On MDS Convolutional Codes of Rate $1/n^\star$

José Ignacio Iglesias Curto, José María Muñoz Porras, Francisco Javier Plaza Martín, and Gloria Serrano Sotelo

joseig@usal.es, jmp@usal.es, fplaza@usal.es, laina@usal.es
University of Salamanca, Spain

Abstract. We study one-dimensional MDS convolutional codes. It is known that such codes form an open subset of a certain algebraic variety. By giving explicit examples we can conclude that in fact this subset is non empty. One of the constructions used allows a parametrization leading to a systematic study of the algebraic equations that determine which algebraic geometric convolutional codes are MDS.

Keywords: Convolutional codes, Goppa codes, MDS codes.

1 Introduction

The characterization of optimal convolutional codes remains a challenging problem. In this work we address the study of the set of MDS convolutional codes of dimension 1. This is a very particular case since the properties of the set of points representing convolutional codes depend on the row degrees of a canonical generator matrix. For 1-dimensional convolutional codes there is only one such value, which is actually the degree of the code.

This will allow us to characterize 1-dimensional convolutional codes as an open subset of a projective space variety. This means that it is possible to give a finite number of algebraic equations satisfied by non MDS codes, and hence the complement to this set is that of MDS codes. Besides, we will show that such complement subset is non-empty by giving explicit examples of MDS convolutional Goppa codes.

A class of such codes will be shown to have a particular interest, since it admits a parametrization and hence a systematic study on them can be done. This would eventually lead to a better understanding of convolutional Goppa codes of dimension 1 or higher.

In Section 2 we present the basic facts and known results that will be needed for our work. In Section 3 we present certain conditions for rate $1/n$ codes to be MDS. We also give explicit examples of MDS convolutional codes of dimension 1. Finally, we make a deeper study of the family of convolutional Goppa codes. In Section 4 we sketch possible lines for further research.

* This work has been partially supported by the research contract MTM2009-11393 of the Spanish Ministry for Science and Innovation.

2 Convolutional codes

Let us recall the basic facts on convolutional codes as they can be found in classical literature as for example [3,6,7].

Let us consider the finite field $\mathbb{F}_q$ with $q = p^r$ elements being p a prime.

A *convolutional code* $\mathcal{C}$ of *length* n and *dimension* k over $\mathbb{F}_q$ is the image of an injective $\mathbb{F}_q(z)$-linear map

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

The representation matrix of this map is called the generator matrix of the code. For every convolutional code it is always possible to get a polynomial generator matrix. If a polynomial generator matrix generates the submodule consisting on the polynomial part of the convolutional code and if its row degrees, i.e. the degrees of the polynomials on each row, can't be lowered by basic row operations then this matrix is called a *canonical* matrix. Every convolutional code has a canonical generator matrix. The row degrees of a canonical generator matrix are invariants of the code and the sum of them is called the *degree* (or *complexity*) δ of the code. This is a critical parameter of convolutional codes without a counterpart for block codes. Indeed, convolutional codes of degree $\delta = 0$ are nothing but block codes.

Given the Hamming weight function defined for constant vectors, w, we may define the *weight* of a vector $x(z) = (x_1(z), \ldots, x_n(z)) \in \mathbb{F}_q(z)^n$, where $x(z) = \sum_t x_t z^t$ and $x_t = (x_{t1}, \ldots, x_{tn}) \in \mathbb{F}_q^n$, as

$$w(x(z)) = \sum_t w(x_t) \, .$$

Obviously the only vectors with finite weight are polynomial ones. It is then possible to define the free distance between two codewords as the weight of their difference, and the *free distance*, d_{free}, of the convolutional code as the minimum free distance between any two polynomial codewords.

Similarly to block codes, different bounds are used to study the free distance of convolutional codes. It is known [10] that the free distance of any convolutional code satisfies

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

This bound was named the *generalized Singleton bound* since for codes of degree 0, i.e. block codes, it comes to the classical Singleton bound on the minimum distance. Consequently, *MDS convolutional codes* are defined as those whose free distance reaches the generalized Singleton bound.

2.1 1-dimensional convolutional codes

One dimensional convolutional codes of degree δ can be represented as an open subset of a projective space $\mathbb{P}^{n(\delta+1)}$ [9]. It has also been proved that one dimensional MDS convolutional codes only exist if all entries on a canonical generator matrix have degree δ. In fact, note that for 1-dimensional codes the generalized Singleton bound states that MDS convolutional codes must have free distance

$$d_{free} = n(\delta + 1) \, . \tag{1}$$

The purpose of our work is to study under which conditions the free distance of convolutional codes reaches this value.

2.2 Convolutional Goppa codes

Let us briefly recall the construction of convolutional Goppa codes (CGC) [8], which we will use on next Section.

Let $(X, \mathcal{O}_X)$ be a smooth projective curve over $\mathbb{F}_q(z)$ of genus g. Let us denote Σ_X the field of rational functions of X. Without loss of generality we may assume that $\mathbb{F}_q(z)$ is algebraically closed in Σ_X.

Let $P_1, \ldots, P_n$ be n different $\mathbb{F}_q(z)$-rational points of X, and take the divisor $\mathsf{D} = P_1 + \cdots + P_n$.

Let $\mathsf{G} = \sum n_i Q_i - \sum n'_j Q'_j$ be a divisor on X of degree $r = \sum n_i - \sum n'_j$, with support disjoint from D, i.e. $\{P_i\}_i \cap \{Q_j, Q'_k\}_{j,k} = \emptyset$. Like any divisor over X, G determines a $\mathbb{F}_q(z)$-vector space of global sections

$$L(\mathsf{G}) \equiv \Gamma(X, \mathcal{O}_X(\mathsf{G})) = \{s \in \Sigma_X \mid (s) + \mathsf{G} \geq 0\} =$$
$$= \left\{ s \text{ rational function } \middle| \begin{array}{l} \text{has zeroes at least at the points } Q'_j, \text{ of order} \geq n'_j, \text{ has} \\ \text{poles only at the points } Q_i, \text{ of order} \leq n_i \end{array} \right\},$$

where (s) denotes the divisor defined by $s \in \Sigma_X$.

In the case where $r = deg\, \mathsf{G} < n = deg\, \mathsf{D}$ it is possible to define an injective $\mathbb{F}_q(z)$-linear map

$$0 \to L(\mathsf{G}) \xrightarrow{\alpha} \mathbb{F}_q(z) \times \overset{n}{\cdots} \times \mathbb{F}_q(z)$$
$$s \mapsto (s(P_1), \ldots, s(P_n)) .$$

Definition 1 ([8]). *The convolutional Goppa code $\mathcal{C}(\mathsf{D}, \mathsf{G})$ associated to the divisors D, G is the image of*

$$\alpha \colon L(\mathsf{G}) \to \mathbb{F}_q(z)^n$$

Analogously, the convolutional Goppa code $\mathcal{C}(\mathsf{D}, \Gamma)$ associated to D and the subspace $\Gamma \subseteq L(\mathsf{G})$ is the image of

$$\alpha_{|_\Gamma} \colon \Gamma \to \mathbb{F}_q(z)^n .$$

Proposition 2. *$\mathcal{C}(\mathsf{D}, \mathsf{G})$ is a convolutional code of length n and dimension*

$$k = \dim L(\mathsf{G}) \leq r + 1 - g$$

Under the condition $2g - 2 < r < n$ the dimension of $\mathcal{C}(\mathsf{D}, \mathsf{G})$ is exactly

$$k = r + 1 - g .$$

3 One-dimensional MDS convolutional codes

We face the question of characterizing one dimensional MDS convolutional codes of degree δ in the open subset of $\mathbb{P}^{n(\delta+1)}$ which represents convolutional codes. It is actually known [10] that being MDS is an open condition. Hence, the set of MDS one-dimensional convolutional codes is the intersection of both open subsets and, consequently, open.

However, up to now, no explicit expression of the conditions that determine this open subset has been given. A first approach, bearing in mind the expression of the generalized

Singleton bound for rate $1/n$ convolutional codes 1, is the necessary condition that all polynomial entries of a canonical generator matrix must have non zero coefficients.

Moreover, the following Theorem states a sufficient condition.

Theorem 3 ([2,1],Theorem 1.11). *Let $G(z) = G_0 + G_1 z + G_2 z^2 + \cdots + G_\delta z^\delta$, $\delta < n$, be the generator matrix of a convolutional code, then if the linear block codes generated by $\begin{pmatrix} G_j \\ \vdots \\ G_0 \end{pmatrix}$ and $\begin{pmatrix} G_\delta \\ \vdots \\ G_{\delta-j} \end{pmatrix}$ are $(n, j+1)$ MDS codes for all $0 \leq j \leq \delta$, then the code generated by $G(z)$ is a MDS convolutional code.*

These two conditions are however not the same in general.

On the other side, we have the question wether the set of MDS convolutional codes (in particular for codes of rate $1/n$) is non-empty.

A particular construction of rate $1/n$ MDS convolutional codes with length up to $q-1$ has been given by Gluessing-Luersen and Langfeld [4]. These codes are generated by matrices of the form

$$G(z) = \sum_{i=0}^{\delta} z^i (1, a^i, a^{2i}, \ldots, a^{(n-1)i}) \,. \tag{2}$$

A careful analysis shows that such codes are indeed MDS, giving therefore a positive answer for codes up to a certain length.

To give a more general statement, we will see that it is possible to obtain examples of one-dimensional convolutional codes for different parameters fulfilling the conditions of the previous Theorem and therefore with the property of being MDS. We will conclude then that the subset of MDS 1-dimensional convolutional codes is a dense open subset in $\mathbb{P}^{n(\delta+1)}$.

Let us consider again the construction of convolutional Goppa codes. These may be constructed over the projective line $\mathbb{P}^1_{\mathbb{F}_q(z)}$ by taking rational points $P_1, \ldots, P_n$ different from $P_0 = (1;0)$ and $P_\infty = (0;1)$, with coordinates $P_i = (1; a_i z + b_i)$ for all $i \leq n$, and $\mathsf{G} = rP_\infty - sP_0$ a divisor of degree $deg\, \mathsf{G} = r - s$ with $0 \leq s \leq r < n$. Then, the space of global sections of G is precisely $L(\mathsf{G}) = \langle t^s, t^{s+1}, \ldots, t^r \rangle$.

Under these conditions the evaluation map $\alpha \colon L(\mathsf{G}) \to \mathbb{F}_q(z)^n$ is injective and its image is the convolutional Goppa code $\mathcal{C}(\mathsf{D}, \mathsf{G})$ of length n and dimension $k = r - s + 1$.

Further, we may define codes of rate $1/n$ by restricting α to a 1-dimensional vector subspace $\Gamma \subset L(\mathsf{G})$ generated by a global section of the form $\lambda_0 t^s + \lambda_1 t^{s+1} + \ldots + \lambda_{r-s} t^r$. Then, 1-dimensional convolutional Goppa codes $\mathcal{C}(\mathsf{D}, \Gamma)$ will be generated by matrices

$$\left(\sum_{i=0}^{r-s} \lambda_i (a_1 z + b_1)^{s+i} \; \sum_{i=0}^{r-s} \lambda_i (a_2 z + b_2)^{s+i} \; \ldots \; \sum_{i=0}^{r-s} \lambda_i (a_n z + b_n)^{s+i} \right) \tag{3}$$

where the choices of D and Γ will determine the values of λ_i, a_j, b_j for all $i \leq r - s$, $j \leq n$.

Let us take $\mathsf{G} = rP_\infty - rP_0$. Then, we obtain a code of degree $\delta = r$ which by (3) is generated by the matrix

$$G(z) = \left((a_1 z + b_1)^\delta \; (a_2 z + b_2)^\delta \; \ldots \; (a_n z + b_n)^\delta \right) .$$

As proved in [1], with a suitable choice of the points $P_1, \ldots, P_n$ it is possible to obtain a convolutional code of this form satisfying the conditions in Theorem and hence MDS.

Another possible construction consists of taking a one dimensional subspace $\Gamma \subset L(\mathsf{G})$ for $\mathsf{G} = rP_\infty - sP_0$ with r, s general values satisfying Proposition 2. In particular, for $r = \delta, s = 0$ and $\Gamma = \langle 1 + t + t^2 + \cdots + t^\delta \rangle$ according to (3) the generator matrix of the code $\mathcal{C}(\mathsf{D}, \Gamma)$ is

$$\left(\sum_{i=0}^{\delta} (a_1 z + b_1)^i \sum_{i=0}^{\delta} (a_2 z + b_2)^i \ldots \sum_{i=0}^{\delta} (a_n z + b_n)^i \right) . \tag{4}$$

It has also been shown in [1] that the points over which the code is constructed may be chosen in such a way that it satisfies Theorem 3 and hence it is an MDS convolutional code.

Note that the codes generated by matrices (2) are, in fact, a particular case of (4) corresponding to the choice $P_i = (1; a^{i-1} z)$, [4].

The examples above show explicitly the existence of MDS codes of rate $1/n$. This, together with the mentioned results from [1,10], proves the following.

Theorem 4. *MDS one dimensional convolutional codes are represented by a dense open subset of* $\mathbb{P}^{n(\delta+1)}$.

As a consequence, non MDS codes are represented by the union of sets given by a finite number of algebraic equations. These equations might be determined, allowing therefore to explicitly characterize MDS convolutional codes. In fact, the set of rate $1/n$ MDS convolutional codes being dense means that over large fields a randomly chosen code of rate $1/n$ is expected to be MDS.

3.1 MDS one-dimensional CGC

The construction of convolutional Goppa codes via the restriction of the evaluation map α to different subspaces Γ has intrinsic interest, in particular for the case with $\mathsf{G} = \delta P_\infty$.

In fact, each such subspace is generated by a section $\lambda_0 + \lambda_1 t + \lambda_2 t^2 + \cdots + \lambda_\delta t^\delta$ and since all constant multiples of the vector $(\lambda_0, \lambda_1, \lambda_2, \ldots, \lambda_\delta)$ correspond to the same subspace $\Gamma = \langle \lambda_0 + \lambda_1 t + \lambda_2 t^2 + \cdots + \lambda_\delta t^\delta \rangle$ then for a fixed divisor D we may parameterize the codes $\mathcal{C}(\mathsf{D}, \Gamma)$ as points $(\lambda_0; \lambda_1; \lambda_2; \ldots; \lambda_\delta)$ of the projective space $\mathbb{P}^\delta$.

Further, we might use this parametrization on the study of the equations that characterize MDS codes.

Let us illustrate this with a rather simple case. We fix four different points $P_i = (1; a_i z + b)$, $1 \leq i \leq 4$, and $\mathsf{G} = 2P_\infty$. Then we obtain different codes of length 4 and degree 2, according to our choice of $\Gamma = \langle \lambda_0 + \lambda_1 t + \lambda_2 t^2 \rangle$. The divisor $\mathsf{D} = P_1 + P_2 + P_3 + P_4$ fixed, these codes are therefore represented as points of $\mathbb{P}^3$ and we wonder which ones of them correspond to MDS codes.

By (3) the generator matrix of such codes is of the form $G(z) = G_0 + G_1 z + G_2 z^2$ with

$$\begin{aligned} G_0 &= \lambda_0 + \lambda_1 b + \lambda_2 b^2 \Big(1, 1, 1, 1\Big) \\ G_1 &= \lambda_1 + 2\lambda_2 b \Big(a_1, a_2, a_3, a_4\Big) \\ G_2 &= \lambda_2 \Big(a_1^2, a_2^2, a_3^2, a_4^2\Big) \end{aligned}$$

and the necessary condition for this code to be MDS, stated at the beginning of this section, implies that if $G(z)$ generates an MDS code, then

$$\begin{aligned} &\lambda_0 + \lambda_1 b + \lambda_2 b^2 \neq 0 \\ &\lambda_1 + 2\lambda_2 b \neq 0 \\ &\lambda_2 \neq 0 \end{aligned} \tag{5}$$

as well as $a_i \neq 0$ for all $i \leq 4$ (so we fix the points P_i satisfying this).

On the other side the sufficient conditions on Theorem 3 imply that if the matrices

$$\begin{pmatrix} G_1 \\ G_0 \end{pmatrix}, \qquad \begin{pmatrix} G_2 \\ G_1 \end{pmatrix}, \qquad \begin{pmatrix} G_2 \\ G_1 \\ G_0 \end{pmatrix}$$

generate MDS block codes, which is equivalent to their maximal minors being non zero, then the code $\mathcal{C}(\mathsf{D}, \Gamma)$ is MDS. Now, note that the maximal minors of those matrices are of the following forms

$$\begin{aligned} \begin{pmatrix} G_1 \\ G_0 \end{pmatrix} &\rightsquigarrow (\lambda_1 + 2\lambda_2 b)(\lambda_0 + \lambda_1 b + \lambda_2 b^2) \begin{vmatrix} a_i & a_j \\ 1 & 1 \end{vmatrix} \\ \begin{pmatrix} G_2 \\ G_1 \end{pmatrix} &\rightsquigarrow \lambda_2(\lambda_1 + 2\lambda_2 b) \begin{vmatrix} a_i^2 & a_j^2 \\ a_i & a_j \end{vmatrix} \\ \begin{pmatrix} G_2 \\ G_1 \\ G_0 \end{pmatrix} &\rightsquigarrow \lambda_2(\lambda_1 + 2\lambda_2 b)(\lambda_0 + \lambda_1 b + \lambda_2 b^2) \begin{vmatrix} a_i^2 & a_j^2 & a_k^2 \\ a_i & a_j & a_k \\ 1 & 1 & 1 \end{vmatrix} \end{aligned}$$

and the determinants are non zero as long as $a_i \neq 0$ (which we have assumed) and $a_i \neq a_j$ for all $i \neq j$ (which holds since $P_i \neq P_j$ for all $i \neq j$).

Hence, the sufficient conditions for our codes to be MDS are also given by (5) and therefore MDS convolutional Goppa codes of the form $\mathcal{C}(\mathsf{D}, \Gamma)$ are represented by the points $(\lambda_0; \lambda_1; \lambda_2) \in \mathbb{P}^3$ that satisfy (5).

The study of the general case and the statement of the precise equations that characterize MDS codes of the form $\mathcal{C}(\mathsf{D}, \Gamma)$ with different parameters is a matter of ongoing work [5].

4 Concluding remarks

It is known that the set of 1-dimensional convolutional codes is an open subset of an algebraic variety (this may not be true for convolutional codes of higher dimension) as well as that of MDS codes. As a result, we conclude that MDS 1-dimensional convolutional codes can be represented as the points of the complement in a projective space of a set determined by certain algebraic equations.

We have studied wether this subset is non-empty. Explicit constructions of convolutional Goppa codes over the projective line make it possible to give a positive answer and to conclude that almost every convolutional code of rate $1/n$ is MDS, i.e., all except those verifying a finite set of equations.

Of particular interest is the second example presented here, that gives a method to parameterize a set of 1-dimensional convolutional Goppa codes defined over the projective line. The

question arises of which of these codes are MDS. An answer consisting on explicit equations would be of high interest since, similarly to the block codes case, the geometric elements involved (some of them directly related to the parametrization) are critical to efficiently decode these codes. In addition, such characterization could lead to a further study of algebraic geometric codes of higher dimension or defined over other curves.

References

1. J.A. Domínguez Pérez, J.M. Muñoz Porras and G. Serrano Sotelo, *One Dimensional Convolutinal Goppa Codes Over the Projective Line*, Preprint.
2. J.A. Domínguez Pérez, J.M. Muñoz Porras and G. Serrano Sotelo, *Convolutional codes of Goppa type*, Appl. Algebra Engrg. Comm. Comput., vol. 15, no. 1, pp. 51-61, 2004.
3. G.D. Forney Jr, Convolutional codes I: Algebraic structure, *IEEE Trans. Inform. Theory*, **16** (3), 720–738, (1970).
4. H. Gluesing-Luerssen and B. Langfeld, *A class of one-dimensional MDS convolutional codes*, Journal of Algebra and its Applications **5** (2006), 505–520.
5. J.I. Iglesias Curto, F.J. Plaza Martín and G. Serrano Sotelo, *On the construction of 1-dimensional MDS convolutional codes*. Under preparation.
6. R. Johannesson and K. Sh. Zigangirov, *Fundamentals of convolutional coding*, IEEE Press, New York, 1999.
7. R.J. McEliece, *The algebraic theory of convolutional codes*, Handbook of Coding Theory (V. Pless and W. Huffman, eds.), vol. 1, 1998, pp. 1065–1138.
8. J.M. Muñoz Porras, J.A. Domínguez Pérez, J.I. Iglesias Curto and G. Serrano Sotelo, *Convolutional Goppa codes*, IEEE Trans. Inform. Theory **52** (2006), no. 1, 340–344.
9. J.M. Muñoz Porras and J.I. Iglesias Curto, *Classification of convolutional codes*, Linear Algebra and its Applications **432** (2010), no. 10, 2701–2725.
10. J. Rosenthal and R. Smarandache, *Maximum distance separable convolutional codes*, AAECC **10** (1999), no. 1, 15–32.