On Superregular Matrices

Ryan Hutchinson
Department of Mathematics
University of Notre Dame
Notre Dame, Indiana 46556-5683, USA
e-mail: rhutchin@nd.edu

Jochen Trumpf
Department of Systems Engineering, RSISE
The Australian National University
Canberra ACT 0200, Australia
e-mail: Jochen.Trumpf@anu.edu.au

April 29, 2004

Maximum distance separable (MDS) convolutional codes were introduced in [1]. These are convolutional codes whose free distance achieves the generalized Singleton bound. Strongly MDS codes are an interesting subclass of MDS codes which were introduced in [2]. These codes are characterized by the property that their column distances reach the generalized Singleton bound at the earliest possible time step. In [2], it was shown that, for any positive integers n and δ, strongly MDS $(n, n-1, \delta)$-convolutional codes exist if the base field is large enough. It was also shown that, if n and δ are not too large, strongly MDS convolutional codes perform very well under feedback decoding in terms of the number of errors that can be corrected per time interval.

The authors of [2] gave a constructive proof of the existence of strongly MDS $(n, n-1, \delta)$-convolutional codes. This construction makes use of superregular lower triangular Toeplitz matrices. The property of superregularity may be described in the following way. Let $\mathbb{F}$ be a field. For a matrix $T \in \mathbb{F}^{n\times n}$, denote by $T^{i_1,\ldots,i_r}_{j_1,\ldots,j_r} \in \mathbb{F}^{r\times r}$ the $r \times r$ submatrix obtained from T by taking the rows with indices $i_1, \ldots, i_r$ and the columns with indices $j_1, \ldots, j_s$.

Definition 0.1 A lower triangular matrix $T \in \mathbb{F}^{n\times n}$ is said to be *superregular* if $T^{i_1,\ldots,i_r}_{j_1,\ldots,j_r}$ is nonsingular for all $1 \leq r \leq n$ and all indices $1 \leq i_1 < \ldots < i_r \leq n$, $1 \leq j_1 < \ldots < j_r \leq n$ which satisfy $j_\nu \leq i_\nu$ for $\nu = 1, \ldots, r$. The submatrices obtained by picking such indices are called the *proper submatrices* and their determinants the *proper minors* of T.

In view of the application of superregular lower triangular Toeplitz matrices to the construction of strongly MDS $(n, n-1, \delta)$-convolutional codes, it is desirable to have a characterization of such matrices. Unfortunately, we are not able to offer a characterization at this time. We present instead a rough upper bound on the field size required for the existence of an $n \times n$ superregular lower triangular Toeplitz matrix. We also present methods for constructing new superregular lower triangular Toeplitz matrices from an existing one.

First, the upper bound:

Theorem 0.2 *Let C_n denote the nth Catalan number: $C_n = \frac{1}{n+1}\binom{2n}{n}$. Let $n \in \mathbb{N}$. Let $\mathbb{F}$ be a finite field such that $|\mathbb{F}^*| \geq \frac{1}{2}\big(C_{n-1} + \binom{n-1}{\lfloor \frac{n-1}{2} \rfloor}\big)$. Then, there exists an $n \times n$ superregular matrix over $\mathbb{F}$.*

Next, we show how to construct new superregular lower triangular Toeplitz matrices from a given one. One construction utilizes an action of the multiplicative group $\mathbb{F}^*$ of nonzero elements of $\mathbb{F}$ on the set of $n \times n$ superregular lower triangular Toeplitz matrices over $\mathbb{F}$. This action can be described in the following way. Suppose that

$$A := \begin{bmatrix} a_0 & 0 & \cdots & 0 \\ a_1 & a_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ a_n & \cdots & a_1 & a_0 \end{bmatrix}$$

is superregular. Let $\alpha \in \mathbb{F}^*$. Then,

$$\alpha * A := \begin{bmatrix} a_0 & 0 & \cdots & \cdots & 0 \\ \alpha a_1 & a_0 & \ddots & & \vdots \\ \alpha^2 a_2 & \alpha a_1 & a_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \alpha^n a_n & \cdots & \alpha^2 a_2 & \alpha a_1 & a_0 \end{bmatrix}$$

is also superregular. This action decomposes this set into a number of disjoint orbits. Combining this action with the operation of matrix inversion, which also preserves the property of superregularity, one can construct $2(|\mathbb{F}| - 1)$ (where $|\mathbb{F}|$ denotes the size of $\mathbb{F}$) new superregular matrices from an existing one.

Another construction utilizes the fact that the fields with which we work are finite and hence have positive characteristic. The Galois group $Aut_{\mathbb{F}_p}\mathbb{F}_{p^k} \cong \mathbb{Z}/k\mathbb{Z}$ acts on the set of $n \times n$ superregular lower triangular Toeplitz matrices over $\mathbb{F}_{p^k}$ in the following way. Suppose again that A above is superregular with entries in $\mathbb{F}_{p^k}$. Then, the matrices

$$i * A := \begin{bmatrix} a_0^{p^i} & 0 & \cdots & 0 \\ a_1^{p^i} & a_0^{p^i} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ a_n^{p^i} & \cdots & a_1^{p^i} & a_0^{p^i} \end{bmatrix}, \; i = 0, 1, 2, \ldots, k-1$$

are superregular as well.

References

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

[2] H. Gluesing-Luerssen, J. Rosenthal, and R. Smarandache. Strongly MDS convolutional codes, March 2003. http://front.math.ucdavis.edu/math.RA/0303254E-print math.RA/0303254.