

# Minimal Gröbner bases and the predictable leading monomial property

M. Kuijper\* and K. Schindelar<sup>†‡</sup>

June 25, 2009

## Abstract

In this paper we focus on Gröbner bases over rings for the univariate case. We identify a useful property of minimal Gröbner bases, that we call the “predictable leading monomial (PLM) property”. The property is stronger than “row reducedness” and is crucial in a range of applications. The first part of the paper is tutorial in outlining how the PLM property enables straightforward solutions to classical realization problems of linear systems over fields. In the second part of the paper we use the ideas of [20] on polynomial matrices over the finite ring  $\mathbb{Z}_{p^r}$  (with  $p$  a prime integer and  $r$  a positive integer) in the more general setting of Gröbner bases and introduce the notion of “Gröbner  $p$ -basis” to achieve a predictable leading monomial property over  $\mathbb{Z}_{p^r}$ . This theory finds applications in error control coding over  $\mathbb{Z}_{p^r}$ . Through this approach we are extending the ideas of [20] to a more general context where the user chooses an ordering of polynomial vectors.

## 1 Introduction

Gröbner bases have proved useful tools for dealing with polynomial vectors, with applications particularly in multidimensional system theory. These applications range from controller design to minimal realization of linear systems over fields. Fundamental linear algebraic results on polynomial matrices over fields can be elegantly achieved via the theory of Gröbner bases [1, 4]. In particular, the wellknown Smith-McMillan form as well as the Wiener-Hopf form (“row reducedness”) can be achieved. Using the theory of Gröbner bases these are two sides of the same coin, obtained by choosing a different ordering for polynomial vectors [11, 35].

In [39, 2, 33, 24, 15, 23, 21] a behavioral approach is adopted to solve realization problems over a field. In the first tutorial part of this paper we demonstrate, by

---

\*M. Kuijper is with the Department of Electrical and Electronic Engineering, University of Melbourne, VIC 3010, Australia [m.kuijper@ee.unimelb.edu.au](mailto:m.kuijper@ee.unimelb.edu.au)

<sup>†</sup>K. Schindelar is with the Lehrstuhl D für Mathematik, RWTH Aachen University Templergraben 64, 52062 Aachen, Germany [Kristina.Schindelar@math.rwth-aachen.de](mailto:Kristina.Schindelar@math.rwth-aachen.de)

<sup>‡</sup>This research is partially supported by the Australian Research Council (ARC) and the Deutscher Akademischer Austausch Dienst (DAAD) and co-financed by the Deutsche Forschungsgemeinschaft (DFG)

way of example, how univariate Gröbner theory is used to arrive at a straightforward solution of these problems. More specifically, we illustrate in Example 3.4 that the minimal partial realization problem of [24] boils down to the construction of a minimal Gröbner basis  $G$  for the module  $\mathcal{B}^\perp$  of the “partial impulse behavior”. In fact, the vectors of the basis  $G$  give rise to a kernel representation of  $\mathcal{B}$  from which all minimal partial realizations are parametrized. In a different application, we illustrate in Example 3.3 how minimal Gröbner bases are used for minimal state space realization by inspection. As illustrated in Examples 3.3 and 3.4, minimal partial realizations over finite fields as well as minimal state space realizations over finite fields are relevant to coding theoretic applications, such as minimal trellis construction for convolutional codes over finite fields and decoding of Reed-Solomon block codes over finite fields.

Motivated by coding applications, recent papers [19, 17, 18] consider behaviors over the finite ring  $\mathbb{Z}_{p^r}$ , where  $p$  is a prime integer and  $r$  is a positive integer. In these papers the theory of [20] is put to work to extend the above two problems to systems over the ring  $\mathbb{Z}_{p^r}$ . Note that the ring  $\mathbb{Z}_{p^r}$  has zero divisors which prevents us to rely on the normal workings of linear algebra. In this paper we use some of the ideas of [20] to arrive at a more general theory based on Gröbner bases.

For univariate polynomial matrices over a field  $\mathbb{F}$  it is wellknown that the concept of row reducedness is alternatively formulated in terms of the *predictable-degree property* (terminology from [7]), which is defined below. Recall that the row degree of a row polynomial vector is defined as the maximum of the degrees of its components.

**Definition 1.1** *Let  $R$  be a matrix in  $\mathbb{F}^{m \times q}[x]$  with row degrees  $d_1, \dots, d_m$ . Then  $R$  is said to have the **predictable-degree property** if for any nonzero polynomial vector*

$$a = [ a_1 \quad a_2 \quad \cdots \quad a_m ] \quad \text{in } \mathbb{F}^m[x]$$

*we have that*

$$\text{row degree of } aR = \max_{1 \leq i \leq m} (d_i + \deg a_i).$$

Thus the row degree of  $aR$  can be *predicted* from the degrees in  $a$  and the row degrees of  $R$ . For the field case it is proven in [38, 7] and in [14, Thm 6.3-13] that the above property is equivalent to the property that the *leading row coefficient matrix* of  $R$  has full row rank, i.e., that  $R$  is *row reduced*. It is wellknown (see also below) that minimal Gröbner bases over fields give rise to row reducedness and thus possess the predictable degree property. This makes them useful for many areas of system theory, ranging from controller parametrization to minimal realizations of linear systems over fields [4, 26, 27, 29, 30, 40, 41]. Below, we identify the “predictable leading monomial property” as the Gröbner notion that is stronger than the predictable degree property and thus row reducedness. We generalize this property to systems over the finite ring  $\mathbb{Z}_{p^r}$  which opens up many applications in coding theory involving codes over  $\mathbb{Z}_{p^r}$ , see also [5, 28].

There are several advantages to the Gröbner approach. Firstly, it offers flexibility through the choice of ordering of monomials. This make it possible to derive several dual results at once. In essence, the paper extends the ideas of [20] to different orderings. Secondly, the approach offers scope for extension to other

areas where Gröbner bases are a standard tool, such as multidimensional systems. Finally, a third advantage of the Gröbner approach is that computational packages are available to compute a minimal Gröbner basis over  $\mathbb{Z}_{p^r}$ , such as the SINGULAR computer algebra system [10]. A preliminary version of this paper is [22].

## 2 Preliminaries on Gröbner bases

In this section we introduce Gröbner bases for the univariate case. There are several textbooks that give a good introduction to Gröbner bases. We choose the textbook [1] as our guide since it is general enough to include the ring case, see also [3, 4, 31]. Since we only consider the univariate case we only need a limited set of preliminaries. However, we stress that the univariate case is not a trivial instance of Gröbner theory. Many of the essential deeper features of the theory are already present in the univariate case. In this paper we focus on *properties* of Gröbner bases rather than *construction* of Gröbner bases. More specifically, we explicitly identify some crucial properties of *minimal* Gröbner bases. For more details on construction the reader is referred to [1, 31, 3].

Recall that a ring is called a *noetherian ring* if all of its ideals are finitely generated. A principal ideal ring, such as  $\mathbb{F}[x]$ , where  $\mathbb{F}$  is a field, is a trivial example of a noetherian ring. Another example of a noetherian ring is the ring  $\mathbb{Z}_{p^r}[x]$ , where  $p$  is a prime integer and  $r$  is a positive integer.

Let us first present some preliminaries on polynomials and polynomial vectors with coefficients in a ring  $\mathcal{R}$ . Throughout this paper we assume that  $\mathcal{R}[x]$  is a noetherian ring.

**Definition 2.1** *The degree of a nonzero polynomial  $f \in \mathcal{R}[x]$ , written as  $f(x) = f_0 + f_1x + \dots + f_nx^n$ , is defined as*

$$\deg(f) = \max_{0 \leq i \leq n} \{i \mid f_i \neq 0\}.$$

*The coefficient of the term  $x^{\deg(f)}$  in  $f(x)$  (i.e.,  $f_{\deg f}$ ) is called the **leading coefficient** of  $f$ .*

The concepts of “degree” and “leading coefficient” for polynomials in  $\mathcal{R}[x]$  can be extended to polynomial *vectors* in  $\mathcal{R}^q[x]$ , as follows. Let  $e_1, \dots, e_q$  denote the unit vectors in  $\mathcal{R}^q$ . The elements  $x^\alpha e_i$  with  $i \in \{1, \dots, q\}$  and  $\alpha \in \mathbb{N}_0$  are called **monomials**. Several orderings can be defined on these monomials; in our univariate context we consider two possible orderings adopting the terminology of [1]:

- The **Term Over Position (TOP)** ordering, defined as

$$x^\alpha e_i < x^\beta e_j \quad :\Leftrightarrow \quad \alpha < \beta \text{ or } (\alpha = \beta \text{ and } i > j).$$

- The **Position Over Term (POT)** ordering, defined as

$$x^\alpha e_i < x^\beta e_j \quad :\Leftrightarrow \quad i > j \text{ or } (i = j \text{ and } \alpha < \beta).$$

Clearly, whatever ordering is chosen, every nonzero element  $f \in \mathcal{R}^q[x]$  can be written uniquely as

$$f = \sum_{i=1}^L c_i X_i,$$

where  $L \in \mathbb{N}$ , the  $c_i$ 's are nonzero elements of  $\mathcal{R}$  for  $i = 1, \dots, L$  and the polynomial vectors  $X_1, \dots, X_L$  are monomials, ordered as  $X_1 > \dots > X_L$ . Using the terminology of [1] we define

- $\text{lm}(f) := X_1$  as the **leading monomial** of  $f$
- $\text{lt}(f) := c_1 X_1$  as the **leading term** of  $f$
- $\text{lc}(f) := c_1$  as the **leading coefficient** of  $f$

Writing  $X_1 = x^{\alpha_1} e_{i_1}$ , where  $\alpha_1 \in \mathbb{N}_0$  and  $i_1 \in \{1, \dots, q\}$ , we define

- $\text{lpos}(f) := i_1$  as the **leading position** of  $f$
- $\text{deg}(f) := \alpha_1$  as the **degree** of  $f$ .

Note that for the TOP ordering the degree of  $f$  equals the highest degree of its nonzero components in  $\mathcal{R}[x]$ , whereas for the POT ordering it equals the degree of the first nonzero component. Further, for the POT ordering the leading position of  $f$  is the position of the first nonzero component, whereas for the TOP ordering the leading position of  $f$  is the position of the first nonzero component of highest degree. It is easily verified that the next lemma holds irrespective of whether TOP or POT ordering is used.

**Lemma 2.2** *Let  $f_1, f_2, \dots, f_m$  be nonzero vectors in  $\mathcal{R}^q[x]$  with distinct leading monomials, ordered accordingly as  $f_1 > f_2 > \dots > f_m$ . Then*

$$\text{lt}(f_1 + f_2 + \dots + f_m) = \text{lt}(f_1).$$

There are several ways to define Gröbner bases, here we adopt the definition of [1] which requires us to first define the concept of “leading submodule”. Below we denote the submodule generated by a polynomial vector  $f$  by  $\langle f \rangle$ .

**Definition 2.3** *Let  $G$  be a subset of  $\mathcal{R}^q[x]$ . Then the submodule  $L(G) \subseteq \mathcal{R}^q[x]$ , defined as*

$$L(G) := \langle \text{lt}(g) \mid g \in G \rangle$$

*is called the **leading submodule** of  $G$ .*

For example, for  $q = 2$ , let  $G = \{[x^2 \ x^3]\}$ . Using TOP we obtain  $L(G) = \langle [0 \ x^3] \rangle$ , whereas using POT we get  $L(G) = \langle [x^2 \ 0] \rangle$ .

**Definition 2.4** *Let  $M \subseteq \mathcal{R}^q[x]$  be a module and  $G \subseteq M$ . Then  $G$  is called a **Gröbner basis** of  $M$  if*

$$L(G) = L(M).$$

Thus, the leading terms of the vectors in  $G$  generate the leading terms of all vectors in  $M$ . It is wellknown [1, Corollary 4.1.7] that a Gröbner basis exists for any module in  $\mathcal{R}^q[x]$ . In general, it can be shown that a Gröbner basis  $G$  of a module  $M$  generates  $M$ , see also Lemma 2.8 below. Note, however that

vice versa not every generating set qualifies as a Gröbner basis. For example, in  $\mathbb{Z}_2[x]$ , consider the module  $M = \langle x, x + 1 \rangle = \mathbb{Z}_2[x]$ . The set  $G = \{x, x + 1\}$  is not a Gröbner basis for  $M$  since  $L(G) = \langle x \rangle \neq L(M)$ . It is easily verified that for the case that  $\mathcal{R}$  is a field and  $q = 1$ , any set that contains the generator polynomial of  $M$  is a Gröbner basis of  $M$ . A further observation is that, despite the suggestive terminology, a Gröbner basis is generally not a basis. Thus, any element of  $M$  can be written as a linear combination of elements of  $G$  but the coefficients in this linear combination are not necessarily unique. The following lemma follows immediately from Definition 2.4.

**Lemma 2.5** *Let  $M$  be a submodule of  $\mathcal{R}^q[x]$  with Gröbner basis  $\{g_1, \dots, g_m\}$  and let  $0 \neq f \in M$ . Then there exist  $\alpha_1, \dots, \alpha_s \in \mathbb{N}_0$  and  $c_1, \dots, c_s \in \mathcal{R}$  with  $s \in \{1, \dots, m\}$  such that*

- $\text{lm}(f) = x^{\alpha_i} \text{lm}(g_{j_i})$  for  $i = 1, \dots, s$  and
- $\text{lt}(f) = c_1 x^{\alpha_1} \text{lt}(g_{j_1}) + \dots + c_s x^{\alpha_s} \text{lt}(g_{j_s})$ .

Note that the  $g_{j_i}$ 's of the above lemma all satisfy  $\text{lpos}(g_{j_i}) = \text{lpos}(f)$  and  $\text{lm}(g_{j_i}) \leq \text{lm}(f)$ . The above lemma inspires the next definition.

**Definition 2.6** ([1]) *Let  $f \in \mathcal{R}^q[x]$  and let  $F = \{f_1, \dots, f_s\} \subseteq \mathcal{R}^q[x]$ . Let  $\alpha_1, \dots, \alpha_s \in \mathbb{N}_0$  and let  $c_1, \dots, c_s$  be elements of  $\mathcal{R}$  such that*

1.  $\text{lm}(f) = x^{\alpha_i} \text{lm}(f_i)$  for  $i = 1, \dots, s$  and
2.  $\text{lt}(f) = c_1 x^{\alpha_1} \text{lt}(f_1) + \dots + c_s x^{\alpha_s} \text{lt}(f_s)$ .

Define

$$h := f - (c_1 x^{\alpha_1} f_1 + \dots + c_s x^{\alpha_s} f_s).$$

Then we say that  $f$  **reduces** to  $h$  modulo  $F$  and we write

$$f \xrightarrow{F} h.$$

If  $f$  cannot be reduced modulo  $F$ , we say that  $f$  is **minimal** with respect to  $F$ .

**Lemma 2.7** *Let  $f, h$  and  $F$  be as in the above definition. If  $f \xrightarrow{F} h$  then  $\text{lm}(h) < \text{lm}(f)$ .*

**Proof** From property 1) of Definition 2.6 it follows that property 2) of Definition 2.6 translates into

$$\begin{aligned} \text{lt}(f) &= c_1 x^{\alpha_1} \text{lt}(f_1) + \dots + c_s x^{\alpha_s} \text{lt}(f_s) \\ &= \text{lt}(c_1 x^{\alpha_1} f_1 + \dots + c_s x^{\alpha_s} f_s). \end{aligned}$$

From this, it immediately follows that

$$\text{lm}(h) = \text{lm}(f - (c_1 x^{\alpha_1} f_1 + \dots + c_s x^{\alpha_s} f_s)) < \text{lm}(f).$$

□

The next lemma is a corollary of Lemma 2.7 that will prove useful in the sequel.

**Lemma 2.8** *Let  $M$  be a submodule of  $\mathcal{R}^q[x]$  with Gröbner basis  $G$  and let  $0 \neq f \in M$ . Then*

$$f \in \langle g \in G \mid \text{lm}(g) \leq \text{lm}(f) \rangle.$$

**Proof** Define  $h_0 := f$ . By Lemma 2.5 there exists

$$h_1 := f - (c_1 x^{\alpha_1} g_{j_1} + \cdots + c_s x^{\alpha_s} g_{j_s}),$$

such that  $\text{lm}(g_{j_i}) \leq \text{lm}(h_0)$  for  $1 \leq i \leq s$  and  $h_0 \xrightarrow{G} h_1$ . If  $h_1 = 0$  then we are done. If not, repeatedly apply Lemma 2.5 to  $h_i$ , yielding  $h_{i+1}$  for  $i = 1, 2, \dots$ . By Lemma 2.7 we have that  $\text{lm}(h_{i+1}) < \text{lm}(h_i)$  for  $i = 0, 1, 2, \dots$ . As a result, there exists an integer  $N$  such that  $h_N = 0$ . Then

$$h_{N-1} \in \langle g \in G \mid \text{lm}(g) \leq \text{lm}(h_{N-1}) \rangle.$$

By construction, then also  $h_i \in \langle g \in G \mid \text{lm}(g) \leq \text{lm}(h_i) \rangle$  for  $i = 0, \dots, N-1$  (use induction). Since  $h_0 = f$  this proves the lemma.  $\square$

**Definition 2.9** ([1]) *A Gröbner basis  $G$  is called **minimal** if all its elements  $g$  are minimal with respect to  $G \setminus \{g\}$ .*

It is wellknown [1, Exercise 4.1.9] that a minimal Gröbner basis exists for any module in  $\mathcal{R}^q[x]$ . For example, for the case that  $\mathcal{R}$  is a field and  $q = 1$ , the generator polynomial of  $M$  constitutes a minimal Gröbner basis of  $M$ . In general, a minimal Gröbner basis  $G = \{g_1, \dots, g_m\}$  has the convenient property that all leading monomials of the  $g_i$ 's are different (otherwise we can reduce them) so that the  $g_i$ 's can be ordered accordingly.

### 3 The field case

In this section we limit our attention to the case that  $\mathcal{R}$  is a field. It is well-known that Gröbner bases are useful for various applications over fields, including univariate applications. In this section we attribute this usefulness to a particular property of minimal Gröbner bases that we label the ‘‘Predictable Leading Monomial (PLM)’’ property. We consider two particular applications and show, in a tutorial kind of way, how the PLM property is useful for these applications.

As mentioned above, the elements of a minimal Gröbner basis  $G$  in  $\mathcal{R}^q[x]$  can be ordered according to their respective leading monomials. Since  $\mathcal{R}$  is a field this implies that all leading positions of elements of  $G$  are distinct, so that  $G$  has at most  $q$  elements. In fact, it is easily seen that the elements are linearly independent, that is, a minimal Gröbner basis is a basis, see also the proof of Theorem 3.2 below. More specifically, when the POT ordering is used, a minimal Gröbner basis of a module  $M$  corresponds to a full row rank *upper triangular* generator matrix for  $M$ . When the TOP ordering is used, a minimal Gröbner basis  $\{g_1, g_2, \dots, g_m\}$  of a module  $M$  corresponds to a matrix

$$\begin{bmatrix} g_1(x) \\ \vdots \\ g_m(x) \end{bmatrix} = \text{diag}(x^{\deg g_1}, \dots, x^{\deg g_m})B(x),$$

where  $B(x)$  is a proper rational matrix such that  $B(\infty)$  is upper triangular and of full row rank. It should be noted that the upper triangularity is crucial—without this requirement the matrix is called *row reduced* in the literature. Clearly, the row vectors of a row reduced matrix do not necessarily constitute a minimal Gröbner basis. For example, for  $q = 2$  and  $\mathcal{R} = \mathbb{Z}_2$  consider

$$G(x) = \begin{bmatrix} x & x \\ x^2 & 0 \end{bmatrix}.$$

This matrix is clearly row reduced since  $G(x) = \text{diag}(x, x^2)B(x)$  with

$$B(\infty) = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}.$$

However, the row vectors of  $G(x)$  do not constitute a minimal Gröbner basis for their span, since the second row vector can be reduced modulo the first row vector, yielding

$$[x^2 \ 0] - x[x \ x] = [0 \ x^2].$$

Focusing on the case that  $\mathcal{R}$  is a field, in the next theorem we identify an important property of a minimal Gröbner basis. We first introduce the following terminologies.

**Definition 3.1** *Let  $\mathcal{R}$  be a field. Let  $M$  be a submodule of  $\mathcal{R}^q[x]$  and let  $F = \{f_1, \dots, f_s\} \subseteq M$ . Then  $F$  has the **Predictable Degree (PD) property** if for any  $0 \neq f \in M$ , written as*

$$f = a_1 f_1 + \dots + a_s f_s, \tag{1}$$

where  $a_1, \dots, a_s \in \mathcal{R}[x]$ , we have

$$\deg(f) = \max_{1 \leq i \leq s} (\deg(a_i) + \deg(f_i)).$$

Next,  $F$  is said to have the **Predictable Leading Position (PLP) property** if

$$\text{lpos}(f) = \max_{1 \leq i \leq s; a_i \neq 0} \text{lpos}(f_i).$$

Finally,  $F$  is said to have the **Predictable Leading Monomial (PLM) property** if

$$\text{lm}(f) = \max_{1 \leq i \leq s; a_i \neq 0} (\text{lm}(a_i) \text{lm}(f_i)). \tag{2}$$

Note that the PD property is well established in the literature, see [7] where it was first introduced. Above we defined the PLM property as a more general and stronger concept that is natural for minimal Gröbner bases. It can be easily verified that the PLM property holds if and only if both the PD property and the PLP property hold. As we shall see below, in applications such as minimal state space realization the PD property suffices whereas an application such as minimal partial realization/interpolation requires the PLM property.

**Theorem 3.2** *Let  $\mathcal{R}$  be a field. Let  $M$  be a submodule of  $\mathcal{R}^q[x]$  with minimal Gröbner basis  $G$ . Then  $G$  has the Predictable Leading Monomial (PLM) property. In particular,  $G$  is a basis of  $M$ .*

**Proof** Write  $G = \{g_1, \dots, g_m\}$ . Since  $G$  is minimal we may assume that  $g_1 > g_2 > \dots > g_m$ . Let  $f = a_1g_1 + \dots + a_mg_m$ . For simplicity of notation we assume that  $a_i$  is nonzero for  $1 \leq i \leq m$ . Since  $\mathcal{R}$  is a field we have that  $\text{lpos}(a_i g_i) = \text{lpos}(g_i)$  for  $1 \leq i \leq m$ . Also, all leading positions of the  $g_i$ 's are distinct, otherwise we can reduce. As a result, all leading monomials of the  $a_i g_i$ 's are distinct. Thus there exists an ordering

$$a_{j_1} g_{j_1} > a_{j_2} g_{j_2} > \dots > a_{j_m} g_{j_m}.$$

It now follows from Lemma 2.2 that

$$\text{lm}(f) = \text{lm}(a_{j_1} g_{j_1}) = \text{lm}(a_{j_1}) \text{lm}(g_{j_1}) = \max_{1 \leq i \leq m} (\text{lm}(a_i) \text{lm}(g_i)),$$

which proves the PLM property. Finally, to prove that  $G$  is a basis of  $M$ , first observe that  $G$  generates  $M$  by Lemma 2.8. Also, it follows immediately from the PLM property that any nontrivial linear combination of vectors from  $G$  has to be nonzero. We conclude that  $G$  is a basis of  $M$ .  $\square$

Note that in the Gröbner basis literature [1, Thm 1.9.1] a weaker property is usually presented that shows that for any  $f \in M$  there *exist*  $a_1, \dots, a_m$  such that  $\text{lm}(f) = \max_{1 \leq i \leq m} (\text{lm}(a_i) \text{lm}(g_i))$ . A Gröbner basis that possesses this weaker property is called a “strong Gröbner basis” in [28]. From the above it is easy to see that the concepts of “minimal Gröbner basis” and “minimal strong Gröbner basis” coincide for the field case. In the next section we see that the same is true for the ring case  $\mathcal{R} = \mathbb{Z}_{p^r}$ .

The next two examples show two applications over fields where the PD property and the PLM property are useful.

**Example 3.3 : Using minimal Gröbner bases for minimal state space realization—convolutional coding application**

Conform [33, 34, 9], a finite support binary convolutional code of length  $n$  is defined as a submodule of  $\mathbb{Z}_2^n[x]$ . Consider the finite support binary convolutional code  $\mathcal{C}$  of length 3 given by the encoder

$$E(x) = \begin{bmatrix} x^2 + 1 & 1 & 0 \\ x & 0 & 1 \end{bmatrix}.$$

A Viterbi decoder for  $\mathcal{C} = \text{im } E(x)$  is based on a so-called “trellis representation” of  $\mathcal{C}$ , which is essentially a state space realization  $E(x) = B(x^{-1}I - A)^{-1}C + D$ , see [12, 13, 9]. The need for low complexity decoding motivates the use of a trellis representation where the matrix  $A$  is of minimal size. In this example a minimal Gröbner basis for the module  $\mathcal{C}$  is given by  $G = \{g_1, g_2\}$ , where

$$g_1(x) = [x \quad 0 \quad 1] \quad \text{and} \quad g_2(x) = [1 \quad x \quad x].$$

Thus

$$\tilde{E}(x) = \begin{bmatrix} x & 0 & 1 \\ 1 & x & x \end{bmatrix}.$$

is also an encoder for  $\mathcal{C}$ ; its controller canonical realization  $(A, B, C, D)$  is given by inspection as

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

Note that the size of  $A$  equals the sum of the row degrees of  $\tilde{E}(x)$ . Because of the PLM property of  $G$  (or actually the PD property), there exists no encoder of  $\mathcal{C}$  whose sum of row degrees is smaller than 2. For this reason  $(A, B, C, D)$  is a minimal state space realization and the corresponding trellis representation is also minimal. Note that the matrix  $C$  is upper triangular because of the PLM property.

**Example 3.4 : Using minimal Gröbner bases for parametrization of all shortest linear recurrence relations**

Consider the sequence  $S_0, S_1, S_2, S_3, S_4 = 1, 4, 3, 3, 2$  over the field  $\mathbb{Z}_5$ . A polynomial  $d(x)$ , written as  $d(x) = x^L + d_{L-1}x^{L-1} + \dots + d_1x + d_0$ , is called a linear recurrence relation of length  $L$  for  $S_0, S_1, S_2, S_3, S_4$  if

$$S_{L+j} + \sum_{i=1}^L d_{L-i} S_{L+j-i} = 0 \quad \text{for } j = 0, \dots, 5 - L - 1. \quad (3)$$

Defining the *partial impulse response trajectory*  $\mathbf{b}$  on the time-axis  $\mathbb{Z}_+$  as

$$\mathbf{b} = \left( \begin{bmatrix} S_0 \\ 0 \end{bmatrix}, \begin{bmatrix} S_1 \\ 0 \end{bmatrix}, \begin{bmatrix} S_2 \\ 0 \end{bmatrix}, \begin{bmatrix} S_3 \\ 0 \end{bmatrix}, \begin{bmatrix} S_4 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \dots \right), \quad (4)$$

we can reformulate (3) as  $[d(\sigma) \quad -h(\sigma)] \mathbf{b} = 0$ , where  $h(x)$  is a polynomial of degree  $\leq L$  and  $\sigma$  is the backward shift operator, acting on trajectories  $\mathbf{w}$  on  $\mathbb{Z}_+$  as  $(\sigma w)(k) = w(k+1)$ . A linear recurrence relation for  $S_0, S_1, S_2, S_3, S_4$  thus corresponds to a kernel representation

$$[d(\sigma) \quad -h(\sigma)] \mathbf{w} = 0$$

whose behavior includes the so-called *partial impulse response behavior*

$$\mathcal{B} := \text{span} \{ \mathbf{b}, \sigma \mathbf{b}, \sigma^2 \mathbf{b}, \dots, \sigma^5 \mathbf{b} \}, \quad (5)$$

where  $\mathbf{b}$  is defined by (4). The search for shortest linear recurrence relations now translates into a search for an annihilator  $[d(\sigma) \quad -h(\sigma)] \mathbf{w} = 0$  for  $\mathcal{B}$  that has minimal row degree and satisfies  $\deg h \leq \deg d$ . Next, define the polynomial  $S(x)$  as

$$S(x) := S_0 x^5 + S_1 x^4 + S_2 x^3 + S_3 x^2 + S_4 x, \quad (6)$$

and consider the module  $M$  spanned by  $\begin{bmatrix} 1 & -S(x) \end{bmatrix}$  and  $\begin{bmatrix} 0 & x^6 \end{bmatrix}$ . Clearly, these two polynomial vectors are linearly independent annihilators of  $\mathcal{B}$  and thus  $M$  essentially consists of all annihilators of  $\mathcal{B}$ . It is not difficult to see that any minimal Gröbner basis for  $M$  must consist of 2 vectors. Exactly one of these vectors has leading position 1. Because of the PLM property this vector yields a shortest linear recurrence relation. In this example a minimal Gröbner basis for  $M$  is given by  $G = \{g_1, g_2\}$ , where

$$g_1(x) = \begin{bmatrix} 2x + 2 & x^4 - 2x^3 + x \end{bmatrix} \quad \text{and} \quad g_2(x) = \begin{bmatrix} x^2 - 3x - 1 & 4x^2 - 3x \end{bmatrix}.$$

It follows that  $x^2 - 3x - 1$  is a shortest linear recurrence relation for the sequence 1, 4, 3, 3, 2. Even stronger, it follows from the PLM property that a parametrization of all shortest linear recurrence relations for the sequence 1, 4, 3, 3, 2 is given by

$$d(x) = x^2 - 3x - 1 + \theta(2x + 2), \quad \text{where } \theta \in \mathbb{Z}_5.$$

The reader is also referred to [6, 25] where Gröbner bases are employed for similar problems.

An interesting observation is that Theorem 3.2 fails in a multivariate context. Indeed, consider the module  $M = \langle x^2y, xy^2 \rangle$  in  $\mathbb{Z}_2[x, y]$ . It can be verified that  $\{x^2y, xy^2\}$  is a minimal Gröbner basis of  $M$ . However, the element  $x^2y^2 \in M$  can be generated in two different ways, namely  $x^2y^2 = x \cdot xy^2$ , but also  $x^2y^2 = y \cdot x^2y$ . Thus, a minimal Gröbner basis is not necessarily a basis in the multivariate context. In the literature this difficulty is solved via the notion of “Janet bases” [8, 32].

In our univariate context Theorem 3.2 fails when  $\mathcal{R}$  is not a field. Indeed, consider the module  $M := \langle x + 1, 2 \rangle$  in  $\mathbb{Z}_4[x]$ . The set  $\{x + 1, 2\}$  is a minimal Gröbner basis for  $M$ . However, the element  $2 \in M$  can be generated in two different ways, namely  $2 = 0 \cdot (x + 1) + 1 \cdot 2$ , but also  $2 = 2 \cdot (x + 1) + x \cdot 2$ . Thus, a minimal Gröbner basis is not necessarily a basis in the ring case and does not necessarily have the PLM property. In this paper we are interested in solving this difficulty for the special case that  $\mathcal{R}$  is a ring of the type  $\mathbb{Z}_{p^r}$ . For this we seek to make use of the special structure of  $\mathbb{Z}_{p^r}$ . Preliminaries are presented in the next section.

## 4 The ring case

### 4.1 Preliminaries on $\mathbb{Z}_{p^r}$

A set that plays a fundamental role throughout this 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  $a = \theta_0 + p\theta_1 + \dots + p^{r-1}\theta_{r-1}$ , where  $\theta_\ell \in \mathcal{A}_p$  for  $\ell = 0, \dots, r - 1$  (*p-adic expansion*).

Next, an element  $a$  in  $\mathbb{Z}_{p^r}$  is said to have **order**  $k$  if the additive subgroup generated by  $a$  has  $p^k$  elements. Elements of order  $r$  are called **units**. Thus the elements  $1, p, p^2, \dots, p^{r-1}$  have orders  $r, r - 1, r - 2, \dots, 1$ , respectively. In this paper we extend the notion of “order” to polynomial vectors as follows.

**Definition 4.1** *The **order** of a nonzero polynomial vector  $f \in \mathcal{R}^q[x]$ , is defined as the order of  $\text{lc}(f)$ , denoted as  $\text{ord}(f)$ .*

To deal with the zero divisors occurring in  $\mathbb{Z}_{p^r}$  it is useful to use notions of “ $p$ -linear dependence” and “ $p$ -generator sequence”, first introduced for modules in  $\mathbb{Z}_p^q$  in [37]. These notions are based on the  $p$ -adic expansion property of  $\mathbb{Z}_{p^r}$ , which expresses a type of linear independence among the elements  $1, p, \dots, p^{r-1}$ . The notions presented below are for *polynomial* vectors; they are extensions of [37], first presented in [20]. In this paper we explore the relationship between the notion of “minimal Gröbner basis” and the notion of “ $p$ -basis”.

**Definition 4.2** ([20]) *Let  $\{v_1, \dots, v_N\} \subset \mathbb{Z}_{p^r}^q[x]$ . A **p-linear combination***

*of  $v_1, \dots, v_N$  is a vector  $\sum_{j=1}^N a_j v_j$ , where  $a_j \in \mathbb{Z}_{p^r}[x]$  is a polynomial with coefficients in  $\mathcal{A}_p$  for  $j = 1, \dots, N$ . Furthermore, the set of all  $p$ -linear combinations of  $v_1, \dots, v_N$  is denoted by **p-span** $(v_1, \dots, v_N)$ , whereas the set of all linear combinations of  $v_1, \dots, v_N$  with coefficients in  $\mathbb{Z}_{p^r}[x]$  is denoted by  $\text{span}(v_1, \dots, v_N)$ .*

**Definition 4.3** ([20]) An ordered sequence  $(v_1, \dots, v_N)$  of vectors in  $\mathbb{Z}_{p^r}^q[x]$  is said to be a  **$p$ -generator sequence** if  $p v_N = 0$  and  $p v_i$  is a  $p$ -linear combination of  $v_{i+1}, \dots, v_N$  for  $i = 1, \dots, N - 1$ .

**Theorem 4.4** ([20]) Let  $v_1, \dots, v_N \in \mathbb{Z}_{p^r}^q[x]$ . If  $(v_1, \dots, v_N)$  is a  $p$ -generator sequence then

$$p\text{-span}(v_1, \dots, v_N) = \text{span}(v_1, \dots, v_N).$$

In particular,  $p\text{-span}(v_1, \dots, v_N)$  is a submodule of  $\mathbb{Z}_{p^r}^q[x]$ .

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

**Definition 4.5** ([20]) The vectors  $v_1, \dots, v_N \in \mathbb{Z}_{p^r}^q[x]$  are said to be  **$p$ -linearly independent** if the only  $p$ -linear combination of  $v_1, \dots, v_N$  that equals zero is the trivial one.

**Definition 4.6** Let  $M$  be a submodule of  $\mathbb{Z}_{p^r}^q[x]$ , written as a  $p$ -span of a  $p$ -generator sequence  $(v_1, \dots, v_N)$ . Then  $(v_1, \dots, v_N)$  is called a  **$p$ -basis** of  $M$  if the vectors  $v_1, \dots, v_N$  are  $p$ -linearly independent in  $\mathbb{Z}_{p^r}^q[x]$ .

**Lemma 4.7** ([20]) Let  $M$  be a submodule of  $\mathbb{Z}_{p^r}^q[x]$  and let  $(v_1, v_2, \dots, v_N)$  be a  $p$ -basis of  $M$ . Then each vector of  $M$  is written in a unique way as a  $p$ -linear combination of  $v_1, \dots, v_N$ .

The following definition adjusts the PLM property, introduced for the field case in Definition 3.1, to the specific structure of  $\mathbb{Z}_{p^r}$ . It extends the  $p$ -predictable degree property introduced in [20] to a stronger property that will prove useful in the sequel.

**Definition 4.8** Let  $M$  be a submodule of  $\mathbb{Z}_{p^r}^q[x]$  and let  $F = \{f_1, \dots, f_s\} \subseteq M$ . Then  $F$  has the  **$p$ -Predictable Degree ( $p$ -PD) property** if for any  $0 \neq f \in M$ , written as

$$f = a_1 f_1 + \dots + a_s f_s, \quad (7)$$

where  $a_1, \dots, a_s \in \mathcal{A}_p[x]$ , we have

$$\deg(f) = \max_{1 \leq i \leq s} (\deg(a_i) + \deg(f_i)).$$

Next,  $F$  is said to have the  **$p$ -Predictable Leading Position ( $p$ -PLP) property** if

$$\text{lpos}(f) = \max_{1 \leq i \leq s; a_i \neq 0} \text{lpos}(f_i).$$

Finally,  $F$  is said to have the  **$p$ -Predictable Leading Monomial ( $p$ -PLM) property** if

$$\text{lm}(f) = \max_{1 \leq i \leq s; a_i \neq 0} (\text{lm}(a_i) \text{lm}(f_i)).$$

Note that in the above definition  $a_i \in \mathcal{A}_p[x]$  rather than  $a_i \in \mathcal{R}[x]$  as in Definition 3.1. In analogy with the field case it is easily seen that the  $p$ -PLM property holds if and only if both the  $p$ -PD property and the  $p$ -PLP property hold.

## 4.2 Main result

As noted before, a minimal Gröbner basis  $G = \{g_1, \dots, g_m\}$  has the convenient property that its elements can be ordered as  $g_1 > \dots > g_m$  since their leading monomials are distinct. Unlike the field case, a minimal Gröbner basis of a module in  $\mathbb{Z}_{p^r}^q[x]$  is *not* a basis. In fact, the leading positions of its elements are not necessarily distinct. We have the following lemma.

**Lemma 4.9** *Let  $M$  be a submodule of  $\mathbb{Z}_{p^r}^q[x]$  with minimal Gröbner basis  $G = \{g_1, \dots, g_m\}$ , ordered as  $g_1 > \dots > g_m$ . Let  $j < i$  be such that  $\text{lpos}(g_j) = \text{lpos}(g_i)$ . Then  $\deg g_j > \deg g_i$  and  $\text{ord}(g_j) > \text{ord}(g_i)$ . In particular,  $m \leq qr$ .*

**Proof** Since  $\text{lpos}(g_j) = \text{lpos}(g_i)$  and  $g_j > g_i$  we must have that  $\deg(g_j) > \deg(g_i)$ , regardless of whether the TOP ordering or the POT ordering of monomials is used. It then follows that  $\text{ord}(g_j) > \text{ord}(g_i)$ , otherwise  $g_j$  could be reduced by  $g_i$  and this would contradict the fact that  $G$  is a minimal Gröbner basis. This proves the main result of the lemma. Since there are only  $r$  values of  $\text{ord}(g_i)$  possible, it also follows that  $m \leq qr$ .  $\square$

As a result of the previous lemma we can define a sequence of "order differences" as follows.

**Definition 4.10** *Let  $M$  be a submodule of  $\mathbb{Z}_{p^r}^q[x]$  with minimal Gröbner basis  $G = \{g_1, \dots, g_m\}$  ordered as  $g_1 > \dots > g_m$ . For  $1 \leq j \leq m$  define*

$$\beta_j := \text{ord}(g_j) - \text{ord}(g_i),$$

where  $i$  is the smallest integer  $> j$  with  $\text{lpos}(g_i) = \text{lpos}(g_j)$ . If  $i$  does not exist we define  $\beta_j := \text{ord}(g_j)$ . The sequence  $(\beta_1, \dots, \beta_m) \in \mathbb{N}^m$  is called the **sequence of order differences** of  $G$ .

The next theorem shows that the natural ordering of elements of a minimal Gröbner basis yields a  $p$ -generator sequence property. Note that the theorem holds irrespective of whether the TOP or the POT ordering of monomials is used.

**Theorem 4.11** *Let  $M$  be a submodule of  $\mathbb{Z}_{p^r}^q[x]$  with minimal Gröbner basis  $G = \{g_1, \dots, g_m\}$ , ordered as  $g_1 > \dots > g_m$ . Let  $(\beta_1, \dots, \beta_m)$  be the sequence of order differences of  $G$  as per Definition 4.10. Then*

$$(g_1, pg_1, \dots, p^{\beta_1-1}g_1, g_2, pg_2, \dots, p^{\beta_2-1}g_2, \dots, g_m, pg_m, \dots, p^{\beta_m-1}g_m) \quad (8)$$

is a  $p$ -generator sequence whose  $p$ -span equals  $M$ .

**Proof** We first prove that (8) satisfies Definition 4.3. By definition  $\beta_m = \text{ord}(g_m)$ , so that

$$\text{lm}(p^{\beta_m}g_m) < \text{lm}(g_m). \quad (9)$$

Suppose  $p^{\beta_m}g_m \neq 0$ , then according to Lemma 2.5 there exists  $g_i \in G$  such that  $\text{lm}(g_i) \leq \text{lm}(p^{\beta_m}g_m)$ . But then (9) implies that  $\text{lm}(g_i) < \text{lm}(g_m)$  which contradicts  $g_1 > \dots > g_m$ . We conclude that

$$p^{\beta_m}g_m = 0. \quad (10)$$

To prove that (8) satisfies Definition 4.3 it now obviously remains to prove that for  $1 \leq j \leq m-1$ ,

$$p^{\beta_j} g_j \text{ is a } p\text{-linear combination of } g_{j+1}, g_{j+2}, \dots, g_m. \quad (11)$$

For this, we first prove that  $p^{\beta_j} g_j$  is a linear combination of  $g_{j+1}, g_{j+2}, \dots, g_m$ . We distinguish two cases:

case I

$\beta_j = \text{ord } g_j$ . Then  $\text{lm}(p^{\beta_j} g_j) < \text{lm}(g_j)$ , so that, by Lemma 2.8,  $p^{\beta_j} g_j$  is a linear combination of  $g_{j+1}, g_{j+2}, \dots, g_m$ .

case II

$\beta_j < \text{ord } g_j$ , so that  $\text{lm}(p^{\beta_j} g_j) = \text{lm}(g_j)$ . By definition, there exists a smallest integer  $i > j$  with  $\text{lpos}(g_i) = \text{lpos}(g_j)$  and  $\beta_j = \text{ord}(g_j) - \text{ord}(g_i)$ . Observe that then  $\text{ord}(p^{\beta_j} g_j) = \text{ord}(g_i)$  and  $\text{deg}(p^{\beta_j} g_j) = \text{deg}(g_j) > \text{deg}(g_i)$  (use Lemma 4.9), whereas  $\text{lpos}(p^{\beta_j} g_j) = \text{lpos}(g_j) = \text{lpos}(g_i)$ . Thus we can find  $a \in \mathbb{Z}_{p^r}[x]$  such that  $\text{lt}(p^{\beta_j} g_j) = \text{lt}(ag_i)$ . As a result,  $\text{lm}(p^{\beta_j} g_j - ag_i) < \text{lm}(p^{\beta_j} g_j) = \text{lm}(g_j)$ . Consequently, by Lemma 2.8,  $p^{\beta_j} g_j - ag_i$  is a linear combination of  $g_{j+1}, g_{j+2}, \dots, g_m$ . Since  $i > j$  it follows that  $p^{\beta_j} g_j$  is also a linear combination of  $g_{j+1}, g_{j+2}, \dots, g_m$ .

Thus for  $1 \leq j \leq m-1$

$$p^{\beta_j} g_j \text{ is a linear combination of } g_{j+1}, \dots, g_m. \quad (12)$$

Finally, we prove by induction that (11) holds for  $1 \leq j \leq m-1$ . For  $j = m-1$  this follows from (10) and the fact that  $p^{\beta_{m-1}} g_{m-1}$  is a multiple of  $g_m$  because of (12). Now suppose that (11) holds for  $j = j_0 \in \{1, \dots, m-1\}$ . Consider the vector  $p^{\beta_{j_0-1}} g_{j_0-1}$ . By (12) there exist  $a_{j_0}, \dots, a_m \in \mathbb{Z}_{p^r}[x]$  such that

$$p^{\beta_{j_0-1}} g_{j_0-1} = a_{j_0} g_{j_0} + \dots + a_m g_m.$$

Now use the  $p$ -adic decomposition to write

$$a_{j_0} = a_{j_0}^0 + p a_{j_0}^1 + \dots + p^{r-1} a_{j_0}^{r-1},$$

where  $a_{j_0}^i \in \mathcal{A}_p[x]$  for  $0 \leq i \leq r-1$ . Repeatedly using the induction hypothesis it follows that

$$p^{\beta_{j_0-1}} g_{j_0-1} = a_{j_0}^0 g_{j_0} + p\text{-linear combination of } g_{j_0+1}, \dots, g_m.$$

This proves that (11) holds for  $j = j_0 - 1$ , so that, by induction, (8) is a  $p$ -generator sequence.

To prove that its  $p$ -span equals  $M$ , we first note that, by Lemma 2.8, any element of  $M$  can be written as a linear combination of  $g_1, g_2, \dots, g_m$ . Using a similar reasoning as above this can be alternatively written as a  $p$ -linear combination of the vectors in (11).  $\square$

The next lemma follows immediately from Definition 4.10.

**Lemma 4.12** *Let  $M$  be a submodule of  $\mathbb{Z}_{p^r}^q[x]$  with minimal Gröbner basis  $G = \{g_1, \dots, g_m\}$ , ordered as  $g_1 > \dots > g_m$ . Let  $(\beta_1, \dots, \beta_m)$  be the sequence of order differences of  $G$  as per Definition 4.10 and let  $N = \beta_1 + \beta_2 + \dots + \beta_m$ . Let  $(v_1, \dots, v_N)$  be the  $p$ -generator sequence given by (8). Then for any  $i, j \in \{1, \dots, N\}$  with  $i \neq j$  we have*

$$\text{lpos}(v_i) = \text{lpos}(v_j) \Rightarrow \text{ord}(v_i) \neq \text{ord}(v_j).$$

The next theorem presents our main result.

**Theorem 4.13** *Let  $M$ ,  $(\beta_1, \dots, \beta_m)$  and  $\{v_1, \dots, v_N\}$  be defined as in the previous lemma. Then  $\{v_1, \dots, v_N\}$  has the  $p$ -PLM property. In particular,  $(v_1, \dots, v_N)$  is a  $p$ -basis of  $M$  and the  $p$ -dimension of  $M$  is given by*

$$N = \beta_1 + \beta_2 + \dots + \beta_m.$$

**Proof** Let

$$f = a_1v_1 + \dots + a_Nv_N \tag{13}$$

with  $a_1, \dots, a_N \in \mathcal{A}_p[x]$ . For simplicity of notation we assume that  $a_i$  is nonzero for  $1 \leq i \leq N$ . Let us first examine two special cases:

Special case I

All  $g_i$ 's have distinct leading positions. Then the proof is analogous to the field case, i.e., the proof of Theorem 3.2.

Special case II

All  $g_i$ 's have the same leading position. Then all  $v_i$ 's also have the same leading position. By Lemma 4.12 their orders are all different. Now observe that  $\text{ord}(a_iv_i) = \text{ord}(v_i)$  for  $1 \leq i \leq N$  since  $a_i \in \mathcal{A}_p[x]$ . Thus all  $a_iv_i$ 's have different orders. In particular, all  $a_iv_i$ 's of largest degree have different orders, so that their leading coefficients add up to a nonzero element of  $\mathbb{Z}_{p^r}$  (use the  $p$ -adic decomposition). This implies that the  $p$ -PLM property holds.

Let us now consider the general case. By grouping together all vectors  $a_iv_i$  of the same leading position we write

$$f = f_1 + f_2 + \dots + f_q,$$

where  $f_i = 0$  if position  $i$  is not used in (13). As in Special case II above it can be shown that  $\text{lpos}(f_i) = i$  whenever  $f_i \neq 0$ . As a result, the nonzero  $f_i$ 's can be ordered and Lemma 2.2 yields

$$\text{lt}(f) = \text{lt}(f_j) \tag{14}$$

for some nonzero  $f_j$  with  $j \in \{1, \dots, q\}$ . Recall that  $f_j$  is defined as the sum of all vectors in the right hand side of (13) that have leading position  $j$ . It now follows from Special case II above that there exists  $\ell \in \{1, \dots, N\}$  such that  $\text{lm}(f_j) = \text{lm}(a_\ell) \text{lm}(v_\ell)$ . As a result, by equation (14),

$$\text{lm}(f) = \text{lm}(a_\ell) \text{lm}(v_\ell). \tag{15}$$

Evidently  $\text{lm}(f) \leq \max_{1 \leq i \leq N; a_i \neq 0} (\text{lm}(a_i) \text{lm}(f_i))$  so that (15) implies that equality holds. This proves the  $p$ -PLM property.

Finally, to prove that  $(v_1, \dots, v_N)$  is a  $p$ -basis for  $M$ , first observe that  $p$ -span  $(v_1, \dots, v_N) = M$  by Theorem 4.11. Also, it follows immediately from the  $p$ -PLM property that any nontrivial  $p$ -linear combination of vectors in  $\{v_1, \dots, v_N\}$  has to be nonzero. We conclude that  $(v_1, \dots, v_N)$  is a  $p$ -basis of  $M$ , so that  $N = p\text{-dim}(M) = \beta_1 + \beta_2 + \dots + \beta_m$ .  $\square$

It follows from the above theorem that a minimal Gröbner basis  $G$  of a submodule of  $\mathbb{Z}_{p^r}^q[x]$  is a minimal *strong* Gröbner basis in the terminology of [28]. Our theorem above goes one step further in showing how, by restricting coefficients,  $G$  gives rise to a set that has the attributes of a *basis*.

**Definition 4.14** *Let  $M$  be a submodule of  $\mathbb{Z}_{p^r}^q[x]$  with minimal Gröbner basis  $G = \{g_1, \dots, g_m\}$ , ordered as  $g_1 > \dots > g_m$ . Let  $(\beta_1, \dots, \beta_m)$  be the sequence of order differences of  $G$  as per Definition 4.10. Let  $(v_1, v_2, \dots, v_N)$  be the  $p$ -generator sequence given by (8). Then  $(v_1, v_2, \dots, v_N)$  is called a **Gröbner  $p$ -basis** for  $M$ .*

Note that if TOP ordering of monomials is used then a Gröbner  $p$ -basis is a reduced  $p$ -basis in the terminology of [20].

**Example 4.15** *Let  $M$  be a submodule of  $\mathbb{Z}_3^2[x]$  generated by the rows of the following matrix*

$$R = \begin{bmatrix} 1 & 8x^5 + 5x^4 + 5x^3 + 2x^2 + 2x \\ 0 & x^6 \\ 3 & 6x^5 + 6x^4 + 6x^3 + 6x^2 + 6x \\ 0 & 3x^6 \end{bmatrix}.$$

Denote the rows of  $R$  by  $R_1, R_2, R_3$  and  $R_4$ .

- Using the TOP ordering:  
a minimal Gröbner basis  $G = \{g_1, \dots, g_4\}$  of  $M$  is given by the rows of

$$\begin{bmatrix} 8 & \underline{x^5} + 4x^4 + 4x^3 + 7x^2 + 7x \\ x + 5 & \underline{3x^4} + 3x^2 + x \\ \underline{x^2} + 3x + 2 & x^2 + 4x \\ \underline{3x} + 6 & 3x \end{bmatrix}.$$

The sequence of ordered differences  $(\beta_1, \beta_2, \beta_3, \beta_4)$  equals  $(1, 1, 1, 1)$ . By Theorem 4.13, the sequence  $(g_1, g_2, g_3, g_4)$  is a Gröbner  $p$ -basis for  $M$ . Thus, in the terminology of [20], the  $p$ -generator sequence  $(g_1, g_2, g_3, g_4)$  is a reduced  $p$ -basis; it has the  $p$ -PLM property. Furthermore,  $p\text{-dim}(M) = \beta_1 + \beta_2 + \beta_3 + \beta_4 = 4$ .

- Using the POT ordering:  
the vectors  $R_1$  and  $R_2$  form a minimal Gröbner basis. The sequence of ordered differences  $(\beta_1, \beta_2)$  equals  $(2, 2)$ . According to Theorem 4.13, the sequence  $(g_1, 3g_1, g_2, 3g_2)$  is a Gröbner  $p$ -basis for  $M$ ; it has the  $p$ -PLM property. Note that  $\beta_1 + \beta_2$  indeed equals  $4 = p\text{-dim}(M)$ .

Note that the example clearly illustrates a corollary of Theorem 4.13, namely that the sum of the  $\beta_i$ 's under TOP is equal to the sum of the  $\beta_i$ 's under POT.

## 5 Conclusions

Over the years, Gröbner bases have been recognized as a powerful conceptual and computational tool for a wide range of areas within systems & control, coding and signal processing, even when restricted to the univariate case. In this paper we focused on this univariate case. We first recalled the usefulness of minimal Gröbner bases for several applications involving systems over fields. For this, we identified a particular property of a minimal Gröbner basis which we labeled the “Predictable Leading Monomial (PLM)” property.

Subsequently, we turned our attention to systems over the finite ring  $\mathbb{Z}_{p^r}$ . Because of the presence of zero divisors, a minimal Gröbner basis for a module in  $\mathbb{Z}_{p^r}^q[x]$  is not a basis. Inspired by [20], we solved this difficulty by restricting coefficients. Our main result is Theorem 4.13 which leads to the novel concept of “Gröbner  $p$ -basis“ (Definition 4.14). In fact, Theorem 4.13 shows that a Gröbner  $p$ -basis has a particular type of PLM property which can then be applied to yield straightforward solutions to several problems involving systems over  $\mathbb{Z}_{p^r}$ .

As an example, for a module in  $\mathbb{Z}_{p^r}^q[x]$  (interpretable as a finite support convolutional code  $\mathcal{C}$  over  $\mathbb{Z}_{p^r}$  as in [36]) a state space realization (interpretable as a trellis representation of  $\mathcal{C}$ ) with a minimal number of state values can be obtained from a Gröbner  $p$ -basis in much the same way as outlined in Example 3.3 for the field case. This parallels Theorem 2 in [17].

As another example, a parametrization of all shortest linear recurrence relations of a finite sequence over  $\mathbb{Z}_{p^r}$  can be obtained from a Gröbner  $p$ -basis for the corresponding partial impulse response behavior  $\mathcal{B}$  in much the same way as outlined in Example 3.4 for the field case. This parallels Theorem 15 in [19].

An advantage of the Gröbner approach is that computational packages are available to compute a minimal Gröbner basis over  $\mathbb{Z}_{p^r}$ , such as the SINGULAR computer algebra system [10]. Another advantage is that the approach offers flexibility through the choice of ordering of monomials. This make it possible to derive several dual results at once. A topic of future research is to investigate the use of the POT ordering to derive novel results on a Smith-McMillan like form for polynomial matrices over  $\mathbb{Z}_{p^r}$ . These are motivated by issues concerning catastrophicity of convolutional codes over  $\mathbb{Z}_{p^r}$ , see [16].

Another topic of future research is to investigate connections with Janet bases [8, 32] for multivariate Gröbner bases over fields, where restrictions on coefficients are also used.

## References

- [1] W. W. Adams and P. Loustau. *An introduction to Gröbner Bases*, volume 3 of *Graduate Stud. Math.* American Mathematical Society, 1994.
- [2] A.C. Antoulas. Recursive modeling of discrete-time time series. In P. Van Dooren and B. Wyman, editors, *Linear Algebra for Control Theory*, volume 62 of *IMA Volumes*, pages 1–20. Springer-Verlag, 1994.

- [3] M. Brickenstein, A. Dreyer, G. M. Greuel, M. Wedler, and O. Wienand. New developments in the theory of Gröbner bases and applications to formal verification. *Special Issue of the Journal of Pure and Applied Algebra*, submitted.
- [4] B. Buchberger. Gröbner bases: A short introduction for systems theorists. In *Computer Aided Systems Theory EUROCAST 2001*, volume 2178/2008 of *Lecture Notes in Computer Science*, pages 1–19. Springer Berlin / Heidelberg, 2001.
- [5] E. Byrne and P. Fitzpatrick. Gröbner bases over Galois rings with an application to decoding alternant codes. *J. Symbolic Comput.*, 31:565–584, 2001.
- [6] P. Fitzpatrick. On the key equation. *IEEE Trans. Inf. Th.*, 41:1290–1302, 1995.
- [7] G.D. Forney, Jr. Minimal bases of rational vector spaces, with applications to multivariable linear systems. *SIAM J. Control*, 13:493–520, 1975.
- [8] V. P. Gerdt and D. A. Yanovich. Parallel computation of Janet and Gröbner bases over rational numbers. *Programming and Computer Software*, 31, Number 2 / March, 2005.
- [9] H. Gluesing-Luersen and G. Schneider. State space realizations and monomial equivalence for convolutional codes. *Linear Algebra and its Applications*, 425:518–533, 2007.
- [10] G. M. Greuel, G. Pfister, and H. Schrömann. SINGULAR 3.0.4, *a computer algebra system for polynomial computations*. Centre for Computer Algebra, University of Kaiserslautern, 2005. <http://www.singular.uni-kl.de>.
- [11] M. Avelino Insua Hermo. *Varias perspectivas sobre las bases de Gröbner: forma normal de Smith, algoritmo de Berlekamp y álgebras de Leibniz*. PhD thesis, Universidade de Santiago de Compostela, 2005.
- [12] R. Johannesson and Z-X. Wan. A linear algebra approach to minimal convolutional encoders. *IEEE Trans. Inf. Th.*, IT-39:1219–1233, 1993.
- [13] R. Johannesson and K.S. Zigangirov. *Fundamentals of Convolutional Coding*. IEEE Press Series in Digital and Mobile Comm., 1999.
- [14] T. Kailath. *Linear Systems*. Prentice Hall, Englewood Cliffs, N.J., 1980.
- [15] M. Kuijper. Algorithms for decoding and interpolation. In Brian Marcus and Joachim Rosenthal, editors, *Codes, Systems, and Graphical Models*, volume 123 of *The IMA Volumes in Mathematics and its Applications*, pages 265–282. Springer-Verlag, 2001.
- [16] M. Kuijper and R. Pinto. On minimality of convolutional ring encoders. accepted for publication in *IEEE Trans. Inf. Th.*, also available from <http://archiv.org/abs/0801.3703>.

- [17] M. Kuijper and R. Pinto. Minimal trellis construction for finite support convolutional ring codes. In A. Barbero, editor, *Coding Theory and Applications (ICMCTA)*, LN in Computer Science 5228, pages 95–106. Springer, 2008.
- [18] M. Kuijper and R. Pinto. Minimal state diagrams for controllable behaviors over finite rings. In *Proceedings of Control'08*, pages 1–6, Vila Real, Portugal, 21-23 July 2008.
- [19] M. Kuijper and R. Pinto. Parametrization of linear recurrence relations by row reduction for sequences over a finite ring. In *Proc. 18th International Symposium on Mathematical Theory of Networks and Systems (MTNS)*, pages 1–12, Virginia Tech, USA, July 2008.
- [20] M. Kuijper, R. Pinto, and J. W. Polderman. The predictable degree property and row reducedness for systems over a finite ring. *Linear Algebra and its Applications*, 425:776–796, 2007.
- [21] M. Kuijper and J.W. Polderman. Reed-Solomon list decoding from a system theoretic perspective. *IEEE Trans. Inf. Th.*, IT-50:259–271, 2004.
- [22] M. Kuijper and K. Schindelar. Gröbner bases and behaviors over finite rings. submitted (March 2009) to 48th IEEE Conf. Decision and Control, Shanghai, China, 2009.
- [23] M. Kuijper, M. van Dijk, H. Hollmann, and A J. Oostveen. A unifying system-theoretic framework for errors-and-erasures Reed-Solomon decoding. In S. Boztas and I.E. Shparlinski, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, LN in Computer Science 2227, pages 343–352. Springer, 2001.
- [24] M. Kuijper and J.C. Willems. On constructing a shortest linear recurrence relation. *IEEE Trans. Aut. Control*, 42:1554–1558, 1997.
- [25] K. Lee and M.E. O’Sullivan. List decoding of Reed-Solomon codes from a gröbner basis perspective. *J. Symbolic Comput.*, 43:645–658, 2008.
- [26] Z. Lin, L. Xu, and N. K. Bose. A tutorial on Gröbner bases with applications in signals and systems. *IEEE Transactions on circuits and systems*, 55:445–461, 2008.
- [27] K. Mori. A new parametrization method for all stabilizing controllers of nD systems without coprime factorizability. In *Proceedings of the 2003 International Symposium on Circuits and Systems*, pages III-678– III-681. HW Comm. Ltd, 2003.
- [28] G. Norton and A. Salagean. Cyclic codes and minimal strong Gröbner bases over a principal ideal ring. *Finite Fields and their Applications*, 9:237–249, 2003.
- [29] U. Oberst. Multidimensional constant linear systems. *Acta Applicandae Mathematicae*, 20:1–175, 1990.
- [30] H. Park and G. Regensburger, editors. *Gröbner Bases in Control Theory and Signal Processing*. Walter de Gruyter, 2007.

- [31] F. Pauer. Gröbner bases with coefficients in rings. *J. Symbolic Comput.*, 42:no. 11–12, 1003–1011, 2007.
- [32] W. Plesken and D. Robertz. Janet’s approach to presentations and resolutions for polynomials and linear PDE’s. *Archiv der Mathematik*, 84, Number 1 / January, 2005.
- [33] J. Rosenthal, J.M. Schumacher, and E.V. York. On behaviors and convolutional codes. *IEEE Trans. Inf. Th.*, 42:1881–1891, 1996.
- [34] J. Rosenthal and R. Smarandache. Maximum distance separable convolutional codes. *Appl. Algebra Engrg. Comm. Comput*, 10(1):15–32, 1999.
- [35] K. Schindelar and V. Levandovskyy. Computing normal forms using Gröbner bases. submitted (March 2009) to Journal of Symbolic Computation.
- [36] P. Solé and V. Sison. Quaternary convolutional codes from linear block codes over galois rings. *IEEE Trans. Inf. Th.*, 53:2267–2270, 2007.
- [37] V.V. Vazirani, H. Saran, and B.S. Rajan. An efficient algorithm for constructing minimal trellises for codes over finite abelian groups. *IEEE Trans. Inf. Th.*, 42:1839–1854, 1996.
- [38] J.H.M. Wedderburn. *Lectures on matrices*. Dover Phoenix, 1934.
- [39] J.C. Willems. Paradigms and puzzles in the theory of dynamical systems. *IEEE Trans. Aut. Control*, 36:259–294, 1991.
- [40] J. Wood, E. Roger, and D. Owens. Minimum lag descriptions and minimal Gröbner bases. *Systems & Control Letters*, 34:289–293, 1998.
- [41] E. Zerz and V. Lomadze. A constructive solution to interconnection and decomposition problems with multidimensional behaviors. *SIAM J. Control Optim.*, 40:1072–1086, 2001.