Convolutional Code Constructions Resulting in Maximal or near Maximal Free Distance[1]

Roxana Smarandache
Department of Mathematics,
University of Notre Dame
Notre Dame, IN 46556-5683 USA
e-mail: Smarandache.1@nd.edu

Joachim Rosenthal
Department of Mathematics,
University of Notre Dame
Notre Dame, IN 46556-5683 USA
e-mail: Rosenthal.1@nd.edu

Abstract — **In this paper we discuss an upper bound on the free distance for a rate k/n convolutional code with complexity δ. Using this bound we introduce the notion of a MDS convolutional code. We also give an algebraic way of constructing binary codes of rate 1/2 and large complexity. The obtained distances compare favorably to the distances found by computer searches and probabilistic methods.**

I. Introduction

Let C be a rate k/n convolutional code defined over a finite field $\mathbb{F}$. Let $G(z) \in \mathbb{F}[z]^{k\times n}$ be a minimal basic encoder. Following [3], we can assume that the row degrees $\nu_1 \geq \ldots \geq \nu_k$ are ordered in decreasing manner. We call ν_1 the memory and $\delta := \sum_{j=1}^{k} \nu_j$ the complexity of the convolutional code. The complexity is on the side of the rate probably the single most important invariant of a convolutional code. In systems theory this notion corresponds to the notion of McMillan degree and we refer to [4, 5] for more details.

It arises the question to determine the maximum value of the free distance among all rate k/n convolutional codes of complexity δ. In general this value depends on the base field. Independent on the base field we can describe a natural upper bound. For this we define:

$$l := k\left(\lfloor \delta/k \rfloor + 1\right) - \delta \tag{1}$$

Then one establishes:

Theorem 1 *For every base field $\mathbb{F}$ and every rate k/n convolutional code C of complexity δ the free distance is bounded by:*

$$d_{free} \leq n\left(\lfloor \delta/k \rfloor + 1\right) - l + 1. \tag{2}$$

In the next section we show that the upper bound (2) is achieved in many instances and based on this we define:

Definition 2 A rate k/n code of complexity δ whose free distance achieves the upper bound (2) will be called a MDS convolutional code.

II. MDS Convolutional Codes

MDS convolutional codes generalize MDS block codes and this is made clear through the following Lemma:

Lemma 3 *If G is a $k \times n$ generator of a MDS block code then G also generates a MDS convolutional codes of rate k/n, complexity $\delta = 0$ and free distance $n-k+1$. In particular if $|\mathbb{F}| \geq n$ MDS convolutional codes of rate k/n and complexity 0 do exist.*

The next result is due to Justesen [2] and it implies that rate $1/n$ MDS codes do exist for every value of δ. A systems theoretic proof of this result was given in [6].

Theorem 4 *If $k = 1$ and $|\mathbb{F}| \geq 3\delta$ MDS convolutional codes of complexity δ do exist.*

[1]This work was supported by NSF grant DMS-96-10389.

On the side of above two cases we can establish the existence of MDS codes in the following situation:

Lemma 5 *If $\delta < k$, $|\mathbb{F}| > 2n$ and $2k \leq n$ then MDS codes do exist.*

The above result mainly consider low rate codes. The following general result shows that for very high rate codes there exist convolutional codes of rate k/n and complexity δ whose distance is at least $\frac{k}{n}100\%$ of the upper bound (2):

Theorem 6 *([4]) Let $r := \max\{n-k, k\}$, let $\epsilon = \max\{n - 2k+1, 0\}$ and assume that $|\mathbb{F}| > \delta r \left\lceil \frac{\delta}{n-k} \right\rceil$. Then there exists a rate k/n convolutional code of complexity δ with free distance $d_{free} \geq \delta + 1 + \epsilon$.*

Based on above cases it is our conjecture that MDS convolutional code do exist for any rate and any complexity δ.

III. Distance Bounds for Binary codes

If the field size is limited then MDS convolutional codes do in general not exist. Over the binary field there are known upper and lower bounds for the free distance for codes having rate $1/n$ and we refer to the survey [1]. E.g. for rate 1/2 one has the general lower bound:

$$0.22\delta \leq d_{free}. \tag{3}$$

In general these bounds were obtained by probabilistic methods. Some constructions of rate $1/n$ binary codes have been done for small values of δ and we refer to [2]. The following result has been obtained by constructive means:

Theorem 7 *Let α be a primitive root of unity from $GF(2^s)$. Let $N = 2^{\lfloor s/2 \rfloor} - 2$. Let m_i be the minimal polynomial of α^i and let*

$$G := (l.c.m.\{m_i | i = 1, \ldots, N\}, l.c.m.\{m_{-i} | i = 1, \ldots, N\}).$$

Then G defines a binary rate 1/2 convolutional code of complexity at most $\lfloor \frac{Ns}{2} \rfloor$ and free distance at least $2(N+1)$.

Remark 8 If $s = 12$ then we obtain a code with complexity at most 372 and distance d_{free} at least 126. If $s = 200$ then we obtain a code with complexity less than 2^{100} and with distance $d_{free} \geq 0.01\delta$.

References

[1] 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.

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

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

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

[5] 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.

[6] 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 Wokshop on Information Theory*, Killarney, Kerry, Ireland, June 1998. To appear.