Minimal Tail-Biting Trellises for Linear MDS Codes over F_{p^m}

B.Sundar Rajan[1]
Department of Electrical Communication Engineering
Indian Institute of Science
Bangalore 560 012, India
bsrajan@ece.iisc.ernet.in

G.Viswanath
Department of Electrical Communication Engineering
Indian Institute of Science
Bangalore 560 012, India
gviswa@protocol.ece.iisc.ernet.in

Abstract — **For all linear (n,k,d) MDS over finite fields F_{p^m}, we identity a generator matrix with the property that the product of trellises of rows of the generator matrix will give a minimal tail-biting linear trellis, and viewing the code as a group code, identify a set of generators, product of whose trellises will give a minimal tail biting group trellis. We also give the necessary and sufficient condition for the existence of flat minimal linear and group tail-biting trellises.**

I. Introduction

Trellis representation of block codes illuminate the structure of the code and also useful for efficient decoding. Recently, unconventional "Tail-biting trellises" (TBT) have been studied for well known codes like (24,12,8) Golay code, hexacode and few other short codes [1].

Minimal Tail-Biting Trellis: A tail-biting trellis with minimum maximum number of states along with the minimum product of all state space sizes, among all tail-biting trellises for the code under all possible coordinate permutations is called a minimal tail-biting trellis for the code.

The total span bound: [1] If C is an (n,k,d) linear code over F_q, then any n-section linear tail-biting trellis for C satisfies

$$\prod_{j=0}^{n-1} |S_j| \geq q^{k(d-1)} \quad (1)$$

$$S_{max} \geq q^{\frac{k}{n}(d-1)} \quad (2)$$

If $q=p^m$, then for group trellises we have

$$S_{max} \geq p^{\frac{mk}{n}(d-1)} \quad (3)$$

Flat Trellis: A tail-biting trellis is said to be flat if it has a constant state complexity profile.

It is well known that any k coordinates of a MDS code can be taken as information positions. This means that minimum weight vectors (of weight $n-k+1$) with circular span $n-k$ can be obtained such that the successive $n-k+1$ nonzero components start from any specified coordinate position from $\{0,1,...,(n-1)\}$. It can be shown that any k such vectors starting from different coordinate positions will constitute a generator matrix for the code. Using these results in the next section we specify the generator matrices that give minimal tail-biting trellises in terms of these k coordinate positions.

II. Minimal Circular Span Generator Matrices

Theorem 1: For a (n,k) linear MDS code over F_{p^m}, let $e=gcd(n,k)$, $n'=\frac{n}{e}$, $k'=\frac{k}{e}$ and $n'=\alpha k'+\beta$, where α and β are integers. The generator matrix which has only minimum weight vectors with consecutive nonzeros and with nonzeros starting from the indices given by the set I given below gives a minimal linear tail-biting trellis when product of trellises corresponding to each row vector is obtained:

$$\begin{aligned} I = \; & \{[\{jn'+i(\alpha+1) | i=0,1,\ldots,\beta\} \cup \\ & \{jn'+\beta(\alpha+1)+(i-\beta)\alpha | i=\beta+1,\ldots,k'-1\}] \\ & j=0,1,...,(e-1).\} \end{aligned} \quad (4)$$

Theorem 2: A necessary and sufficient condition for an (n,k) linear MDS code over any finite field to admit a minimal linear flat-trellis is that "n divides k^2".

Notice that the condition in Theorem 2 is independent of the size of the field.

Theorem 3: For a (n,k) linear MDS code over F_{p^m}, let $e=gcd(n,mk)$, $n'=\frac{n}{e}$, $k'=\frac{mk}{e}$. Also, let $k'=an'+k''$ where $0\leq k''<n'$ and $n'=\alpha k''+\beta$, where $0\leq\beta<k''$ and a and α are integers. The group-generator matrix which has $a+1$ minimum weight vectors with consecutive nonzeros with nonzeros starting from the indices given by the set I given below and a minimum weight vectors with consecutive nonzeros with nonzeros starting at all other time indices gives a minimal group tail-biting trellis when product of trellises corresponding to each row vector is obtained, if the rows starting at the same index are p-linearly independent (which can always be achieved):

$$\begin{aligned} I = \; & \{[\{jn'+i(\alpha+1) | i=0,1,\ldots,\beta\} \cup \\ & \{jn'+\beta(\alpha+1)+(i-\beta)\alpha | i=\beta+1,\ldots,k''-1\}] \\ & j=0,1,...,(e-1).\} \end{aligned} \quad (5)$$

Theorem 4: A necessary and sufficient condition for a linear (n,k) MDS code over F_{p^m} to admit a minimal group flat-trellis is that "n divides mk^2".

Observe that the condition in Theorem 4 depends only on m and not on the characteristic of the field.

Acknowledgments

B.S.Rajan gratefully acknowledges IBM India Research Lab, for the travel support to present this paper.

References

[1] A.R.Calderbank, G.D.Forney and A.Vardy, "Minimal Tail-Biting Trellises: The Golay Code and More", *IEEE Trans. on Information Theory*, Vol.45, No.5, pp.1435-1455, July 1999.

[2] F.R.Kschischang and V.Sorokine, "On the trellis structure of Block codes ", *IEEE Trans. Information Theory*, Vol.41, pp.1924-1937, Nov. 1995.

[1] This work was partly supported by CSIR, India, through Research Grants (No:25(0086)/97/EMRI-II) and (22(0298)/99/EMR-II) to B.S.Rajan