

# Minimal Trellis Construction for Finite Support Convolutional Ring Codes

Margreta Kuijper and Raquel Pinto\*

<sup>1</sup> Department of EE Engineering, University of Melbourne, VIC 3010, Australia  
m.kuijper@unimelb.edu.au,

<sup>2</sup> Department of Mathematics, University of Aveiro, 3810-193 Aveiro, Portugal  
raquel@ua.pt

**Abstract.** We address the concept of “minimal polynomial encoder” for finite support linear convolutional codes over  $\mathbb{Z}_{p^r}$ . These codes can be interpreted as polynomial modules which enables us to apply results from the 2007-paper [8] to introduce the notions of “ $p$ -encoder” and “minimal  $p$ -encoder”. Here the latter notion is the ring analogon of a row reduced polynomial encoder from the field case. We show how to construct a minimal trellis representation of a delay-free finite support convolutional code from a minimal  $p$ -encoder. We express its number of trellis states in terms of a degree invariant of the code. The latter expression generalizes the wellknown expression in terms of the degree of a delay-free finite support convolutional code over a field to the ring case. The results are also applicable to block trellis realization of polynomial block codes over  $\mathbb{Z}_{p^r}$ , such as CRC codes over  $\mathbb{Z}_{p^r}$ .

**Keywords:** polynomial module, finite ring, row reduced,  $p$ -generator sequence, convolutional code, minimal trellis.

## 1 Introduction

In this paper we consider finite support linear convolutional codes over a finite ring of the type  $\mathbb{Z}_{p^r}$ , where  $r$  is a positive integer and  $p$  is a prime integer. Let  $\mathbb{Z}_{p^r}[z]$  denote, as usual, the ring of polynomials in the indeterminate  $z$  with coefficients in  $\mathbb{Z}_{p^r}$ . Conform [15,16,5,17] we define a *finite support convolutional code* of length  $n$  over  $\mathbb{Z}_{p^r}$  as a submodule of  $\mathbb{Z}_{p^r}^n[z]$ . In case  $\mathcal{C}$  admits a basis, that is, can be written as  $\mathcal{C} = \text{im } G(z)$ , then  $G(z) \in \mathbb{Z}_{p^r}^{k \times n}[z]$  is called an *encoder* for  $\mathcal{C}$  and  $\mathcal{C}$  is said to have *dimension*  $k$ . Note that, for the ring case  $r > 1$ , there exist finite support convolutional codes that do not have an encoder. A simple example over  $\mathbb{Z}_4$  with  $n = 1$  is the code  $\mathcal{C} = \text{span} \{2, 1 + z\}$ .

In this paper we are interested in minimal trellis representations for finite support convolutional codes over  $\mathbb{Z}_{p^r}$ , i.e., trellis representations with a minimal

---

\* The research is partially supported by the *Unidade de Investigação Matemática e Aplicações (UIMA)*, University of Aveiro, Portugal, through the *Programa Operacional Ciência e Tecnologia e Inovação (POCTI)* of the *Fundaçã o para a Ciência e Tecnologia (FCT)*, co-financed by the European Union fund FEDER.

number of trellis states. Since decoders, such as the Viterbi decoder, are based on trellis representations, minimality is a desirable property that leads to low complexity decoding. Convolutional codes over  $\mathbb{Z}_{p^r}$  have obtained a considerable amount of attention in the literature because of their relevance to nonbinary modulation schemes. For  $n = 1$  the class of finite support convolutional codes coincides with the so-called *polynomial block codes*, a terminology from [2]. This class contains all cyclic codes and shortened cyclic codes, i.e., CRC codes, see also [12]. The relevance of polynomial block codes over  $\mathbb{Z}_{p^r}$  was established by the landmark paper [6] which shows that important families of nonlinear binary codes are images under a Gray map of linear codes over the ring  $\mathbb{Z}_4$ , see also [1,14].

In the field case, any delay-free finite support convolutional code (that is, a convolutional code which has an encoder  $G(z)$  with  $G(0)$  full row rank) admits a minimal encoder that gives rise to a minimal trellis representation. Here minimality is defined as “row-reducedness” and a minimal trellis is simply constructed as the controller canonical realization of a row reduced encoder. The number of states in a minimal trellis can then be expressed in terms of the degree of the code which is the sum of the row degrees of a minimal encoder. In this paper we are interested in determining a similar procedure for the ring case.

Although methods to construct a minimal trellis from code sequences carry through from the field case, as in [4], the literature does not provide a practical trellis realization method that starts from a minimal polynomial encoder and parallels the field case. In particular, it is an open problem, as observed in the 2007 paper [17], to express the minimum number of trellis states in terms of the row degrees of a particular polynomial encoder of the code. The reason for this seems to be that an appropriate minimality concept involving “row reducedness” was, until recently, not available for polynomial matrices over  $\mathbb{Z}_{p^r}$ . The recent paper [8] develops the concept of “row reducedness” for polynomial matrices over  $\mathbb{Z}_{p^r}$ . Using this concept we define a particular type of polynomial encoder, called *p-encoder*. We also define the concept of a *delay-free p-encoder*. We show that any delay-free finite support convolutional code over  $\mathbb{Z}_{p^r}$  (“delay-free” meaning that it admits a delay-free *p-encoder*) admits a *minimal p-encoder* whose controller canonical realization is a minimal trellis representation for the code. We find that this minimal trellis exhibits nonlinear features. We give a simple expression for the minimum number of trellis states in terms of the sum of the row degrees of a minimal *p-encoder*. To prove that our practical construction is minimal, we use the minimal trellis of [4] that is constructed from code sequences.

The algorithm of [20,21] also gives a practical trellis construction method but differs from ours in that it considers associated block codes of the type  $\mathcal{C}|_{[0,\ell]}$  and then uses the block trellis algorithm of [18] to build a minimal trellis for  $\mathcal{C}$ . In contrast, our method makes use of the polynomial structure of the convolutional code and gives rise to a simple expression for the minimum number of trellis states in terms of a degree invariant of the code.

In most of the literature on convolutional ring codes, code sequences are Laurent series, so do not necessarily have finite support. In this classical setting it is

natural to assume  $n > k$  and to interpret code sequences as trajectories on the time-axis  $\mathbb{Z}$ , rather than  $\mathbb{Z}_+$ . Also, catastrophicity issues arise that play no role in the finite support case. The reader is referred to our paper [9] for an account on minimal polynomial encoders and minimal trellis construction of convolutional codes over  $\mathbb{Z}_{p^r}$  in this classical setting.

## 2 Preliminaries

A set that plays a fundamental role throughout the paper is the set of “digits”, denoted by  $\mathcal{A}_p = \{0, 1, \dots, p-1\} \subset \mathbb{Z}_{p^r}$ . Recall that any element  $a \in \mathbb{Z}_{p^r}$  can be written uniquely as  $a = \theta_0 + \theta_1 p + \dots + \theta_{r-1} p^{r-1}$ , where  $\theta_\ell \in \mathcal{A}_p$  for  $\ell = 0, \dots, r-1$  (*p-adic expansion*). This fundamental property of the ring  $\mathbb{Z}_{p^r}$  expresses a type of linear independence among the elements  $1, p, \dots, p^{r-1}$ . It leads to the notions of “ $p$ -linear independence” and “ $p$ -generator sequence” for modules in  $\mathbb{Z}_{p^r}^n$ , as developed in the 1996 paper [18]. For example, for the simplest case  $n = 1$ , the elements  $1, p, p^2, \dots, p^{r-1}$  are called “ $p$ -linearly independent” in [18] and the module  $\mathbb{Z}_{p^r} = \text{span} \{1\}$  is written as  $\mathbb{Z}_{p^r} = p\text{-span} \{1, p, p^2, \dots, p^{r-1}\}$ . The module  $\mathbb{Z}_{p^r}$  is said to have “ $p$ -dimension”  $r$ .

In this section we recall the main concepts from [8] on modules in  $\mathbb{Z}_{p^r}^n[z]$ , that are needed in the sequel. We present the notions of  $p$ -basis and  $p$ -dimension of a submodule of  $\mathbb{Z}_{p^r}^n[z]$ , which are extensions from [18]’s notions for submodules of  $\mathbb{Z}_{p^r}^n$ . From [8] we also recall the concept of a reduced  $p$ -basis in  $\mathbb{Z}_{p^r}^n[z]$  that plays a crucial role in this paper.

**Definition 1.** [8] Let  $\{v_1(z), \dots, v_m(z)\} \subset \mathbb{Z}_{p^r}^n[z]$ . A  **$p$ -linear combination** of  $v_1(z), \dots, v_m(z)$  is a vector  $\sum_{j=1}^m a_j(z)v_j(z)$ , where  $a_j(z) \in \mathbb{Z}_{p^r}[z]$  is a polynomial with coefficients in  $\mathcal{A}_p$  for  $j = 1, \dots, m$ . Furthermore, the set of all  $p$ -linear combinations of  $v_1(z), \dots, v_m(z)$  is denoted by  **$p$ -span** $(v_1(z), \dots, v_m(z))$ , whereas the set of all linear combinations of  $v_1(z), \dots, v_m(z)$  with coefficients in  $\mathbb{Z}_{p^r}[z]$  is denoted by **span** $(v_1(z), \dots, v_m(z))$ .

**Definition 2.** [8] An ordered sequence  $(v_1(z), \dots, v_m(z))$  of vectors in  $\mathbb{Z}_{p^r}^n[z]$  is said to be a  **$p$ -generator sequence** if  $p v_m(z) = 0$  and  $p v_i(z)$  is a  $p$ -linear combination of  $v_{i+1}(z), \dots, v_m(z)$  for  $i = 1, \dots, m-1$ .

**Lemma 1.** Let  $(v_1(z), \dots, v_m(z))$  be a  $p$ -generator sequence in  $\mathbb{Z}_{p^r}^n[z]$ . Then  $(v_1(0), \dots, v_m(0))$  is a  $p$ -generator sequence in  $\mathbb{Z}_{p^r}^n$ .

**Theorem 1.** [8] Let  $v_1(z), \dots, v_m(z) \in \mathbb{Z}_{p^r}^n[z]$ . If  $(v_1(z), \dots, v_m(z))$  is a  $p$ -generator sequence then  $p\text{-span}(v_1(z), \dots, v_m(z)) = \text{span}(v_1(z), \dots, v_m(z))$ . In particular,  $p\text{-span}(v_1(z), \dots, v_m(z))$  is a submodule of  $\mathbb{Z}_{p^r}^n[z]$ .

All submodules of  $\mathbb{Z}_{p^r}^n[z]$  can be written as the  $p$ -span of a  $p$ -generator sequence. In fact, if  $M = \text{span}(g_1(z), \dots, g_k(z))$  then  $M$  is the  $p$ -span of the  $p$ -generator sequence  $(g_1(z), p g_1(z), \dots, p^{r-1} g_1(z), \dots, g_k(z), p g_k(z), \dots, p^{r-1} g_k(z))$ .

**Definition 3.** [8] The vectors  $v_1(z), \dots, v_m(z) \in \mathbb{Z}_{p^r}^n[z]$  are said to be  **$p$ -linearly independent** if the only  $p$ -linear combination of  $v_1(z), \dots, v_m(z)$  that equals zero is the trivial one.

**Definition 4.** Let  $M$  be a submodule of  $\mathbb{Z}_{p^r}^n[z]$ , written as a  $p$ -span of a  $p$ -generator sequence  $(v_1(z), \dots, v_m(z))$ . Then  $(v_1(z), \dots, v_m(z))$  is called a  **$p$ -basis** for  $M$  if the vectors  $v_1(z), \dots, v_m(z)$  are  $p$ -linearly independent in  $\mathbb{Z}_{p^r}^n[z]$ .

**Lemma 2.** [8] Let  $M$  be a submodule of  $\mathbb{Z}_{p^r}^n[z]$  and let  $(v_1(z), v_2(z), \dots, v_m(z))$  be a  $p$ -basis for  $M$ . Then each vector of  $M$  is written in a unique way as a  $p$ -linear combination of  $v_1(z), \dots, v_m(z)$ .

**Lemma 3.** Let  $M$  be a submodule of  $\mathbb{Z}_{p^r}^n[z]$  and let  $(v_1(z), v_2(z), \dots, v_m(z))$  be a  $p$ -basis for  $M$ , such that  $v_1(0), \dots, v_m(0)$  are  $p$ -linearly independent in  $\mathbb{Z}_{p^r}^n$ . Let  $(w_1(z), w_2(z), \dots, w_m(z))$  be another  $p$ -basis for  $M$ . Then  $w_1(0), \dots, w_m(0)$  are also  $p$ -linearly independent in  $\mathbb{Z}_{p^r}^n$ .

*Proof.* It follows from Lemma 1 that  $(v_1(0), \dots, v_m(0))$  and  $(w_1(0), \dots, w_m(0))$  are  $p$ -generator sequences in  $\mathbb{Z}_{p^r}^n$ . Define modules  $V$  and  $W$  in  $\mathbb{Z}_{p^r}^n$  by  $V := p$ -span  $(v_1(0), \dots, v_m(0))$  and  $W := p$ -span  $(w_1(0), \dots, w_m(0))$ . Since the  $p$ -generator sequence  $(v_1(z), v_2(z), \dots, v_m(z))$  is a  $p$ -basis for  $M$ , the vector  $w_i(z)$  (with  $i \in \{1, \dots, m\}$ ) can be written as a  $p$ -linear combination of  $v_1(z), \dots, v_m(z)$ . Substituting  $z = 0$ , it now follows that  $w_i(0)$  is a  $p$ -linear combination of  $v_1(0), \dots, v_m(0)$  and therefore  $W$  is a submodule of  $V$ . Vice versa, by the same reasoning,  $V$  is a submodule of  $W$ . Consequently  $W = V$  has  $p$ -dimension  $m$  because of the  $p$ -linear independence of  $v_1(0), \dots, v_m(0)$ . It now follows from Lemma 2.10 of [8] that  $w_1(0), \dots, w_m(0)$  are  $p$ -linearly independent and this proves the lemma.

Next, we recall a particular  $p$ -basis for a submodule of  $\mathbb{Z}_{p^r}^n[z]$ , called “reduced  $p$ -basis”. We first recall the concept of “degree” of a vector in  $\mathbb{Z}_{p^r}^n[z]$ , which is the same as in the field case.

**Definition 5.** Let  $v(z)$  be a nonzero vector in  $\mathbb{Z}_{p^r}^n[z]$ , written as  $v(z) = v_0 + v_1z + \dots + v_dz^d$ , with  $v_i \in \mathbb{Z}_{p^r}^n$ ,  $i = 0, \dots, d$ , and  $v_d \neq 0$ . Then  $v(z)$  is said to have **degree**  $d$ , denoted by  $\deg v(z) = d$ . Furthermore,  $v_d$  is called the **leading coefficient vector** of  $v(z)$ , denoted by  $v^{lc}$ .

**Lemma 4.** [8] Let  $M$  be a submodule of  $\mathbb{Z}_{p^r}^n[z]$ , written as a  $p$ -span of a  $p$ -generator sequence  $(v_1(z), \dots, v_m(z))$  with  $v_1^{lc}, \dots, v_m^{lc}$   $p$ -linearly independent in  $\mathbb{Z}_{p^r}^n$ . Then  $(v_1(z), \dots, v_m(z))$  is a  $p$ -basis for  $M$ .

**Definition 6.** [8] Let  $M$  be a submodule of  $\mathbb{Z}_{p^r}^n[z]$ , written as a  $p$ -span of a  $p$ -generator sequence  $(v_1(z), \dots, v_m(z))$ . Then  $(v_1(z), \dots, v_m(z))$  is called a **reduced  $p$ -basis** for  $M$  if the vectors  $v_1^{lc}, \dots, v_m^{lc}$  are  $p$ -linearly independent in  $\mathbb{Z}_{p^r}^n$ .

A reduced  $p$ -basis in  $\mathbb{Z}_{p^r}^n[z]$  generalizes the concept of row reduced basis from the field case. Moreover, it also leads to the predictable degree property and gives rise to several invariants of  $M$ , see [8]. In particular, the number of vectors in a reduced  $p$ -basis as well as the degrees of these vectors (called  $p$ -degrees), are invariants of  $M$ . Consequently, their sum is also an invariant of  $M$ .

Every submodule  $M$  of  $\mathbb{Z}_{p^r}^n[z]$  has a reduced  $p$ -basis. A constructive proof is given by Algorithm 3.11 in [8] that takes as its input a set of spanning vectors and produces a reduced  $p$ -basis of  $M$ . Moreover, it is easy to see that if the input is already a  $p$ -basis of  $M$ , consisting of  $m$  vectors, then the algorithm produces a reduced  $p$ -basis consisting of  $m$  vectors. Since  $m$  is an invariant of the module, it follows that all  $p$ -bases of  $M$  have the same number of elements. As a result, the next definition is well-defined and not in conflict with the slightly different definition of [8].

**Definition 7.** *The number of elements of a  $p$ -basis of a submodule  $M$  of  $\mathbb{Z}_{p^r}^n[z]$  is called the  $p$ -dimension of  $M$ , denoted as  $p\text{-dim}(M)$ .*

The following lemma will be used in the next section.

**Lemma 5.** *Let  $M = \text{span}(g_1(z), \dots, g_k(z))$  be a submodule of  $\mathbb{Z}_{p^r}^n[z]$ , where  $g_1(z), \dots, g_k(z) \in \mathbb{Z}_{p^r}^n[z]$  are linearly independent. Then  $p\text{-dim } M = rk$ .*

*Proof.* The result follows immediately from the obvious fact that

$$(g_1(z), pg_1(z), \dots, p^{r-1}g_1(z), \dots, g_k(z), pg_k(z), \dots, p^{r-1}g_k(z))$$

is a  $p$ -basis for  $M$ .

### 3 $p$ -Encoders and Trellises

It follows from the preceding section that any finite support convolutional code  $\mathcal{C}$  of length  $n$  admits a  $p$ -basis. In the sequel we denote the  $p$ -dimension (see Definition 7) of  $\mathcal{C}$  by  $\kappa$ . Recall that  $\mathcal{A}_p = \{0, 1, \dots, p-1\} \subset \mathbb{Z}_{p^r}$ .

**Definition 8.** *Let  $\mathcal{C}$  be a finite support convolutional code over  $\mathbb{Z}_{p^r}$  of length  $n$  and  $p$ -dimension  $\kappa$ . Then  $E(z) \in \mathbb{Z}_{p^r}^{\kappa \times n}[z]$  is said to be a  $p$ -encoder of  $\mathcal{C}$  if the rows of  $E(z)$  are a  $p$ -basis for  $\mathcal{C}$ .*

**Definition 9.** *Let  $E(z)$  be a  $p$ -encoder of a finite support convolutional code over  $\mathbb{Z}_{p^r}$  of length  $n$ , such that the rows of  $E(0)$  are a  $p$ -basis in  $\mathbb{Z}_{p^r}^n$ . Then  $E(z)$  is said to be a delay-free  $p$ -encoder.*

The next lemma follows immediately from Lemma 3.

**Lemma 6.** *Let  $\mathcal{C}$  be a finite support convolutional code over  $\mathbb{Z}_{p^r}$  of length  $n$  that admits a delay-free  $p$ -encoder. Then all  $p$ -encoders of  $\mathcal{C}$  are delay-free.*

**Definition 10.** *A finite support convolutional code over  $\mathbb{Z}_{p^r}$  of length  $n$  is said to be a delay-free code if all its  $p$ -encoders are delay-free.*

Not all finite support convolutional codes are delay-free. A simple example over  $\mathbb{Z}_2$  with  $n = 1$  is the code  $\mathcal{C} = \text{span} \{z + z^2\}$ . In fact, convolutional codes that are not delay-free seem to be of limited interest, as they employ an artificially high lag. From now on we focus on delay-free codes.

**Definition 11.** Let  $\mathcal{C}$  be a delay-free finite support convolutional code over  $\mathbb{Z}_{p^r}$  of length  $n$ . Then  $E(z)$  is said to be a **minimal  $p$ -encoder** of  $\mathcal{C}$  if the rows of  $E(z)$  are a reduced  $p$ -basis for  $\mathcal{C}$ .

A minimal  $p$ -encoder for a delay-free finite support convolutional code  $\mathcal{C}$  is obtained by applying Algorithm 3.11 in [8] to any  $p$ -encoder of  $\mathcal{C}$ .

In the sequel, we denote the *leading row coefficient matrix* of a polynomial matrix  $V(z)$  by  $V^{lrc}$ . If a delay-free finite support convolutional code  $\mathcal{C}$  admits an encoder  $G(z)$  such that  $G^{lrc}$  has full row rank, then a minimal  $p$ -encoder is trivially constructed as

$$E(z) = \text{col} (G(z), pG(z), \dots, p^{r-1}G(z)). \tag{1}$$

An important observation is that all delay-free finite support convolutional codes admit a minimal  $p$ -encoder but they do not all admit an encoder  $G(z)$  such that  $G^{lrc}$  has full row rank.

Note that, because of Lemma 5, the  $p$ -dimension  $\kappa$  of a finite support convolutional code of dimension  $k$  equals  $\kappa = rk$ . Also, if such a code is delay-free, it can be easily verified that all its encoders  $G(z)$  have the property that  $G(0)$  has full row rank.

A convolutional code can be represented by a trellis. Formally, we define a *trellis section* as a four-tuple  $X = (\mathbb{Z}_{p^r}^n, S, S', K)$ , where  $S$  and  $S'$  are the *left state set* and *right state set*, respectively, and  $K$  is the *set of branches* which is a subset of  $S \times \mathbb{Z}_{p^r}^n \times S'$ , such that every state is part of at least one branch, see also [4,11,10]. A *trellis* is a sequence  $\mathcal{X} = \{X_t\}_{t \in \mathbb{Z}_+}$  of trellis sections  $X_t = (\mathbb{Z}_{p^r}^n, S_t, S'_t, K_t)$ , such that for all  $t \in \mathbb{Z}_+$ ,  $S'_t = S_{t+1}$  and  $S_0 = \{0\}$ . A *path* through the trellis is a sequence  $(b_0, \dots, b_{t-1}, b_t, b_{t+1}, \dots)$  of branches  $b_t = (s_t, c_t, s_{t+1}) \in K_t$  such that  $b_{t+1}$  starts in the trellis state where  $b_t$  ends, for  $t \in \mathbb{Z}_+$ . The set of all trellis paths that end at the zero state is denoted by  $\pi(\mathcal{X})$ . The mapping  $\lambda : \pi(\mathcal{X}) \mapsto (\mathbb{Z}_{p^r}^n)^{\mathbb{Z}_+}$  assigns to every path  $(b_0, \dots, b_{t-1}, b_t, b_{t+1}, \dots)$  its label sequence  $(c_0, \dots, c_{t-1}, c_t, c_{t+1}, \dots)$ . We say that a sequence  $\{c_t\}_{t \in \mathbb{Z}_+}$  *passes through state  $s$  at time  $t$*  if there exists a corresponding path of branches  $\{b_t\}_{t \in \mathbb{Z}_+}$ , where  $b_t = (s_t, c_t, s_{t+1})$ , such that  $s_t = s$ . A trellis  $\mathcal{X}$  is called a *trellis representation* for a finite support convolutional code  $\mathcal{C}$  if  $\mathcal{C} = \lambda(\pi(\mathcal{X}))$ <sup>1</sup>.

A trellis representation of a finite support convolutional code can be constructed from a  $p$ -encoder of the code. Let us first recall the wellknown controller canonical form. A  $\kappa \times n$  matrix  $E(z)$  is realized in controller canonical form [7] (see also [3, Sect. 5]) as

$$E(z) = B(z^{-1}I - A)^{-1}C + D. \tag{2}$$

---

<sup>1</sup> We identify a polynomial  $\mathbf{c} = c_0 + c_1z + \dots + c_mz^m$  in  $\mathbb{Z}_{p^r}[z]$  with the finite support sequence  $(c_0, c_1, \dots, c_m) \in \mathbb{Z}_{p^r}^{m+1}$ .

Denoting the  $i$ 'th row of  $E(z)$  by  $e_i(z) = \sum_{\ell=0}^{\delta_i} e_{i,\ell} z^\ell$ , where  $e_{i,\ell} \in \mathbb{Z}_{p^r}^{1 \times n}$ , the matrices  $A$ ,  $B$ ,  $C$  and  $D$  in (2) are given by

$$A = \begin{bmatrix} A_1 & & & \\ & \ddots & & \\ & & & A_\kappa \end{bmatrix}, \quad B = \begin{bmatrix} B_1 & & & \\ & \ddots & & \\ & & & B_\kappa \end{bmatrix}, \quad C = \begin{bmatrix} C_1 \\ \vdots \\ C_\kappa \end{bmatrix}, \quad D = \begin{bmatrix} e_{1,0} \\ \vdots \\ e_{\kappa,0} \end{bmatrix},$$

with

$$A_i = \begin{bmatrix} 0 & 1 & & & \\ & \ddots & \ddots & & \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ & & & & 0 \end{bmatrix}, \quad B_i = [1 \ 0 \ \cdots \ 0], \quad C_i = \begin{bmatrix} e_{i,1} \\ \vdots \\ e_{i,\delta_i} \end{bmatrix} \quad \text{for } i = 1, \dots, \kappa. \quad (3)$$

Whenever  $\delta_i = 0$ , the  $i$ th block in  $A$  as well as  $C$  is absent and a zero row occurs in  $B$ . Denoting the sum of the  $\delta_i$ 's by  $\delta$ , it is clear that  $A$  is a  $\delta \times \delta$  nilpotent matrix. The above controller canonical realization can be visualized as a shift-register with  $\delta$  registers or, equivalently, as a trellis representation with  $p^\delta$  trellis states, as expressed in the next definition.

**Definition 12.** Let  $\mathcal{C}$  be a finite support convolutional code over  $\mathbb{Z}_{p^r}$  of length  $n$  and  $p$ -dimension  $\kappa$ , and let  $E(z) \in \mathbb{Z}_{p^r}^{\kappa \times n}[z]$  be a  $p$ -encoder of  $\mathcal{C}$ . Let  $\delta = \sum_{i=1}^{\kappa} \text{rowdeg } e_i(z)$ , where  $e_i(z)$  denotes the  $i$ -th row of  $E(z)$ , and let

$$(A, B, C, D) \in \mathbb{Z}_{p^r}^{\delta \times \delta} \times \mathbb{Z}_{p^r}^{\kappa \times \delta} \times \mathbb{Z}_{p^r}^{\delta \times n} \times \mathbb{Z}_{p^r}^{\kappa \times n}$$

be a controller canonical realization of  $E(z)$  as defined above. Then the **controller canonical trellis** corresponding to  $E(z)$  is defined as  $\mathcal{X}_{E(z)} = \{X_t\}_{t \in \mathbb{Z}_+}$ , where  $X_t = (\mathbb{Z}_{p^r}^n, S_t, S'_t, K_t)$  with

$$S_0 = \{0\} \text{ and } S'_t = \{sA + uB : s \in S_t \text{ and } u \in \mathcal{A}_p^\kappa\}, \quad t \in \mathbb{Z}_+ \quad \text{and}$$

$$K_t = \{(s(t), s(t)C + u(t)D, s(t)A + u(t)B) \mid s(t) \in S_t \text{ and } u(t) \in \mathcal{A}_p^\kappa\}.$$

Note that both inputs and states take their values in a set that is not closed with respect to addition or scalar multiplication (namely  $\mathcal{A}_p^\kappa$  and  $\mathcal{A}_p^\delta$ , respectively).

## 4 Minimal Trellis Construction from a $p$ -Encoder

A trellis representation  $\mathcal{X}$  for a finite support convolutional code  $\mathcal{C}$  is called *minimal* if for all  $t \in \mathbb{Z}_+$  the size of its trellis state set  $S_t$  is minimal among all trellis representations of  $\mathcal{C}$ . It is wellknown how to construct a minimal trellis representation in terms of the code sequences of  $\mathcal{C}$ . In fact, the theory of canonical trellis representations from the field case carries through to the ring case, see [19,4,13,10,11,20]. We recall the construction of such a representation (called *two-sided realization* in [19]), adapting it for our case of finite support codes.

Consider two code sequences  $\mathbf{c} \in \mathcal{C}$  and  $\tilde{\mathbf{c}} \in \mathcal{C}$ . Conform [19], the *concatenation* at time  $t \in \mathbb{Z}_+$  of  $\mathbf{c}$  and  $\tilde{\mathbf{c}}$ , denoted by  $\mathbf{c} \wedge_t \tilde{\mathbf{c}}$ , is defined as

$$\mathbf{c} \wedge_t \tilde{\mathbf{c}}(t') := \begin{cases} \mathbf{c}(t') & \text{for } 0 \leq t' < t \\ \tilde{\mathbf{c}}(t') & \text{for } t' \geq t \end{cases}.$$

We define a relation in  $\mathcal{C}$ , for each  $t \in \mathbb{Z}_+$ , as follows

$$\mathbf{c} \simeq_t \tilde{\mathbf{c}} \Leftrightarrow \mathbf{c} \wedge_t \tilde{\mathbf{c}} \in \mathcal{C}, \tag{4}$$

for  $\mathbf{c}, \tilde{\mathbf{c}} \in \mathcal{C}$ . The linearity of  $\mathcal{C}$  immediately implies that  $\simeq_t$  is an equivalence relation on  $\mathcal{C}$ .

**Definition 13.** Let  $\mathcal{C}$  be a finite support convolutional code over  $\mathbb{Z}_{p^r}$  of length  $n$ . The **canonical trellis** of  $\mathcal{C}$  is defined as  $\mathcal{X}_{\mathcal{C}} = \{X_t\}_{t \in \mathbb{Z}_+}$ , where  $X_t = (\mathbb{Z}_{p^r}^n, S_t, S'_t, K_t)$  with

$$S_t := \mathcal{C} \bmod \simeq_t, \quad S'_t := \mathcal{C} \bmod \simeq_{t+1} \quad \text{and} \quad K_t := \{([c]_t, c(t), [c]_{t+1})\}.$$

It can be shown as in [19,10] that the above trellis is minimal. Intuitively this is explained from the fact that, by construction, states cannot be merged.

In the field case, a minimal trellis representation for a delay-free finite support convolutional code is obtained as the controller canonical trellis realization of a row reduced encoder. The next theorem presents our main result for delay-free finite support convolutional codes over  $\mathbb{Z}_{p^r}$ . It obtains a minimal trellis representation as the controller canonical trellis realization of a minimal  $p$ -encoder  $E(z)$ .

**Theorem 2.** Let  $\mathcal{C}$  be a delay-free finite support convolutional code over  $\mathbb{Z}_{p^r}$  of length  $n$  and  $p$ -dimension  $\kappa$ . Let  $E(z)$  be a minimal  $p$ -encoder for  $\mathcal{C}$ . Denote the  $p$ -degrees of  $\mathcal{C}$  by  $\gamma_i$  for  $i = 1, \dots, \kappa$ , and denote  $\gamma_{max} := \max \{\gamma_i : i = 1, \dots, \kappa\}$  and  $\gamma := \sum_{i=1}^{\kappa} \gamma_i$ . Then the controller canonical trellis  $\mathcal{X}_{E(z)}$ , defined in Definition 12, is a minimal trellis representation for  $\mathcal{C}$ . In particular, the number of trellis states of  $\mathcal{X}_{E(z)}$  at each instant  $t$  equals  $p^\gamma$ , for  $t \geq \gamma_{max}$ .

*Proof.* Consider the mapping  $\Theta_t : S_t \mapsto \mathcal{C} \bmod \simeq_t$ , given by  $\Theta_t(s) := [c]_{\simeq_t}$ , where  $\mathbf{c} \in \mathcal{C}$  passes through state  $s$  at time  $t$ . For every  $t \in \mathbb{Z}_+$ , the mapping  $\Theta_t$  is well-defined since for any  $s$  there exists such a code sequence and any two code sequences that pass through state  $s$  at time  $t$  are obviously equivalent.

Since the canonical trellis  $\mathcal{X}_{\mathcal{C}}$  of Definition 13 is minimal, it suffices to prove that  $\Theta_t$  is a bijection for every  $t \in \mathbb{Z}_+$ . Surjectivity follows immediately from the fact that all code sequences pass through some state at time  $t$ . To prove that  $\Theta_t$  is injective, let  $s$  and  $\tilde{s} \in S_t$  be such that  $\Theta_t(s) = \Theta_t(\tilde{s})$ . Let  $\mathbf{c}$  and  $\tilde{\mathbf{c}}$  be code sequences that pass through  $s$  and  $\tilde{s}$  at time  $t$ , respectively. Then  $\mathbf{c} = \mathbf{u}E(z)$  and  $\tilde{\mathbf{c}} = \tilde{\mathbf{u}}E(z)$ , for some  $\mathbf{u}, \tilde{\mathbf{u}} \in \mathcal{A}_p^\kappa[z]$ . From  $\Theta_t(s) = \Theta_t(\tilde{s})$  it follows that the sequence  $\mathbf{c} \wedge_t \tilde{\mathbf{c}} \in \mathcal{C}$ . Denote its state at time  $t$  by  $s'$  and let  $\mathbf{u}' \in \mathcal{A}_p^\kappa[z]$  be such that  $\mathbf{c} \wedge_t \tilde{\mathbf{c}} = \mathbf{u}'E(z)$ . We now prove that  $s = s'$ , as follows. Firstly, it is clear

that

$$\begin{aligned}
 [c(0) \ c(1) \ \cdots \ c(t-1)] &= [u(0) \ u(1) \ \cdots \ u(t-1)] \begin{bmatrix} D \ BC \ BAC \ \cdots \\ 0 \ D \ BC \ \cdots \\ 0 \ 0 \ D \ \cdots \\ \vdots \\ \vdots \end{bmatrix} \quad (5) \\
 &= [u'(0) \ u'(1) \ \cdots \ u'(t-1)] \begin{bmatrix} D \ BC \ BAC \ \cdots \\ 0 \ D \ BC \ \cdots \\ 0 \ 0 \ D \ \cdots \\ \vdots \\ \vdots \end{bmatrix} \cdot (6)
 \end{aligned}$$

From the fact that the rows of  $D = E(0)$  are  $p$ -linearly independent it then follows that  $u(\ell) = u'(\ell)$  for  $0 \leq \ell \leq t-1$ . As a result  $s = s'$ .

We now prove that  $s = \tilde{s}$ . By the above,  $\mathbf{c} \wedge_t \tilde{\mathbf{c}}$  is a code sequence that passes through  $s$  at time  $t$ . Denote by  $M'$  the degree of  $\mathbf{u}'$  and by  $M''$  the degree of  $\tilde{\mathbf{u}}$ . Let  $M = \max\{M', M''\}$ . By construction the states of  $\tilde{\mathbf{c}}$  and  $\mathbf{c} \wedge_t \tilde{\mathbf{c}}$  are both zero at time  $M + \gamma_{max} + 1$ . Denote by  $s(j)$  the state at time  $j$  of the code sequence  $\mathbf{c} \wedge_t \tilde{\mathbf{c}}$  and by  $\tilde{s}(j)$  the state at time  $j$  of the code sequence  $\tilde{\mathbf{c}}$ . Now recall the formula (3) for the controller canonical form. Since  $s(j) = 0$  for  $j \geq M + \gamma_{max} + 1$ , we have that  $0 = s(M + \gamma_{max})A = \tilde{s}(M + \gamma_{max})A$ , and thus the nonzero components of  $s(M + \gamma_{max})$  and  $\tilde{s}(M + \gamma_{max})$  must be last components in a  $1 \times \gamma_i$ -block. Also,  $\tilde{c}(M + \gamma_{max}) = s(M + \gamma_{max})C = \tilde{s}(M + \gamma_{max})C$ , which means that the last components of the  $1 \times \gamma_i$ -blocks of  $s(M + \gamma_{max})$  and  $\tilde{s}(M + \gamma_{max})$  are equal. This follows from the fact that states only take values in  $\mathcal{A}_p$  and that, by construction, the last rows of the  $\gamma_i \times n$ -blocks of  $C$  are rows from  $E^{lrc}$  and are therefore  $p$ -linearly independent. Thus  $s(M + \gamma_{max}) = \tilde{s}(M + \gamma_{max})$ . Repeating this argument again and again, we conclude that  $s(j) = \tilde{s}(j)$ , for  $j \geq M$ . As a result,  $u(j) = u'(j)$  for  $j = M - \gamma_{max} - 1, \dots, M - 1$ .

If  $t \geq M$  the theorem is proved. Suppose now that  $t < M$ . From the fact that  $s(M) = \tilde{s}(M)$  and that  $u(M-1) = u'(M-1)$ , it follows that  $s(M-1)A = \tilde{s}(M-1)A$  which means that the first  $\gamma_i - 1$  components of the  $1 \times \gamma_i$ -blocks of  $s(M-1)$  and  $\tilde{s}(M-1)$  are equal. On the other hand, since  $s(M-1)C = \tilde{s}(M-1)C = \tilde{c}(M-1) - u(M-1)D$  we conclude, by the same reasoning as before, that also the last components in the  $1 \times \gamma_i$ -blocks of  $s(M-1)$  and  $\tilde{s}(M-1)$  are equal, which means that  $s(M-1) = \tilde{s}(M-1)$ . Repeating this argument again and again, we conclude that  $s = \tilde{s}$ , which proves the theorem. Obviously, the number of trellis states at each instant  $t$  equals  $p^\gamma$ , for  $t \geq \gamma_{max}$ .

*Example 1.* Over  $\mathbb{Z}_4$ : consider the finite support convolutional code  $\mathcal{C}$  of length  $n = 3$ , with encoder

$$G(z) = \begin{bmatrix} g_1(z) \\ g_2(z) \end{bmatrix} = \begin{bmatrix} z^2 + 1 & 1 & 0 \\ 2z & 1 & 2 \end{bmatrix}.$$

The controller canonical trellis associated with  $G(z)$  has  $4^3 = 64$  trellis states.

Note that  $G(0)$  has full row rank but that  $G^{lrc}$  does not have full row rank, that is,  $G(z)$  is not row reduced. In fact, this code does not admit a row reduced encoder. As a result, it is not possible to construct a minimal trellis as a controller canonical realization of an encoder of  $\mathcal{C}$ . We now compute a minimal  $p$ -encoder for  $\mathcal{C}$  from which we construct a minimal trellis.

Firstly, a nonminimal  $p$ -encoder of  $\mathcal{C}$  is given by

$$E(z) = \begin{bmatrix} g_1(z) \\ 2g_1(z) \\ g_2(z) \\ 2g_2(z) \end{bmatrix} = \begin{bmatrix} z^2 + 1 & 1 & 0 \\ 2z^2 + 2 & 2 & 0 \\ 2z & 1 & 2 \\ 0 & 2 & 0 \end{bmatrix}, \quad \text{with } E^{lrc} = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 0 & 0 \\ 2 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix}.$$

Note that the rows of  $E(0)$  constitute a  $p$ -basis in  $\mathbb{Z}_{p^r}^n$ . The row reduction algorithm of [8, Algorithm 3.11] is particularly simple in this case: by adding  $z$  times the third row to the second row, we obtain the following minimal  $p$ -encoder  $\bar{E}(z)$  given by:

$$\bar{E}(z) = \begin{bmatrix} z^2 + 1 & 1 & 0 \\ 2 & z + 2 & 2z \\ 2z & 1 & 2 \\ 0 & 2 & 0 \end{bmatrix} \quad \text{with } \bar{E}^{lrc} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 2 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix}.$$

Indeed, the rows of  $\bar{E}^{lrc}$  are  $p$ -linearly independent. The  $p$ -degrees of  $\mathcal{C}$  are 2, 1, 1, 0, so that their sum  $\gamma$  equals 4. The controller canonical trellis corresponding to  $\bar{E}(z)$  is given by

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}; \quad B = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}; \quad C = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 2 \\ 2 & 0 & 0 \end{bmatrix}; \quad D = \begin{bmatrix} 1 & 1 & 0 \\ 2 & 2 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 0 \end{bmatrix}.$$

By Theorem 2, this trellis is minimal with  $2^4 = 16$  trellis states for  $t \geq \gamma_{max} = 2$ .

## 5 Conclusions

In this paper we focus on polynomial encoders for delay-free finite support convolutional codes over  $\mathbb{Z}_{p^r}$ . We introduce the notion of  $p$ -encoder and show that any delay-free finite support convolutional code  $\mathcal{C}$  over  $\mathbb{Z}_{p^r}$  admits a minimal  $p$ -encoder. We present a simple and efficient method to construct a minimal trellis representation for  $\mathcal{C}$  from such a minimal  $p$ -encoder. The method extends the well-known procedure for constructing minimal trellises for delay-free finite support convolutional codes over a field from a controller canonical realization of a row reduced encoder. In addition, similar to the field case, we obtain an expression for the minimal number of trellis states in terms of the sum of row degrees of a minimal  $p$ -encoder. A major difference with the field case is that our minimal trellis employs a nonlinear state space as well as a nonlinear input space.

Finite support convolutional codes of length  $n = 1$  are also known as polynomial block codes, which includes all cyclic and CRC codes. It follows from our account that minimal block trellises (not allowing code component permutations) of polynomial block codes over  $\mathbb{Z}_{p^r}$  are obtained as minimal trellises of finite support convolutional codes of length  $n = 1$ . It is a topic of future research to investigate the connections of the results of this paper with the literature on cyclic block codes over  $\mathbb{Z}_{p^r}$ , see for example [1,14].

## References

1. Calderbank, A.R., Sloane, N.J.A.: Modular and  $p$ -adic cyclic codes. *Designs, Codes and Cryptography* 6, 21–35 (1995)
2. Clark, G.C., Cain, J.B.: *Error-Correction Coding for Digital Communications*. Plenum Press, New York (1981)
3. Fornasini, E., Pinto, R.: Matrix fraction descriptions in convolutional coding. *Linear Algebra and its Applications* 392, 119–158 (2004)
4. Forney, G.D., Trott, M.D.: The dynamics of group codes: state spaces, trellis diagrams, and canonical encoders. *IEEE Trans. Inf. Th.* 39, 1491–1513 (1993)
5. Gluesing-Luersen, H., Schneider, G.: State space realizations and monomial equivalence for convolutional codes. *Linear Algebra and its Applications* 425, 518–533 (2007)
6. Hammons, A.R., Kumar, P.V., Calderbank, A.R., Sloane, N.J.A., Solé, P.: The  $\mathbb{Z}_4$ -linearity of Kerdock, Preparata, Goethals, and related codes. *IEEE Trans. Inf. Th.* 40, 301–319 (1994)
7. Kailath, T.: *Linear Systems*. Prentice Hall, Englewood Cliffs (1980)
8. Kuijper, M., Pinto, R., Polderman, J.W.: The predictable degree property and row reducedness for systems over a finite ring. *Linear Algebra and its Applications* 425, 776–796 (2007)
9. Kuijper, M., Pinto, R.: On minimality of convolutional ring encoders (submitted; av), <http://arxiv.org/abs/0801.3703>
10. Loeliger, H.-A., Forney Jr., G.D., Mittelholzer, T., Trott, M.D.: Minimality and observability of group systems. *Linear Algebra and its Applications* 205-206, 937–963 (1994)
11. Loeliger, H.-A., Mittelholzer, T.: Convolutional codes over groups. *IEEE Trans. Inf. Th.* IT-42, 1660–1686 (1996)
12. Manganiello, F.: Computation of the weight distribution of CRC codes (2006), <http://archiv.org/abs/cs/0607068>
13. Mittelholzer, T.: Minimal encoders for convolutional codes over rings. In: Honory, B., Darnell, M., Farrell, P.G. (eds.) *Communications Theory and Applications*, pp. 30–36. HW Comm. Ltd (1993)
14. Pless, V.S., Qian, Z.: Cyclic codes and quadratic residue codes over  $\mathbb{Z}_4$ . *IEEE Trans. Inf. Th.* 42, 1594–1600 (1996)
15. Rosenthal, J., Schumacher, J.M., York, E.V.: On behaviors and convolutional codes. *IEEE Trans. Inf. Th.* 42, 1881–1891 (1996)
16. Rosenthal, J., Smarandache, R.: Maximum distance separable convolutional codes. *Appl. Algebra Engrg. Comm. Comput.* 10(1), 15–32 (1999)
17. Solé, P., Sison, V.: Quaternary convolutional codes from linear block codes over galois rings. *IEEE Trans. Inf. Th.* 53, 2267–2270 (2007)

18. Vazirani, V.V., Saran, H., Rajan, B.S.: An efficient algorithm for constructing minimal trellises for codes over finite abelian groups. *IEEE Trans. Inf. Th.* 42, 1839–1854 (1996)
19. Willems, J.C.: Models for dynamics. *Dynamics Rep.* 2, 171–282 (1988)
20. Wittenmark, E.: An Encounter with Convolutional Codes over Rings. PhD dissertation, Lund University, Lund, Sweden (1998)
21. Wittenmark, E.: Minimal trellises for convolutional codes over rings. In: *Proceedings 1998 IEEE International Symposium in Information Theory (ISIT 1998)*, Cambridge, USA, p. 15 (1998)