A State Space Approach for Constructing MDS Rate $1/n$ Convolutional Codes [1]

Roxana Smarandache, Joachim Rosenthal

Department of Mathematics, University of Notre Dame, Notre Dame, Indiana 46556, USA.
e-mail: Smarandache.1@nd.edu Rosenthal.1@nd.edu, WWW: http://www.nd.edu/˜rosen

Abstract — **In this paper we provide a state space approach for constructing convolutional codes of rate $1/n$ and complexity δ, whose free distance is $n(\delta+1)$, the maximal possible free distance.**

I. Introduction

In contrast to the situation of block codes there are few algebraic constructions for convolutional codes whose free distance has a designed value. The constructions which do exist often depend on construction techniques for quasi-cyclic codes and we refer to [2, 7] where also more references are provided.

One such construction was provided by Justesen in [1] where a convolutional code of rate $1/n$ and complexity δ is given whose free distance is $n(\delta+1)$, the maximal possible distance of all codes with these parameters. Since the designed distance is maximal we call such a code a maximal distance separable (MDS) convolutional code.

More recently the authors of this paper in collaboration with E. York [4, 5, 6, 7] gave for arbitrary rates k/n constructions of convolutional codes with a designed free distance. The techniques employed in these papers were new and they heavily relied on algebraic representations of linear systems. The achieved distances in [4, 6, 7] were approximately $\frac{k}{n}$ times the best possible free distance found among all convolutional codes of rate k/n and complexity δ. In particular for high rates the results were near optimal.

The authors of this paper showed in [5] that the constructions can be refined in order to achieve better distances also for low rate codes. In this paper we further refine the technique and we show how to rederive the result of Justesen [1] for rate $1/n$ codes.

We want to emphasize that the construction we present here is not just a reproof of a result already obtained. Indeed one can show that subfield constructions can be carried out and in this way codes can be constructed over an arbitrary base field. In addition it is our belief that the construction carries over to arbitrary rates as well. Finally we would like to mention that the presented codes are very suitable for the decoding algorithm presented by the second author in [3].

II. Rate $1/n$ convolutional codes

Let $\mathbb{F}$ denote an arbitrary finite field with q elements and let $\mathcal{C}$ be a convolutional code over $\mathbb{F}$ of rate $1/n$. As it was shown in [4, 7] we can describe $\mathcal{C}$ through a familiar looking input/state/output description. Thus let:

$$v(z) = v_0 z^{\gamma} + v_1 z^{\gamma-1} + \ldots + v_{\gamma};\ v_t \in \mathbb{F}^n, t = 0, \ldots, \gamma.$$

If one partitions the vector v_t into $v_t = \binom{y_t}{u_t}$, where y_t has $n-1$ components and u_t has 1 components then the convolutional code is equivalently described by the familiar looking '(A,B,C,D)' representation

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

Here (A,B,C,D) are matrices of size $\delta\times\delta$, $\delta\times k$, $(n-k)\times\delta$ and $(n-k)\times k$ respectively. We say that (A,B) forms a *controllable* matrix pair if rank $\begin{pmatrix} B & AB \ldots & A^{\delta-1}B\end{pmatrix} = \delta$, and that (A,C) forms an *observable pair* if (A^t, C^t) is a controllable pair.

Once (A,B) forms a controllable pair and (A,C) forms an observable pair then it was shown in [4, 6, 7] that (1) forms a noncatastrophic convolutional code of complexity δ and rate k/n. Assume now that $k=1$. By taking

$$A := \begin{pmatrix} \alpha & 0 & \cdots & 0 \\ 0 & \alpha^2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \alpha^{\delta} \end{pmatrix}, \quad B := \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}, \tag{2}$$

where α is a primitive element of the field $\mathbb{F}$, and by choosing C, D such that the pair (A,C) is observable it was shown in [4] that we obtain a code having distance more than $(\delta+1)$, as long as we allow large enough fields. In this paper we will explain how a MDS convolutional code can be obtained by choosing special matrices C, D. For this let A, B be defined as above and let

$$D := \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}.$$

For the better understanding of the construction we will present the case $n=2$ first. In the end we will outline the cases $n>2$. Let $\mathbb{F} = \mathbb{F}_q$ with $q-1 \geq 3\delta$, A and B as above, $D = (1)$, and let

$$A' := \begin{pmatrix} \alpha^{\delta+1} & 0 & \cdots & 0 \\ 0 & \alpha^{\delta+2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \alpha^{2\delta} \end{pmatrix}.$$

The system (1) can be rewritten as

$$\begin{array}{rcrcl} x_{t+1} & = & (A-BC)x_t & + & By_t \\ u_t & = & -Cx_t & + & Dy_t. \end{array} \tag{3}$$

In (3) the input u_t interchanged its meaning with the output y_t. We want to transform (3) into an equivalent system, having the form $x_{t+1} = A'x_t + B'y_t$, $u_t = C'x_t + y_t$, with A' defined as above. This is possible if there exists an invertible matrix S such that

$$S(A-BC)S^{-1} = A'$$

or else if $\det(sI-(A-BC)) = \det(sI-A') = \prod_{k=1}^{\delta}(s-\alpha^{\delta+k})$. In order to achieve this we will have to solve a linear equation resulting in a matrix $C := \begin{pmatrix} c_1 & c_2 & \ldots & c_{\delta} \end{pmatrix}$ such that

$$\det(sI-(A-BC)) = \det(sI-A').$$

[1] Research supported in part by NSF grant DMS-96-10389.

In particular there exists an invertible matrix S such that $S(A-BC)S^{-1}=A'$. Now (3) is equivalent with:

$$\begin{array}{rcrcl} x_{t+1} &=& A'x_t &+& SBy_t \\ u_t &=& -CS^{-1}x_t &+& y_t. \end{array} \tag{4}$$

Let $B':=SB$ and $C':=CS^{-1}$. It can be proved that (A',B') forms a controllable pair and that (A',C') forms an observable pair. It remains to be shown that the obtained code has distance $2(\delta+1)$. First we remind that if

$$\begin{array}{rcl} u(s) &=& u_0s^{\gamma}+u_1s^{\gamma-1}+\cdots+u_{\gamma}, \\ y(s) &=& y_0s^{\gamma}+y_1s^{\gamma-1}+\cdots+y_{\gamma}, \end{array}$$

where γ is the degree of v, the first equations of the systems (1) and (4) give that (see [4, 7]):

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

and

$$(y_{\gamma},\ldots,y_0)^t\in\ker\left(B'\ A'B'\ldots\ A'^{\gamma}B'\right).$$

We suppose $u_0\neq 0$ hence $y_0\neq 0$. We look at the degree γ of a codeword v. In case $\gamma<q-1$ then

$$\left(B\ AB\ldots\ A^{\gamma}B\right)$$

and

$$\left(B'\ A'B'\ldots\ A'^{\gamma}B'\right)$$

are full rank Vandermonde matrices (multiplied eventually by some nonsingular diagonal matrices), therefore $(u_{\gamma},\ldots,u_0)^t$ and $(y_{\gamma},\ldots,y_0)^t$ both have weight greater than $\delta+1$. Hence $(v_{\gamma},...,v_0)^t$ has weight more than $2(\delta+1)$. If $\gamma\geq q-1$, $A^{q-1}=I$ so

$$(u_{\gamma},\ldots,u_0)^t\in\ker\left(B\ AB\ldots\ A^{\gamma}B\right)$$

implies that

$$u':=\begin{pmatrix} u_0+u_{q-1}+\ldots \\ u_1+u_q+\ldots \\ \vdots \\ u_{q-2}+u_{2q-3}+\ldots \end{pmatrix}\in\ker\left(A^{q-2}B\ldots\ AB\ B\right)$$

that has rank δ. The case $u'\neq 0$ gives (as in the first case) that the weight of $u'\geq\delta+1$ hence the weight of u will be $\geq\delta+1$ as well. Also defining y' in the same way, we have that the weight of $y'\geq\delta+1$ unless $y'=0$, therefore again $\mathrm{wt}(v)\geq 2(\delta+1)$. If $u'=0$ and $y'\neq 0$, from the first equations of the systems (1) and (4) we have

$$\begin{array}{rcl} x_1+x_q+\ldots &=& A(x_0+x_{q-1}+\ldots) \\ &\vdots& \\ x_{q-2}+x_{2q-3}+\ldots &=& A^{q-2}(x_t+x_{q-1}+\ldots). \end{array} \tag{5}$$

That gives

$$\begin{pmatrix} y_o+y_{q-1}+\ldots \\ \vdots \\ y_{q-2}+y_{2q-3}+\ldots \end{pmatrix}=\begin{pmatrix} C \\ CA \\ \vdots \\ CA^{q-2} \end{pmatrix}(x_0+x_{q-1}+\ldots). \tag{6}$$

Since $\begin{pmatrix} C \\ CA \\ \vdots \\ CA^{q-2} \end{pmatrix}$ is a Vandermonde matrix multiplied by a nonsingular diagonal matrix we get the estimate

$$\mathrm{wt}\begin{pmatrix} C \\ CA \\ \vdots \\ CA^{q-2} \end{pmatrix}(x_0+x_{q-1}+\ldots)\geq q-1-\delta\geq 3\delta-\delta\geq 2\delta.$$

So $\mathrm{wt}(v)=\mathrm{wt}\binom{y}{u}=\mathrm{wt}(y)+\mathrm{wt}(u)\geq 2\delta+2=2(\delta+1)$. The case $u'\neq 0$ and $y'=0$ is analogous. The case $u'=0$, $y'=0$ implies that $x_0+x_{q-1}+x_{2(q-1)}+\ldots=0$ and it can be reduced to the anterior cases.

Let us now consider the situation where $n\geq 3$. Let

$$y_t=\begin{pmatrix} y_t^{(1)} \\ \vdots \\ y_t^{(n-1)} \end{pmatrix}, C=\begin{pmatrix} (c_1) \\ \vdots \\ (c_{n-1}) \end{pmatrix},$$

with $(c_i)^t\in\mathbb{F}^{\delta}$ represents the ith row vector of C, and let

$$A_i=\begin{pmatrix} \alpha^{r_i+1} & 0 & \cdots & 0 \\ 0 & \alpha^{r_i+2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \alpha^{r_i+\delta} \end{pmatrix},\ i=0,\ldots,n-1$$

where $r_0,\ldots,r_{n-1}$ are chosen for simplicity such that no two matrices among $A_0,A_1,\ldots,A_{n-1}$ have the same entries. This requires that the field is sufficiently large, i.e. $q-1\geq n\delta$. As shown in [1] it is possible to relax this requirement and we will address this in future work.

Split the system

$$\begin{array}{rcl} x_{t+1} &=& A_0x_t+Bu_t \\ \begin{pmatrix} y_t^{(1)} \\ \vdots \\ y_t^{(n-1)} \end{pmatrix} &=& \begin{pmatrix} (c_1) \\ \vdots \\ (c_{n-1}) \end{pmatrix}x_t+\begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}u_t \end{array} \tag{7}$$

into $n-1$ systems:

$$\begin{array}{rcrcl} x_{t+1} &=& (A-B(c_i))x_t &+& By_t^{(i)} \\ u_t &=& -(c_i)x_t &+& Dy_t^{(i)} \end{array} \tag{8}$$

and choose (c_i), such that $\det(sI-(A-B(c_i))=\prod_{k=1}^{\delta}(s-\alpha^{r_i+k})$. In analogy to the discussion of the case $n=2$ (of course more cases have to be considered) one can show that the resulting code is a MDS convolutional code of rate $1/n$ and complexity δ.

References

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

[2] Y. Levy and D.J. Costello Jr. An algebraic approach to constructing convolutional codes from quasi-cyclic codes. *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, 14:189–198, 1993.

[3] J. Rosenthal. An algebraic decoding algorithm for convolutional codes. Preprint, January 1998.

[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 R. Smarandache. Construction of convolutional codes using methods from linear systems theory. In *Proc. of the 35-th Annual Allerton Conference on Communication, Control, and Computing*, pages 953–960, 1997.

[6] 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.

[7] 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.