23rd International Symposium on Mathematical Theory of Networks and Systems
Hong Kong University of Science and Technology, Hong Kong, July 16-20, 2018

A simple state-space realization method for a class of periodic encoders

Diego Napp[1] Ricardo Pereira[2] and Paula Rocha[3]

I. Extended Abstract

Convolutional codes [5] are an important type of error correcting codes that can be represented as a time-invariant discrete linear system over a finite field [10]. Since the seminal work in [2] time-varying convolutional codes raised a great interest as they can attain larger free distance than their time-invariant counterpart with equivalent parameters [1], [7], [8], [9].

In this work we aim at investigating time-varying convolutional codes from a system theoretical point of view. In particular, we study the realization of periodic encoders by means of periodic state-space models with the aim of efficient implementation. More concretely, in this preliminary work we focus on period two and investigate under which conditions a given periodic encoder obtained by alternating two time-invariant encoders can be realized by a periodic state-space system. We first observe that, in general, one cannot expect to obtain a periodic state-space realization by means of the individual realizations of each associated time-invariant encoders. However, we give conditions for such procedure to hold. The presented results are illustrated by examples.

II. Preliminaries

This section contains the background needed for the development of our results. We first introduce time-invariant and periodically time-varying convolutional codes and finally state-space representations of time-invariant convolutional codes.

A. Time-invariant convolutional codes

Let $\mathbb{F}$ be a finite field and n, k be positive integers with $k < n$. A *time-invariant convolutional code* $\mathcal{C}$ of rate k/n is a submodule $\mathbb{F}^n[z]$ described as

$$\mathcal{C} = \{v(z) \in \mathbb{F}^n[z] : v(z) = G(z)u(z),\ u(z) \in \mathbb{F}^k[z]\}$$

where $G(z) \in \mathbb{F}^{n\times k}[z]$ is a full column rank $n \times k$ polynomial matrix over $\mathbb{F}$, called the *encoder*, $u(z)$ taking values in $\mathbb{F}^k[z]$ is the *information vector* and $v(z)$ is the *codeword*.

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

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

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

The encoders of a code $\mathcal{C}$ differ by unimodular matrices over $\mathbb{F}[z]$. An encoder $G(z)$ is called *column reduced* if the sum of its column degrees attains the minimal possible value among all the encoders of the same code.

We define the *degree* δ of a convolutional code as the sum of the column degrees of one, and hence any, column reduced encoder. A code $\mathcal{C}$ of rate k/n and degree δ is said to be an (n, k, δ) code.

B. Periodically time-varying convolutional codes

In this work we consider convolutional codes $\mathcal{C}$ with 2-periodic encoders. The definition of such encoders (or encoding maps) is introduced next together with the definition of the corresponding 2-periodic (time-varying) convolutional codes, see [2], [9], [12].

Definition 1: Given two polynomial matrices $G^0(z), G^1(z) \in \mathbb{F}^{n\times k}[z]$, the *periodic encoding map* induced by G^0 and G^1 is defined as

$$\begin{array}{rccc} \phi_{G^0G^1}: & \mathbb{F}^k[z] & \longrightarrow & \mathbb{F}^n[z] \\ & u(z) & \longmapsto & v(z) \end{array}$$

where $v(z) = \sum_{i=0}^{+\infty} v_i z^i$ and $v_{2\ell+t} = \left(G^t(z)u(z)\right)_{2\ell+t}$, $t=0,1,\ \ell \in \mathbb{N}_0$, and, moreover, $\left(G^t(z)u(z)\right)_{2\ell+t}$ represents the $(2\ell+t)$-coefficient of the polynomial $G^t(z)u(z)$.

The corresponding *periodic convolutional code* $\mathcal{C}_p$ is

$$\mathcal{C}_p = \{v(z) \in \mathbb{F}^n[z] : v(z) = \phi_{G^0G^1}(u(z)),\ u(z) \in \mathbb{F}^k[z]\}. \tag{1}$$

Such codes will be called *2-periodic* convolutional codes.

C. State-space realizations

In systems theory, input-state-output models are mainly used to describe the time evolution of the system signals, which, in the discrete-time case, are time sequences. Therefore, in the sequel, we sometimes identify an element $a(z) = \sum_{i=0}^{N} a_i z^i \in \mathbb{F}[z]$ with the finite support sequence $a_0 = (a(z))_0,\ a_1 = (a(z))_1, \ldots, a_N = (a(z))_N$ formed by its coefficients, and also use the notation $a(\ell)$ to denote $a_\ell = (a(z))_\ell$. The same applies for vectors with components in $\mathbb{F}[z]$.

A state-space system

$$\left\{ \begin{array}{rcl} x(\ell+1) & = & Ax(\ell) + Bu(\ell) \\ v(\ell) & = & Cx(\ell) + Du(\ell) \end{array} \right. ,\ l \in \mathbb{N}_0,$$

denoted by (A, B, C, D), where $A \in \mathbb{F}^{\delta \times \delta}, B \in \mathbb{F}^{\delta \times k}, C \in \mathbb{F}^{n \times \delta}$ and $D \in \mathbb{F}^{n \times k}$, is said to be a state-space realization of the time-invariant (n, k, δ) convolutional code $\mathcal{C}$ if $\mathcal{C}$ is the set of codewords $v(z) \in \mathbb{F}^n[z]$ identified with the finite support output sequences v corresponding to finite support input sequences u (i.e., to information sequences $u(z) \in \mathbb{F}^k[z]$) and zero initial conditions, i.e., $x(0) = 0$.

This definition implicitly assumes that (A, B, C, D) is a minimal realization of $\mathcal{C}$, i.e., that A has the minimal possible dimension [11].

State-space realizations of convolutional codes can be obtained as minimal state-space realizations of column reduced encoders. If $G(z) \in \mathbb{F}^{n \times k}[z]$ is an encoder of $\mathcal{C}$, (A, B, C, D) is a state-space realization of $G(z)$ if

$$G(z) = C(I - Az)^{-1}Bz + D.$$

If $G(z) = \sum_{i \in \mathbb{N}} G_i z^i$, with $G_i \in \mathbb{F}^{n \times k}$, then

$$G_0 = D, \;\; G_i = CA^{i-1}B, \; i \geq 1. \tag{2}$$

Note that $G(z)$ admits many realizations. It is well-known that a state-space realization (A, B, C, D) of $G(z)$ has minimal dimension among all the realizations of $G(z)$ if (A, B) is controllable and (A, C) is observable, i.e., the polynomial matrices $\begin{bmatrix} z^{-1}I - A & | & B \end{bmatrix}$ and $\begin{bmatrix} z^{-1}I - A \\ C \end{bmatrix}$ have, respectively, right and left polynomial inverses (in z^{-1}). The minimal dimension of a state-space realization of $G(z)$ is called the McMillan degree [6] of $G(z)$ and it is represented as $\mu(G)$.

The next proposition, adapted from [3], [4], provides a state-space realization for a given (not necessarily column reduced) encoder.

Proposition 1: Let $G(z) \in \mathbb{F}^{n \times k}[z]$ be a polynomial matrix with rank k and column degrees $\nu_1, \ldots, \nu_k$. Consider $\bar{\delta} = \sum_{i=1}^{k} \nu_i$. Let $G(z)$ have columns $g_i(z) = \sum_{\ell=0}^{\nu_i} g_{\ell,i} z^\ell$, $i = 1, \ldots, k$ where $g_{\ell,i} \in \mathbb{F}^n$. For $i = 1, \ldots, k$ define the matrices

$$A_i = \begin{bmatrix} 0 & \cdots & \cdots & 0 \\ 1 & & & \vdots \\ & \ddots & & \vdots \\ & & 1 & 0 \end{bmatrix} \in \mathbb{F}^{\nu_i \times \nu_i}, \;\; B_i = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \in \mathbb{F}^{\nu_i},$$

$$C_i = \begin{bmatrix} g_{1,i} & \cdots & g_{\nu_i,i} \end{bmatrix} \in \mathbb{F}^{n \times \nu_i}.$$

Then a state-space realization of G is given by the matrix quadruple $(A, B, C, D) \in \mathbb{F}^{\bar{\delta} \times \bar{\delta}} \times \mathbb{F}^{\bar{\delta} \times k} \times \mathbb{F}^{n \times \bar{\delta}} \times \mathbb{F}^{n \times k}$ where

$$A = \begin{bmatrix} A_1 & & \\ & \ddots & \\ & & A_k \end{bmatrix}, \;\; B = \begin{bmatrix} B_1 & & \\ & \ddots & \\ & & B_k \end{bmatrix},$$

$$C = \begin{bmatrix} C_1 & \cdots & C_k \end{bmatrix}, \;\; D = \begin{bmatrix} g_{0,1} & \cdots & g_{0,k} \end{bmatrix} = G(0).$$

In the case where $\nu_i = 0$ the ith block of A and C are void and in B a zero column occurs.

In this realization (A, B) is controllable and if $G(z)$ is a column reduced encoder, (A, C) is observable. Thus, the McMillan degree of a column reduced encoder is equal to the sum of its column degrees.

III. State-space realizations of periodic convolutional codes

Definition 2: Let $\Sigma_i = (A_i, B_i, C_i, D_i), \; i = 0, 1$, be two state-space systems with the same dimension. We define a *periodic state-space system* Σ_p as

$$\begin{cases} x(\ell + 1) &= A(\ell)x(\ell) + B(\ell)u(\ell) \\ v(\ell) &= C(\ell)x(\ell) + D(\ell)u(\ell) \end{cases}, \; l \in \mathbb{N}_0 \tag{3}$$

where $A(\cdot), B(\cdot), C(\cdot), D(\cdot)$ are periodic functions with period 2, such that

$$\big(A(2j), B(2j), C(2j), D(2j)\big) = (A_0, B_0, C_0, D_0)$$

and

$$\big(A(2j + 1), B(2j + 1), C(2j + 1), D(2j + 1)\big) = (A_1, B_1, C_1, D_1), j \in \mathbb{N}_0.$$

The dimension of Σ_p is defined as the dimension of the state vector x. In this case we say that Σ_p is obtained from Σ_0 and Σ_1.

Moreover, Σ_p is a realization of a periodic encoding map $\phi_{G^0G^1}$ if the output of Σ_p that corresponds to an input $u(z)$ is equal to $\phi_{G^0G^1}(u(z))$, for all $u(z) \in \mathbb{F}^k[z]$.

Let Σ_0 and Σ_1 be two state-space realizations (of the same dimension) of two encoders $G^0(z)$ and $G^1(z)$. It is possible to show that the 2-periodic system Σ_p obtained from Σ_0 and Σ_1 is not always a state-space realization of $\phi_{G^0G^1}$.

However, in the next theorem we provide a sufficient condition for a periodic state-space system to be a realization of a periodic encoding map.

Theorem 1: Consider two encoders $G^0(z) \in \mathbb{F}^{n \times k}[z]$ and $G^1(z) \in \mathbb{F}^{n \times k}[z]$ with the same column degrees and let Σ_i be the realizations of $G^i(z), i = 0, 1$ obtained by Proposition 1. Then, the periodic state-space system Σ_p obtained from Σ_0 and Σ_1 is a realization of the periodic encoding map $\phi_{G^0G^1}$.

In case $G^0(z)$ and $G^1(z)$ have different column degrees the following procedure can be applied in order to obtain a 2-periodic state-space realization of the periodic encoding map from state-space realizations of $G^0(z)$ and $G^1(z)$:

1) Let ν_i be the maximum degree of the i-th columns of $G^0(z)$ and $G^1(z)$, $i = 1, \ldots, k$;
2) Realize $G^0(z)$ and $G^1(z)$ as in Proposition 1 considering the columns of $G^j(z)$ as $g_i^j(z) = \sum_{\ell=0}^{\nu_i} g_{\ell,i}^j z^\ell$, $i = 1, \ldots, k$, where some of the coefficients of higher degree may be zero.

Using this the following theorem holds.

Theorem 2: Let $G^0(z), G^1(z) \in \mathbb{F}^{n\times k}[z]$ be two encoders with state-space realizations Σ_0 and Σ_1, respectively, obtained from the procedure above. Then the 2-periodic system obtained from Σ_0 and Σ_1 is a state-space realization of the periodic encoding map $\phi_{G^0G^1}$.

Example 1: Consider the encoders

$$G^0(z) = G_0^0 + G_1^0 z + G_2^0 z^2 = \begin{bmatrix} 1 & 1 & 1+z \\ 1+z & z^2 & 1 \\ 1 & 1+z & 1 \\ 1 & 1+z^2 & 0 \end{bmatrix}$$

and

$$G^1(z) = G_0^1 + G_1^1 z + G_2^1 z^2 = \begin{bmatrix} 1 & 0 & 1 \\ 1+z & 1+z^2 & 1 \\ 1+z^2 & 1 & 1 \\ 1 & 1+z & 0 \end{bmatrix}.$$

Let $\nu_1 = 2$, $\nu_2 = 2$, $\nu_3 = 1$ be the maximum degrees of the first, second and third columns, respectively, of $G^0(z)$ and $G^1(z)$. The state-space realizations $\Sigma_0 = (A, B, C(0), D(0))$ and $\Sigma_1 = (A, B, C(1), D(1))$ of $G^0(z)$ and $G^1(z)$, respectively, obtained from the procedure above, are such that

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$C(0) = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \quad D(0) = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

$$C(1) = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \quad D(1) = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

The 2-periodic system obtained from Σ_0 and Σ_1 is a state-space realization of $\phi_{G^0G^1}$.

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] I. E. Bocharova and B. D. Kudryashov, "Rational rate punctured convolutional codes for soft-decision viterbi decoding," *IEEE Transactions on Information Theory*, vol. 43, no. 4, pp. 1305–1313, Jul 1997.

[2] D. J. Costello, "Free distance bounds for convolutional codes," *IEEE Transactions on Information Theory*, vol. 20, no. 3, pp. 356–365, May 1974.

[3] E. Fornasini and R. Pinto, "Matrix fraction descriptions in convolutional coding," *Linear Algebra and its Applications*, vol. 392, no. Supplement C, pp. 119 – 158, 2004. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0024379504002836

[4] H. Gluesing-Luerssen and G. Schneider, "State space realizations and monomial equivalence for convolutional codes," *Linear Algebra and its Applications*, vol. 425, no. 2, pp. 518 – 533, 2007, special Issue in honor of Paul Fuhrmann. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S002437950700122X

[5] R. Johannesson and K. S. Zigangirov, *Fundamentals of Convolutional Coding*. New York: IEEE Press, 1999.

[6] T. Kailath, *Linear systems*, ser. Prentice Hall information and system sciences series. Englewood Cliffs: Prentice-Hall, 1980.

[7] P. J. Lee, "There are many good periodically time-varying convolutional codes," *IEEE Transactions on Information Theory*, vol. 35, no. 2, pp. 460–463, Mar 1989.

[8] M. Mooser, "Some periodic convolutional codes better than any fixed code (corresp.)," *IEEE Transactions on Information Theory*, vol. 29, no. 5, pp. 750–751, September 1983.

[9] R. Palazzo, "A time-varying convolutional encoder better than the best time-invariant encoder," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 1109–1110, May 1993.

[10] J. Rosenthal, "Connections between linear systems and convolutional codes," in *Codes, Systems and Graphical Models*, ser. IMA Vol. 123, B. Marcus and J. Rosenthal, Eds. Springer-Verlag, 2001, pp. 39–66.

[11] J. Rosenthal and E. V. York, "BCH convolutional codes," *IEEE Trans. Automat. Control*, vol. 45, no. 6, pp. 1833–1844, 1999.

[12] D. Truhachev, K. S. Zigangirov, and D. J. Costello, "Distance bounds for periodically time-varying and tail-biting ldpc convolutional codes," *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4301–4308, Sept 2010.