Construction Results for MDS-Convolutional Codes[1]

Roxana Smarandache
Department of Mathematics,
University of Notre Dame
Notre Dame, IN 46556-5683 USA
Smarandache.1@nd.edu
www.nd.edu/~rsmarand/

Heide Gluesing-Luerssen
Fachbereich Mathematik,
Universität Oldenburg
D-26111, Oldenburg, Germany
gluesing@mathematik.uni-oldenburg.de

Joachim Rosenthal
Department of Mathematics,
University of Notre Dame
Notre Dame, IN 46556-5683 USA
Rosenthal.1@nd.edu
www.nd.edu/~rosen/

Abstract — **The generalized Singleton bound and MDS-convolutional codes are reviewed. For each n, k and δ an elementary construction of rate k/n MDS convolutional codes of degree δ is given.**

I. Introduction

The minimum distance of a block code is upper bounded by the Singleton bound $d_{min} \leq n-k+1$. Codes attaining this bound are called MDS block codes and Reed Solomon codes are examples of such codes. Since convolutional codes generalize block codes, it is natural to study the way the Singleton bound is generalized to convolutional codes.

Let $\mathbb{F}$ be a finite field and $G(D)$ be a $k \times n$ full rank matrix over $\mathbb{F}[D]$. Let $\mathcal{C} = \{u(D)G(D) \mid u(D) \in \mathbb{F}^k[D]\}$ be the rate k/n convolutional code generated by $G(D)$. Two generator matrices $G(D)$ and $G'(D)$ are equivalent if they generate the same convolutional code $\mathcal{C}$. Then there exists a $k \times k$ unimodular matrix $U(D)$ with $G'(D) = U(D)G(D)$. We say that $G(D)$ is *catastrophic* if a non-polynomial message $u(D)$ can result in a polynomial codeword $u(D)G(D)$. This can happen if and only if the $k \times k$-minors of the matrix $G(D)$ have a non-constant common divisor other than D. We will suppose $G(D)$ is noncatastrophic.

Along with n and k, there is a third important parameter of a convolutional code $\mathcal{C}$, called the *degree*. It is defined as the maximal degree δ of the $k \times k$ minors of $G(D)$. Equivalent encoding matrices have the same degree so the degree is an invariant of the code. See [3] for details.

We define the weight of a polynomial $v(D) \in \mathbb{F}^n[D]$ as the sum of the Hamming weights of all its $\mathbb{F}^n$-coefficients and the *free distance* of the code as:

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

Lemma 1 [3] *Let $\mathcal{C}$ be a convolutional code of rate k/n and degree δ. Then the free distance must satisfy:*

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

We call the bound (1) the generalized Singleton bound. For $\delta = 0$ the bound is the classical bound $n-k+1$. We showed in [3] that there are codes attaining this bound over sufficiently large finite fields. We called such codes *MDS convolutional codes*. The existence proof in [3] was non-constructive and it was based on methods from algebraic geometry.

II. A construction of rate k/n-MDS Convolutional Codes

In this section we follow [5] and provide a concrete construction of an MDS convolutional code for each degree δ and each rate k/n. The construction makes use of [1, 2].

As defined in [1, 2], a convolutional code is said to be *generated by a polynomial*

$$g(D) = g_0(D^n) + g_1(D^n)D + \ldots + g_{n-1}(D^n)D^{n-1},$$

if it has a polynomial encoder of the form

$$G(D) = \begin{bmatrix} g_0(D) & g_1(D) & \cdots & g_{n-1}(D) \\ Dg_{n-1}(D) & g_0(D) & \cdots & g_{n-2}(D) \\ \vdots & \vdots & & \vdots \\ Dg_{n-k+1}(D) & Dg_{n-k+2}(D) & \cdots & g_{n-k}(D) \end{bmatrix}. \tag{2}$$

The code $\mathcal{C}$ generated by $G(D)$ is isomorphic to

$$\left\{\left(u_0(D^n) + u_1(D^n)D + \ldots + u_{k-1}(D^n)D^{k-1}\right) \cdot g(D)\right\},$$

where $(u_0(D), \ldots, u_{k-1}(D)) \in \mathbb{F}^k[D]$ is an information vector.

Lemma 2 [5] *Let p be a prime and $k < n$, δ nonnegative integers with p and n relatively prime. Then there exist positive integers r and a with*

$$a \geq \lfloor \delta/k \rfloor + 1 + \delta/(n-k), \ an = p^r - 1.$$

Assume that a, r is as in the Lemma 2 and let $N = an$, $K = N - (n-k)\left(\lfloor \delta/k \rfloor + 1\right) - \delta$, and $\alpha \in \mathbb{F}_{p^r}$ a primitive element of $\mathbb{F}_{p^r}$. Define $g(D) = (D-\alpha^0)(D-\alpha^1)\cdots(D-\alpha^{N-K-1}) \in \mathbb{F}_{p^r}[D]$. The polynomial $g(D)$ defines an $[N, K]$ Reed-Solomon block code with distance $d_g = N-K+1 = (n-k)\left(\lfloor \delta/k \rfloor + 1\right) + \delta + 1$.

Using [1, Theorem 3] we obtain:

Theorem 3 [5] *Let $g(D)$ be defined as above. Then the convolutional code defined by (2) is MDS.*

Example 4 [5] Let α be a primitive of $\mathbb{F}_{2^6}$. The rate 2/3 encoder

$$\begin{bmatrix} \alpha^{28}+\alpha^{35}D+\alpha^{57}D^2 & 1+\alpha^6 D+\alpha^{42}D^2 & \alpha^8+\alpha^{26}D+D^2 \\ \alpha^8 D+\alpha^{26}D^2+D^3 & \alpha^{28}+\alpha^{35}D+\alpha^{57}D^2 & 1+\alpha^6 D+\alpha^{42}D^2 \end{bmatrix}.$$

has degree 5 and has free distance 9. The code attains the generalized Singleton bound (1) and therefore is an MDS convolutional code.

If one is interested to do the construction with small fields then one should construct a prime power q for which

$$n \mid (q-1) \text{ and } q > \delta \frac{n^2}{k(n-k)}. \tag{3}$$

The first author recently showed [4] that there are alternative constructions for unit memory MDS convolutional codes, these are codes where $\delta \leq k$.

[1] The authors were supported in part by NSF grant DMS-96-10389. The first author was also supported by a fellowship from the Center of Applied Mathematics at the University of Notre Dame.

References

[1] J. Justesen. New convolutional code constructions and a class of asymptotically good time-varying codes. *IEEE Trans. Inform. Theory*, IT-19(2):220–225, 1973.

[2] J. L. Massey, D. J. Costello, and J. Justesen. Polynomial weights and code constructions. *IEEE Trans. Inform. Theory*, IT-19(1):101–110, 1973.

[3] J. Rosenthal and R. Smarandache. Maximum distance separable convolutional codes. *Appl. Algebra Engrg. Comm. Comput.*, 10(1):15–32, 1999.

[4] R. Smarandache. Unit memory convolutional codes with maximum distance. In B. Marcus and J. Rosenthal, editors, *Codes, Systems and Graphical Models*, IMA Vol. in Math. and its Appl. Springer-Verlag, 2000. To appear.

[5] R. Smarandache, H. Gluesing-Luerssen, and J. Rosenthal. Constructions of MDS-convolutional codes. Submitted to IEEE Trans. Inform. Theory, August 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.