State Space Realizations of Periodic Convolutional Codes

Raquel Pinto
University of Aveiro

joint work with
E. Fornasini, D. Napp, R. Pereira, P. Rocha

CTC, July 11-15, 2022, Zurich

Time-invariant Convolutional Codes

Definition: A time-invariant convolutional code $\mathcal{C}$ of rate k/n is a submodule of $\mathbb{F}^n[d]$ of rank k.
A full column rank matrix $G(d) \in \mathbb{F}^{n \times k}[d]$ such that

$$\begin{array}{rcl} \mathcal{C} & = & \{v(d) \in \mathbb{F}^n[d] \,:\, v(d) = G(d)u(d); u(d) \in \mathbb{F}^k[d]\} \\ & = & \mathrm{Im}_{\mathbb{F}[d]}\, G(d) \end{array}$$

is called an encoder of $\mathcal{C}$. The degree of $\mathcal{C}$ is equal to the internal degree of $G(d)$ (i.e., the greatest degree of the full size minors of $G(d)$).

The free distance of $\mathcal{C}$ is given by

$$d_{free}(\mathcal{C}) = min\{\sum_{i=0}^{+\infty} \mathrm{wt}(v_t) : \sum_{i=0}^{+\infty} v_t d^t \in \mathcal{C} \backslash \{0\}\}$$

Periodic Convolutional Codes

Definition: The periodic encoding map induced by r fcr polynomial matrices $G^0(d), G^1(d), \ldots, G^{r-1}(d) \in \mathbb{F}^{n\times k}[d]$ is defined as

$$\begin{array}{rccc} \Phi_{(G^0,G^1,\ldots,G^{r-1})}: & \mathbb{F}^k[d] & \rightarrow & \mathbb{F}^n[d] \\ & u(d) & \mapsto & v(d) \end{array}$$

with $v(d) = \sum_{i=0}^{+\infty} v_i d^i$ and $v_{r\ell+t} = (G^t(d)u(d))_{r\ell+t}$, $t = 0, 1, \ldots, r-1$, $\ell \in \mathbb{N}_0$

Example:

$$\Phi_{(G^0,G^1)} : \begin{array}{ccc} \mathbb{Z}_3[d] & \to & \mathbb{Z}_3^3[d] \\ u(d) & \mapsto & v(d) \end{array}$$

with $G^0(d) = \begin{bmatrix} d \\ 1 \\ d \end{bmatrix}, \quad G^1(d) = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}.$

Considering $u(d) = 1 + 2d$:

$$G^0(d)u(d) = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix} d + \begin{bmatrix} 2 \\ 0 \\ 1 \end{bmatrix} d^2$$

$$G^1(d)u(d) = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 0 \\ 2 \\ 2 \end{bmatrix} d$$

$$\begin{aligned} v(d) &= \Phi_{(G^0,G^1)}(u(d)) \\ &= \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 2 \\ 2 \end{bmatrix} d + \begin{bmatrix} 2 \\ 0 \\ 1 \end{bmatrix} d^2 \end{aligned}$$

Periodic Convolutional Codes

Definition: The periodic encoding map induced by r fcr polynomial matrices $G^0(d), G^1(d), \ldots, G^{r-1}(d) \in \mathbb{F}^{n\times k}[d]$ is defined as

$$\begin{array}{rccc} \Phi_{(G^0,G^1,\ldots,G^{r-1})}: & \mathbb{F}^k[d] & \rightarrow & \mathbb{F}^n[d] \\ & u(d) & \mapsto & v(d) \end{array}$$

with $v(d) = \sum_{i=0}^{+\infty} v_i d^i$ and $v_{r\ell+t} = (G^t(d)u(d))_{r\ell+t}$, $t = 0, 1, \ldots, r-1$, $\ell \in \mathbb{N}_0$

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

$$\begin{array}{rcl} \mathcal{C}_p & = & \{v(d) \in \mathbb{F}^n[d] : \exists\, u(d) \in \mathbb{F}^k[d] \text{ s.t. } v(d) = \Phi_{(G^0,G^1,\ldots,G^{r-1})}(u(d))\} \\ & = & \mathrm{Im}_{\mathbb{F}[d]}\, \Phi_{(G^0,G^1,\ldots,G^{r-1})} \end{array}$$

$\mathcal{C}_p$ is called an r-periodic convolutional code of rate k/n and $\Phi_{(G^0,G^1,\ldots,G^{r-1})}$ is called a periodic encoding map of $\mathcal{C}$.

If $G^0(d), G^1(d), \ldots, G^{r-1}(d) \in \mathbb{F}^{n\times k}[d]$ and $\tilde{G}^0(d), \tilde{G}^1(d), \ldots,$ $\tilde{G}^{r-1}(d) \in \mathbb{F}^{n\times k}[d]$ are fcr matrices such that

$$\mathrm{Im}_{\mathbb{F}[d]}\, \Phi_{(G^0,G^1,\ldots,G^{r-1})} = \mathrm{Im}_{\mathbb{F}[d]}\, \Phi_{(\tilde{G}^0,\tilde{G}^1,\ldots,\tilde{G}^{r-1})},$$

then $G^0(d), G^1(d), \ldots, G^{r-1}(d)$ and $\tilde{G}^0(d), \tilde{G}^1(d), \ldots, \tilde{G}^{r-1}(d)$ are said to be equivalent r-tuples of matrices.

Remark: Periodic codes are not necessarily $\mathbb{F}[d]$- submodules $\mathbb{F}^n[d]$.

From now on we will consider $r = 2$.

Motivation

The 2-periodic convolutional code $\mathcal{C}_p$, of rate $\frac{2}{3}$, with encoding map

$$\Phi_{(G^0,G^1)} : \mathbb{F}_2^2[d] \to \mathbb{F}_2^3[d]$$

such that

$$G^0(d) = \begin{bmatrix} 1+d & 0 \\ 1+d & 1+d \\ 1 & d \end{bmatrix} \quad \text{and} \quad G^1(d) = \begin{bmatrix} 1+d & 1 \\ 1 & 1+d \\ 0 & 1+d \end{bmatrix}.$$

has free distance 4, whereas any time-invariant convolutional code of the same rate $\frac{2}{3}$ and degree 2 over $\mathbb{F}_2$ cannot have free distance larger than 3 [Palazzo,93].

Lifted Code

Consider the linear map

$$\mathcal{L} : \mathbb{F}^n[d] \to \mathbb{F}^{2n}[d]$$

where for $v(d) = v_0 + v_1 d + v_2 d^2 + v_3 d^3 + \cdots \in \mathbb{F}^n[d]$,

$$\mathcal{L}(v(d)) = \begin{bmatrix} v_0 \\ v_1 \end{bmatrix} + \begin{bmatrix} v_2 \\ v_3 \end{bmatrix} d + \begin{bmatrix} v_4 \\ v_5 \end{bmatrix} d^2 + \cdots \in \mathbb{F}^{2n}[d].$$

The lifted version of a 2-periodic conv. code $\mathcal{C}_p$, is defined as

$$\boxed{\mathcal{C}^L = \left\{ \widetilde{v}(d) \in \mathbb{F}^{2n}[d] : \ \widetilde{v}(d) = \mathcal{L}(v(d)), \ v(d) \in \mathcal{C}_p \right\}}$$

Lifted Code

Consider the fcr matrices $G(d) = \sum_{i=0}^{s} G_i d^i \in \mathbb{F}^{n\times k}[d]$ and $J(d) = \sum_{i=0}^{s} J_i d^i \in \mathbb{F}^{n\times k}[d]$ and the induced periodic encoding map $\Phi_{(G,J)}$.

Then for $u(d) \in \mathbb{F}^k[d]$ and $v(d) = \Phi_{(G,J)}(u(d))$ we have that

$$\mathcal{L}(v(d)) = L(d)\, \mathcal{L}(u(d))$$

where

$$L(d) = \begin{bmatrix} G_0 & 0 \\ J_1 & J_0 \end{bmatrix} + \begin{bmatrix} G_2 & G_1 \\ J_3 & J_2 \end{bmatrix} d + \begin{bmatrix} G_4 & G_3 \\ J_5 & J_4 \end{bmatrix} d^2 + \cdots .$$

Lifted Code

Thus, the lifted code can be represented as

$$\boxed{\begin{array}{rcl} \mathcal{C}^L & = & \left\{ \widetilde{v}(d) \in \mathbb{F}^{2n}[d] : \widetilde{v}(d) = L(d)\widetilde{u}(d),\ \tilde{u}(d) \in \mathbb{F}^{2k}[d] \right\} \\ & = & \mathrm{Im}_{\mathbb{F}[d]}\, L(d) \end{array}}$$

Lemma: Let $\mathcal{C}_p$ and $\widetilde{\mathcal{C}}_p$ be two periodic convolutional codes. Then $\mathcal{C}_p = \widetilde{\mathcal{C}}_p$ if and only if the corresponding lifted codes $\mathcal{C}_p^L$ and $\widetilde{\mathcal{C}}_p^L$, respectively, coincide.

Injectivity

!! Two full column rank matrices $G(d)$ and $J(d)$ may yield a non-injective periodic encoding map $\Phi_{(G,J)}$.

Example: Consider the fcr matrices

$$G(d) = G_0 + G_1 d + G_2 d^2 \quad \text{and} \quad J(d) = J_0 + J_1 d + J_2 d^2 \in \mathbb{F}^{2\times 1}[d],$$

with $G_0 = G_2 = J_1 = 0$. Then $\Phi_{(G,J)}$ is not injective since with $u(d) = 1$ we obtain $v(d) = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$:

$$v_0 = G_0\, 1 = \begin{bmatrix} 0 \\ 0 \end{bmatrix};\; v_1 = J_1\, 1 = \begin{bmatrix} 0 \\ 0 \end{bmatrix};\; v2 = G_2\, 1 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \cdots$$

Theorem: Let $G(d) = \sum_{i=0}^{+\infty} G_i d^i, J(d) = \sum_{i=0}^{+\infty} J_i d^i \in \mathbb{F}^{n \times k}[d]$. Then $\Phi_{(G,J)}$ is injective if and only if

$$L(d) = \begin{bmatrix} G_0 & 0 \\ J_1 & J_0 \end{bmatrix} + \begin{bmatrix} G_2 & G_1 \\ J_3 & J_2 \end{bmatrix} d + \begin{bmatrix} G_4 & G_3 \\ J_5 & J_4 \end{bmatrix} d^2 + \cdots$$

is full column rank.

Corollary: If $G(d)$ and $J(d)$ are delay-free (i.e., G_0 and J_0 are fcr) then the periodic encoding map $\Phi_{(G,J)}$ is injective.

Lemma: The polynomial matrices $G(d)$ and $J(d)$ generate an injective periodic encoding map $\Phi_{(G,J)}$ if and only if all equivalent pairs of polynomial matrices generate an injective periodic encoding map.

State-space realizations of TI convolutional codes

Definition: A state-space system (A, B, C, D)

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

where $A \in \mathbb{F}^{m \times m}$, $B \in \mathbb{F}^{m \times k}$, $C \in \mathbb{F}^{n \times m}$ and $D \in \mathbb{F}^{n \times k}$, with state x, input u and output v, is said to be an m-dimensional state-space realization of the time-invariant convolutional code $\mathcal{C}$ of rate k/n if $\mathcal{C}$ is constituted by the outputs of (A, B, C, D) corresponding to finite support (polynomial) input sequences u and to $x(0) = 0$.

Remark:(A, B, C, D) must produce finite support output sequences v for all finite support input sequences u and zero initial state.

State-space realizations of 2-periodic convolutional codes

Let

- $G(d) = \sum_{i=0}^{+\infty} G_i d^i, J(d) = \sum_{i=0}^{+\infty} J_i d^i \in \mathbb{F}^{n \times k}[d]$ be two fcr matrices and $\mathcal{C}_p = \operatorname{Im} \Phi_{(G,J)}$.
- $\Sigma = (A, B, C, D)$ be a realization of $\begin{bmatrix} G(d) \\ J(d) \end{bmatrix}$, with

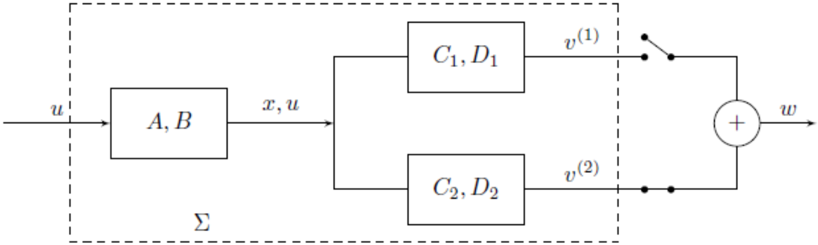
$$C = \begin{bmatrix} C_1 \\ C_2 \end{bmatrix}, \; C_1, C_2 \in \mathbb{F}^{n \times m} \text{ and } D = \begin{bmatrix} G_0 \\ J_0 \end{bmatrix},$$

- $\begin{bmatrix} v^{(1)}(d) \\ v^{(2)}(d) \end{bmatrix}$, with $v^{(1)}(d) = \sum_{i \in \mathbb{N}} v_i^{(1)} d^i \in \mathbb{F}^n[d]$ and $v^{(2)}(d) = \sum_{i \in \mathbb{N}} v_i^{(2)} d^i \in \mathbb{F}^n[d]$, be the output of Σ corresponding to the input $u(d) \in \mathbb{F}^k[d]$.

Let us consider as a new output $w(d) \in \mathbb{F}^n[d]$ defined as $w_{2j} = v_{2j}^{(1)}$ and $w_{2j+1} = v_{2j+1}^{(2)}$, $j \in \mathbb{N}$.

Switched output realizations

In this way, we obtain the system Σ_p represented by



Note that only one switch is on at each time instant and the switches change from on to off alternatively.
The switch corresponding to $v^{(1)}$ is on at the initial time instant and the initial state is zero.

Switched output realizations

Σ_p is called a periodic switched output state-space system and it corresponds to the periodic equations

$$\begin{cases} x(\ell+1) &= A(\ell)x(\ell) + B(\ell)u(\ell) \\ w(\ell) &= C(\ell)x(\ell) + D(\ell)u(\ell) \end{cases}$$

with

$$\begin{aligned} A(\ell) &:= A \quad , \quad B(\ell) := B, \\ C(2\ell) &:= C_1 \quad , \quad D(2\ell) := G_0, \\ C(2\ell+1) &:= C_2 \quad , \quad D(2\ell+1) := J_0, \quad \ell \in \mathbb{N}_0 \end{aligned}$$

For short, we write $\Sigma_p = (A, B, C(\ell), D(\ell))$

Definition: Σ_p is a state-space realization of the periodic encoding map $\Phi_{(G,J)}$ if for zero initial state, the output $w(d)$ of Σ_p that corresponds to an input $u(d)$ is equal to $\Phi_{(G,J)}(u(d))$, for all $u(d) \in \mathbb{F}^k[d]$.

Theorem: A periodic switched output system Σ_p is a realization of the periodic encoding map $\Phi_{(G,J)}$ if and only if the system Σ given by $\left(A, B, \begin{bmatrix} C_1 \\ C_2 \end{bmatrix}, \begin{bmatrix} G_0 \\ J_0 \end{bmatrix}\right)$ is a realization of $\begin{bmatrix} G(d) \\ J(d) \end{bmatrix}$.

$\mathbb{F}[d^2]$-generator of a code

Let

$$G(d) = \sum_{i=0}^{s} G_i d^i \quad \text{and} \quad J(d) = \sum_{i=0}^{s} J_i d^i$$

be two fcr matrices with $G_i, J_i \in \mathbb{F}^{n \times k}$, $i = 0, 1, \ldots, s$.

Given $u(d) = \sum_{i=0}^{+\infty} u_i d^i \in \mathbb{F}^k[d]$, let us write

$$u(d) = p_0(d^2) + d\, p_1(d^2)$$

for $p_0(d^2), p_1(d^2) \in \mathbb{F}^k[d^2]$, i.e.,

$$p_0(d^2) = \sum_{j \in \mathbb{N}} u_{2j} d^{2j} \text{ and } p_1(d^2) = \sum_{j \in \mathbb{N}} u_{2j+1} d^{2j}.$$

Then

$$\Phi_{(G,J)}(u(d)) = \left[\begin{array}{c|c} R(d) & dS(d) \end{array}\right] \left[\begin{array}{c} p_0(d^2) \\ p_1(d^2) \end{array}\right],$$

where

$$R(d) = \sum_{i=0}^{s} R_i d^i \quad \text{and} \quad S(d) = \sum_{i=0}^{s} S_i d^i$$

with, for $j \in \mathbb{N}$,

- $R_i = G_i$ and $S_i = J_i$, if $i = 2j$
- $R_i = J_i$ and $S_i = G_i$, if $i = 2j+1$

and therefore $\mathcal{C}_p = \mathrm{Im}_{\mathbb{F}[d^2]} \left[\begin{array}{c|c} R(d) & dS(d) \end{array}\right]$.

We call a representation of this type an $\mathbb{F}[d^2]$-generator of $\mathcal{C}_p$.

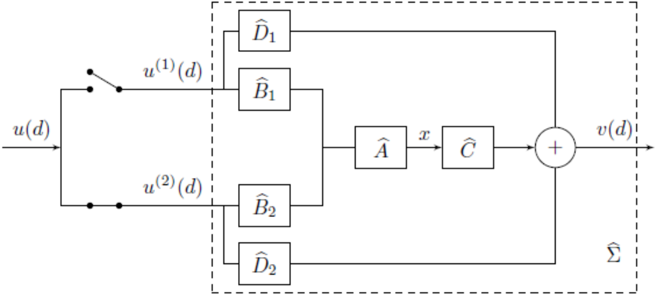
State-space realizations of 2-periodic convolutional codes

Let

- $R(d)$ and $S(d)$ polynomial matrices defined as before.
- $\widehat{\Sigma} = (\widehat{A}, \widehat{B}, \widehat{C}, \widehat{D})$ be a realization of $\begin{bmatrix} R(d) & S(d) \end{bmatrix}$
- $\widehat{B} = \begin{bmatrix} \widehat{B}_1 & \widehat{B}_2 \end{bmatrix}$ and $\widehat{D} = \begin{bmatrix} \widehat{D}_1 & \widehat{D}_2 \end{bmatrix}$ be partitioned according to the partition of $\begin{bmatrix} R(d) & S(d) \end{bmatrix}$.
- Write the input of Σ as $\begin{bmatrix} u^{(1)}(d) \\ u^{(2)}(d) \end{bmatrix}$, with $u^{(1)}(d) = p_0(d^2) \in \mathbb{F}^k[d]$ and $u^{(2)}(d) = dp_1(d^2) \in \mathbb{F}^k[d]$.

Switched input realizations

In this way, we obtain the system $\widehat{\Sigma}_p$ represented by



In the scheme, the switches alternate between the positions on and off at each time instant.

At time $t = 0$, the switch corresponding to $u^{(1)}$ is on, and the state initial condition is zero.

Switched input realizations

$\widehat{\Sigma}_p$ is called a periodic switched input state-space system and it corresponds to the periodic equations

$$\begin{cases} \widehat{x}(\ell+1) & = & \widehat{A}(\ell)\widehat{x}(\ell) + \widehat{B}(\ell)u(\ell) \\ w(\ell) & = & \widehat{C}(\ell)\widehat{x}(\ell) + \widehat{D}(\ell)u(\ell) \end{cases}$$

where $\widehat{A}(\ell) = \widehat{A}$ and $\widehat{C}(\ell) = \widehat{C}$ are fixed and

$$\widehat{B}(2\ell) = \widehat{B}_1 \ , \widehat{B}(2\ell+1) = \widehat{B}_2 \ ,$$

$$\widehat{D}(2\ell) = \widehat{D}_1 = R(0) = G_0,$$

$$\widehat{D}(2\ell+1) = \widehat{D}_2 = S(0) = J_0, \ \ell \in \mathbb{N}_0.$$

For short, we write $\widehat{\Sigma}_p = (\widehat{A}, \widehat{B}(\ell), \widehat{C}, \widehat{D}(\ell))$.

Switched output systems - minimality

A switched output system Σ_p is said to be a switched output realization of a periodic convolutional code $\mathcal{C}_p$ if the set of outputs of Σ_p corresponding to polynomial inputs and zero initial state is equal to $\mathcal{C}_p$.

Switched output realizations of a periodic convolutional code $\mathcal{C}_p$ are realizations of the same type of the periodic encoding maps of $\mathcal{C}_p$.

A minimal switched output realization of $\mathcal{C}_p$ is a realization of $\mathcal{C}_p$ of this type with minimal dimension among all realizations of $\mathcal{C}_p$ of the same type.

Lemma: Let $\mathcal{C}_p$ be a periodic conv. code and $\Phi_{(G,J)}$ a periodic encoding map of $\mathcal{C}_p$, for some fcr matrices $G(d), J(d) \in \mathbb{F}^{n\times k}[d]$.

A switched output periodic system Σ_p is a minimal switched output realization of $\Phi_{(G,J)}$ if and only if the associated system Σ is a minimal realization of $\begin{bmatrix} G(d) \\ J(d) \end{bmatrix}$.

Moreover, the minimal dimension of a switched output realization of $\Phi_{(G,J)}$ is equal to the maximal degree of the minors of $\begin{bmatrix} G(d) \\ J(d) \end{bmatrix}$ and it is called the McMillan degree of $\Phi_{(G,J)}$.

$\begin{bmatrix} G(d) \\ J(d) \end{bmatrix}$ is column reduced if its internal degree is equal to the sum of its column degrees, μ. This means that the McMillan degree of $\Phi_{(G,J)}$ is equal to μ

Lemma: If $\begin{bmatrix} G(d) \\ J(d) \end{bmatrix}$ is not column reduced, there exists a unimodular matrix $U(d)$ such that

$$\begin{bmatrix} \widetilde{G}(d) \\ \widetilde{J}(d) \end{bmatrix} = \begin{bmatrix} G(d) \\ J(d) \end{bmatrix} U(d)$$

is column reduced. Then $\Phi_{(\widetilde{G},\widetilde{J})}$ and $\Phi_{(G,J)}$ are equivalent periodic encoding maps and the McMillan degree of $\Phi_{(\widetilde{G},\widetilde{J})}$ is smaller or equal than the McMillan degree of $\Phi_{(G,J)}$.

Example

Consider the periodic code $\mathcal{C}_p = \Phi_{(G,J)}$ with

$$G(d) = G_0 \quad \text{and} \quad J(d) = J_0 + J_1 d + J_2 d^2 + J_2 d^3,$$

where $G_0, J_0, J_1, J_2 \in \mathbb{F}^{n \times k}$ and G_0 and J_2 are full column rank matrices. Then

$$\begin{bmatrix} G(d) \\ J(d) \end{bmatrix} = \begin{bmatrix} G_0 \\ J_0 + J_1 d + J_2 d^2 + J_2 d^3 \end{bmatrix}$$

is column reduced which implies $\Phi_{(G,J)}$ has switched output McMillan degree equal to the sum of the column degrees of $\begin{bmatrix} G(d) \\ J(d) \end{bmatrix}$, which is equal to $3k$.

Example (contd)

The corresponding lifted code has encoder

$$L(d) = \begin{bmatrix} G_0 & 0 \\ J_1 & J_0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ J_2 & J_2 \end{bmatrix} d$$

and therefore

$$L(d) \begin{bmatrix} I_k & 0 \\ -I_k & I_k \end{bmatrix} = \begin{bmatrix} G_0 & 0 \\ J_1 - J_0 & J_0 + J_2 d \end{bmatrix}$$

is another encoder of the lifted code, which means that

$$\widetilde{G}(d) = G_0 \quad \text{and} \quad \widetilde{J}(d) = J_0 + (J_1 - J_0)d + J_2 d^2$$

are such that $\Phi_{(\widetilde{G},\widetilde{J})}$ is another encoding map which originates the periodic code $\mathcal{C}_p$. Since

$$\begin{bmatrix} \widetilde{G}(d) \\ \widetilde{J}(d) \end{bmatrix} = \begin{bmatrix} G_0 \\ J_0 + (J_1 - J_0)d + J_2 d^2 \end{bmatrix}$$

is also column reduced, we have that the switched output McMillan degree of $\Phi_{(\widetilde{G},\widetilde{J})}$ is equal to $2k$.

Joachim,

Ettore, Diego, Paula, Raquel and Ricardo

This work is supported by Portuguese funds through the CIDMA - Center for Research and Development in Mathematics and Applications, and the Portuguese Foundation for Science and Technology (FCT-Fundação para a Ciência e a Tecnologia), within project UIDB/04106/2020. Moreover, it was also partially supported by Base Funding - UIDB/00147/2020 and Programmatic funding - UIDP/00147/2020 of the Systems and Technologies Center - SYSTEC - funded by national funds through the FCT/MCTES (PIDDAC). The work of D. Napp was is partially supported by the Spanish grants PID2019-108668GB-I00 of the Ministerio de Ciencia e Innovación of the Gobierno de España and VIGROB-287 of the Universitat d'Alacant.