Construction and Decoding of Strongly MDS Convolutional Codes[1]

Roxana Smarandache
Department of Mathematics
San Diego State University
5500 Campanile Dr.
San Diego, CA 92182-7720, USA
e-mail: rsmarand@sciences.sdsu.edu
Heide Gluesing-Luerssen
Fachbereich Mathematik
Universität Oldenburg
Postfach 2503
D-26111 Oldenburg, Germany
e-mail: gluesing@mathematik.uni-oldenburg.de
Joachim Rosenthal[2]
Department of Mathematics
University of Notre Dame
Notre Dame, Indiana 46556-5683, USA
e-mail: Rosenthal.1@nd.edu

Abstract

A new class of of rate 1/2 convolutional codes called strongly MDS convolutional codes are introduced and studied. These are codes having optimal column distances. Properties of these codes are given and a concrete construction is provided. This construction has the ability to correct δ errors in any **sliding** window of length $4\delta+2$ whereas the best known MDS block code with parameters $[n, n/2], n = 4\delta+2$, can correct δ errors in any **slotted** window of length $4\delta+2$. A decoding algorithm for these codes is given in the end of the paper.

1 Introduction

In comparison to the literature on linear block codes there exist only relatively few algebraic constructions of convolutional codes which come with an algebraic decoding algorithm.

Convolutional codes are typically decoded by the Viterbi decoding algorithm which has the advantage that soft information can be processed. The algorithm has however the disadvantage that it is too complex for codes with large degree (or memory). The algorithm is also not practical for convolutional codes defined over large alphabets. In applications where

[1]The results of this paper were also presented at the 2002 IEEE International Symposium on Information Theory in Lausanne, Switzerland, June 30–July 5, 2002
[2]Supported in Part by NSF grant DMS-00-72383

codes over large alphabets are required the code of choice are linear block codes with large distance such as Reed-Solomon codes.

In this paper we introduce a new class of rate 1/2 codes which we call strongly MDS convolutional codes. The concept of MDS convolutional codes was introduced by the authors in [2, 4, 3]. An $[n,k,\delta]$ convolutional code is called MDS if its free distance is maximal among all rate k/n convolutional codes of degree δ.

Strongly MDS codes are a subclass of MDS codes which have a remarkable decoding capability. We show in this paper that a $[2,1,\delta]$ strongly MDS code (rate 1/2, degree δ) can correct up to δ errors in any *sliding window* of $4\delta+2$ code symbols. This compares to an MDS block code with parameters $[n, n/2]$, $n = 4\delta+2$, which corrects up to δ errors in any *slotted window* (block) of length $4\delta+2$. An algebraic decoding algorithm for strongly MDS codes is outlined in the end of the paper.

2 Rate 1/2 strongly MDS convolutional codes

Let $\mathcal{C}$ be a 1/2 rate convolutional code over a field $\mathbb{F}$, generated by $G(D) = \begin{bmatrix} a(D) & b(D) \end{bmatrix}$, with $a(D) = a_0 + \ldots + a_\delta D^\delta, b(D) = b_0 + \ldots + b_\delta D^\delta$. We suppose $a_0 \neq 0$ or $b_0 \neq 0$ and $a(D), b(D)$ are coprime.

A parity check matrix for $\mathcal{C}$ is given by $H(D) = \begin{bmatrix} -b(D) & a(D) \end{bmatrix}$. We expand the matrices $G(D)$ and $H(D)$ into $G(D) = G_0 + \ldots + G_\delta D^\delta$ and $H(D) = H_0 + \ldots + H_\delta D^\delta, G_j, H_j \in \mathbb{F}^{1\times 2}, j = 0, \ldots, \delta$.

Let:

$$G_j^c = \begin{bmatrix} G_0 & G_1 & \ldots & G_j \\ & G_0 & \ldots & G_{j-1} \\ & & \ddots & \vdots \\ & & & G_0 \end{bmatrix}, H_j^c = \begin{bmatrix} H_0 & & & \\ H_1 & H_0 & & \\ \vdots & \vdots & \ddots & \\ H_j & H_{j-1} & \ldots & H_0 \end{bmatrix}, \tag{2.1}$$

the $(j+1)\times 2(j+1)$ truncatted matrices. Let

$$d_j^c = \min_{u_0 \neq 0} \mathrm{wt}\ \left((u_0, \ldots, u_j) \cdot G_j^c\right),$$

be the jth column distance of the convolutional code $\mathcal{C}$. We have the following natural bound on the d_j^c.

Theorem 1 *A convolutional code of rate 1/2 has the jth column distance bounded above by: $d_j^c \leq j+2$. We also have: $d_{free} \leq 2\delta+2$.*

Definition 2 A code with $d_{free} = 2\delta+2$ will be called MDS convolutional code.

Corollary 3 *The index $j = 2\delta$ is the earliest step at which a rate 1/2 MDS convolutional code ($d_{free} = 2\delta+2$) can attain equality $d_j^c = d_{free}$ in the distance inequality:*

$$d_0^c \leq d_1^c \leq \ldots \leq d_\infty^c = d_{\mathrm{free}} = 2\delta+2.$$

Definition 4 A rate 1/2, degree δ, convolutional code is called *strongly MDS* if $d^c_{2\delta} = 2\delta + 2 = d_{free}$.

Theorem 5 *Let $\mathcal{C}$ be a 1/2 rate convolutional code of degree δ. Let $H^c_{2\delta} = \begin{bmatrix} A & B \end{bmatrix}$, $\hat{H}^c_{2\delta} = B^{-1}H^c_{2\delta} = \begin{bmatrix} T & I \end{bmatrix}$. The following statements are equivalent:*

1. *The code $\mathcal{C}$ is strongly MDS;*

2. $d^c_{2\delta} = 2\delta + 2 = d_{\text{free}}$;

3. *The first column $[a_0, a_1, \ldots, a_\delta, 0, \ldots, 0]^T$ of the parity check matrix, (obtained after column permutations to separate the two blocks),*

$$H^c_{2\delta} = \begin{bmatrix} a_0 & & & & & & & b_0 & & & & & & \\ a_1 & a_0 & & & & & & b_1 & b_0 & & & & & \\ \vdots & \vdots & \ddots & & & & & \vdots & \vdots & \ddots & & & & \\ a_\delta & a_{\delta-1} & \ldots & a_0 & & & & b_\delta & b_{\delta-1} & \ldots & b_0 & & & \\ & a_\delta & \ldots & a_1 & a_0 & & & & b_\delta & \ldots & b_1 & b_0 & & \\ & & \ddots & & \ddots & \ddots & & & & \ddots & & \ddots & \ddots & \\ & & & a_\delta & \ldots & a_1 & a_0 & & & & b_\delta & \ldots & b_1 & b_0 \end{bmatrix}, \quad (2.2)$$

   can not be written as a linear combination of any other 2δ columns.

4. *The first column $(h_0, h_1, \ldots, h^T_{2\delta)}$ of*

$$\hat{H}^c_{2\delta} = \begin{bmatrix} h_0 & & & & 1 & & \\ h_1 & h_0 & & & & 1 & \\ \vdots & & \ddots & & & & \ddots \\ h_{2\delta} & h_{2\delta-1} & \ldots & h_0 & & & & 1 \end{bmatrix}$$

   is not a linear combination of 2δ other columns of $\hat{H}^c_{2\delta}$.

5. *The matrix $T = \begin{bmatrix} h_0 & & & \\ h_1 & h_0 & & \\ \vdots & & \ddots & \\ h_{2\delta} & h_{2\delta-1} & \ldots & h_0 \end{bmatrix}$ has the property that all its square submatrices $A^{i_1,\ldots,i_r}_{j_1,\ldots,j_r}$ formed by the $i_1, \ldots, i_r$ rows and $j_1, \ldots, j_r$ columns of T, are invertible, for all $1 \leq r \leq 2\delta+1$ and all indices $1 \leq i_1 < \ldots < i_r \leq 2\delta+1, 1 \leq j_1 < \ldots < j_r \leq 2\delta+1$ which satisfy $j_\nu \leq i_\nu$ for $\nu = 1, \ldots, r$.*

The following process gives us an example of Toeplitz matrices T that satisfyproperty 5 over finite fields.

Example 6 Let $n = 2\delta$ and $T' = X^n$, with X the $(n+1)\times(n+1)$ matrix

$$X = \begin{bmatrix} 1 & & & & & \\ 1 & 1 & & & & \\ & 1 & 1 & & & \\ & & \ddots & \ddots & & \\ & & & 1 & 1 & \\ & & & & 1 & 1 \end{bmatrix}, T' = \begin{bmatrix} 1 & & & & & \\ n & 1 & & & & \\ \binom{n}{2} & n & 1 & & & \\ \vdots & \vdots & \ddots & \ddots & & \\ \binom{n}{n-1} & \binom{n}{n-2} & \dots & n & 1 & \\ 1 & \binom{n}{n-1} & \dots & & n & 1 \end{bmatrix}. \qquad (2.3)$$

Note that the entries on first column of T' are the coefficients of the expanded polynomial $(X+1)^n$. The minors are all positive integers ([1]), and taking the smallest prime p that does not divide any of them we obtain the matrix T, $T := T' \mod p$, with the desired property.

We want to decode the new constructed codes.

Let $\mathcal{C}$ be a rate 1/2 MDS convolutional matrix generated by $G(D) = \begin{bmatrix} a(D) & b(D) \end{bmatrix}$ with $a(D), b(D)$ of degree δ, satisfying the properties of Theorem 5.

Then we state that the code $\mathcal{C}$ is theoretically capable of correcting δ errors in any sliding window of length $4\delta+2$. Indeed, let $(y(D), z(D)) \in (\mathbb{F}[D])^2$ be a received message. Then there exists a codeword $(v(D), w(D)) \in \mathcal{C}$, and an error vector $(f(D), e(D)) \in (\mathbb{F}[D])^2$ such that $y(D) = v(D) + f(D), z(D) = w(D) + e(D)$.

Let $y_0, \dots, y_{2\delta}, z_0, \dots, z_{2\delta}$ be some $4\delta+2$ consecutive components of the received message $y(D), z(D)$. Multiplying the received message with the sliding parity check matrix of the code we obtain the syndrome equations.

We consider a window of $2\delta+1$ syndrome equations:

$$\begin{bmatrix} T & I \end{bmatrix} \begin{bmatrix} y_0 \\ \vdots \\ y_{2\delta} \\ z_0 \\ \vdots \\ z_{2\delta} \end{bmatrix} = \begin{bmatrix} T & I \end{bmatrix} \begin{bmatrix} f_0 \\ \vdots \\ f_{2\delta} \\ e_0 \\ \vdots \\ e_{2\delta} \end{bmatrix} =: \begin{bmatrix} s_0 \\ s_1 \\ \vdots \\ s_{2\delta} \end{bmatrix}. \qquad (2.4)$$

Suppose we have corrected all the components received before y_0, z_0. Assuming that the weight of the error $\begin{bmatrix} f_0 & \dots & f_{2\delta} & e_0 & \dots & e_{2\delta} \end{bmatrix}^T$ in this $4\delta+2$ window is at most δ, we find an algorithm that computes f_0 and e_0. Knowing f_0 and e_0 we update our received message, and move one step further. We consider the next sliding window and the sequence $f_1, \dots, f_{2\delta+1}, e_1, \dots, e_{2\delta+1}$ and correct now f_1, e_1.

The following theorem tells that such an algorithm theoretically exists.

Theorem 7 *Let $f = (f_0, \dots, f_{2\delta})^T, e = (e_0, \dots, e_{2\delta})^T$ be two vectors in $\mathbb{F}^{2\delta+1}$ such that* $\mathrm{wt} \begin{bmatrix} f \\ e \end{bmatrix} \leq \delta$. *Let*

$$\begin{bmatrix} T & I \end{bmatrix} \begin{bmatrix} f_0 & \dots & f_{2\delta} & e_0 & \dots & e_{2\delta} \end{bmatrix}^T = \begin{bmatrix} s_0 & s_1 & \dots & s_{2\delta} \end{bmatrix}^T. \qquad (2.5)$$

If $\begin{bmatrix} \tilde{f} \\ \tilde{e} \end{bmatrix}$ *is another solution of the equation (2.5) with* wt $\begin{bmatrix} \tilde{f} \\ \tilde{e} \end{bmatrix} \leq \delta$ *then* $f_0 = \tilde{f}_0, e_0 = \tilde{e}_0$.

We sketch here an algorithm for finding f_0 and e_0. It is a searching algorithm and it uses heavily the Gaussian elimination method for finding if a vector is in the column space of a certain matrix.

For any s, $s = 1, 2, \ldots, (\delta - 1)$, form all the $(2\delta + 1 - s) \times (2\delta + 1)$ submatrices of the matrix T, (column indices are consecutive):

$$T_{i_0,\ldots,i_{2\delta-s}} = \begin{bmatrix} h_{i_0} & h_{i_0-1} & \ldots & h_0 & & & \\ h_{i_1} & h_{i_1-1} & \ldots & \ldots & h_0 & & \\ \vdots & \vdots & & & & & \\ h_{i_{2\delta-s}} & h_{i_{2\delta-s}-1} & \ldots & \ldots & \ldots & h_0 & \end{bmatrix}. \tag{2.6}$$

For any l, $l = 1, 2, \ldots, (\delta - s)$ check if

$$\begin{bmatrix} s_{i_0} & s_{i_1} & \ldots & s_{i_{2\delta-s}} \end{bmatrix}^T$$

can be written as a linear combination of l columns of the matrix $T_{i_0,\ldots,i_{2\delta-s}}$. We start with $s = 1$ and let $l = 1, l = 2, \ldots, l = \delta - 1$, then $s = 2$ and try all possible values for l.

After finding one such matrix, we check if

$$\begin{bmatrix} s_{i_0} & s_{i_1} & \ldots & s_{i_{2\delta}} \end{bmatrix}^T$$

is a linear combination of the corresponding l columns of the matrix T. If it is, then the coefficients will be the corresponding components of an error f. Store f_0, compute $e_0 = s_0 - h_0 f_0$, and move to the next window. If not, keep searching until a good matrix is found.

This algorithm becomes impractical for large δ and q.

3 Conclusion

In this short paper we introduced a new class of codes which we call strongly MDS convolutional codes.

As parity check matrices for a block code, the matrices $[A\ B]$, $[T\ I_{2\delta+1}]$, give a block code very far from being MDS. In fact the minimum distance of this code is 2. However, as part of the sliding parity check matrix of a rate 1/2 convolutional code, this matrix gives an excellent code!

Therefore this is one example where a convolutional code performs better than the block code that stays at the base of the convolution construction.

The field over which we construct the matrix T may be large. An alternative that we currently consider is to take $T := \prod_1^n X_i$,

$$X_i = \begin{bmatrix} 1 & & & & & \\ x_i & 1 & & & & \\ & x_i & 1 & & & \\ & & \ddots & \ddots & & \\ & & & x_i & 1 & \\ & & & & x_i & 1 \end{bmatrix}, \tag{3.7}$$

with all the entries $x_i, 1 \leq i \leq n$ equal to consecutive powers of a primitive element of an arbitrary finite field $\mathbb{F}_q$, with at least $n+2$ elements. The minor in the lower part of the matrix T thus obtained, are the *skew-Schur-functions* in terms of $\{x_1, \ldots, x_n\}$, [5, page 344]. Imposing the nonzero conditions on this functions, we might be able to obtain estimates for the field size, and a matrix T with the desired property, over a suitable field. This method is subject of further research.

In this paper, we therefore obtain a rate 1/2 convolutional code of degree δ, capable to correct δ errors in any **sliding** window of length $4\delta + 2$.

The best known MDS block code with parameters $[n, n/2], n = 4\delta + 2$, can correct δ errors in any **slotted** window of length $4\delta + 2$.

References

[1] I. G. Macdonald. *Symmetric functions and Hall polynomials.* The Clarendon Press Oxford University Press, New York, second edition, 1995. With contributions by A. Zelevinsky, Oxford Science Publications.

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

[3] R. Smarandache. *Maximum Distance Separable Convolutional Codes, Construction and Decoding.* PhD thesis, University of Notre Dame, August 2001. Available at http://www.nd.edu/˜rosen/preprints.html.

[4] R. Smarandache, H. Gluesing-Luerssen, and J. Rosenthal. Constructions for MDS-convolutional codes. *IEEE Trans. Inform. Theory*, 47(5):2045–2049, 2001.

[5] R. P. Stanley. *Enumerative combinatorics. Vol. 2.* Cambridge University Press, Cambridge, 1999. With a foreword by Gian-Carlo Rota and appendix 1 by Sergey Fomin.