MTNS 2016 - extended abstract

On periodically time-varying convolutional codes

Ricardo Pereira[1] and Paula Rocha[2]

I. Extended Abstract

Convolutional codes [4] are an important type of error correcting codes that can be represented as a time-invariant discrete linear system over a finite field [8]. They are used to achieve reliable data transfer, for instance, in mobile communications, digital video and satellite communications [9]. In particular, periodically time-varying convolutional codes have attracted the attention of several researchers [2], [3]. One of the advantages of this type of codes is that they can have better distance properties than the best time-invariant convolutional code of the same rate and total encoder memory [7].

In this work we consider convolutional codes $\mathcal{C}$ with P-periodic encoders, i.e.:

$$\begin{aligned} \mathcal{C} := \{w : w(Pl+t) = (G^t(D)u)(Pl+t); \\ t = 0, ..., P-1; l = 0, 1, ...\}, \end{aligned} \tag{1}$$

where each $G^t(D)$ is a $n \times k$ polynomial matrix over a finite field $\mathbb{F}$, i.e., $G^t(D) \in \mathbb{F}^{n\times k}[D]$, D represents the shift $Du(l) = u(l-1)$, and u is an information sequence in $\mathbb{F}^k$.

Inspired by the ideas developed in [6] and [1] for the case of behaviors, considering the linear map

$$L_p : (\mathbb{R}^n)^{\mathbb{Z}} \to \left(\mathbb{R}^{Pn}\right)^{\mathbb{Z}}$$

defined by

$$(L_p w)(l) := \begin{bmatrix} w(Pl) \\ w(Pl+1) \\ \vdots \\ w(Pl+P-1) \end{bmatrix}, \quad P \in \mathbb{N}$$

we associate with $\mathcal{C}$ a time-invariant convolutional code $\mathcal{C}^L$, the "lifted" version of $\mathcal{C}$, defined as

$$\mathcal{C}^L := \left\{ \widetilde{w} \in \left(\mathbb{R}^{Pn}\right)^{\mathbb{Z}} | \widetilde{w} = L_p w, \ w \in \mathcal{C} \right\}.$$

Note that, since

$$(G^t(D)u)(Pl+t) = \left(\left(D^{-t}G^t(D)\right)u\right)(Pl),$$

Equation (1) can also be written as

$$(\Omega_{P,n}(D)w)(Pl) = (G(D)u)(Pl), l = 0, 1, \ldots,$$

with

$$\Omega_{P,n}(D) = \begin{bmatrix} I_n \\ D^{-1}I_n \\ \vdots \\ D^{-P+1}I_n \end{bmatrix}$$

and

$$G(D) = \begin{bmatrix} G^0(D) \\ D^{-1}G^1(D) \\ \vdots \\ D^{-P+1}G^{P-1}(D) \end{bmatrix} \in \mathbb{R}^{Pn\times k}.$$

Moreover, by decomposing the matrix G as

$$G(D) = G^L\left(D^P\right)\Omega_{P,n}(D)$$

with

$$G^L(D) = \begin{bmatrix} G^{L_0}(D) & G^{L_1}(D) & \cdots & G^{L_{P-1}}(D) \end{bmatrix},$$

the lifted code can be represented as

$$\mathcal{C}^L := \left\{\widetilde{w} : \widetilde{w}(l) = (G^L(D)\widetilde{u})(l), l = 0, 1, ...\right\},$$

where $\widetilde{w} = L_P w$ and $\widetilde{u} = L_P u$.

In the sequel, we consider convolutional codes $\mathcal{C}$ with 2-periodic encoders, i.e., such $P = 2$ and

$$G^t(D) = G_0^t + G_1^t D + \cdots + G_N^t D^N \in \mathbb{F}^{n\times k}[D], \ t = 0, 1.$$

Moreover we assume that the matrices G_0^0, G_0^1, G_N^0 and G_N^1 are full column rank. This implies that the matrices $G^t(D)$ are column reduced (see [5] for a definition), $t = 0, 1$. Assuming also that $G^t(D)$ are right-prime, $t = 0, 1$, we have that $G^t(D)$ are minimal encoders, $t = 0, 1$ [4]. Minimal encoders are particularly important since their McMillan degrees correspond to the code degree, which is a measure of its complexity.

The parameters of the encoders G^t, $t = 0, 1$, are (n, k, δ), where $\delta = kN$ is the degree of the code $\mathcal{C}^t$ generated by $G^t(D)$.

The generalized Singleton bound for each code $\mathcal{C}^t$ is

$$\begin{aligned} & (n-k)\left(\left\lfloor \tfrac{\delta}{k} \right\rfloor + 1\right) + \delta + 1 \\ = \ & (n-k)\left(\left\lfloor \tfrac{kN}{k} \right\rfloor + 1\right) + kN + 1 \\ = \ & nN + n - k + 1. \end{aligned} \tag{2}$$

By definition,

$$\begin{aligned} G^0(D) &= G_0^0 + G_1^0 D + \cdots + G_N^0 D^N + 0D^{N+1} \\ DG^1(D) &= 0 + G_0^1 D + G_1^1 D^2 + \cdots + \\ & \quad G_{N-1}^1 D^N + G_N^1 D^{N+1} \end{aligned}$$

[1]CIDMA - Center for Research and Development in Mathematics and Applications, Department of Mathematics, University of Aveiro, Aveiro, Portugal ricardopereira@ua.pt

[2]SYSTEC, Faculty of Engineering, University of Porto, Portugal mprocha@fe.up.pt

which can be decomposed as

$$\begin{bmatrix} G^0(D) \\ DG^1(D) \end{bmatrix} = \left(\begin{bmatrix} G_0^0 \\ 0 \end{bmatrix} + \begin{bmatrix} G_2^0 \\ G_1^1 \end{bmatrix} D^2 + \dots \right) + \left(\begin{bmatrix} G_1^0 \\ G_0^1 \end{bmatrix} + \begin{bmatrix} G_3^0 \\ G_2^1 \end{bmatrix} D^2 + \dots \right) D$$

The matrix G^L can be written as

$$G^L(D) = \begin{bmatrix} G_0^0 & G_1^0 \\ 0 & G_0^1 \end{bmatrix} + \begin{bmatrix} G_2^0 & G_3^0 \\ G_1^1 & G_2^1 \end{bmatrix} D + \dots + \begin{bmatrix} G_N^0 & 0 \\ G_{N-1}^1 & G_N^1 \end{bmatrix} D^{\lceil \frac{N}{2} \rceil} \quad (3)$$

We will prove the following result.

Theorem 1: $G^L(D)$ is a minimal time-invariant encoder.

Proof: Since, by hypothesis, G_0^0, G_0^1, G_N^0 and G_N^1 are full column rank, we have that $G^L(D)$ is column reduced. We prove now that $G^L(D)$ is right-prime. By hypothesis, $\begin{bmatrix} G^0(D) \\ DG^1(D) \end{bmatrix}$ is right-prime and

$$\begin{bmatrix} G^0(D) \\ DG^1(D) \end{bmatrix} = G^L\left(D^2\right) \begin{bmatrix} I_n \\ DI_n \end{bmatrix} \quad (4)$$

If $G^L\left(D^2\right) = \left[G^{L_0}\left(D^2\right) \quad G^{L_1}\left(D^2\right)\right]$ is not right-prime, then $G^{L_0}\left(D^2\right)$ and $G^{L_1}\left(D^2\right)$ have a squared non unimodular common factor, $F(D) \in \mathbb{F}^{k\times k}[D]$, i.e.,

$$G^{L_0}\left(D^2\right) = \widetilde{G}^{L_0}(D)F(D) \text{ and } G^{L_1}\left(D^2\right) = \widetilde{G}^{L_1}(D)F(D)$$

Then, by equation (4),

$$\begin{aligned} \begin{bmatrix} G^0(D) \\ DG^1(D) \end{bmatrix} &= \left[\widetilde{G}^{L_0}(D)F(D) \quad \widetilde{G}^{L_1}(D)F(D)\right] \begin{bmatrix} I_n \\ DI_n \end{bmatrix} \\ &= \widetilde{G}^{L_0}(D)F(D) + \widetilde{G}^{L_1}(D)F(D)D \\ &= \widetilde{G}^{L_0}(D)F(D) + \widetilde{G}^{L_1}(D)DF(D) \\ &= \left(\widetilde{G}^{L_0}(D) + \widetilde{G}^{L_1}(D)D\right)F(D) \end{aligned}$$

which is a contradiction because $\begin{bmatrix} G^0(D) \\ DG^1(D) \end{bmatrix}$ is right-prime. Hence $G^L\left(D^2\right)$ is right-prime and therefore also $G^L(D)$ is right-prime. ∎

The parameters of the encoder $G^L(D)$ are $(2n, 2k, kN)$ since it can be shown, by equation (3), that if N is even the degree is $\delta = 2k\left\lceil \frac{N}{2} \right\rceil = 2k\frac{N}{2} = kN$ and if N is odd the degree is $\delta = k\left\lceil \frac{N}{2} \right\rceil + k\left\lfloor \frac{N}{2} \right\rfloor = kN$. Then the generalized Singleton bound is

$$(2n-2k)\left(\left\lfloor \frac{kN}{2k} \right\rfloor + 1\right) + kN + 1$$

$$= \begin{cases} nN + 2n - 2k + 1, & \text{if} N \text{ even} \\ nN + n - k + 1, & \text{if } N \text{ odd} \end{cases}$$

which, is equal to the bound of each periodic encoder (2) when N is odd, but has an increase of $n-k$ when N is even.

This result is similar to the one derived in [2] using a different reasoning.

Obtaining a larger bound for the odd case is encouraging from the point of view of achieving a larger distance for the periodic case. However, the question whether the obtained bound can be reached is still the subject of current investigation.

Acknowledgement

This work was supported in part by the Portuguese Foundation for Science and Technology (FCT-Fundação para a Ciência e a Tecnologia), through CIDMA - Center for Research and Development in Mathematics and Applications, within project UID/MAT/04106/2013

This work was financially supported by: Project POCI-01-0145-FEDER-006933 - SYSTEC - Research Center for Systems and Technologies - funded by FEDER funds through COMPETE2020 - Programa Operacional Competitividade e Internacionalização (POCI) - and by national funds through FCT - Fundação para a Ciência e a Tecnologia.

References

[1] J.C. Aleixo, J.W. Polderman and P. Rocha, State space representation of SISO periodic behaviors, *Proceedings of the 50th IEEE Conference on Decision and Control and European Control Conference (CDC-ECC)*, Orlando, FL, USA, 12-15 Dec. 2011, pp. 1545-1550.

[2] J-J Climent, V. Herranz, C. Perea and V. Tomás, A construction of periodically time-varying convolutional codes, *Proceedings of the International Symposium on the Mathematical Theory of Networks and Systems (MTNS 2008), Virginia Institute of Technology, Blacksburg, USA*, 2008.

[3] Q. Hu and L.C. Perez, Some periodic time-varying convolutional codes with free distance achieving the Heller bound, *Proceedings of the IEEE International Symposium on Information Theory*, pp. 247, 2001.

[4] R. Johannesson and K.S. Zigangirov, Fundamentals of convolutional coding, IEEE press, New York, 1999.

[5] T. Kailath, Linear Systems, Prentice-Hall, 1980.

[6] M. Kuijper and J. C. Willems, A behavioral framework for periodically time-varying systems, *Proceedings of the 36th IEEE Conference on Decision & Control - CDC'97*, Vol. 3, San Diego, California USA, 10-12 Dec. 1997, pp. 2013-2016.

[7] M. Mooser, Some periodic convolutional codes better than any fixed code, *IEEE Transactions on Information Theory*, Vol. 29, No 5, pp. 750-751, 1983.

[8] J. Rosenthal, Connections between linear systems and convolutional codes, *Codes, Systems, and Graphical Models*, B. Marcus and J. Rosenthal, eds, Springer New York, Vol. 123, pp. 39-66, 2001.

[9] A.J. Viterbi, Convolutional codes and their performance in communication systems, *IEEE Transactions on Communication Technology*, Vol. 19, No 5, pp. 751-772, 1971.