Degree structures of polynomial vector modules with applications to systems over fields and rings

Margreta Kuijper

***Abstract*— In this paper we consider polynomial vector modules, i.e., modules in $\mathcal{R}[x]^q$. We are interested in integer invariants of such modules. In the case that $\mathcal{R}$ is a field, one such integer invariant is the "'McMillan degree"' of a module. We consider the wellknown statement that the McMillan degree of a row reduced polynomial matrix equals the sum of its row degrees. We reformulate this statement as a relationship between minimal Gröbner bases of M under different monomial orders (POT and TOP). We investigate the extension of this result to weighted monomial orders and to the case that $\mathcal{R}$ is a finite ring of the type $\mathbb{Z}_{p^r}$, where p is a prime integer and r is a positive integer. These issues are relevant and fundamental to various applications involving codes and sequences over $\mathbb{Z}_{p^r}$.**

I. Introduction and preliminaries

The theory of Gröbner bases for modules in $\mathcal{R}[x]^q$ is generally recognized as a powerful conceptual and computational tool that plays a role similar to Euclidean division for modules in $\mathcal{R}[x]$. Judging by several recent papers [10], [9] that point out the vast range of applications, this recognition seems to be gaining momentum. More specifically, minimal Gröbner bases prove themselves an effective tool for minimal realization and interpolation problems. In recent papers [6], [8], [7] this effectiveness was ascribed to a powerful property of minimal Gröbner bases, explicitly identified as the "Predictable Leading Monomial Property". Before recalling this property let us first recall some terminology and basic results on Gröbner bases.

Recall that a ring is called *Noetherian* if all of its ideals are finitely generated. Let us first present some preliminaries on polynomial vectors with coefficients in a noetherian commutative ring $\mathcal{R}$. Note that $\mathcal{R}[x]$ is then also a noetherian ring. Let $\mathrm{e}_1, \ldots, \mathrm{e}_q$ denote the unit vectors in $\mathcal{R}^q$. The elements $x^\alpha \mathrm{e}_i$ with $i \in \{1, \ldots, q\}$ and $\alpha \in \mathbb{N}_0$ are called **monomials**. The textbook [1] introduces two types of orders on these monomials:

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

$$x^\alpha \mathrm{e}_i < x^\beta \mathrm{e}_j \quad :\Leftrightarrow \quad \alpha < \beta \text{ or } (\alpha = \beta \text{ and } i > j).$$

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

$$x^\alpha \mathrm{e}_i < x^\beta \mathrm{e}_j \quad :\Leftrightarrow \quad i > j \text{ or } (i = j \text{ and } \alpha < \beta).$$

This research is supported by the Australian Research Council (ARC)

M. Kuijper is with the Department of Electrical and Electronic Engineering, University of Melbourne, VIC 3010, Australia m.kuijper@ee.unimelb.edu.au

Clearly, whatever order is chosen, every nonzero element $f \in \mathcal{R}[x]^q$ 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 $i = 1, \ldots, L$ and $X_1, \ldots, X_L$ are monomials, ordered as $X_1 > \cdots > X_L$. Using the terminology of [1] we define

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

Writing $X_1 = x^{\alpha_1} \mathrm{e}_{i_1}$, where $\alpha_1 \in \mathbb{N}_0$ and $i_1 \in \{1, \ldots, q\}$, we define

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

Note that for the TOP order the degree of f equals the highest degree of its nonzero components in $\mathcal{R}[x]$. For the POT order the degree of f equals the degree of the first nonzero component. Further, for the POT order the leading position of f is the position of the first nonzero component, whereas for the TOP order the leading position of f is the position of the first nonzero component of highest degree.

Below we denote the submodule generated by a polynomial vector f by $\langle f \rangle$. 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 term submodule".

Definition I.1 *Let F be a subset of $\mathcal{R}[x]^q$. Then the submodule $\mathrm{L}(F)$, defined as*

$$\mathrm{L}(F) := \langle \mathrm{lt}(f) \mid f \in F \rangle$$

*is called the **leading term submodule** of F.*

Definition I.2 *Let $M \subseteq \mathcal{R}[x]^q$ be a module and $G \subseteq M$. Then G is called a **Gröbner basis** of M if*

$$\mathrm{L}(G) = \mathrm{L}(M).$$

In order to define a concept of minimality we have the following definition.

Definition I.3 ([1, Def. 4.1.1]) *Let $0 \neq f \in \mathcal{R}[x]^q$ and let $F = \{f_1, \ldots, f_s\}$ be a set of nonzero elements of $\mathcal{R}[x]^q$. Let $\alpha_1, \ldots, \alpha_s \in \mathbb{N}_0$ and let $c_1, \ldots, c_s$ be elements of $\mathcal{R}$ such that*

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

Define

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

ISBN 978-963-311-370-7

*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 I.4 ([1, Lemma 4.1.3]) *Let f, h and F be as in the above definition. If $f \xrightarrow{F} h$ then $h = 0$ or $\mathrm{lm}(h) < \mathrm{lm}(f)$.*

Definition I.5 ([1]) *A Gröbner basis G is called **minimal** if all its elements g are minimal with respect to $G \backslash \{g\}$.*

It is wellknown [1, Exercise 4.1.9] that a minimal Gröbner basis exists for any module in $\mathcal{R}[x]^q$. In general, a minimal Gröbner basis $G = \{g_1, \ldots, g_m\}$ has the following convenient property (for a proof see for example [6]).

Lemma I.6 *Let $G = \{g_1, \ldots, g_m\}$ be a minimal Gröbner basis. Then $\mathrm{lm}(g_i) \neq \mathrm{lm}(g_j)$ for all $i, j \in \{1, \ldots, m\}$.*

In the case that $\mathcal{R}$ is a field it is useful to identify another important property of a minimal Gröbner basis.

Definition I.7 *Let $\mathcal{R}$ be a field. Let M be a submodule of $\mathcal{R}[x]^q$ and let $F = \{f_1, \ldots, f_s\} \subseteq M$. Then F has the **Predictable Leading Monomial (PLM) property** if for any $0 \neq f \in M$, written as*

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

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

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

In the Gröbner basis literature usually a weaker property than the above PLM property is presented, namely: for any $f \in M$ there *exist* $a_1, \ldots, a_s \in \mathcal{R}[x]$ such that (1) and (2) hold, see [1, Thm 1.9.1]. In the field case this is clearly equivalent to the PLM property; for this reason the next theorem merely reformulates a result that is essentially wellknown in the literature (for a proof see [6]).

Theorem I.8 *Let $\mathcal{R}$ be a field. Let M be a submodule of $\mathcal{R}[x]^q$ with minimal Gröbner basis G. Then G has the Predictable Leading Monomial (PLM) property. In particular, G is a basis of M.*

Note that the PLM property is somewhat stronger than the well established **predictable degree property** from [2], [3], since it involves not only degree information but also leading position information. Also, the theorem holds irrespective of whether TOP or POT is used. The above PLM property makes minimal Gröbner bases into ideal tools for minimal partial realization and interpolation problems. In particular, the PLM property straightforwardly leads to parametrizations of all minimal solutions.

II. Extension to weighted monomial orders

In this section we wish to introduce the concept of "weight" to the two monomial orders TOP and POT. This is motivated by applications in list decoding of Reed-Solomon codes, see [4] and references therein. Let $n_1, \ldots, n_q$ be integers.

Definition II.1 *The $(\boldsymbol{n_1, \cdots, n_q})$-weighted Term Over Position (TOP) order, is defined as*

$$x^\alpha \mathrm{e}_i < x^\beta \mathrm{e}_j \;\; :\Leftrightarrow \;\; \alpha + \boldsymbol{n_i} < \beta + \boldsymbol{n_j} \;\; \text{or}$$

$$(\alpha + \boldsymbol{n_i} = \beta + \boldsymbol{n_j} \;\; \text{and} \;\; i > j).$$

Again, every nonzero element $f \in \mathcal{R}[x]^q$ 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 $i = 1, \ldots, L$ and the polynomial vectors $X_1, \ldots, X_L$ are monomials, ordered as $X_1 > \cdots > X_L$. Concepts of "leading monomial", "leading term", "leading coefficient" and "leading position" are defined as in the previous section. However, the concept of "degree" needs some care:

Definition II.2 *Let $f \in \mathcal{R}[x]^q$ with $\mathrm{lm}(f) = X_1$, where X_1 is written as $X_1 = x^{\alpha_1} \mathrm{e}_{i_1}$. Then the **weighted degree** of f is defined as* $\mathrm{wdeg}\,(f) := \alpha_1 + n_{i_1}$.

Obviously, for zero weights $n_1 = \cdots = n_q = 0$ the $(n_1, \cdots, n_q)$-weighted TOP order coincides with the TOP order defined in section I. Evidently, Theorem I.8 also applies when the $(n_1, \cdots, n_q)$-weighted TOP order is used. Again, a minimal Gröbner basis can be easily computed using SINGULAR.

The $(n_1, \cdots, n_q)$-weighted POT order is defined in an analogous way; note that, unlike with TOP, the introduction of weights does not change the POT ordering of monomials. In this paper we only need the weighted POT order because we need the associated notion of "'weighted degree"'.

For any module M, it follows from Theorem I.8 that all minimal Gröbner bases of M must have the same number of elements, no matter which monomial order is chosen. Furthermore, we have the following theorem.

Theorem II.3 *Let $\mathcal{R}$ be a field. Let M be a module in $\mathcal{R}[x]^q$ and let $G = \{g_1, \ldots, g_m\}$ be a minimal Gröbner basis of M with respect to the $(n_1, \cdots, n_q)$-weighted TOP order; denote $\ell_i := \mathrm{wdeg}\; g_i$ for $i = 1, \ldots, m$. Let $\tilde{G} = \{\tilde{g}_1, \ldots, \tilde{g}_m\}$ be a minimal Gröbner basis of M with respect to the $(n_1, \cdots, n_q)$-weighted POT order; denote $\tilde{\ell}_i := \mathrm{wdeg}\; \tilde{g}_i$ for $i = 1, \ldots, m$. Then*

$$\sum_{i=1}^{m} \ell_i = \sum_{i=1}^{m} \tilde{\ell}_i.$$

Proof: We first prove the theorem for the case $m = q$. It follows easily from the fact that both G and $\tilde{G}$ are bases for M (in a linear algebraic sense) that there exists a unimodular polynomial matrix $U \in \mathcal{R}[x]^{q \times q}$ such that

$$\mathrm{col}\,\{g_1, \ldots, g_q\} = U \mathrm{col}\,\{\tilde{g}_1, \ldots, \tilde{g}_q\}.$$

Without restrictions we may assume that the leading positions within each Gröbner basis are strictly increasing. Clearly it follows from the above equation that also

$$\text{col}\,\{g_1,\ldots,g_q\}\text{diag}\,\{x^{n_1},\cdots,x^{n_q}\} =$$

$$U\text{col}\,\{\tilde{g}_1,\ldots,\tilde{g}_q\}\text{diag}\,\{x^{n_1},\cdots,x^{n_q}\}.$$

Taking determinants left and right in the above equation now yields the desired result. The general case $m \leq q$ follows analogously. ∎

For zero weights $n_1 = \cdots = n_q = 0$ the above result expresses that the sum of the degrees of a TOP minimal Gröbner basis of a module M coincides with the sum of the degrees of a POT minimal Gröbner basis of M. This result is merely a reformulation of the wellknown fact [3] that the McMillan degree (i.e. maximum degree of the minors) of a row reduced polynomial matrix equals the sum of its row degrees.

III. The ring case

In this section we turn our attention to the case where $\mathcal{R}$ is a finite ring of the form $\mathbb{Z}_{p^r}$ where r is a positive integer and p is a prime integer. This finite ring case is motivated from applications on codes and sequences over $\mathbb{Z}_{p^r}$. It was shown in [6], [8] how a PLM property can be achieved for modules in $\mathbb{Z}_{p^r}[x]^q$. We first recall this theory.

A. Preliminaries on $\mathbb{Z}_{p^r}$

A set that plays a fundamental role in this section is the set of "digits", denoted by $\mathcal{A}_p = \{0,1,\ldots,p-1\} \subset \mathbb{Z}_{p^r}$. Recall that any element $a \in \mathbb{Z}_{p^r}$ can be written uniquely as $a = \theta_0 + p\theta_1 + \cdots + p^{r-1}\theta_{r-1}$, where $\theta_\ell \in \mathcal{A}_p$ for $\ell = 0,\ldots,r-1$ (*p-adic expansion*).

Next, adopting terminology from [11], a scalar a in $\mathbb{Z}_{p^r}$ is said to have **order** k if the additive subgroup generated by a has p^k elements. Scalars of order r are called **units**. Thus the scalars $1, p, p^2, \ldots, p^{r-1}$ have orders $r, r-1, r-2, \ldots, 1$, respectively. Let us now choose a positional monomial order TOP or POT as in section I. Given this monomial order, we extend the above notion of "order" for scalars to polynomial vectors as follows.

Definition III.1 *The **order** of a nonzero polynomial vector $f \in \mathbb{Z}_{p^r}[x]^q$, is defined as the order of the scalar* $\text{lc}(f)$*, denoted as* $\text{ord}\,(f)$.

To deal with zero divisors occurring in $\mathbb{Z}_{p^r}$, it is useful to use notions defined in [5] of "p-linear dependence" and "p-generator sequence". Such notions were first introduced for "constant" modules, i.e., modules in $\mathbb{Z}_{p^r}^q$ in [11].

Definition III.2 ([5]) *Let $\{v_1,\ldots,v_N\} \subset \mathbb{Z}_{p^r}[x]^q$. A **p-linear combination** of $v_1,\ldots,v_N$ is a vector $\sum_{j=1}^{N} a_j v_j$, where $a_j \in \mathcal{A}_p[x]$ for $j = 1,\ldots,N$. Furthermore, the set of all p-linear combinations of $v_1,\ldots,v_N$ is denoted by **p-span**$(v_1,\ldots,v_N)$, whereas the set of all linear combinations of $v_1,\ldots,v_N$ with coefficients in $\mathbb{Z}_{p^r}[x]$ is denoted by* $\text{span}\,(v_1,\ldots,v_N)$.

Definition III.3 ([5]) *An ordered sequence $(v_1,\ldots,v_N)$ of vectors in $\mathbb{Z}_{p^r}[x]^q$ is said to be a **p-generator sequence** if $p\,v_N = 0$ and $p\,v_i$ is a p-linear combination of $v_{i+1},\ldots,v_N$ for $i = 1,\ldots,N-1$.*

Theorem III.4 ([5]) *Let $v_1,\ldots,v_N \in \mathbb{Z}_{p^r}[x]^q$. If $(v_1,\ldots,v_N)$ is a p-generator sequence then*

$$p\text{–span}\,(v_1,\ldots,v_N) = \text{span}\,(v_1,\ldots,v_N).$$

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

All submodules of $\mathbb{Z}_{p^r}[x]^q$ can be written as the p-span of a p-generator sequence. In fact, if $M = \text{span}\,(g_1,\ldots,g_m)$ then M is the p-span of the p-generator sequence $(g_1, pg_1, \ldots, p^{r-1}g_1, \ldots, g_m, pg_m, \ldots, p^{r-1}g_m)$.

Definition III.5 ([5]) *The vectors $v_1,\ldots,v_N \in \mathbb{Z}_{p^r}[x]^q$ are said to be **p-linearly independent** if the only p-linear combination of $v_1,\ldots,v_N$ that equals zero is the trivial one.*

Definition III.6 ([5]) *Let M be a submodule of $\mathbb{Z}_{p^r}[x]^q$, written as a p-span of a p-generator sequence $(v_1,\cdots,v_N)$. Then $(v_1,\cdots,v_N)$ is called a **p-basis** of M if the vectors $v_1,\ldots,v_N$ are p-linearly independent in $\mathbb{Z}_{p^r}[x]^q$. The number of elements of a p-basis is called the **p-dimension** of M, denoted as p–dim (M).*

The following definition adjusts the PLM property, introduced for the field case in Definition I.7, to the specific structure of $\mathbb{Z}_{p^r}$.

Definition III.7 *Let M be a submodule of $\mathbb{Z}_{p^r}[x]^q$ and let $F = \{f_1,\ldots,f_s\} \subseteq M$. Then F has the **p-Predictable Leading Monomial (p-PLM) property** if for any $0 \neq f \in M$, written as*

$$f = a_1 f_1 + \cdots + a_s f_s, \tag{3}$$

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

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

Note that in the above definition the restriction is imposed that $a_i \in \mathcal{A}_p[x]$ rather than $a_i \in \mathcal{R}[x]$ as in Definition I.7.

A minimal Gröbner basis $G = \{g_1,\ldots,g_m\}$ has the convenient property that its elements can be ordered so that $\text{lm}(g_1) > \cdots > \text{lm}(g_m)$ since their leading monomials are distinct. Unlike the field case, a minimal Gröbner basis of a module in $\mathbb{Z}_{p^r}[x]^q$ is *not* a basis. In fact, the leading positions of its elements are not necessarily distinct.

The next theorem is the ring analogon of Theorem I.8: the theorem shows that the natural ordering of elements of a minimal Gröbner basis gives rise to a p-basis. Note that the theorem holds no matter which monomial order is used.

Theorem III.8 *([6]) Let M be a submodule of $\mathbb{Z}_{p^r}[x]^q$ with minimal Gröbner basis $G = \{g_1,\ldots,g_m\}$, ordered so that*

$\mathrm{lm}(g_1) > \cdots > \mathrm{lm}(g_m)$. *For* $1 \leq j \leq m$ *define*

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

where i *is the smallest integer* $> j$ *with* $\mathrm{lpos}(g_i) = \mathrm{lpos}(g_j)$. *If* i *does not exist we define* $\beta_j := \mathrm{ord}\,(g_j)$. *Then*

$$(g_1, pg_1, \cdots, p^{\beta_1 - 1} g_1, g_2, pg_2, \cdots, p^{\beta_2 - 1} g_2, \cdots, \cdots, g_m, pg_m, \cdots, p^{\beta_m - 1} g_m) \quad (4)$$

is a p*-basis of* M *that has the* p*-PLM property. In particular,*

$$N = p\text{-}\dim\,(M) = \beta_1 + \beta_2 + \cdots + \beta_m.$$

In [6] the p-generator sequence given by (4) is called a **minimal Gröbner *p*-basis** of M. Again, the p-PLM property is useful for a range of minimal partial realization and interpolation problems, see [6], [7] for examples.

In the field case we saw that the number of elements of a minimal Gröbner basis is independent of the type of monomial order that is chosen. A similar result holds for the case $\mathcal{R} = \mathbb{Z}_{p^r}$ (see also [6]):

Theorem III.9 *Let* M *be a submodule of* $\mathbb{Z}_{p^r}[x]^q$. *Let* $(v_1, v_2, \ldots, v_N)$ *be a minimal Gröbner* p*-basis for* M *with respect to the POT monomial order. Let* $(\tilde{v}_1, \tilde{v}_2, \ldots, \tilde{v}_{\tilde{N}})$ *be a minimal Gröbner* p*-basis for* M *with respect to the* $(n_1, \ldots, n_q)$*-weighted TOP monomial order. Then*

$$N = \tilde{N}.$$

In other words,

$$\beta_1 + \beta_2 + \cdots + \beta_m = \tilde{\beta}_1 + \tilde{\beta}_2 + \cdots + \tilde{\beta}_{\tilde{m}},$$

where $(\beta_1, \ldots, \beta_m)$ *is the sequence of order differences of* $(v_1, v_2, \ldots, v_N)$ *and* $(\tilde{\beta}_1, \ldots, \tilde{\beta}_m)$ *is the sequence of order differences of* $(\tilde{v}_1, \tilde{v}_2, \ldots, \tilde{v}_N)$.

This result is fundamental and useful because often a POT minimal Gröbner p-basis is easier to compute than a TOP minimal Gröbner p-basis. For example, to compute shortest linear recurrence relations for a finite sequence of n numbers from $\mathbb{Z}_{p^r}$, we consider a module M spanned by $\begin{bmatrix} 0 & x^{n+1} \end{bmatrix}$ and a polynomial vector of the type $\begin{bmatrix} 1 & \star \end{bmatrix}$. Clearly a POT minimal Gröbner p-basis for M has $2r$ elements. It now follows immediately from the above theorem that a TOP minimal Gröbner p-basis for M must also have $2r$ elements. Parametrizations of shortest linear recurrence relations (i.e. minimal partial realizations) over $\mathbb{Z}_{p^r}$ follow from the p-PLM property of a TOP minimal Gröbner p-basis for M, see [6], [7].

We now ask ourselves whether Theorem II.3 from the field case can also be extended to the ring case, i.e. to a module M in $\mathbb{Z}_{p^r}[x]^q$. In other words, does a similar result exist in the ring case that equates the "McMillan degree" of a TOP minimal Gröbner p-basis to the sum of its TOP row degrees? We are particularly interested in submodules M of $\mathbb{Z}_{p^r}[x]^2$ of p-dimension $2r$ because of its relevance to a range of minimal realization and interpolation problems. Let G be a minimal TOP Gröbner p-basis for M and let $\tilde{G}$ be a minimal POT Gröbner p-basis for M. We examine the relationship between the sum of the TOP degrees of G and the sum of the POT degrees of $\tilde{G}$.

References

[1] W. W. Adams and P. Loustaunau. *An introduction to Gröbner Bases*, volume 3 of *Graduate Stud. Math.* American Mathematical Society, 1994.

[2] G.D. Forney. Convolutional codes I: Algebraic structure. *IEEE Trans. Inf. Th*, 16:720–738, 1970. ;correction, vol. IT-17, p.360, 1971.

[3] G.D. Forney, Jr. Minimal bases of rational vector spaces, with applications to multivariable linear systems. *SIAM J. Control*, 13:493–520, 1975.

[4] M. Kuijper and M. Ali. A parametric approach to list decoding of Reed-Solomon codes using interpolation. in preparation; will also be available on: http://arxiv.org.

[5] 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.

[6] M. Kuijper and K. Schindelar. Minimal Gröbner bases and the predictable leading monomial property. *Linear Alg. Appl.* submitted (June 2009). Available: http://arxiv.org/abs/0906.4602v2.

[7] M. Kuijper and K. Schindelar. The predictable leading monomial property for polynomial vectors over a ring. In *Proceedings 2010 IEEE International Symposium in Information Theory (ISIT)*, Austin, Texas, USA, 2010.

[8] M. Kuijper and K. Schindelar. Gröbner bases and behaviors over finite rings. In *Proceedings of 48th IEEE Conf. Decision and Control (CDC'09)*, pages 8101–8106, Shanghai, China, December 2009.

[9] 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.

[10] H. Park and G. Regensburger, editors. *Gröbner Bases in Control Theory and Signal Processing*. Walter de Gruyter, 2007.

[11] 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.