MAXIMUM DISTANCE SEPARABLE CONVOLUTIONAL CODES

JOACHIM ROSENTHAL AND ROXANA SMARANDACHE

Abstract. A maximum distance separable (MDS) block code is a linear code whose distance is maximal among all linear block codes of rate k/n. It is well known that MDS block codes do exist if the field size is more than n. In this paper we generalize this concept to the class of convolutional codes of a fixed rate k/n and a fixed code degree δ. In order to achieve this result we will introduce a natural upper bound for the free distance generalizing the Singleton bound. The main result of the paper shows that this upper bound can be achieved in all cases if one allows sufficiently many field elements.

1. Introduction

Let $\mathbb{F}$ be a finite field and let $\mathcal{C} \subset \mathbb{F}^n$ be an $[n, k]$ linear block code. Let $d(\mathcal{C})$ be the distance of $\mathcal{C}$, i.e. $d(\mathcal{C})$ is equal to the minimum Hamming distance between any two different code words $x, y \in \mathcal{C}$.

The main linear coding problem asks for the construction of linear $[n, k]$ codes whose distance $d(\mathcal{C})$ is maximal among all linear $[n, k]$ codes.

The distance $d(\mathcal{C})$ is always upper bounded by the Singleton bound [8], i.e. one has the inequality

$$d(\mathcal{C}) \leq n - k + 1. \tag{1.1}$$

If the base field $\mathbb{F}$ has sufficiently many elements then the Reed Solomon construction shows that there are $[n, k]$ codes whose distance is equal to $n-k+1$. Such codes are called maximum distance separable (MDS) codes. It is the purpose of this paper to derive a generalization for the Singleton bound which is valid for convolutional codes and to prove that there exist codes which achieve this generalized Singleton bound. We call then such a convolutional code an MDS convolutional code.

In the literature there were already several papers [5, 11] which considered the concept of a maximum distance separable convolutional code. In each of these approaches it was necessary to restrict the total class of rate k/n convolutional codes to

---

Date: December 11, 1998.

1991 *Mathematics Subject Classification.* Primary: 94B10. Secondary: 94B65.

Key words and phrases. Convolutional codes, MDS block codes.

Both authors were supported in part by NSF grant DMS-96-10389. The first author acknowledges support from MSRI through NSF grant DMS-9701755. The second author was supported by a fellowship from the Center for Applied Mathematics at the University of Notre Dame. A summary of this paper was presented at the 1998 IEEE International Symposium on Information Theory in Boston and at the 36-th Annual Allerton Conference on Communication, Control, and Computing in Monticello, Illinois, 1998.

a suitable subclass. This is simply due to the fact that there is in general no upper bound for the free distance of a rate k/n convolutional code.

We argue that the single most important parameter for a rate k/n convolutional code is the *degree* and we will define this parameter in a moment. The set of all convolutional codes of rate k/n and degree at most δ forms a finite set and consequently the free distances of these codes have to be bounded from above. The generalized Singleton bound which we are going to derive will have the property that every convolutional code of rate k/n and degree δ will have a free distance of less than this bound and the main result of this paper states that there are codes which achieve this distance.

In the sequel we follow the module theoretic approach to convolutional codes as it was described in [15]. This has the advantage that we can utilize by duality well known first order representations studied in the systems literature. The difference to the classical approach as provided in [1, 10] will turn out to be minor.

Consider the polynomial ring $R = \mathbb{F}[z]$. For the purpose of this paper we will define a convolutional code as an R submodule of the module R^n. Since R is a principal ideal domain (PID) the submodule $\mathcal{C}$ is free and it has therefore a well defined rank k. If $\mathcal{C}$ has rank k we will say that the convolutional code $\mathcal{C}$ has transmission rate k/n.

As it was shown in [15] $\mathcal{C}$ is dual to a linear behavior $\mathcal{C}^\perp := \mathcal{B} \subset \mathbb{F}^n[[z]]$ and $\mathcal{B}$ has a well defined McMillan degree δ. Using this duality we will define the degree of the convolutional code $\mathcal{C}$ as the McMillan degree of the behavior $\mathcal{C}^\perp$.

The degree is also easily computed from the module $\mathcal{C}$ directly. For this let $G(z)$ be an $n \times k$ polynomial matrix whose columns form an R-basis of the submodule $\mathcal{C}$. We say that $G(z)$ is a generator matrix for the convolutional code $\mathcal{C}$. In terms of $G(z)$ the degree is exactly equal to the maximal degree of the $k \times k$ full size minors of $G(z)$. (See [15] for details). Note that our definition is independent of the particular choice of generator matrix. Indeed if $G_1(z)$ and $G_2(z)$ are two generator matrices then there exists a unimodular matrix $U(z)$ such that $G_2(z) = G_1(z)U(z)$ and the $k \times k$ full size minors of $G_2(z)$ correspond to the full size minors of $G_1(z)$ multiplied by the constant factor $\det U(z)$. In particular the highest degree of the minors are the same.

Let ν_i be the degree of the ith column of $G(z)$. I.e. $\nu_i = \max_j \deg g_{ji}(z)$. We denote by G_∞ the high order coefficient matrix of $G(z)$. In general G_∞ has not full rank k. Every module $\mathcal{C}$ of rank k has however an $n \times k$ generator matrix $G(z)$ whose column degrees $\nu_1, \ldots, \nu_k$ are non-increasing and whose high order coefficient matrix G_∞ has rank k. The degree δ is in this case equal to $\delta = \sum_i \nu_i$ and we say that $G(z)$ is in *column proper form*. The ordered indices $\nu_1 \geq \cdots \geq \nu_k$ are invariants of the convolutional code and we call these indices the *column degrees* or *Kronecker indices* of the convolutional code $\mathcal{C}$.

For any n-component vector $v \in \mathbb{F}^n$, we define its weight and denote it by $wt(v)$, the number of all its nonzero components. The weight of a polynomial with coefficients in $\mathbb{F}^n$ is then the sum of the weights of all its coefficients. Finally we define the free distance of the convolutional code $\mathcal{C} \subset \mathbb{F}^n[z]$ through:

$$d_{free} = \min\{wt(v(z)) \mid v(z) \in \mathcal{C}, v(z) \neq 0\}.$$

Remark 1.1. The module theoretic approach as presented above is slightly non-standard. In the coding literature [1, 3, 10] convolutional codes are usually defined as linear subspaces (i.e. submodules) of R^n where R is either the field of rationals $\mathbb{F}(z)$ or the field of formal Laurent series $\mathbb{F}((z))$. If the code is defined over $\mathbb{F}((z))$ it has to be required that the code is generated by an $n \times k$ polynomial generator matrix $G(z)$. Over $\mathbb{F}(z)$ such a representation is guaranteed. The column span of $G(z)$ with respect to $\mathbb{F}[z]$ corresponds then to the finite weight code words of the column span generated by $G(z)$ with respect to $\mathbb{F}(z)$. The restriction to finite weight code words is of little significance. In fact McEliece [9, Section 2] points out that finite weight code words are the only ones that can occur in engineering practice. For this paper it is of importance that the set of rate k/n convolutional codes of degree δ can be equipped with the structure of a variety and this explains our preference for the module theoretic approach.

The paper is structured as follows: In Section 2 we give a natural bound on the free distance which codes of rate k/n and degree δ must satisfy. This bound naturally generalizes the Singleton bound [8, Chapter 1] of linear block codes. The main theorem (Theorem 2.10) states that there exists a code attaining this upper bound, as long as we allow sufficiently large field sizes. We will call such codes MDS convolutional codes. In Section 3 we exhibit some first order representations for the convolutional codes that are used along the paper. In Section 4 we present a detailed proof of the main result, that is, the existence of MDS-convolutional codes. Finally in the last section we explain shortly the underlying geometric aspects of the construction.

2. Main Results

Let $\mathcal{C}$ be a convolutional code of rate k/n and degree δ defined over an arbitrary base field $\mathbb{F}$. Let G be a polynomial encoder in column proper form with ordered column degrees $\nu_1 \geq \cdots \geq \nu_k$. We have the following upper bound on the free distance of the code:

Lemma 2.1. *Let ℓ be the number of indices ν_i among the ordered indices $\nu_1 \geq \cdots \geq \nu_k$ having the value $\nu_i = \nu_k$. Then the free distance must satisfy*

$$d_{free} \leq n(\nu_k + 1) - \ell + 1. \tag{2.1}$$

Proof. Let G_∞ be the high order coefficient matrix of $G(z)$. After some possible permutation of the rows of $G(z)$ we can use elementary column operations and transform the last ℓ columns of the matrix G_∞ into a matrix $\left[\begin{smallmatrix} I_\ell \\ M \end{smallmatrix}\right]$ where M is a matrix of size $(n-\ell) \times \ell$ over $\mathbb{F}$. The transforming operations can be done by an invertible matrix $T \in Gl_\ell$ which acts on the last ℓ columns of the matrix $G(z)$. This transformation has no effect on the column space of $G(z)$ and it also does not affect the column degrees ν_i.

After this transformation the last column of the new generator matrix $G(z)$ will have $(\ell - 1)$ polynomials of weight strictly less than $\nu_k + 1$, one with weight exactly

ν_k+1, and the remaining $(n-\ell)$ polynomials with weight less or equal than ν_k+1. Therefore the input $(0,0,\dots,0,1)^t$ gives a codeword with weight less or equal than

$$(\ell-1)\nu_k+(\nu_k+1)+(n-\ell)(\nu_k+1)=n(\nu_k+1)-\ell+1.$$

This gives the upper bound (2.1). □

The set of rate k/n convolutional codes of degree δ is partitioned into sets of codes with different column degrees $\nu_1\geq\cdots\geq\nu_k$. Taking the maximum of the bound (2.1) over all such possible sets we obtain the following:

Theorem 2.2. *For every base field $\mathbb{F}$ and every rate k/n convolutional code $\mathcal{C}$ of degree δ, the free distance is bounded by:*

$$d_{free}\leq(n-k)\left(\lfloor\delta/k\rfloor+1\right)+\delta+1. \tag{2.2}$$

Proof. The upper bound (2.1) is largest if ν_k is as large as possible and ℓ as small as possible. The largest possible value for ν_k is $\nu_k=\lfloor\delta/k\rfloor$. Minimizing ℓ results in the constraint length values

$$\nu_1=\lfloor\delta/k\rfloor+1,\cdots,\nu_{k-\ell}=\lfloor\delta/k\rfloor+1,\nu_{k-\ell+1}=\lfloor\delta/k\rfloor,\cdots,\nu_k=\lfloor\delta/k\rfloor.$$

Substituting $\nu_k=\lfloor\delta/k\rfloor$ and $\ell=k-\delta+k\lfloor\delta/k\rfloor$ in (2.1) we get the bound (2.2). □

Remark 2.3. In the systems literature, the above set of indices are sometimes referred to as the 'generic set of column indices'. McEliece [9, Section 4] calls a code having a right prime generator matrix with the generic set of column indices 'a compact code'.

Remark 2.4. The upper bound (2.2) on the free distance seems to be new. In the coding literature [2, 3, 9] there are many known upper bounds for convolutional codes of a fixed rate and a fixed degree. These bounds usually are valid for a particular finite field $\mathbb{F}_q$. In contrast to this, (2.2) is valid for any field (even an infinite field) and we believe that the bound naturally generalizes the Singleton bound.

The main theorem 2.10 will state that there exist always rate k/n convolutional codes of degree δ whose free distance is equal to the right hand side of (2.2). Based on this we define:

Definition 2.5. A rate k/n code of degree δ whose free distance achieves the upper bound given in (2.2) will be called an MDS convolutional code. The bound (2.2) will be called the generalized Singleton bound.

Remark 2.6. MDS convolutional codes were defined before in the literature. Justesen and Hughes [5] study maximum distance separable convolutional codes among the class of systematic polynomial encoders. Since systematic polynomial encoders represent a very restricted class of convolutional codes the results are quite different from the ones presented here.

Piret and Krol [11] consider MDS convolutional codes with respect to a non-standard Hamming metric. They consider subspaces of R^n where $R=\mathbb{F}(z)$ is the field of rationals. Their Hamming distance is then defined as the number of coordinates where two vectors inside R^n differ. This definition amounts to a linear block code over the infinite field $R=\mathbb{F}(z)$ and the standard Singleton bound (1.1) applies.

The concepts studied in [5, 11] are therefore different from the MDS concept we consider in this paper.

The following lemma gives sufficient conditions for a code to be an MDS convolutional code:

Lemma 2.7. *If a codeword $v(z)$ in $\mathcal{C}$ has the property that any of its k components have weight at least $(\delta+1)$ then the weight of the codeword $v(z)$ is necessarily greater than or equal to*

$$(n-k)\left(\lfloor \delta/k \rfloor + 1\right) + \delta + 1. \tag{2.3}$$

We will refer to the property that any k components of an n component vector have weight more than $\delta + 1$ as the *weight property.*

Proof. Let

$$v(z) = \left(\begin{array}{ccc} v_1(z) & ,\ldots, & v_n(z) \end{array} \right)^t \in \mathcal{C}.$$

The weight property implies that at least $n-k+1$ of the components of $v(z)$ must have the weight more or equal to $\lfloor \delta/k \rfloor + 1$. Indeed, taking the first k components of v, by the weight property, the sum of their weight is $\geq \delta+1$, therefore there is one component, say v_1 , with the weight $\geq \lfloor \delta/k \rfloor + 1$. Cut v_1 from the sequence and add v_{k+1}.The new sequence of components has again the weight property, so there is once again a component, say v_2 with weight $\geq \lfloor \delta/k \rfloor + 1$. With this reasoning we obtain that at least $n-k+1$ of the components must have the weight more or equal to $\lfloor \delta/k \rfloor + 1$. We have now that $n-k$ of the components have weight at least $\geq \lfloor \delta/k \rfloor + 1$, and from the weight property that the remaining k components have weight greater than $\delta + 1$. Therefore

$$\mathrm{wt}(v(z)) \geq (n-k)\left(\lfloor \delta/k \rfloor + 1\right) + (\delta+1)$$

which is equal to the upper bound 2.2.

□

Before we state the main theorem we summarize some known results:

For $\delta = 0$ the bound (2.2) coincides with the Singleton bound (see e.g. [8]). In this situation we therefore have:

Lemma 2.8. *If G is an $n \times k$ generator of an MDS block code then G generates also an MDS convolutional codes of rate k/n, degree $\delta = 0$ and free distance $n-k+1$. In particular if $|\mathbb{F}| \geq n$, MDS convolutional codes of rate k/n and degree 0 do exist.*

The next result implies that rate $1/n$ MDS codes do exist for every value of δ. The result was derived by Justesen [4]. A systems theoretic proof of this result is given in [18].

Theorem 2.9 ([4])**.** *Let δ, n be fixed and assume that $\mathbb{F}$ is a finite field with $q := |\mathbb{F}| > 3\delta$ elements. Then there exists a rate $1/n$ MDS convolutional code.*

The main result of this paper now states:

Theorem 2.10. *For any rate k/n and any degree δ there exist MDS convolutional codes for sufficiently large field sizes.*

The proof of Theorem 2.10 will be given in Section 4.

3. First order representations for convolutional codes

This section reviews some first order representations for convolutional codes that are heavily used in the next sections. As it was shown in [15] we have the following existence and uniqueness theorems:

Theorem 3.1. *Assume $\mathcal{C} \subset \mathbb{F}^n[z]$ is a rate k/n convolutional code of degree δ. Let $\mathbb{K}$ be the algebraic closure of $\mathbb{F}$. Then there exist matrices $K, L \in \mathbb{F}^{(\delta+n-k)\times\delta}$ and $M \in \mathbb{F}^{(\delta+n-k)\times n}$ such that:*

$$\mathcal{C} = \{v(z) \in \mathbb{F}^n[z] \mid \exists x(z) \in \mathbb{F}^\delta[z] : (zK + L)x(z) + Mv(z) = 0\}. \tag{3.1}$$

Moreover, the following conditions are satisfied:

1. *K has full column rank;*
2. *$(K \mid M)$ has full row rank;*
3. *rank $(z_0K + L \mid M) = \delta + n - k, \forall z_0 \in \mathbb{K}$.*

The theorem allows one to work with matrix triples (K, L, M) instead of a polynomial description. A convolutional code which is described by the matrices (K, L, M) will be simply denoted by $\mathcal{C}(K, L, M)$. If $\delta = 0$, (3.1) reduces to the parity check equation $Mv(z) = 0$. The representation (3.1) is unique in the following sense:

Theorem 3.2. *Let (K, L, M) and (K', L', M') be two matrix triples with the sizes as in the previous theorem and satisfying the minimality conditions* $1, 2, 3$.

Then $\mathcal{C}(K, L, M) = \mathcal{C}(K', L', M')$ if and only if

$$(K', L', M') = (SKT^{-1}, SLT^{-1}, SM) \tag{3.2}$$

for some $T \in Gl_{\delta+k}(\mathbb{F})$ and $S \in Gl_{\delta+n-k}(\mathbb{F})$.

Starting with a (K, L, M) representation for a convolutional code $\mathcal{C}$ we can derive an input/state/output representation. Performing a suitable similarity transformation and permutation of the components of $v(z)$ we can rewrite the (K, L, M) matrix triple in the following way (compare with [15, Section IV]):

$$K = \begin{bmatrix} I_\delta \\ 0 \end{bmatrix}, L = \begin{bmatrix} -A \\ -C \end{bmatrix}, M = \begin{bmatrix} 0 & -B \\ I_{n-k} & -D \end{bmatrix}.$$

In the partitioning, $A \in \mathbb{F}^{\delta\times\delta}, B \in \mathbb{F}^{\delta\times k}, C \in \mathbb{F}^{(n-k)\times\delta}$ and $D \in \mathbb{F}^{(n-k)\times k}$. Let:

$$x(z) = x_0z^\gamma + x_1z^{\gamma-1} + \ldots + x_\gamma;\ x_t \in \mathbb{F}^\delta, t = 0, \ldots, \gamma,$$
$$v(z) = v_0z^\gamma + v_1z^{\gamma-1} + \ldots + v_\gamma;\ v_t \in \mathbb{F}^n, t = 0, \ldots, \gamma.$$

If one partitions the vector v_t into $v_t = \binom{y_t}{u_t}$, where y_t has $n - k$ components and u_t has k component then the convolutional code is equivalently described by the familiar looking '(A, B, C, D)' representation:

$$\begin{aligned} x_{t+1} &= Ax_t + Bu_t \\ y_t &= Cx_t + Du_t, \quad x_0 = 0,\ x_{\gamma+1} = 0. \end{aligned} \tag{3.3}$$

This system is known as the input/state/output representation for a convolutional code. It describes the dynamics for a *systematic and rational encoder*. We refer to [15, 17, 19] for more details.

We say that the matrices (A, B) form a *controllable* pair if

$$\text{rank}\,\left(B\ AB \ldots\ A^{\delta-1}B\right) = \delta,$$

and we say that (A, C) form an *observable pair* if (A^t, C^t) is a controllable pair. Once (A, B) form a controllable pair and (A, C) form an observable pair then it was shown in [15, 17, 19] that the system (3.3) represents a non-catastrophic convolutional code of degree δ and rate k/n.

If one is interested in the construction of convolutional codes with some designed distance there is no limitation if one attempts to construct matrices A, B, C, D, with (A, B) controllable and (A, C) an observable pair. The following result was obtained by such a construction:

Theorem 3.3 ([15]). *Let $r := \max\{n-k, k\}$, and assume that the cardinality of the field $\mathbb{F}$ satisfies*

$$|\mathbb{F}| > \delta r \left\lceil \frac{\delta}{n-k} \right\rceil.$$

Then there exists a rate k/n convolutional code of degree δ having free distance

$$d_{free} \geq \delta + 1.$$

Remark 3.4. The proof of Theorem 3.3 as given in [15] came with a concrete construction of a set of matrices A, B, C, D. The reader observes that for very high rates the free distance of $\delta+1$ is only a fraction away from the optimal upper bound (2.2). For low rates the distance of $\delta+1$ is less than optimal.

In order to prove Theorem 2.10 we will need a strengthening of Theorem 3.3:

Theorem 3.5. *Let δ, k, n, ρ be fixed and assume that*

$$\rho = \delta\left(2\left\lceil \frac{\delta}{n-k}\right\rceil + \left\lfloor \frac{\delta}{k} \right\rfloor + 1\right).$$

If the matrices A, B, C have the property that $(B\ AB \ldots\ A^{\rho-1}B)$ is the parity check of an MDS block code and that $\left(C^t\ A^tC^t \ldots\ {A^{\rho-1}}^t C^t\right)$ is the generator matrix of an MDS block code then for any codeword

$$v(z) = \begin{pmatrix} y(z) \\ u(z) \end{pmatrix} \in \mathbb{F}^n[z]$$

either

$$\text{wt}(u(z)) \geq \delta + 1 \text{ or } \text{wt}(v(z)) \geq (n-k)\left(\lfloor \delta/k \rfloor + 1\right) + \delta + 1.$$

Before we give the proof we want to mention that the choice of ρ is not the minimum that we can have so that the result is correct. The proof for a smaller choice of ρ would involve more cases. For the purpose of this paper this is not necessary.

Proof. Assume

$$\begin{aligned} u(z) &= u_0 z^\gamma + u_1 z^{\gamma-1} + \cdots + u_\gamma, \\ y(z) &= y_0 z^\gamma + y_1 z^{\gamma-1} + \cdots + y_\gamma, \end{aligned}$$

where γ is the degree of v, and that $u_0 \neq 0$. The first equations of the systems (3.3) give that (see [15]):

$$(u_\gamma, \dots, u_0)^t \in \ker\left(B\ AB \dots\ A^\gamma B\right).$$

If $\gamma < \rho$ then $\mathrm{wt}(u(z)) \geq \delta + 1$ and the proof is complete.

We therefore assume that $\gamma \geq \rho$ and that $\mathrm{wt}(u(z)) \leq \delta$. By the 'pigeonhole principle' there exist an index $i < \rho - \frac{\rho}{\delta}$ and an input sequence

$$u_{i+1} = u_{i+2} = \dots = u_{i+\frac{\rho}{\delta}} = 0.$$

In analogy to the proof of [17, Theorem 3.1] it follows that the state $x_{i+1} \neq 0$ and that

$$\begin{pmatrix} y_{i+1} \\ y_{i+2} \\ \vdots \\ y_{i+\frac{\rho}{\delta}} \end{pmatrix} = \begin{pmatrix} C \\ CA \\ \vdots \\ CA^{\frac{\rho}{\delta}-1} \end{pmatrix} x_{i+1}.$$

The assumption on the matrix $\left(C^t\ A^tC^t \dots\ A^{\rho-1^t}C^t\right)$ gives that

$$\begin{aligned} \mathrm{wt}(y) &\geq (n-k)\cdot\frac{\rho}{\delta} - \delta + 1 = (n-k)\left(2\left\lceil\frac{\delta}{n-k}\right\rceil + \left\lfloor\frac{\delta}{k}\right\rfloor + 1\right) - \delta + 1 \\ &\geq 2\delta + (n-k)\left(\left\lfloor\frac{\delta}{k}\right\rfloor + 1\right) - \delta + 1 = (n-k)\left(\left\lfloor\frac{\delta}{k}\right\rfloor + 1\right) + \delta + 1. \end{aligned}$$

□

In the proof of Theorem 2.10 the following lemma will be needed:

Lemma 3.6. *Let δ, k, n, ρ be fixed, $r = \max\{n-k, k\}$ and assume that the cardinality of the field $\mathbb{F}$ satisfies $|\mathbb{F}| > r\rho$. Then there exist matrices A, B, C satisfying the conditions of Theorem 3.5.*

Proof. Let $\alpha \in \mathbb{F}$ be an element of multiplicative order at least $r\rho$. Then

$$A := \begin{pmatrix} \alpha^r & 0 & \cdots & 0 \\ 0 & \alpha^{2r} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \alpha^{\delta r} \end{pmatrix},\ B := \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{k-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(k-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^\delta & \alpha^{2\delta} & \cdots & \alpha^{\delta(k-1)} \end{pmatrix},$$

$$C := \begin{pmatrix} 1 & \cdots & 1 \\ \alpha & \cdots & \alpha^\delta \\ \alpha^2 & \cdots & \alpha^{2\delta} \\ \vdots & & \vdots \\ \alpha^{n-k-1} & \cdots & \alpha^{\delta(n-k-1)} \end{pmatrix}$$

satisfy the conditions of Theorem 3.5. □

4. Proof of the main result

In this section we will give the proof for Theorem 2.10, the main result of this paper. The idea of the proof goes as follows:

We exhibit a parameterization on the set of all rate k/n convolutional codes of degree δ using a large $\mathbb{F}$-vector space, where $\mathbb{F}$ is a finite field. Then we show that the set of codes which are not MDS forms an algebraic subset. Over a finite field an algebraic subset might be the whole parameter space. Over the algebraic closure however the algebraic subset describing the convolutional codes which are not MDS forms a strictly proper subset. This reasoning will allow us to predict an MDS convolutional code with entries in a finite extension of the (finite) base field $\mathbb{F}$ which is itself a finite field.

For the parameterization we will use the first order representation as presented in Theorem 3.1 of Section 3. We do this by viewing a triple of matrices (K, L, M) as a point in the vector space $\mathbb{F}^{(\delta+n-k)(2\delta+n)}$. By Theorem 3.2 this parameterization is not unique. This is however of minor importance in the proof. In the last section we will show that the proof can also be derived in a variety which parameterizes the rate k/n convolutional codes of degree δ exactly. We start the proof with a short Lemma:

Lemma 4.1. *The set of matrices (K, L, M) satisfying the property $1, 2$ and 3 of Theorem 3.1 is open and nonempty inside $\mathbb{F}^{(\delta+n-k)(2\delta+n)}$.*

Proof. We recall from the paper of Ravi and Rosenthal [13] that the conditions 2 and 3 can be equivalently written as the following rank condition:

$$(4.1)\qquad \underbrace{\left[\begin{array}{ccccc|ccccc} K & 0 & \dots & & 0 & M & 0 & \dots & \dots & 0 \\ L & K & \ddots & & \vdots & 0 & M & \ddots & & \vdots \\ 0 & L & \ddots & & 0 & \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & & K & \vdots & & \ddots & M & 0 \\ 0 & \dots & 0 & & L & 0 & \dots & \dots & 0 & M \end{array}\right]}_{2\delta-1 \text{ blocks}} \delta \text{ blocks}$$

has full row rank. Thus all (K, L, M) matrices satisfying the conditions $1, 2, 3$ are in the complementary set of all zeros of the polynomial equations describing the determinant of some full size minors of the matrices K and (4.1) being 0. Therefore the set of all matrix 3-tuples (K, L, M) satisfying the conditions $1, 2, 3$ is open in $\mathbb{F}^{(\delta+n-k)(2\delta+n)}$ and it is obviously nonempty since there is an one to one correspondence between this set and the set of all convolutional codes as we defined them. $\square$

The rest of the section will be devoted to the proof of the main theorem.

Proof of Theorem 2.10. Let $\mathbb{F}$ be a fixed finite field, with q elements, having characteristic p. Let $\mathbb{K}$ denote the algebraic closure of $\mathbb{F}$. As an algebraically closed field, $\mathbb{K}$ is infinite. We will call a matrix with all full size minors invertible, an MDS matrix.

Consider now some fixed numbers δ, k, n, ρ with $k < n$ and ρ chosen as in Theorem 3.5.

We are looking at the set of all 3-tuple matrices (K, L, M) with the properties $1, 2, 3$ and of sizes as in Theorem 3.1, such that the matrix $[K \mid M]$ is an MDS matrix. Let this set be denoted by V. V is the intersection of two open nonempty sets, one given by all (K, L, M) such that the conditions $1, 2, 3$ are satisfied, and the other given by the complementary of the set of the zeros of all the full size minors of $[K \mid M]$. Over the algebraic closure $\mathbb{K}$, the intersection of nonempty open sets is nonempty and V is therefore a nonempty Zariski open set in $\mathbb{K}^{(\delta+n-k)(2\delta+n)}$.

Let now (K, L, M) be an element in V, and let

$$\mathbf{j} = \{1 \le j_1 < j_2 < \ldots < j_k \le n\}$$

be a subset of the set $\{1, \ldots, n\}$ having cardinality k. We would like to show that the code $\mathcal{C}$ defined by (K, L, M) has the property that the k components $\{v_{j_i}(z) \mid i = 1, \ldots, k\}$, of a code word $v(z) \in \mathcal{C}$ satisfy either

$$\sum_{i=1}^{k} \mathrm{wt}(v_{j_i}(z)) \ge \delta + 1 \text{ or } wt(v(z)) \ge (n-k)\left(\lfloor \delta/k \rfloor + 1\right) + \delta + 1.$$

In order to apply Theorem 3.5, let $P_{\mathbf{j}}$ be an $n \times n$ permutation matrix such that

$$P_{\mathbf{j}} v(z) = \begin{pmatrix} y(z) \\ u(z) \end{pmatrix}$$

where the k components $v_{j_1}(z), \ldots, v_{j_k}(z)$ of $v(z)$ are mapped onto the k components of $u(z)$.

Partition the matrix $MP_{\mathbf{j}}^{-1} = [M_1 \mid N]$ where M_1 is the matrix formed by the first $n-k$ columns of $MP_{\mathbf{j}}^{-1}$ and N denotes the rest of the columns in $MP_{\mathbf{j}}^{-1}$. The property of V tells us that the matrix $[K \mid M_1]$ is invertible.

For every K, L, M and every $\mathbf{j}$ we define matrices $A_{\mathbf{j}}, B_{\mathbf{j}}, C_{\mathbf{j}}, D_{\mathbf{j}}$ in the following way:

$$[K \mid M_1]^{-1} \left[K \mid L \mid MP_{\mathbf{j}}^{-1}\right] =: \left[\begin{array}{c|c|cc} I_\delta & -A_{\mathbf{j}} & 0 & -B_{\mathbf{j}} \\ 0 & -C_{\mathbf{j}} & I_{n-k} & -D_{\mathbf{j}} \end{array}\right]. \tag{4.2}$$

Rewriting the equation (3.1) in the new terms we obtain the (A, B, C, D) polynomial description from the previous chapter:

$$\begin{bmatrix} zI_\delta - A_{\mathbf{j}} & 0 & -B_{\mathbf{j}} \\ -C_{\mathbf{j}} & I_{n-k} & -D_{\mathbf{j}} \end{bmatrix} \begin{bmatrix} x(z) \\ y(z) \\ u(z) \end{bmatrix} = 0. \tag{4.3}$$

If the matrices $A_{\mathbf{j}}, B_{\mathbf{j}}, C_{\mathbf{j}}$ satisfy the conditions of Theorem 3.5 then the weight $\sum_{i=1}^{k} \mathrm{wt}(v_{j_i}(z)) \ge \delta + 1$ or the weight of $v(z)$ is larger than the bound (2.2).

The algebraic conditions on A, B, C expressed in Theorem 3.5 translate into algebraic conditions inside the parameter space $\mathbb{K}^{(\delta+n-k)(2\delta+n)}$. Let

$$S_{\mathbf{j}} = \{(K, L, M) \in \mathbb{F}^{(\delta+n-k)(2\delta+n)} \text{ s.t.}$$

$$\left(B_{\mathbf{j}}\ A_{\mathbf{j}}B_{\mathbf{j}} \ldots\ A_{\mathbf{j}}^{\rho-1}B_{\mathbf{j}}\right) \text{ and } \left(C_{\mathbf{j}}^t\ A_{\mathbf{j}}^t C_{\mathbf{j}}^t \ldots\ {A_{\mathbf{j}}^{\rho-1}}^t C_{\mathbf{j}}^t\right) \text{ are MDS}\}.$$

Applying Lemma 3.6 one sees that $S_{\mathbf{j}} \cap V$ is a nonempty Zariski open subset of $\mathbb{K}^{(\delta+n-k)(2\delta+n)}$.

Let $J = \{\mathbf{j} = \{1 \leq j_1 < j_2 < \ldots < j_k \leq n\}\}$ be the set of all k-subsets of $\{1, \ldots, n\}$, and consider all $\{S_{\mathbf{j}} \cap V \mid \mathbf{j} \in J\}$. All of these sets form a finite number of open nonempty sets in V, therefore their intersection is nonempty. It implies the existence of a vector $x = (K, L, M)$ having the property of all the sets $S_{\mathbf{j}} \cap V$.

So far we obtained a vector $x \in V$ having the components in $\mathbb{K}$, the algebraic closure of $\mathbb{F}$, and laying in the intersection

$$\bigcap_{\mathbf{j} \in J} (S_{\mathbf{j}} \cap V) \subset V \subset \mathbb{K}^{(\delta+n-k)(2\delta+n)}.$$

Since the extension $\mathbb{F} \subset \mathbb{K}$ is algebraic, it implies that every component of x is algebraic over $\mathbb{F}$, therefore in a finite extension. If we denote with x_j the components of x we have that all $x_j \in \mathbb{F}[x_j, 1 \leq j \leq (\delta+n-k)(2\delta+n)]$, which is a finite extension over $\mathbb{F}$, therefore is finite of degree say m. Therefore the code $\mathcal{C} = \mathcal{C}(K, L, M)$ associated to the matrices (K, L, M) will be a code over a finite field $\mathbb{F}_{q^m}$, with m possibly rather large.

We will show that this code is actually an MDS convolutional code, in other words it has the free distance equal to the upper bound (2.2). Let

$$v(z) = \begin{pmatrix} v_1(z) & , \ldots , & v_n(z) \end{pmatrix}^t \in \mathcal{C}$$

be a nonzero code word. We will show that the weight of $v(z)$ is larger than the upper bound by applying Lemma 2.7 and Theorem 3.5.

Since the code $\mathcal{C}$ belongs to the intersection of all the Zariski open sets $S_{\mathbf{j}} \cap V$, we can apply Theorem 3.5 for all the k-combinations of the components $v_1, v_2, \ldots, v_n$ to form the part u of the codeword. By construction of the sets $S_{\mathbf{j}} \cap V$, we get that either the weight of the k-combination of components $v_1, v_2, \ldots, v_n$ is more than $\delta + 1$, or the weight of the whole codeword is larger than

$$(n-k)\left(\lfloor \delta/k \rfloor + 1\right) + \delta + 1$$

which is the bound we want. If we have the first situation for all k-combinations of the components we get the conditions of Lemma 2.7. The weight of the codeword is therefore greater then the upper bound (2.2). In either case we predict the existence of an MDS code $\mathcal{C}$ over the finite field $\mathbb{F}_{q^m}$. □

Remark 4.2. The proof does not construct MDS convolutional codes in an explicit way. Concrete constructions exist when $\delta = 0$ (Reed-Solomon construction) and when $k = 1$ (see Theorem 2.9).

5. Remarks on the geometry of the construction

We conclude this paper with some remarks about the algebraic geometric aspect of the constructions considered in the previous section.

As it was explained in [7, 12, 13] a submodule of rank k and degree δ in $\mathbb{F}^n[z]$ describes a quotient sheaf of rank k and degree δ over the projective line $\mathbb{P}^1$. The column degrees $\nu_1 \geq \cdots \geq \nu_k$ of the submodule $\mathcal{C} \subset \mathbb{F}^n[z]$ correspond then to the Grothendieck indices of the quotient sheaf. By a general theorem of Grothendieck it is possible to equip the set of all rank k submodules (quotient sheaves) of degree δ with the structure of a scheme. Such a scheme is referred to as a *quot scheme* in the algebraic geometry literature. The quot scheme which parameterizes the rank k submodules of degree δ turns out to be a smooth projective variety [12]. This variety has been of prominent interest recently in the area of conformal quantum field theory and we refer to [14] for more details.

If the degree $\delta = 0$ the Grothendieck quot scheme is exactly the Grassmann variety $\mathrm{Grass}(k, \mathbb{F}^n)$ consisting of all k dimensional subspaces of the vector space $\mathbb{F}^n$. This variety parameterizes the set of all linear block codes of rate $\frac{k}{n}$ defined over the field $\mathbb{F}$. For an arbitrary degree δ the Grothendieck quot scheme parameterizes in a natural way all rate $\frac{k}{n}$ convolutional codes of degree δ.

Linear systems described by matrix triples (K, L, M) have been studied widely in the systems literature and probably the most comprehensive account is given in the monograph of Kuijper [6]. It was pointed out by Lomadze [7] that a matrix pencil of the form $[zK + L \mid M]$ represents exactly the linear free resolution of the associated quotient sheaf and in this way such matrix pencils appear naturally in the algebraic geometry literature as well. Finally we would like to note that we can view (3.2) as a group action of the reductive group $Gl_{\delta+k} \times Gl_\delta$ on the vector space consisting of all matrix triples (K, L, M) of a fixed size. The uniqueness Theorem 3.2 expresses the fact that the group orbits in (3.2) correspond to the submodules of $\mathbb{F}^n[z]$, i.e. the convolutional codes.

Actually much more is true: The geometric quotient in the sense of GIT (=geometric invariant theory) induced by the group action (3.2) is exactly the Grothendieck quot scheme. The minimality conditions provided in Theorem 3.1 and characterized by the set $V \subset \mathbb{F}^{(\delta+n-k)(2\delta+n)}$ appearing in the proof of the main theorem, guarantee that the associated orbit is a 'stable orbit' in the sense of GIT. This is true for an arbitrary base field and this statement is a geometric formulation of the uniqueness Theorem 3.2. The reader who is interested in more details is referred to [13]. For the purpose of this paper the following is important. The open set $V \subset \mathbb{F}^{(\delta+n-k)(2\delta+n)}$ which we introduced in the proof of Theorem 2.10 describes exactly the stable orbits and the quotient of V under the group action (3.2) describes the Grothendieck quot scheme $X_{k,n}^{\delta}$. The sets $S_{\mathbf{j}}$ induces Zariski open sets inside the scheme $X_{k,n}^{\delta}$ and by abuse of notation we will denotes these sets with $S_{\mathbf{j}}$ as well. The set of MDS convolutional codes contains then the Zariski open subset

$$\bigcap S_{\mathbf{j}} \subset X_{k,n}^{\delta}.$$

The main result states that $\bigcap S_{\mathbf{j}}$ is nonempty as soon as the field size is sufficiently large. A set which contains a non-empty Zariski open subset is sometimes referred to as a *generic set* and in this way we can say that the set of MDS convolutional codes forms a generic set inside the set of rate k/n convolutional codes of degree δ as soon as the field size is sufficiently large.

For $\delta = 0$ the result says that the set of MDS block codes viewed as a subset of the Grassmann variety forms a Zariski open subset and that this set is nonempty as soon as the field is sufficiently large. In the block code situation we know that $|\mathbb{F}| \geq n$ is sufficient to guarantee that the set is nonempty. In particular the existence of MDS block codes over the field $\mathbb{F}(z)$ as studied by Piret and Krol [11] follows from our theory.

After generalizing the notion of MDS block code it naturally arises the question on the nature of the dual code. We know that a dual of an MDS-block code is MDS, so we want to find out if this generalizes to the case of general convolutional codes with degree $\delta > 0$. In the sequel we cover two special cases where this turns out to be true and then we give two examples of MDS-convolutional codes whose dual is not MDS.

In order to introduce the notion of a dual convolutional code in our module theoretical setting, consider the following bilinear form:

$$\begin{array}{rccc} <,>: & \mathbb{F}^n[z] \times \mathbb{F}^n[z] & \longrightarrow & \mathbb{F}[z] \\ & (v(z), w(z)) & \longmapsto & v(z)w(z)^t. \end{array} \tag{5.1}$$

Using this bilinear form we define the dual of a code $\mathcal{C}$ as

$$\mathcal{C}^{\perp} := \{w(z) \mid < v(z), w(z) >= 0, \forall v(z) \in \mathcal{C}\}.$$

One always has that

$$\mathcal{C}^{\perp\perp} \supseteq \mathcal{C}.$$

If the code $\mathcal{C}$ has a minimal basis encoder (i.e. it is non-catastrophic) then $\mathcal{C}^{\perp\perp} = \mathcal{C}$.

The following two lemmas cover some cases where the dual of an MDS convolutional code is MDS.

Lemma 5.1. *If $\mathcal{C}$ is a convolutional code of degree $\delta = 0$ then $\mathcal{C}$ is MDS if and only if $\mathcal{C}^{\perp}$ is MDS.*

Lemma 5.2. *Assume $k = 1, n = 2$. A non-catastrophic code $\mathcal{C}$ of rate $1/2$ is MDS if and only if $\mathcal{C}^{\perp}$ is MDS.*

We will present now a very simple example of a rate $1/3$ MDS convolutional code which has a non-MDS convolutional code of rate $2/3$ as its dual. In this example the degree $\delta = 1$ and the finite field is $\mathbb{F}_3$:

Example 5.3. Let $k = 1$, $n = 3$, $\delta = 1$ and consider the generator matrix

$$G(z) = \begin{pmatrix} (z+2) & (z+1) & (z+1) \end{pmatrix}^t.$$

Then the code generated by $G(z)$ is non-catastrophic and MDS but the dual code is not an MDS convolutional code.

Indeed it is easy to see that any codeword $v(z) = G(z)i(z), i(z) \in \mathbb{F}^k[z]$ has weight at least 6, so the code generated by $G(z)$ is MDS. The dual code has a generator matrix given by:

$$G^{\perp} = \begin{pmatrix} z+1 & 0 \\ 0 & 1 \\ 2z+1 & 2 \end{pmatrix},$$

which is not MDS.

The above example shows that in general the dual code of an MDS convolutional code is not an MDS convolutional code anymore in contrast to the situation of block codes. In [16] more details on the issue of duality of MDS convolutional codes were given.

References

[1] G. D. Forney. Convolutional codes I: Algebraic structure. *IEEE Trans. Inform. Theory*, IT-16(5):720–738, 1970.

[2] R. Johannesson and K. Zigangirov. Distances and distance bounds for convolutional codes – an overview. In *Topics in Coding Theory. In honour of L. H. Zetterberg.*, Lecture Notes in Control and Information Sciences # 128, pages 109–136. Springer Verlag, 1989.

[3] R. Johannesson and K. Sh. Zigangirov. *Fundamentals of Convolutional Coding*. IEEE Press, New York, 1999.

[4] J. Justesen. An algebraic construction of rate $1/\nu$ convolutional codes. *IEEE Trans. Inform. Theory*, IT-21(1):577–580, 1975.

[5] J. Justesen and L.R. Hughes. On maximum-distance-separable convolutional codes. *IEEE Trans. Information Theory*, IT-20:288, 1974.

[6] M. Kuijper. *First-Order Representations of Linear Systems*. Birkhäuser, Boston, 1994.

[7] V. Lomadze. Finite-dimensional time-invariant linear dynamical systems: Algebraic theory. *Acta Appl. Math*, 19:149–201, 1990.

[8] F. J. MacWilliams and N. J.A. Sloane. *The Theory of Error-Correcting Codes*. North Holland, Amsterdam, 1977.

[9] R.J. McEliece. The algebraic theory of convolutional codes. In R. Brualdi, W.C. Huffman, and V. Pless, editors, *Handbook of Coding Theory*. Elsevier Science Publishers, Amsterdam, The Netherlands, 1998. To appear.

[10] Ph. Piret. *Convolutional Codes, an Algebraic Approach*. MIT Press, Cambridge, MA, 1988.

[11] Ph. Piret and T. Krol. MDS convolutional codes. *IEEE Trans. Inform. Theory*, 29(2):224–232, 1983.

[12] M. S. Ravi and J. Rosenthal. A smooth compactification of the space of transfer functions with fixed McMillan degree. *Acta Appl. Math*, 34:329–352, 1994.

[13] M. S. Ravi and J. Rosenthal. A general realization theory for higher order linear differential equations. *Systems & Control Letters*, 25(5):351–360, 1995.

[14] M. S. Ravi, J. Rosenthal, and X. Wang. Degree of the generalized Plücker embedding of a quot scheme and quantum cohomology. *Math. Ann.*, 311(1):11–26, 1998.

[15] J. Rosenthal, J. M. Schumacher, and E.V. York. On behaviors and convolutional codes. *IEEE Trans. Inform. Theory*, 42(6):1881–1891, 1996.

[16] J. Rosenthal and R. Smarandache. On the dual of MDS convolutional codes. In *Proc. of the 36-th Annual Allerton Conference on Communication, Control, and Computing*, 1998. To appear.

[17] J. Rosenthal and E.V. York. BCH convolutional codes. Technical report, University of Notre Dame, Dept. of Mathematics, October 1997. Preprint # 271. Available at http://www.nd.edu/~rosen/preprints.html.

[18] R. Smarandache and J. Rosenthal. A state space approach for constructing MDS rate $1/n$ convolutional codes. In *Proceedings of the 1998 IEEE Information Theory Workshop on Information Theory*, pages 116–117, Killarney, Kerry, Ireland, June 1998.

[19] E.V. York. *Algebraic Description and Construction of Error Correcting Codes, a Systems Theory Point of View.* PhD thesis, University of Notre Dame, 1997. Available at http://www.nd.edu/~rosen/preprints.html.

Department of Mathematics, University of Notre Dame, Notre Dame, Indiana 46556.
E-mail address: Rosenthal.1@nd.edu, Smarandache.1@nd.edu