end{aligned} \tag{7}$$

which explicitly are

$$s_i = a_{i1}\sigma_1 + \ldots + a_{in}\sigma_n = \sum_{r=1}^{n} (-1)^r t^{n-r} \sum_{j=1}^{n} a_{ij}\lambda_j S_r(\alpha_1, \ldots, \hat{\alpha}_j, \ldots, \alpha_n)$$

for all $i = 1, \ldots, k$. By construction $\alpha(s_i) = (a_{i1}, \ldots, a_{in})$.

Let us consider then the subspace $\Gamma = \langle s_1, \ldots, s_k \rangle \subset L(G)$. By construction the matrix representation of $\alpha|_\Gamma$ is precisely $\mathcal{G}$, and therefore D and Γ are the data that allow us to obtain $\mathcal{C}$ as a convolutional Goppa code over $\mathbb{P}^1_{\mathbb{F}_q(z)}$ $\mathcal{C}(D, \Gamma)$.

Remark 3.3: Note that the choice of the points $p_1, \ldots, p_n$ does not depend on the code $\mathcal{C}$. That is to say, we can take any n different rational points on the affine line and once the points are fixed a basis (7) of the linear system Γ is obtained.

The previous construction proves a version on the projective line of [6, Theorem III.1].

Theorem 3.4: Every convolutional code of length n can be obtained as a convolutional Goppa code $\mathcal{C}(D, \Gamma)$ over the projective line with $G = (n-1)p_\infty$.

Example 5.5 illustrates this process, applied there to a convolutional code of degree 0, i.e., a block code.

IV. CGC DEFINED BY COMPLETE LINEAR SYSTEMS

In the previous Section we have seen how we can identify any code $\mathcal{C}$ with a vector subspace Γ of a space of sections $L(G)$, with $G = (n-1)p_\infty$, over the projective line. Since $\dim L(G) = n > k = \dim \mathcal{C}$, $\Gamma \subsetneq L(G)$. However it is specially interesting to know if one may identify a code with a whole subspace $L(G)$, i.e. if we can carry out our construction taking $G = (k-1)p_\infty$, i.e. if a code is defined by a complete linear system over $\mathbb{P}^1_{\mathbb{F}_q(z)}$ as a convolutional Goppa code.

Let $\mathcal{C}$ be a convolutional code generated by a matrix $\mathcal{G}$ (4) and let us assume without loss of generality the first k columns of $\mathcal{G}$ are linearly independent. Let $x_0, ..., x_{k-1}$ be the homogeneous coordinates , of $\mathbb{P}^{k-1}_{\mathbb{F}_q(z)}$ and recall that t is the affine coordinate in $\mathbb{A}^1_{\mathbb{F}_q(z)}$. We want to determine whether $\mathcal{C} = \mathcal{C}(D, G)$ is a CGC defined by a complete linear system $L(G)$ and by divisors $D = \sum_{i=1}^n p_i$ and $G = (k-1)p_\infty$ over $\mathbb{P}^1_{\mathbb{F}_q(z)}$.

Let us consider the immersion $\varphi_\mathcal{L}$ defined by the sheaf $\mathcal{L} = \mathcal{O}_{\mathbb{P}^1_{\mathbb{F}_q(z)}}(G)$. We have that $L(G) = \langle 1, t, \ldots, t^{k-1} \rangle$. The equations of $\mathbb{P}^1_{\mathbb{F}_q(z)} \subset \mathbb{P}^{k-1}_{\mathbb{F}_q(z)}$ are [4]

$$x_i x_j - x_{i-1} x_{j+1} = 0 \qquad 1 \leq i \leq j \leq k-2 \quad . \tag{8}$$

Definition 4.1: Let us call the *column-points* of a $k \times n$ matrix $\mathcal{G}$ to each of the points in $\mathbb{P}^{k-1}_{\mathbb{F}_q(z)}$

$$p_i = [a_{1i}; \ldots; a_{ki}] \in \mathbb{P}^{k-1}_{\mathbb{F}_q(z)}, \qquad i = 1, \ldots, n$$

whose coordinates are given by the columns $(a_{1i}, \ldots, a_{ki})^T$ of $\mathcal{G}$.

We assume that the column points of a generator matrix of a code verify $p_i \neq p_j$ for each $i \neq j$, otherwise there would

be 2 linearly dependent columns on the generator matrix, i.e. a repeated coordinate times a constant in every codeword.

Since we are assuming that the first k columns of $\mathcal{G}$ are linearly independent then $p_1, \ldots, p_k \in \mathbb{P}^{k-1}_{\mathbb{F}_q(z)}$ is a set of k linearly independent points.

Lemma 4.2 ([6]): Given k linearly independent rational points of $\mathbb{P}^{k-1}_{\mathbb{F}_q(z)}$

$$p_1 = [\alpha_{11}; \ldots; \alpha_{k1}], \ldots, p_k = [\alpha_{1k}; \ldots; \alpha_{kk}]$$

there always exists a generator matrix $\mathcal{G}'$ of the code $\mathcal{C}$ whose first k column-points are $p_1, \ldots, p_k$.

Proof: Let

$$\mathcal{T} = \begin{pmatrix} \alpha_{11} & \ldots & \alpha_{1k} \\ \vdots & & \vdots \\ \alpha_{k1} & \ldots & \alpha_{kk} \end{pmatrix} \tag{9}$$

be the square matrix whose column-points are $p_1, \ldots, p_k$, and let

$$\mathcal{R} = \begin{pmatrix} a_{11} & \ldots & a_{1k} \\ \vdots & & \vdots \\ a_{k1} & \ldots & a_{kk} \end{pmatrix} \tag{10}$$

be the left-most square submatrix of a given generator matrix $\mathcal{G}$ of the code. The lemma follows by taking $\mathcal{G}' = B\mathcal{G}$ with $B = \mathcal{T}\mathcal{R}^{-1}$. ∎

Let us consider now k points $p_1, \ldots, p_k \in \mathbb{P}^1_{\mathbb{F}_q(z)} \subset \mathbb{P}^{k-1}_{\mathbb{F}_q(z)}$ with coordinates $p_i = [1; \alpha_i]$ and $\mathcal{L}$ the invertible sheaf associated to the divisor $G = (k-1)p_\infty$. Their images by $\varphi_{\mathcal{L}}$, $\varphi_{\mathcal{L}}(p_i) = [1; \alpha_i; \alpha_i^2; \ldots; \alpha_i^{k-1}]$, are clearly linearly independent points in $\mathbb{P}^{k-1}_{\mathbb{F}_q(z)}$. Then, by Lemma 4.2, we may consider a generator matrix $\mathcal{G}'$ of the code such that its first k columns are the coordinates of the points $\varphi_{\mathcal{L}}(p_i)$ for $i \leq k$.

Hence, we have the following Theorem, which is a version of [6, Theorem IV.2] and can be proved in an analogous way.

Theorem 4.3: $\mathcal{C}$ is a convolutional Goppa code over the projective line defined by a complete linear system if and only if the n column-points of a generator matrix $\mathcal{G}$ lie in $\varphi_{\mathcal{L}}(\mathbb{P}^1_{\mathbb{F}_q(z)})$.

Therefore, the convolutional code $\mathcal{C}$ generated by the matrix $\mathcal{G}$ is a CGC defined by a complete linear system over the projective line by divisors $D = \sum p_i$ and $G = (k-1)p_\infty$ if and only if the columns of the matrix

$$\mathcal{G}' = \begin{pmatrix} 1 & \ldots & 1 \\ \alpha_1 & \ldots & \alpha_k \\ \vdots & & \vdots \\ \alpha_1^{k-1} & \ldots & \alpha_k^{k-1} \end{pmatrix} \mathcal{R}^{-1} \begin{pmatrix} a_{1k+1} & \ldots & a_{1n} \\ a_{2k+1} & \ldots & a_{2n} \\ \vdots & & \vdots \\ a_{kk+1} & \ldots & a_{kn} \end{pmatrix}$$

satisfy equations (8), with α_i the affine coordinate of p_i for all $i \leq k$ and $\mathcal{R}$ as in (10).

Example 5.3 in the following section illustrates a version of this result over finite fields by carrying out the study of certain block cyclic codes. However note that everything in the example works if $\mathbb{F}_q(z)$ is considered instead of $\mathbb{F}_q$ and therefore it can be taken as an example of the general case.

In addition, we can conclude that a subclass of convolutional codes can be defined by a complete linear system over the projective line.

Proposition 4.4 ([6]): Every convolutional code of dimension up to 2 is a CGC defined by a complete linear system over $\mathbb{P}^1_{\mathbb{F}_q(z)}$.

Remark 4.5: Block codes defined by complete linear systems over the projective line are, by construction, MDS. This is not in general the case for convolutional codes. However, it is far easier to construct MDS codes over $\mathbb{P}^1_{\mathbb{F}_q(z)}$ than over curves with higher genus, as exposed and illustrated with examples in [8]. For a explicit characterization of MDS convolutional codes we refer to [9].

V. Block codes are CGC over $\mathbb{P}^1_{\mathbb{F}_q(z)}$

We want to point out that so far the only, yet crucial, fact that makes a difference when using $\mathbb{F}_q(z)$ instead of $\mathbb{F}_q$ is the availability of an infinite number of rational points on the projective line. Otherwise, all the elements presented in this work concerning convolutional codes are valid as long as q is big enough so that the projective line has enough rational points. Therefore, as shown in [6, §V] we may consider the same procedure to construct block codes and we can restate Theorem 3.4 and Theorem 4.3 for block codes as follows.

Theorem 5.1: Every q-ary block code of length $n \leq q$ can be obtained as a Goppa code $\mathcal{C}(D, \Gamma)$ over $\mathbb{P}^1_{\mathbb{F}_q}$ with $G = (n-1)p_\infty$.

Theorem 5.2: $\mathcal{C}$ is a convolutional Goppa code over $\mathbb{P}^1_{\mathbb{F}_q}$, defined by the complete linear system $L(G)$ if and only if the columns of a generator matrix of $\mathcal{C}$ lie in $\varphi_{\mathcal{L}}(\mathbb{P}^1_{\mathbb{F}_q})$.

As an application of the last Theorem let us check explicitly which binary cyclic codes of length 7 can be constructed as evaluation codes over the projective line.

Example 5.3: As it was pointed out before, we may only construct Goppa codes over $\mathbb{P}^1_{\mathbb{F}_q}$ of length $n \leq q$. Hence, to obtain binary codes of length 7 one should construct a code over an extension $\mathbb{P}^1_{\mathbb{F}_q}$, $q = 2^s \geq 7$, and then obtain the code as a subfield subcode by intersecting the resulting code with $\mathbb{F}_2^7$.

Let us consider the cyclic code of length 7 over $\mathbb{F}_q$ generated by $m(x) = x^3 + x + 1$ and let us check wether it can be constructed as a convolutional Goppa code defined by a complete linear series over the projective line.

According to Remark 3.2, we can proceed by studying its dual code, i.e., the code with generator matrix

$$\mathcal{H}_{m(x)} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

By Theorem 5.2 the code must have a generator matrix whose column-points are points in $\mathbb{P}^{k-1}_{\mathbb{F}_q}$ satisfying equations (8).

Hence, if $\mathcal{H}_{m(x)}$ generates a Goppa code over $\mathbb{P}^1_{\mathbb{F}_q}$ there would be an immersion $\mathbb{P}^1_{\mathbb{F}_q} \hookrightarrow \mathbb{P}^2_{\mathbb{F}_q}$ and three different rational points in general position in the image $p_\alpha = [\alpha_0; \alpha_1; \alpha_2], p_\beta = [\beta_0; \beta_1; \beta_2], p_\gamma = [\gamma_0; \gamma_1; \gamma_2]$, i.e., satisfying

$$x_0 x_2 - x_1^2 = 0 \tag{11}$$

such that the code, as a Goppa code, would be defined over $p_\alpha, p_\beta, p_\gamma, p_4, p_5, p_6, p_7$ for certain rational points p_4, p_5, p_6, p_7. Since $p_\alpha, p_\beta, p_\gamma$ are in general position, the matrix

$$\begin{pmatrix} \alpha_0 & \beta_0 & \gamma_0 \\ \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \end{pmatrix}$$

is invertible, and another generator matrix of the code would be

$$\begin{pmatrix} \alpha_0 & \beta_0 & \gamma_0 \\ \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \end{pmatrix} \mathcal{H}_{m(x)} =$$

$$\begin{pmatrix} \alpha_0 & \beta_0 & \gamma_0 & \alpha_0+\beta_0 & \beta_0+\gamma_0 & \alpha_0+\beta_0+\gamma_0 & \alpha_0+\gamma_0 \\ \alpha_1 & \beta_1 & \gamma_1 & \alpha_1+\beta_1 & \beta_1+\gamma_1 & \alpha_1+\beta_1+\gamma_1 & \alpha_1+\gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 & \alpha_2+\beta_2 & \beta_2+\gamma_2 & \alpha_2+\beta_2+\gamma_2 & \alpha_2+\gamma_2 \end{pmatrix}$$

In order to check that the conditions of Theorem 5.2 are satisfied, our study will consist of checking whether the columns 4 through 7 of this matrix are the coordinates of points which are also in the image of the immersion, i.e., whether those columns satisfy (11).

If we check column 4, equation (11) means that we shall have

$$(\alpha_0+\beta_0)(\alpha_2+\beta_2) - (\alpha_1+\beta_1)^2 = 0$$

Bearing in mind that both $(\alpha_0, \alpha_1, \alpha_2), (\beta_0, \beta_1, \beta_2)$ satisfy (11), this is equivalent to

$$\alpha_0\beta_2 = \beta_0\alpha_2$$

and that either one of these cases arises

1) $\alpha_0 = 0$. Since $\alpha_0\alpha_2 = \alpha_1^2$ then $\alpha_1 = 0$ and it must be $\alpha_2 \neq 0$. Therefore, the equation implies $\beta_0 = 0$ and consequently $\beta_1 = 0$, $\beta_2 \neq 0$.
2) $\alpha_2 = 0$. Similarly to 1) it must then be $\alpha_1 = 0, \alpha_0 \neq 0$. The equation implies $\beta_2 = 0$, and hence $\beta_1 = 0$, $\beta_0 \neq 0$.
3) $\alpha_0, \alpha_2 \neq 0$, which by the equation implies $\beta_0, \beta_2 \neq 0$. Indeed, the equation is equivalent to $\frac{\alpha_0}{\beta_0} = \frac{\alpha_2}{\beta_2}$. We have that $\frac{\alpha_0^2}{\beta_0^2} = \frac{\alpha_0\alpha_2}{\beta_0\beta_2} = \frac{\alpha_1^2}{\beta_1^2}$, and therefore $\frac{\alpha_0}{\beta_0} = \frac{\alpha_1}{\beta_1} = \frac{\alpha_2}{\beta_2}$.

In any of the cases we conclude that it must be $(\alpha_0, \alpha_1, \alpha_2) = \lambda(\beta_0, \beta_1, \beta_2)$, which contradicts our assumption that $p_\alpha \neq p_\beta$.

We therefore conclude that the code generated by $\mathcal{H}_{m(x)}$ and its dual code, the cyclic code with generator polynomial $m(x)$, are not Goppa codes defined by a complete linear system over the projective line.

Note that the parity check matrix of the cyclic code generated by $m'(x) = x^3 + x^2 + 1$ has the same columns as $\mathcal{H}_{m(x)}$ but in a different order. Hence the previous analysis would be also valid for the cyclic code generated by $m'(x)$ and its dual. Furthermore, since $x^7 - 1 = m(x)m'(x)(x+1)$ every cyclic code of length 7, except the trivial repetition code and its dual, is either generated by $m(x)$ or $m'(x)$ or it is dual to one of them. We conclude then that any of the non trivial binary cyclic codes of length 7 is not a Goppa code defined by a complete linear series over the projective line.

Theorem 5.1 proves that every linear block code is a subcode of a strongly algebraic geometric code defined over the projective line over a sufficiently large field. In [10, Theorem 2] it was proved that any code was weakly algebraic geometric and a construction over one particular curve, in general of high genus, was given. The construction presented here allows to carry out the construction over the projective line. In fact, it has been shown by the authors that one can consider any curve as long as it has enough rational points [6].

As previously mentioned, a major obstacle for the construction of block Goppa codes is that curves over finite fields have a limited number of points. This number is even more restricted if the field size and the genus of the curve are small, as in the case of this work, which is usually required for reasons of efficiency.

A classical solution for this problem has been to consider an extension of the ground field so that the curve has enough rational points and then intersecting the resulting code with the ground field. These are called subfield subcodes.

However, our approach to the problem allows us to give another procedure which is based on the crucial fact that block codes are simply convolutional codes of degree 0. Therefore they can be defined on the projective line over an infinite field, which does not have a limited number of points.

Since block codes can be viewed as convolutional codes of degree 0 we may consider the particular case of convolutional Goppa codes of degree 0, and we know therefore that they can be always obtained as a code $\mathcal{C}(D, \Gamma)$ over $\mathbb{P}^1_{\mathbb{F}_q(z)}$. Hence, it only needs to be checked which of them are defined by a complete linear system.

If we restrict ourselves to the case of binary block codes we can give some explicit conditions in order to be CGC over the projective line.

Proposition 5.4 ([6]):
1) A necessary condition for a binary block code to be a Goppa code defined by a complete linear system over $\mathbb{P}^1_{\mathbb{F}_2(z)}$ is that its systematic generator matrix does not have any column of weight 2.
2) A necessary condition for a binary block code to be a Goppa code defined by a complete linear system over $\mathbb{P}^1_{\mathbb{F}_2(z)}$ is that none of its systematic generator matrix or its systematic parity check matrix has a row of weight 3.
3) The length of a k-dimensional binary block Goppa code defined by a complete linear system over $\mathbb{P}^1_{\mathbb{F}_2(z)}$ is at most $min\{2^k - \binom{k}{2} - 1,\ 2^{n-k} - \binom{n-k}{2} - 1\}$.
4) A necessary condition for a maximal binary cyclic code to be a Goppa code over $\mathbb{P}^1_{\mathbb{F}_2(z)}$ is that its generator polynomial must have more than 3 non zero coefficients.
5) Binary Hamming codes are not Goppa codes defined by a complete linear system over $\mathbb{P}^1_{\mathbb{F}_2(z)}$.

Example 5.5: According to last Proposition the binary $[7, 4, 3]$ Hamming code can't be constructed by a complete linear system over the projective line. It has been shown in

[10] that it can be obtained as a Goppa code on a curve over $\mathbb{F}_2$ of genus at least 3. We may, however, give it a Goppa structure over the projective line by considering it as a convolutional code of degree 0.

Let us consider the points $p_i \in \mathbb{P}^1_{\mathbb{F}_2(z)}$, $i \leq 7$ with affine coordinates $p_1 = (1), p_2 = (z), p_3 = (1+z), p_4 = (1/z), p_5 = (1/(z+1)), p_6 = (z/(z+1)), p_7 = ((z+1)/z)$ and the divisor $D = \sum p_i$.

Proceeding as in Theorem 3.4 we obtain $\Gamma = \langle s_1, s_2, s_3, s_4 \rangle$ with

$$
\begin{aligned}
s_1 = \;& t^6 + t^5 + t^3 + t + 1 + \tfrac{z^6+z^5+z^3+z+1}{z^4+z^2}(t^4 + t^2) \\
s_2 = \;& \tfrac{t^6+t^5z+tz^{-2}+z^{-1}}{z^5+z^4+z^3+z^2+z+1} + \tfrac{t^4(z^5+z^3+z^2+z+1)}{z^9+z^8+z^3+z^2} + \\
& \tfrac{t^3(z^4+z^3+z^2+z+1)}{z^8+z^2} + \tfrac{t^2(z^5+z^4+z^3+z^2+1)}{z^9+z^8+z^3+z^2} \\
s_3 = \;& \tfrac{t^6+t^5(z+1)}{z^5+z^3+z} + \tfrac{t^4(z^5+z^4+z^3+z+1)}{z^9+z^3} + \\
& + \tfrac{t^3(z^5+z^4+z)+t^2(z^5+z^3+1)+tz^2}{z^9+z^3} + \tfrac{1}{z^6+z^5+z^4+z^3+z^2+z} \\
s_4 = \;& \tfrac{t^6z^5+t^5z^4+tz^7+z^6}{z^5+z^4+z^3+z^2+z+1} + \tfrac{t^4(z^9+z^8+z^7+z^6+z^4)}{z^7+z^6+z+1} + \\
& \tfrac{t^3(z^8+z^7+z^6+z^5+z^4)}{z^6+1} + \tfrac{t^2(z^9+z^7+z^6+z^5+z^4)}{z^7+z^6+z+1}
\end{aligned}
$$

Hence, the convolutional Goppa code $\mathcal{C}(D, \Gamma)$ is generated by the matrix

$$
\mathcal{G} = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1
\end{pmatrix}
$$

and it is therefore a code of degree 0, i.e. a block code. In fact, $\mathcal{G}$ is precisely the systematic generator matrix of the $[7, 4]$ binary Hamming code.

VI. Concluding remarks

The simplest curve, the projective line, can be taken as the support to construct any convolutional code as an evaluation code. Furthermore, it can be done over any n of its rational points.

However not all of them may be constructed as Goppa codes defined by a complete linear system. For those who can be defined like that we have given a characterization in this work, as well as some more explicit conditions for certain particular cases.

In particular we have considered the case of block codes as convolutional codes of degree 0. The approach presented here allows to overcome the classical drawback of the limited number of rational points on curves over finite fields.

References

[1] 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.

[2] V.D. Goppa, *Codes associated with divisors*, Probl. Peredachi Inform., 13(1), 1977 pp. 33–39.

[3] H. Gluesing-Luerssen and B. Langfeld, *A class of one-dimensional MDS convolutional codes*, Journal of Algebra and its Applications, vol. 5, pp. 505–520, 2006.

[4] J. Harris, *Algebraic Geometry: A First Course*, Graduate Texts in Mathematics, vol. 133, Springer-Verlag, New York, 1992.

[5] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, vol. 52, Springer-Verlag, New York, 1977.

[6] J.I. Iglesias Curto, A.L. Muñoz Castañeda, J.M. Muñoz Porras and G. Serrano Sotelo, *Every convolutional code is a Goppa code*, IEEE Transactions on Information Theory **59** (2013), no. 10, 6628–6641.

[7] S. Lang, *Algebra*, Springer. Third edition, 2002.

[8] J.M. Muñoz Porras, J.A. Domínguez Pérez, J.I. Iglesias Curto, and G. Serrano Sotelo, *Convolutional Goppa codes*, IEEE Transactions on Information Theory **52** (2006), no. 1, 340–344.

[9] F.J. Plaza Martín, J.I. Iglesias Curto and G. Serrano Sotelo, *On the construction of 1-dimensional MDS convolutional Goppa codes*, IEEE Transactions on Information Theory **59** (2013), no. 7, 4615–4625.

[10] R. Pellikaan, B.-Z. Shen, and G.J.M. van Wee, *Which linear codes are algebraic-geometric?*, IEEE Transactions on Information Theory **IT-37** (1991), 583–602.