MDP Periodically Time-Varying Convolutional Codes

Ricardo Pereira, Paula Rocha and Diego Napp

Abstract In this paper we use some classical ideas from linear systems theory to analyse convolutional codes. In particular, we exploit input-state-output representations of periodic linear systems to study periodically time-varying convolutional codes. In this preliminary work we focus on the column distance of these codes and derive explicit necessary and sufficient conditions for an $(n, 2, 1)$ periodically time-varying convolutional code to have Maximum Distance Profile (MDP).

Keywords Convolutional codes · Periodically codes · MDP codes

1 Introduction

Convolutional codes [1] are an important type of error correcting codes that can be represented as a time-invariant discrete linear system over a finite field [2]. They are used to achieve reliable data transfer, for instance, in mobile communications, digital video and satellite communications [3]. In particular, maximum distance profile (MDP) convolutional codes are relevant in applications since they have the potential to correct a maximal number of errors per time interval.

In contrast to block codes, the mathematical theory for the construction of good convolutional codes is not fully exploited. In fact, most convolutional codes used in practice have been found by systematic computer search and their distance properties must be also computed by full search. In recent years a great deal of effort has been

R. Pereira (✉) · D. Napp
CIDMA—Center for Research and Development in Mathematics and Applications,
Department of Mathematics, University of Aveiro, Aveiro, Portugal
e-mail: ricardopereira@ua.pt

D. Napp
e-mail: diego@ua.pt

P. Rocha
SYSTEC, Faculty of Engineering, University of Porto, Porto, Portugal
e-mail: mprocha@fe.up.pt

P. Garrido et al. (eds.), *CONTROLO 2016*, Lecture Notes
in Electrical Engineering 402, DOI 10.1007/978-3-319-43671-5_2

dedicated to develop constructions of non-binary convolutional codes having good distance [4, 5].

The idea of considering time-varying and, in particular, periodically time-varying convolutional codes has attracted the attention of several researchers [6, 7]. 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 [8, 9].

In this paper we start by presenting the necessary concepts about convolutional code within a input-state-output approach. Then we introduce periodically time-varying convolutional codes and find necessary and sufficient conditions on the subcodes to obtain a $(n, 2, 1)$ MDP time-varying convolutional code combining (possibly) non MDP subcodes.

2 Definitions and Basic Properties

Let $\mathbb{F}$ be a finite field. Let n, k and δ be positive integers with $k < n$. Following [10], a *rate k/n convolutional code $\mathcal{C}$ of degree δ* can be described by the linear system governed by the equations:

$$\begin{cases} x_{t+1} &= Ax_t + Bu_t \\ y_t &= Cx_t + Du_t \\ v_t &= \begin{pmatrix} y_t \\ u_t \end{pmatrix}, \quad x_0 = 0 \end{cases}, \qquad t = 0, 1, 2, \dots, \tag{1}$$

where $A \in \mathbb{F}^{\delta\times\delta}$, $B \in \mathbb{F}^{\delta\times k}$, $C \in \mathbb{F}^{(n-k)\times\delta}$ and $D \in \mathbb{F}^{(n-k)\times k}$. Moreover we assume that the pair (A, B) is controllable and the pair (A, C) is observable. We call $x_t \in \mathbb{F}^\delta$ the *state vector*, $u_t \in \mathbb{F}^k$ the *information vector*, $y_t \in \mathbb{F}^{n-k}$ the *parity vector* and $v_t \in \mathbb{F}^n$ the *code vector*. The associated code consists of all the finite sequences of code vectors, called *codewords*, produced by (1). We will refer to such a code as an (n, k, δ)-code and (A, B, C, D) is its input-state-output representation.

The *Hamming weight* of a vector $v \in \mathbb{F}^n$ is defined to be the number of nonzero components of v and is denoted by $\mathrm{wt}(v)$. The weight of a codeword is the sum of the Hamming weights of all the code vectors that form that word.

It follows from our assumptions that in this paper we are concerned only with finite-weight codewords. These are defined as follows:

Definition 1 A sequence $\{v_t = \left(\begin{smallmatrix} y_t \\ u_t \end{smallmatrix}\right) \in \mathbb{F}^n | t = 0, 1, 2, \dots\}$ represents a finite-weight codeword if

1. Eq. (1) is satisfied for all $t = 0, 1, 2, \dots$;
2. There exists an integer j such that $u_t = 0$ for $t \geq j + 1$.

Due to the observability of (A, C), this definition implies that $y_t = 0$ for $t \geq j + 1$ and $x_{j+1} = 0$; the codeword, therefore, has finite weight.

Important distance measures of a code are the *free distance* and the *column distance*. They are defined in the sequel as in [11] by means of this input-state-output approach.

Definition 2 The free distance of the code C described by (1) is defined as

$$d_{free}(C) = \min \left\{ \sum_{t=0}^{\infty} \mathrm{wt}(u_t) + \sum_{t=0}^{\infty} \mathrm{wt}(y_t) \right\},$$

where the minimum weight is to be taken over all nonzero codewords.

Rosenthal and Smarandache [12] showed that the free distance of an (n, k, δ) convolutional code is upper bounded by

$$d_{free}(C) \leq (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1.$$

This bound is called the *generalized Singleton bound*.

In this paper we focus on the following more local distance measure.

Definition 3 The *jth column distance* of the code C described by (1) is defined as

$$d_j^c(C) = \min_{u_0 \neq 0} \left\{ \sum_{t=0}^{j} \mathrm{wt}(u_t) + \sum_{t=0}^{j} \mathrm{wt}(y_t) \right\},$$

where the minimum weight is to be taken among all the codewords that start with a nonzero information vector.

The column distances satisfy

$$d_0^c \leq d_1^c \leq \cdots \leq \lim_{j \to \infty} d_j^c = d_{free}(C),$$

and have the following upper bounds [11].

Proposition 1 *For every $j \in \mathbb{N}_0$, we have*

$$d_j^c(C) \leq (n-k)(j+1) + 1.$$

It can be shown [5] that if the upper bound is attained for a certain j, then it is attained for all the preceding ones. Moreover, since no column distance can exceed the generalized Singleton bound, the largest integer j for which the previous bound can be attained is for $j = L$, with

$$L = \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta}{n-k} \right\rfloor .$$

Definition 4 An (n, k, δ)-convolutional code $\mathcal{C}$ is said to have *maximum distance profile (MDP)* if

$$d_L^c(\mathcal{C}) = (n-k)(L+1)+1, \quad L = \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta}{n-k} \right\rfloor .$$

MDP convolutional codes are characterized by the property that their initial column distances increase as rapidly as possible for as long as possible and therefore they are very important since they have the potential to correct a maximal number of errors per time interval [11]. Existence and characterizations of these codes in terms of the matrices (A, B, C, D) can be found in [11]. Here we present necessary and sufficient conditions for the periodically time-varying convolutional codes introduced in the next section to be MDP.

3 Periodically Time-Varying Convolutional Codes

In this section we start by defining periodically time-varying convolutional codes. Assume now that the matrices A_t, B_t, C_t and D_t at time t are of sizes $\delta \times \delta$, $\delta \times k$, $(n-k) \times \delta$ and $(n-k) \times k$, respectively. A time-varying convolutional code can be defined by means of the system

$$\begin{cases} x_{t+1} &= A_t x_t + B_t u_t \\ y_t &= C_t x_t + D_t u_t \\ v_t &= \begin{pmatrix} y_t \\ u_t \end{pmatrix}, \quad x_0 = 0 \end{cases}, \quad t = 0, 1, 2, \dots, \tag{2}$$

If the matrices change periodically with periods τ_A, τ_B, τ_C and τ_D respectively, (that is $A_{\tau_A+t} = A_t, B_{\tau_B+t} = B_t, C_{\tau_C+t} = C_t$ and $D_{\tau_D+t} = D_t$ for all t) then we have a *periodically time-varying convolutional code* of period $\tau = \operatorname{lcm}(\tau_A, \tau_B, \tau_C, \tau_D)$. For each fxed $t_0 \in \{0, 1, \dots, \tau - 1\}$ the code represented by $(A_{t_0}, B_{t_0}, C_{t_0}, D_{t_0})$ is called a *subcode* of the time-varying convolutional code (2) [13]. Note that, contrary to what the name seems to indicate, the codewords generated by the "subcode" do not constitute a subset of the time-varying code.

Our aim is to find necessary and sufficient conditions on the subcodes to obtain a MDP time-varying convolutional code, combining (possibly) non MDP subcodes. The $(n, 1, 1)$ case was already studied in [13]. Here we present the $(n, 2, 1)$ case.

3.1 MDP $(n,2,1)$ *Convolutional Codes*

In this section we assume that our convolutional codes are over a finite field $\mathbb{F}$ with a large enough number of elements. Consider a periodically time-varying code of period τ. Then we have the matrices

$$A_t = \begin{bmatrix} a_t \end{bmatrix}, \quad B_t = \begin{bmatrix} b_{t,1} \ b_{t,2} \end{bmatrix}, \quad C_t = \begin{bmatrix} c_{t,1} \\ c_{t,2} \\ \vdots \\ c_{t,n-2} \end{bmatrix},$$

$$D_t = \left[\begin{array}{c|c} d_{t,11} & d_{t,12} \\ d_{t,21} & d_{t,22} \\ \vdots & \vdots \\ d_{t,(n-2)1} & d_{t,(n-2)2} \end{array}\right] =: \begin{bmatrix} D_{t,1} | D_{t,2} \end{bmatrix},$$

with $t = 0, 1, \dots, \tau - 1$.

According to Definition 4, since

$$L = \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta}{n-k} \right\rfloor = \left\lfloor \frac{1}{2} \right\rfloor + \left\lfloor \frac{1}{n-2} \right\rfloor = \begin{cases} 0, \ n > 3 \\ 1, \ n = 3 \end{cases},$$

this convolutional code is MDP if

$$d_0^c(\mathcal{C}) = (n-2)(0+1) + 1 = n - 1$$

when $n > 3$ and

$$d_1^c(\mathcal{C}) = (3-2)(1+1) + 1 = 3$$

when $n = 3$.

- Suppose first that $n > 3$. By Definition 3 and Eq. (2) we have

$$\begin{aligned} d_0^c(\mathcal{C}) &= \min_{u_0 \neq 0} \left\{ \mathrm{wt}(u_0) + \mathrm{wt}(y_0) \right\} \\ &= \min_{u_0 \neq 0} \left\{ \mathrm{wt}(u_0) + \mathrm{wt}(C_0 x_0 + D_0 u_0) \right\}, \ x_0 = 0 \\ &= \min_{u_0 \neq 0} \left\{ \mathrm{wt}\left(\begin{bmatrix} u_{0,1} \\ u_{0,2} \end{bmatrix} \right) + \mathrm{wt}\left(D_{0,1} u_{0,1} + D_{0,2} u_{0,2} \right) \right\}, \end{aligned}$$

  where $u_0 = \left[\begin{smallmatrix} u_{0,1} \\ u_{0,2} \end{smallmatrix}\right]$.

Since the minimum is taken over $u_0 \neq 0$ then $\mathrm{wt}(u_0)$ can be either 1 or 2. We study these two cases separately.

If $\mathrm{wt}(u_0) = 1$, assume without loss of generality that $u_{0,1} \neq 0$ and $u_{0,2} = 0$. If $D_{0,1}$ has a zero element, then $\mathrm{wt}(D_{0,1}u_{0,1}) \leq n - 3$,

$$\mathrm{wt}(u_0) + \mathrm{wt}(D_{0,1}u_{0,1}) \leq 1 + n - 3 = n - 2 < n - 1,$$

and the code is not MDP. The same happens for $D_{0,2}$. This implies that all entries of the matrix D_0 must be nonzero. In this case $\mathrm{wt}\left(D_{0,1}u_{0,1}\right) = n - 2$ and hence $\mathrm{wt}(u_0) + \mathrm{wt}(y_0) = 1 + n - 2 = n - 1$.

If $\mathrm{wt}(u_0) = 2$, $\mathrm{wt}\left(D_{0,1}u_{0,1}\right) = \mathrm{wt}\left(D_{0,2}u_{0,2}\right) = n - 2$, but adding both terms can provoke cancellations and the weight decreases. A necessary condition to obtain the desired result is the following. If

$$d_{0,l1}d_{0,m2} - d_{0,l2}d_{0,m1} \neq 0,\ \forall l, m = 1, \ldots, n - 2,\ l \neq m,$$

at most one component of $D_{0,1}u_{0,1} + D_{0,2}u_{0,2}$ can be zero and so its weight is greater or equal than $n - 3$. Thus, $\mathrm{wt}(u_0) + \mathrm{wt}(y_0) \geq 2 + n - 3 = n - 1$.

This shows that for $n > 3$, $d_0^c(C) = n - 1$, i.e., the convolutional code is MDP.

- Suppose now that $n = 3$. Again by Definition 3 and Eq. (2) we have

$$\begin{aligned}
d_1^c(C) &= \min_{u_0 \neq 0} \left\{ \sum_{t=0}^{1} \mathrm{wt}(u_t) + \sum_{t=0}^{1} \mathrm{wt}(y_t) \right\} \\
&= \min_{u_0 \neq 0} \left\{ \mathrm{wt}(u_0) + \mathrm{wt}(u_1) + \mathrm{wt}(y_0) + \mathrm{wt}(y_1) \right\} \\
&= \min_{u_0 \neq 0} \left\{ \mathrm{wt}(u_0) + \mathrm{wt}(u_1) + \mathrm{wt}(C_0x_0 + D_0u_0) + \mathrm{wt}(C_1x_1 + D_1u_1) \right\},\ x_0 = 0 \\
&= \min_{u_0 \neq 0} \left\{ \mathrm{wt}\left(\begin{bmatrix} u_{0,1} \\ u_{0,2} \end{bmatrix} \right) + \mathrm{wt}\left(\begin{bmatrix} u_{1,1} \\ u_{1,2} \end{bmatrix} \right) + \mathrm{wt}\left(d_{0,11}u_{0,1} + d_{0,12}u_{0,2}\right) \right. \\
&\qquad \left. + \,\mathrm{wt}\left(c_{1,1}(b_{0,1}u_{0,1} + b_{0,2}u_{0,2}) + d_{1,11}u_{1,1} + d_{1,12}u_{1,2}\right) \right\}
\end{aligned}$$

We want to establish conditions such that $d_1^c(C) = 3$. Since the minimum is taken over $u_0 \neq 0$ then $\mathrm{wt}(u_0)$ can be either 1 or 2 and therefore $\mathrm{wt}(u_0) + \mathrm{wt}(u_1) \in \{1, 2, 3, 4\}$.

If $\mathrm{wt}(u_0) + \mathrm{wt}(u_1)$ is 3 or 4, obviously $\mathrm{wt}(u_0) + \mathrm{wt}(u_1) + \mathrm{wt}(y_0) + \mathrm{wt}(y_1) \geq 3$.

If $\mathrm{wt}(u_0) + \mathrm{wt}(u_1) = 1$, then $\mathrm{wt}(u_1) = 0$ and $\mathrm{wt}(u_0) = 1$ and assume without loss of generality that $u_{0,1} \neq 0$ and $u_{0,2} = 0$. Then, it is easy to check that

$$\mathrm{wt}(u_0) + \mathrm{wt}(u_1) + \mathrm{wt}(y_0) + \mathrm{wt}(y_1) = 1 + 0 + 1 + 1 = 3,$$

if and only if the elements $b_{0,1}, c_{1,1}$ and $d_{0,11}$ are nonzero. Note that, if $u_{0,1} = 0$ and $u_{0,2} \neq 0$, the previous condition holds when the elements $b_{0,2}$, $c_{1,1}$ and $d_{0,12}$ are nonzero.

When $\mathrm{wt}(u_0) + \mathrm{wt}(u_1) = 2$, two different situations can occur which will studied separately. If $\mathrm{wt}(u_0) = \mathrm{wt}(u_1) = 1$, analogously to the previous cases it follows that $\mathrm{wt}(u_0) + \mathrm{wt}(u_1) + \mathrm{wt}(y_0) + \mathrm{wt}(y_1) \geq 3$.

If $\mathrm{wt}(u_0) = 2$ and $\mathrm{wt}(u_1) = 0$, then

$$\begin{aligned} &\mathrm{wt}(u_0) + \mathrm{wt}(u_1) + \mathrm{wt}(y_0) + \mathrm{wt}(y_1) \\ = &\ 2 + \mathrm{wt}\left(d_{0,11}u_{0,1} + d_{0,12}u_{0,2}\right) + \mathrm{wt}\left(c_{1,1}(b_{0,1}u_{0,1} + b_{0,2}u_{0,2})\right). \end{aligned}$$

In this situation we need that at least one of these weights be nonzero, which implies that

$$d_{0,11}b_{0,2} - d_{0,12}b_{0,1} \neq 0, \ c_{1,1} \neq 0.$$

This leads to the following result.

Theorem 1 *The* $(n, 2, 1)$ *periodically time-varying convolutional code* (2) *is MDP if and only if*

(a) *When* $n > 3$*, all the entries of the matrix* D_0 *are nonzero and*

$$d_{0,l1}d_{0,m2} - d_{0,l2}d_{0,m1} \neq 0, \ \forall l, m = 1, \ldots, n-2, \ l \neq m.$$

(b) *When* $n = 3$*, all the entries of matrices* B_0, C_1 *and* D_0 *are nonzero and*

$$d_{0,11}b_{0,2} - d_{0,12}b_{0,1} \neq 0.$$

Example 1 Let C be a time-varying code of period $\tau = 2$ over the finite field $\mathbb{F}_7$ constituted by the $(3, 2, 1)$ subcodes

$$C_0 = (A_0, B_0, C_0, D_0), \quad C_1 = (A_1, B_1, C_1, D_1)$$

where

$$A_0 = A_1 = \begin{bmatrix}1\end{bmatrix}, \ B_0 = \begin{bmatrix}1 & 2\end{bmatrix}, \ B_1 = \begin{bmatrix}2 & 3\end{bmatrix},$$

$$C_0 = C_1 = \begin{bmatrix}1\end{bmatrix}, \ D_0 = \begin{bmatrix}2 & 1\end{bmatrix}, \ D_1 = \begin{bmatrix}4 & 6\end{bmatrix}.$$

By Proposition 1. (b) this code is MDP since

$$d_{0,11}b_{0,2} - d_{0,12}b_{0,1} = 2 \times 2 - 1 \times 1 \neq 0.$$

However, the subcode C_1 is not MDP, since by Definition 4 we have that $L = 1$ but $d_1^c(C_1) < 3$. Indeed, considering the inputs $u_0 = \left[\begin{smallmatrix}2\\1\end{smallmatrix}\right]$ and $u_1 = \left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]$, we have that

$$\begin{aligned}
&\mathrm{wt}(u_0) + \mathrm{wt}(u_1) + \mathrm{wt}(y_0) + \mathrm{wt}(y_1) \\
&= \mathrm{wt}(u_0) + \mathrm{wt}(u_1) + \mathrm{wt}(C_1x_0 + D_1u_0) + \mathrm{wt}(C_1x_1 + D_1u_1),\ x_0 = 0 \\
&= 2 + 0 + \mathrm{wt}(D_1u_0) + \mathrm{wt}(C_1B_1u_0) = 2 + 0 + 0 + 0 = 2.
\end{aligned}$$

The previous example showed that it is possible to obtain an MDP time-varying convolutional combining time-invariant subcodes which are not all MDP.

4 Conclusions

In this paper we used input-state-output representations of periodic linear systems to study periodically time-varying convolutional codes. In particular, we derived explicit necessary and sufficient conditions for an $(n, 2, 1)$ periodically time-varying convolutional code to have Maximum Distance Profile (MDP). The extension of these results to codes with other rates is under investigation.

Acknowledgments 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 COMPETE 2020—Programa Operational Competitividade e Internacionalização (POCI)—and by national funds through FCT—Fundação para a Ciência e a Tecnologia.

References

1. Johannesson, R., Zigangirov, K.S.: Fundamentals of Convolutional Coding. IEEE press, New York (1999)
2. Rosenthal, J.: Connections between linear systems and convolutional codes. In: Marcus B., Rosenthal, J. (eds.) Codes, Systems, and Graphical Models, vol. 123, pp. 39–66. Springer, New York (2001)
3. Viterbi, A.J.: Convolutional codes and their performance in communication systems. IEEE Trans. Commun. Technol. **19**(5), 751–772 (1971)
4. Almeida, P., Napp, D., Pinto, R.: A new class of superregular matrices and MDP convolutional codes. Linear Algebra Appl. **439**(7), 2145–2147 (2013)
5. Gluesing-Luerssen, H., Rosenthal, J., Smarandache, R.: Strongly-MDS convolutional codes. IEEE Trans. Inf. Theory **52**(2), 584–598 (2006)
6. Climent, J.-J., Herranz, V., Perea C., Tomás, V.: A systems theory approach to periodically time-varying convolutional codes by means of their invariant equivalent. In: Bras-Amorós, M., Høholdt, T. (eds.) Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, vol. 5527, pp. 73–82. Springer, Heidelberg (2009)
7. Hu, Q., Perez, L.C.: Some periodic time-varying convolutional codes with free distance achieving the Heller bound. In: Proceedings of the IEEE International Symposium on Information Theory, p. 247 (2001)
8. Lee, P.J.: There are many good periodically time-varying convolutional codes. IEEE Trans. Inf. Theory **35**(2), 460–463 (1989)

9. Mooser, M.: Some periodic convolutional codes better than any fixed code. IEEE Trans. Inf. Theory **29**(5), 750–751 (1983)
10. Rosenthal, J., Schumacher, J.M., York, E.V.: On behaviors and convolutional codes. IEEE Trans. Inf. Theory **42**(6), 1981–1991 (1996)
11. Hutchinson, R., Rosenthal, J., Smarandache, R.: Convolutional codes with maximum distance profile. Syst. Control Lett. **54**(1), 53–63 (2005)
12. Rosenthal, J., Smarandache, R.: Maximum distance separable convolutional codes. Appl. Algebra Eng. Commun. Comput. **10**, 15–32 (1999)
13. Tomás, V.: Complete-MDP convolutional codes over the erasure channel. PhD Thesis, University of Alicante (2010)

http://www.springer.com/978-3-319-43670-8

CONTROLO 2016
Proceedings of the 12th Portuguese Conference on
Automatic Control
Garrido, P.; Soares, F.; Moreira, A.P. (Eds.)
2017, XVIII, 889 p. 457 illus., 351 illus. in color.,
Hardcover
ISBN: 978-3-319-43670-8