



# Gröbner Bases with Respect to Generalized Term Orders and their Application to the Modelling Problem

FRANZ PAUER<sup>†</sup> AND SANDRO ZAMPIERI<sup>‡</sup>

<sup>†</sup>*Institut für Mathematik, Universität Innsbruck, Austria.*

<sup>‡</sup>*Dipartimento di Elettronica ed Informatica, Università di Padova, Italy*

*(Received 23 May 1995)*

---

We present an algorithm to decide whether a homogeneous linear partial difference equation with constant coefficients provides an unfalsified model for a finite set of observations, which consist in multiindexed signals, known on a finite subset of  $\mathbf{N}^n$ . To this aim we introduce the concept of “generalized term order” and extend the theory of Gröbner bases accordingly.

© 1996 Academic Press Limited

---

## 1. Introduction and Motivation

The modelling problem is a very important issue in system and control theory. It consists in finding a mathematical description (the model) of a phenomenon starting from measured data, making the best possible use of the information contained in the data. A modelling procedure can be simply considered as an algorithm that, within a certain model class, selects the model which provides the best fitting to the observed data. A large number of modelling procedures have been proposed in the literature. They usually differ in the nature of the data which are considered and in the model class in which the model is chosen. An important distinction that can be done is between procedures which work with perfectly known data and procedures which deal with noisy and imprecise data. The first class of procedures is interesting mainly from the theoretical point of view. However, the development of such procedures is an important preliminary step in order to deal with more realistic situations.

In this paper we make the following assumptions. The data consist in multiindexed signals (for instance space-time trajectories) that can be modelled by functions from  $\mathbf{N}^n$  to  $K^q$  (where  $K$  is a field) and they are known only on a subset  $\Delta$  of  $\mathbf{N}^n$ . We want to model these data by homogeneous linear partial difference equations with constant

<sup>†</sup> E-mail: [Franz.Pauer@uibk.ac.at](mailto:Franz.Pauer@uibk.ac.at)

<sup>‡</sup> E-mail: [zampi@dei.unipd.it](mailto:zampi@dei.unipd.it)

coefficients, i.e. equations like

$$\sum_{(i_1, \dots, i_n) \in S} R_{i_1, \dots, i_n} w(t_1 + i_1, \dots, t_n + i_n) = 0,$$

where the unknown  $w \in (K^q)^{\mathbf{N}^n}$  is a function from  $\mathbf{N}^n$  to  $K^q$ ,  $S$  is a finite subset of  $\mathbf{N}^n$ , and, for each  $(i_1, \dots, i_n) \in S$ ,  $R_{i_1, \dots, i_n} \in K^{l \times q}$  is an  $l \times q$ -matrix with entries in the field  $K$ .

The set of solutions of this difference equation is the kernel  $\ker(R)$  of the  $K$ -linear map  $R$  from  $(K^q)^{\mathbf{N}^n}$  to  $(K^l)^{\mathbf{N}^n}$  defined as follows:  $R$  is the  $l \times q$ -matrix

$$\sum_{(i_1, \dots, i_n) \in S} R_{i_1, \dots, i_n} x_1^{i_1} \cdots x_n^{i_n} \in K[x_1, \dots, x_n]^{l \times q}$$

and it specifies a  $K$ -linear map by defining

$$(Rw)(t_1, \dots, t_n) := \sum_{(i_1, \dots, i_n) \in S} R_{i_1, \dots, i_n} w(t_1 + i_1, \dots, t_n + i_n),$$

for all  $w \in (K^q)^{\mathbf{N}^n}$  and  $(t_1, \dots, t_n) \in \mathbf{N}^n$ .

In this setup, given the observations  $v_1, \dots, v_m \in (K^q)^\Delta$ , a homogeneous linear partial difference equation  $Rw = 0$ ,  $R \in K[x_1, \dots, x_n]^{l \times q}$ , is said to be an unfalsified model of  $v_1, \dots, v_m$ , if there exist  $w_1, \dots, w_m \in \ker(R)$  such that  $w_1|_\Delta = v_1, \dots, w_m|_\Delta = v_m$ . In this case the model fits exactly the observations  $v_1, \dots, v_m$  and therefore the problem of finding an unfalsified model is called exact modelling problem. Such a problem, that is a very classical one in the 1D case, i.e. when  $n = 1$  (Willems, 1986; Heij, 1992; Antoulas and Willems, 1991), has been treated in the multidimensional case in Oberst (1993), Zampieri (1994) and Sakata (1988), where Gröbner bases have been heavily used to obtain efficient modelling procedures. Gröbner bases were first introduced by Buchberger in 1965. We refer the reader to Buchberger (1985); Becker and Weispfenning (1993) for a detailed exposition of Gröbner basis theory.

Given a difference equation  $Rw = 0$ ,  $R \in K[x_1, \dots, x_n]^{l \times q}$ , and a set of observations  $v_1, \dots, v_m \in (K^q)^\Delta$ ,  $\Delta \subseteq \mathbf{N}^n$ , it is important to have a procedure to decide whether the given difference equation provides an unfalsified model for the data  $v_1, \dots, v_m$ . Such a procedure can be easily obtained appealing to the theory of Gröbner bases (Zampieri, 1994). However, the applicability of this procedure is restricted to situations in which observations have a support  $\Delta \subset \mathbf{N}^n$  with special structure.

Gröbner bases are defined with respect to a given term order  $<$ , i.e. a total order on the monoid of power-products in  $K[x_1, \dots, x_n]$  which fulfills the following two requirements: 1 is the smallest element and  $r < s$  implies  $rt < st$ , for all power-products  $r, s, t$ . The above mentioned procedure can be applied when  $\Delta$  has the following property:  $a \in \Delta$  and  $x^b < x^a$  implies  $b \in \Delta$ .

It is clear that the class of subsets  $\Delta$  satisfying the previous requirements is very small: for instance for  $n = 2$  the subsets like rectangles, that are very commonly used in the applications, are not included in this class. This motivates the need to extend Gröbner basis theory to a class of more general total orders. In the next two sections we will propose an extension of this theory that seems to cover many cases of the common interest. In the last section we will present the procedure for checking whether a model is unfalsified and we will show explicitly how Gröbner bases can be used in this setup.

For other generalizations of Gröbner bases and other approaches to partial difference equations see Buchberger (1984), Petkovsek (1990) and Stifter (1988).

## 2. Generalized Term Orders

Let  $K$  be a field,  $K[x] := K[x_1, \dots, x_n]$  the commutative polynomial ring over  $K$  and  $T := \{x^i := x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \mid i \in \mathbf{N}^n\}$  the monoid of power-products (or terms) in  $K[x]$ . The monoid  $T$  is isomorphic to  $\mathbf{N}^n$  (with componentwise addition). Let  $Mon(T, \mathbf{Q})$  be the set of monoid-homomorphisms from  $T$  to  $(\mathbf{Q}, +)$ .  $Mon(T, \mathbf{Q})$  is in a natural way a  $n$ -dimensional vector space over  $\mathbf{Q}$ .

For subsets  $M \subseteq Mon(T, \mathbf{Q})$ ,  $N \subseteq T$  we define

$$M^* := \{t \in T \mid \text{for all } \varphi \in M, \varphi(t) \geq 0\},$$

$$N^* := \{\varphi \in Mon(T, \mathbf{Q}) \mid \text{for all } t \in N, \varphi(t) \geq 0\}.$$

Clearly,  $M^*$  is a saturated submonoid of  $T$  (i.e.:  $1 \in M^*$ ;  $s \in M$  and  $t \in M^*$  imply  $st \in M^*$ ;  $n \in \mathbf{N}_{>0}$  and  $t^n \in M^*$  imply  $t \in M^*$ ), and  $N^*$  is a convex cone in  $Mon(T, \mathbf{Q})$ . If  $M$  is finite, then  $M^*$  is a finitely generated monoid (Gordan's Lemma).

Conversely, if  $N$  is a finitely generated saturated submonoid of  $T$ , then there exists a finite subset  $M$  of  $Mon(T, \mathbf{Q})$  such that  $N = M^*$ . Then we say “ $N$  is defined by  $M$ ”. We denote by  $N^\circ$  the set  $\{t \in N \mid \text{for all } \varphi \in N^* \setminus \{0\}, \varphi(t) > 0\}$  (the “interior of  $N$ ”), by  $N^\perp$  the rational vector space  $\{\varphi \in Mon(T, \mathbf{Q}) \mid \text{for all } t \in N, \varphi(t) = 0\}$ , and by  $rk(N)$  (“rank of  $N$ ”) the codimension of  $N^\perp$  in  $Mon(T, \mathbf{Q})$  (i.e.:  $rk(N) = n - \dim_{\mathbf{Q}}(N^\perp)$ ). It is easy to verify that  $rk(N) = n$  if and only if the interior of  $N$  is not empty.

EXAMPLE 2.1. Let  $n = 2$ . Denote by  $y_i$  the monoid-homomorphism from  $T$  to  $\mathbf{Q}$  defined by  $y_i(x_j) = \delta_{ij}$ ,  $1 \leq i, j \leq 2$ . Then  $\{y_1, y_2\}$  is a  $\mathbf{Q}$ -basis of  $Mon(T, \mathbf{Q})$ . Let  $N$  be the monoid generated by  $x_1^2 x_2$  and  $x_1 x_2^2$ . Then  $N$  is not saturated, since  $x_1^3 x_2^3 = (x_1^2 x_2)(x_1 x_2^2) \in N$ , but  $x_1 x_2 \notin N$ .

The convex cone  $M := N^*$  is generated by  $2y_1 - y_2$  and  $2y_2 - y_1$ . Its rank is 2.  $M^*$  is the saturated monoid  $\{x_1^i x_2^j \mid 2i - j \geq 0, 2j - i \geq 0\}$  and its minimal set of generators is  $\{x_1 x_2, x_1^2 x_2, x_1 x_2^2\}$ .

DEFINITION 2.1. A “conic decomposition” of  $T$  is a finite family  $(T_i)_{i \in I}$  of finitely generated saturated submonoids of  $T$  of rank  $n$ , such that

$$\bigcup_{i \in I} T_i = T$$

and

$$rk(T_i \cap T_j) < n, \text{ for all } i, j \in I \text{ with } i \neq j.$$

EXAMPLE 2.2. Let  $n = 2$ , consider  $\mathbf{N}^2$  as subset of  $\mathbf{Q}^2$ , and choose

$$z_1 := (1, 0), z_2 = (z'_2, z''_2), \dots, z_k = (z'_k, z''_k), z_{k+1} := (0, 1) \in \mathbf{N}^2$$

such that  $z'_i/z''_i > z'_{i+1}/z''_{i+1}$ ,  $1 < i \leq k$ . Let  $T_i := \{x_1^{j_1} x_2^{j_2} \mid (j_1, j_2) \text{ is an element of the convex cone generated by } z_i \text{ and } z_{i+1}\}$ ,  $1 \leq i \leq k$ . Then  $(T_i)_{1 \leq i \leq k}$  is a conic decomposition of  $T$ .

DEFINITION 2.2. Let  $(T_i)_{i \in I}$  be a conic decomposition of  $T$ . A “generalized term order” for  $(T_i)_{i \in I}$  is a total order on  $T$  such that

- (i) 1 is the smallest element in  $T$ ,

(ii)  $r < s$  implies  $rt < st$ , for all  $i \in I$ ,  $s, t \in T_i$ , and  $r \in T$ .

REMARK 2.1. If  $|I| = 1$ , then  $T$  is a (trivial) conic decomposition of  $T$ . In this case a generalized term order is a term order.

EXAMPLE 2.3. Let  $u \in (\mathbf{N}_{>0})^n$  and consider the map

$$\phi : \mathbf{N}^n \longrightarrow \mathbf{Q} \quad , \quad a \longmapsto \max_{1 \leq i \leq n} \left( \frac{a_i}{u_i} \right) .$$

Define

$$T_j := \{ x^a \mid \max_{1 \leq i \leq n} \left( \frac{a_i}{u_i} \right) = \frac{a_j}{u_j} \}, \quad 1 \leq j \leq n .$$

Obviously,  $(T_1, \dots, T_n)$  is a conic decomposition of  $T$ . (For  $n = 2$ , we have  $T_1 = \{ x_1^{i_1} x_2^{i_2} \mid i_1 u_2 \geq i_2 u_1 \}$  and  $T_2 = \{ x_1^{i_1} x_2^{i_2} \mid i_1 u_2 \leq i_2 u_1 \}$ ). Let  $<_T$  be a term order on  $T$ . For  $a, b \in \mathbf{N}^n$  we define

$$x^a < x^b \text{ if and only if } \phi(a) < \phi(b) \text{ or } (\phi(a) = \phi(b) \text{ and } x^a <_T x^b).$$

It is easy to verify that  $<$  is a generalized term order for  $(T_1, \dots, T_n)$ .

Note that  $x^a < x^u$  if and only if  $a_1 \leq u_1, \dots, a_n \leq u_n$  and  $a \neq u$ . (If  $a_1 \leq u_1, \dots, a_n \leq u_n$  and  $a \neq u$ , then  $\phi(a) \leq \phi(u) = 1$  and  $x^a <_T x^u$ , hence  $x^a < x^u$ . If  $x^a < x^u$ , then  $\phi(a) \leq \phi(u) = 1$ , hence  $a_1 \leq u_1, \dots, a_n \leq u_n$ ). In other words,  $\{ a \in \mathbf{N}^n \mid x^a \leq x^u \}$  is the set of integer points in the parallelotope generated by  $(u_1, 0, \dots, 0), (0, u_2, 0, \dots, 0), \dots, (0, \dots, 0, u_n)$ .

If  $n \geq 2$ , then the generalized term order defined above is not a term order. Actually, suppose that  $<$  is a term order. Then consider  $a := (u_1 - 1, u_2, u_3, \dots, u_n)$  and  $b := (u_1, u_2 - 1, u_3, \dots, u_n)$ . If  $x_1 < x_2$ , then  $x_1 x^b < x_2 x^b = x^u$ . If  $x_1 > x_2$ , then  $x_2 x^a < x_1 x^a = x^u$ . Hence either  $x_1 x^b < x^u$  or  $x_2 x^a < x^u$ , but

$$\phi((u_1 - 1, u_2 + 1, u_3, \dots, u_n)) = \frac{u_2 + 1}{u_2} > 1 = \phi(u)$$

and

$$\phi((u_1 + 1, u_2 - 1, u_3, \dots, u_n)) = \frac{u_1 + 1}{u_1} > 1 = \phi(u)$$

which leads to a contradiction.

DEFINITION 2.3. Let  $(T_i)_{i \in I}$  be a conic decomposition of  $T$  and let  $<$  be a generalized term order for  $(T_i)_{i \in I}$ . Let  $f = \sum_{t \in T} c_t t$  be a non-zero polynomial in  $K[x]$ ,  $c_t \in K$ . Then we define

$$\begin{aligned} \text{supp}(f) &:= \{ t \in T \mid c_t \neq 0 \} \text{ (the "support of } f \text{")}, \\ \text{lt}(f) &:= \max \text{supp}(f) \text{ (the "leading term of } f \text{")}, \\ \text{lc}(f) &:= \text{the coefficient of } f \text{ at } \text{lt}(f), \\ T_i(f) &:= \{ t \in T \mid \text{lt}(t f) \in T_i \}, \quad 1 \leq i \leq n. \end{aligned}$$

From now on we fix a conic decomposition  $(T_i)_{i \in I}$  of  $T$  and a generalized term order  $<$  for it.

REMARK 2.2. Let  $i \in I$  and  $0 \neq f \in K[x]$ . Then  $T_i(f)$  is stable under the action of  $T_i$  on  $T$  (i.e.:  $s \in T_i$ ,  $t \in T_i(f)$  imply  $st \in T_i(f)$ ), and  $T_i \subseteq T_i(f)$  if and only if  $\text{lt}(f) \in T_i$ .

LEMMA 2.1. *Let  $N$  be a finite subset of  $T$  and let  $i \in I$ . Then there exists a  $p \in T_i$  such that  $pN \subseteq T_i^\circ$ .*

PROOF. Let  $M \subseteq \text{Mon}(T, \mathbf{Q})$  be a finite subset of  $T_i^*$  such that  $T_i$  is defined by  $M$ . Since  $T_i^\circ$  is not empty, there exists a  $t \in T_i$  such that  $\varphi(t) > 0$ , for all  $\varphi \in M$ .

For  $s \in N$  choose  $e_s \in \mathbf{N}_{>0}$  such that  $e_s\varphi(t) + \varphi(s) > 0$ , for all  $\varphi \in M$ . Then  $\varphi(t^{e_s}s) > 0$ , for all  $\varphi \in M$ , hence  $t^{e_s}s \in T_i^\circ$ . Now set  $p := t^e$ , where  $e := \max_{s \in N} e_s$ .

LEMMA 2.2. *Let  $0 \neq f \in K[x]$  and  $s, t \in T_i(f)$ . Then*

$$\frac{lt(tf)}{t} = \frac{lt(sf)}{s} \ (\in \text{supp}(f)) .$$

PROOF. Let  $u, v \in \text{supp}(f)$  such that  $lt(tf) = tu \in T_i$ ,  $lt(sf) = sv \in T_i$ . We have to show:  $u = v$ .

Since  $u, v \in \text{supp}(f)$ ,  $tv \leq tu$  and  $su \leq sv$ . Choose  $p \in T_i$  such that  $pu, pv, ps, pt \in T_i$  (Lemma 2.1). Then

$$tu \in T_i, tv \leq tu, p^2 \in T_i \text{ imply } p^2tv \leq p^2tu$$

and

$$sv \in T_i, su \leq sv, p^2 \in T_i \text{ imply } p^2su \leq p^2sv .$$

Hence

$$(pt)(pv) \leq (pt)(pu) \text{ and } (ps)(pu) \leq (ps)(pv) .$$

This implies

$$(ps)(pt)(pv) \leq (ps)(pt)(pu) \text{ and } (pt)(ps)(pu) \leq (pt)(ps)(pv)$$

Therefore  $(ps)(pt)(pv) = (pt)(ps)(pu)$  and  $u = v$ .

DEFINITION 2.4. Let  $0 \neq f \in K[x]$ ,  $i \in I$  and  $t \in T_i(f)$ . Then define

$$lt_i(f) := \frac{lt(tf)}{t} \text{ and } lc_i(f) := lc(tf) .$$

REMARK 2.3. By Lemma 2.2,  $lt_i(f)$  is well-defined (i.e. it does not depend on the choice of  $t \in T_i(f)$ ). Furthermore,  $lc_i(f)$  is the coefficient of  $f$  at  $lt_i(f)$ . We can compute  $lt_i(f)$  in the following way: choose  $p \in T_i$  such that  $p \cdot \text{supp}(f) \subseteq T_i$  (cf. Lemma 2.1). Then  $lt(pf) \in T_i$  and  $lt_i(f) = \frac{lt(pf)}{p}$ .

EXAMPLE 2.4. Let  $n = 2$  and consider the generalized term order defined in Example 2.3, where  $u := (1, 1)$  and  $<_T$  is the lexicographic order with  $x_1 > x_2$ . Then  $T_1 = \{x_1^i x_2^j \mid i \geq j\}$  and  $T_2 = \{x_1^i x_2^j \mid i \leq j\}$ . Let  $f := x_1^2 + 2x_1 x_2$ . Then  $lt(f) = x_1^2$ ,  $T_1(f) = T_1 \cdot 1 \cup T_1 \cdot x_2$ ,  $T_2(f) = T_2 \cdot x_2^2$ ,  $lt_1(f) = lt(f)$ ,  $lt_2(f) = x_1 x_2$ ,  $lc_1(f) = 1$ , and  $lc_2(f) = 2$ .

DEFINITION 2.5. For  $i \in I$  let  $k[T_i]$  be the subalgebra of all polynomials in  $K[x]$ , whose support is contained in  $T_i$ .

REMARK 2.4. Since  $T_i$  is finitely generated as a monoid,  $k[T_i]$  is a finitely generated algebra. By Hilbert's Basissatz every ideal of  $k[T_i]$  is finitely generated and every strictly increasing sequence of ideals of  $k[T_i]$  is finite.

LEMMA 2.3. *Every strictly descending sequence in  $T$  is finite. In particular, any subset of  $T$  contains a smallest element.*

PROOF. Let  $s_1 > s_2 > s_3 > \dots$  be a strictly descending sequence in  $T$ . Since  $I$  is finite, it is sufficient to prove the assertion under the assumption that all  $s_j$  are elements of  $T_i$ . But then for all  $j$  there exists no  $t \in T_i$  such that  $s_j = ts_k$ , for some  $k < j$ . In particular, the sequence

$$\langle s_1 \rangle \subset \langle s_1, s_2 \rangle \subset \langle s_1, s_2, s_3 \rangle \subset \dots$$

of ideals in  $k[T_i]$  is strictly increasing. Now Remark 2.4 yields the assertion.

LEMMA 2.4. *Let  $J \triangleleft K[x]$  and let  $lt(J) := \{lt(f) \mid f \neq 0, f \in J\}$ . There are finite subsets  $E_i \subseteq lt(J) \cap T_i$ , such that  $lt(J) \cap T_i = T_i \cdot E_i$ ,  $i \in I$ .*

PROOF. By Remark 2.4 we can choose a finite subset  $E_i$  of  $lt(J) \cap T_i$  which generates the ideal  $\langle lt(J) \cap T_i \rangle$  in  $k[T_i]$ . Now

$$lt(J) \cap T_i = T \cap_{K[T_i]} \langle lt(J) \cap T_i \rangle = T \cap_{K[T_i]} \langle E_i \rangle = T_i \cdot E_i .$$

LEMMA 2.5. *Let  $f \in K[x]$ ,  $f \neq 0$ . There are finite subsets  $F_i \subseteq T_i(f)$ , such that  $T_i(f) = T_i \cdot F_i$ ,  $i \in I$ .*

PROOF. Let  $J$  be the ideal in  $K[x]$  generated by  $f$ . By Lemma 2.4 there are finite subsets  $E_i \subseteq lt(J) \cap T_i = T_i(f)lt_i(f)$ , such that  $T_i(f)lt_i(f) = T_i \cdot E_i$ ,  $i \in I$ . Set  $F_i := \{ \frac{t}{lt_i(f)} \mid t \in E_i \}$ .

LEMMA 2.6. *Let  $f, g \in K[x]$ ,  $f \neq 0$  and  $i \in I$ . There exists a finite subset  $R(i, f, g) \subseteq T_i$ , such that  $T_i(f)lt_i(f) \cap T_i(g)lt_i(g) = T_i \cdot R(i, f, g)$ .*

PROOF. By Lemma 2.5 there are finite subsets  $E(f) \subseteq T_i(f)$ ,  $E(g) \subseteq T_i(g)$  such that  $T_i(f)lt_i(f) = T_i \cdot E(f)$  and  $T_i(g)lt_i(g) = T_i \cdot E(g)$ .

Let  $u \in E(f)$ ,  $v \in E(g)$ . The set  $A := \{a \in K[T_i] \mid av \in K[T_i] \cdot u\}$  (here  $K[T_i] \cdot u$  is the  $K[T_i]$ -submodule of  $K[x]$  generated by  $u$ ) is an ideal in  $K[T_i]$ , which is generated by  $A \cap T_i$ . By Remark 2.4 there exists a finite subset  $B \subseteq A \cap T_i$  which generates the ideal  $A$ , in particular we have  $A \cap T_i = T_i \cdot B$ . Since  $(A \cap T_i) \cdot v = T_i \cdot u \cap T_i \cdot v$ , we get  $T_i \cdot u \cap T_i \cdot v = T_i \cdot E(u, v)$ , where  $E(u, v)$  is the finite set  $\{bv \mid b \in B\}$ . Hence

$$\begin{aligned} T_i(f)lt_i(f) \cap T_i(g)lt_i(g) &= T_i \cdot E(f) \cap T_i \cdot E(g) = \bigcup_{u \in E(f), v \in E(g)} T_i \cdot u \cap T_i \cdot v = \\ &= \bigcup_{u \in E(f), v \in E(g)} T_i \cdot E(u, v) = T_i \cdot \bigcup_{u \in E(f), v \in E(g)} E(u, v) . \end{aligned}$$

Define  $R(i, f, g) := \bigcup_{u \in E(f), v \in E(g)} E(u, v)$ . Since the sets  $E(f)$ ,  $E(g)$ ,  $E(f, g)$  are finite,  $R(i, f, g)$  is finite, too.

### 3. Gröbner Bases and Buchberger Algorithm with Respect to Generalized Term Orders

PROPOSITION 3.1. *Let  $F \subseteq K[x] \setminus \{0\}$  be a finite subset and let  $g \in K[x] \setminus \{0\}$  such*

that  $lt(g) \in \bigcup_{f \in F, i \in I} T_i(f)lt_i(f)$ . Then there are polynomials  $h_f$ ,  $f \in F$ , such that

$$\max_{f \in F} lt(h_f f) = lt(g) \quad \text{and}$$

$$g = \sum_{f \in F} h_f f \quad \text{or} \quad lt(g - \sum_{f \in F} h_f f) \notin \bigcup_{f \in F, i \in I} T_i(f)lt_i(f).$$

The polynomials  $h_f$  can be computed as follows (“Division algorithm”):

First set  $h_f := 0$ ,  $f \in F$ .

As long as there are  $f \in F$  and  $t \in T$  such that  $lt(tf) = lt(g)$ , replace  $h_f$  with  $h_f + lc(g)lc(f)^{-1}t$  and  $g$  with  $g - lc(g)lc(f)^{-1}tf$ .

PROOF. We only have to show that the algorithm above terminates after a finite number of steps. Since in each step  $lt(g - lc(g)lc(f)^{-1}tf) < lt(g)$ , this follows from Lemma 2.3.

DEFINITION 3.1. Let  $F, g, h_f$  be as in the proposition 3.1. Then  $rem(g, F) := g - \sum_{f \in F} h_f f$  is “a remainder of  $g$  after division by  $F$ ”. (It is clear that  $rem(g, F)$  is not uniquely determined by  $g$  and  $F$ ).

EXAMPLE 3.1. Let  $n = 2$  and consider the generalized term order defined in Example 2.3, where  $u := (1, 1)$  and  $<_T$  is the lexicographic order with  $x_1 > x_2$ . Let  $f := x_1^2 + 2x_1x_2$ ,  $g := x_1x_2^2 + x_2$  and  $F = \{f, g\}$ . Then

$$\begin{aligned} T_1 &= \{x_1^i x_2^j \mid i \geq j\}, \quad T_2 = \{x_1^i x_2^j \mid i \leq j\}, \\ lt(f) &= lt_1(f) = x_1^2, \quad lt_2(f) = x_1x_2, \quad lt(g) = lt_1(g) = lt_2(g) = x_1x_2^2, \\ T_1(f) &= T_1 \cdot 1 \cup T_1 \cdot x_2, \quad T_2(f) = T_2 \cdot x_2^2, \quad T_1(g) = T_1 \cdot x_1, \quad T_2(g) = T_2 \cup T_2 \cdot x_1. \end{aligned}$$

We compute a remainder of  $2x_1^2x_2^3 - x_1^2x_2$  after division by  $F$ :

$$\begin{aligned} lt(2x_1^2x_2^3 - x_1^2x_2) &= x_1^2x_2^3 \in T_2(g)lt_2(g), \\ 2x_1^2x_2^3 - x_1^2x_2 - 2x_1x_2g &= -x_1^2x_2 - 2x_1x_2^2, \\ lt(-x_1^2x_2 - 2x_1x_2^2) &= x_1^2x_2 \in T_1(f)lt_1(f), \\ -x_1^2x_2 - 2x_1x_2^2 - x_2f &= 0. \end{aligned}$$

Hence  $2x_1^2x_2^3 - x_1^2x_2 = 2x_1x_2g - x_2f$  and  $rem(2x_1^2x_2^3 - x_1^2x_2, F) = 0$ .

For  $x_1^2x_2^2 - 2x_2^2$  we get:

$$\begin{aligned} lt(x_1^2x_2^2 - 2x_2^2) &= x_1^2x_2^2 \in T_2(g)lt_2(g), \\ x_1^2x_2^2 - 2x_2^2 - x_1g &= -x_1x_2 - 2x_2^2. \end{aligned}$$

Then

$$lt(-x_1x_2 - 2x_2^2) = x_1x_2 \notin T_1(f)lt_1(f) \cup T_2(f)lt_2(f) \cup T_1(g)lt_1(g) \cup T_2(g)lt_2(g),$$

and thus  $-x_1x_2 - 2x_2^2 = rem(x_1^2x_2^2 - 2x_2^2, F)$ .

DEFINITION 3.2. A finite subset  $G$  of an ideal  $J$  of  $K[x]$  is a “Gröbner basis of  $J$ ” if and only if  $0 \notin G$  and

$$\{lt(f) \mid f \neq 0, f \in J\} = \bigcup_{g \in G, i \in I} T_i(g)lt_i(g).$$

PROPOSITION 3.2. *Let  $J$  be a non-zero ideal in  $K[x]$ . Then*

- 1  $J$  contains a Gröbner basis.
- 2 Let  $G$  be a Gröbner basis of  $J$ . Then a polynomial  $f$  is an element of  $J$  if and only if a remainder (or all remainders) of  $f$  after division by  $G$  is zero.
- 3 A Gröbner basis of  $J$  generates the ideal  $J$ .

PROOF. 1 By Lemma 2.4 there are finite subsets  $E_i \subseteq T_i$  such that  $lt(J) = \bigcup_{i \in I} T_i \cdot E_i$ . For all  $t \in \bigcup_{i \in I} E_i$  choose an element  $f_t \in J$  such that  $lt(f_t) = t$ . Then  $\{f_t \mid t \in \bigcup_{i \in I} E_i\}$  is a Gröbner basis of  $J$ .

2 follows from proposition 3.1.

3 follows from 2.

DEFINITION 3.3. Let  $f, g \in K[x]$  and  $i \in I$ . Let  $R(i, f, g)$  be a finite subset of  $T_i$  (see Lemma 2.6) such that

$$T_i(f)lt_i(f) \cap T_i(g)lt_i(g) = T_i \cdot R(i, f, g) .$$

For every  $r \in R(i, f, g)$  define

$$S(i, f, g, r) := lc_i(g) \frac{r}{lt_i(f)} f - lc_i(f) \frac{r}{lt_i(g)} g .$$

Note that  $lc_i(f) = lc(\frac{r}{lt_i(g)} f)$ .

LEMMA 3.1. *Let  $F \subseteq K[x] \setminus \{0\}$  be a finite subset and  $i \in I$ . Assume that there are  $u \in T_i$ , a family  $(t_f)_{f \in F}$  in  $T$  such that*

$$u = lt(t_f f), \quad \text{for all } f \in F ,$$

*and a family  $(c_f)_{f \in F}$  in  $K$  such that*

$$\sum_{f \in F} c_f lc_i(f) = 0 .$$

*Then there are elements  $d_{r, f, g}$  in  $K$ , such that*

$$\sum_{f \in F} c_f t_f f = \sum_{r \in R(i, f, g), f \in F, g \in F} d_{r, f, g} \frac{u}{r} S(i, f, g, r) \quad \text{and} \quad \frac{u}{r} \in T_i .$$

PROOF. Induction on  $|F|$ :

$|F| = 2$  : Let  $F = \{f, g\}$ ,  $f \neq g$ . Then  $c_f lc_i(f) = -c_g lc_i(g)$ ,

$$t_f lt_i(f) = lt(t_f f) = u = lt(t_g g) = t_g lt_i(g) ,$$

and  $t_f \in T_i(f)$ ,  $t_g \in T_i(g)$ . Hence  $u \in T_i(f)lt_i(f) \cap T_i(g)lt_i(g)$  and there are  $r \in R(i, f, g)$  and  $p \in T_i$  such that  $u = p \cdot r$ . Since  $r$  is a multiple of  $lt_i(f)$  and of  $lt_i(g)$ , the power products  $t_f$  and  $t_g$  are multiples of  $p$ . Hence

$$c_f t_f f + c_g t_g g = \frac{c_f}{lc_i(g)} p (lc_i(g) \frac{t_f}{p} f - lc_i(f) \frac{t_g}{p} g) = \frac{c_f}{lc_i(g)} p S(i, f, g, r) .$$

$|F| > 2$  : Let  $\{g, h\} \subseteq F$ ,  $g \neq h$ , and  $F^1 := F \setminus \{g, h\}$ . Then

$$\sum_{f \in F} c_f t_f f = c_h t_h h + \left(-\frac{c_h lc_i(h)}{lc_i(g)} t_g g\right) + \left((c_g + \frac{c_h lc_i(h)}{lc_i(g)}) t_g g\right) + \sum_{f \in F^1} c_f t_f f .$$



Applying the induction hypothesis to

$$c_h t_h h + \left(-\frac{c_h l_{c_i}(h)}{l_{c_i}(g)}\right) t_g g$$

and to

$$\left(c_g + \frac{c_h l_{c_i}(h)}{l_{c_i}(g)}\right) t_g g + \sum_{f \in F^1} c_f t_f f$$

yields the assertion.

**PROPOSITION 3.3.** *Let  $F \subseteq K[x] \setminus \{0\}$  be a finite set of polynomials and let  $J$  be the ideal generated by  $F$ . Then the following assertions are equivalent:*

- 1  $F$  is a Gröbner basis of  $J$ .
- 2 For all  $f, g \in F$ , for all  $i \in I$ , for all  $r \in R(i, f, g)$ , a remainder of  $S(i, f, g, r)$  is zero.

**PROOF.** (1  $\Rightarrow$  2) Since  $S(i, f, g, r)$  is an element of  $J$ , the assertion follows from proposition 3.2.

(2  $\Rightarrow$  1) Let  $h \in J$ ,  $h \neq 0$ . We have to show

$$lt(h) \in \bigcup_{g \in G, i \in I} T_i(g) lt_i(g) .$$

Since  $J$  is generated by  $F$ , we have

$$h = \sum_{f \in F, t \in T} c_{t,f} t f ,$$

for some  $c_{t,f} \in K$ . Let  $u := \max\{lt(tf) \mid t \in T, f \in F, c_{t,f} \neq 0\}$ . We choose the elements  $c_{t,f}$  such that  $u$  is minimal, i.e. if  $h = \sum_{f \in F, t \in T} d_{t,f} t f$ , then

$$u \leq \max\{lt(tf) \mid t \in T, f \in F, d_{t,f} \neq 0\} .$$

Let  $i \in I$  be such that  $u \in T_i$ . If  $lt(h) = u$ , then  $lt(h) = lt(tf) = lt_i(f)$ , for some  $f \in F$ ,  $t \in T_i(f)$ . Hence it remains to show that  $lt(h)$  cannot be smaller than  $u$ .

Suppose  $lt(h) < u$ . Let  $Z := \{(t, f) \in T \times F \mid lt(tf) = u, c_{t,f} \neq 0\}$ . Then

$$\sum_{(t,f) \in Z} c_{t,f} l_{c_i}(f) = 0 .$$

By Lemma 3.1 there are  $d_{r,f,g} \in K$  such that

$$\sum_{(f,t) \in Z} c_{t,f} f = \sum_{r \in R, f \in F, g \in F} d_{r,f,g} \frac{u}{r} S(i, f, g, r) \quad \text{and} \quad \frac{u}{r} \in T_i .$$

By (2), for every  $S(i, f, g, r)$  there are  $d_{s,e} \in K$  (depending on  $r, f, g$ ) such that

$$S(i, f, g, r) = \sum_{s \in T, e \in F} d_{s,e} s e$$

and

$$lt(S(i, f, g, r)) = \max\{lt(se) \mid e \in F, s \in T, d_{s,e} \neq 0\} .$$

Every element of  $\text{supp}(S(i, f, g, r))$  is smaller than  $r$ , hence the same holds for  $\text{supp}(se)$ , where  $d_{s,e} \neq 0$ .

Now  $r \in T_i$  and  $\frac{u}{r} \in T_i$  imply  $lt(\frac{u}{r}se) < u$ . Hence  $\sum_{(f,t) \in F} c_f t f$  can be written as a linear combination of polynomials  $se$ , where  $s \in T$ ,  $e \in F$ , and  $lt(se) < u$ . This contradicts the minimality of  $u$ .

**PROPOSITION 3.4.** *Let  $F \subseteq K[x] \setminus \{0\}$  be a finite set of polynomials and let  $J$  be the ideal generated by  $F$ . By the following algorithm a Gröbner basis of  $J$  can be computed:*

$$F_0 := F$$

$$F_{j+1} := F_j \cup (\{ \text{rem}(S(i, f, g, r) \mid f, g \in F_j, i \in I, r \in R(i, f, g)) \} \setminus \{0\}).$$

*If  $F_j = F_{j+1}$ , then  $F_j$  is a Gröbner basis of  $J$ .*

**PROOF.** By proposition 3.3 we only have to show that there exists a  $k \in \mathbf{N}$  such that  $F_k = F_{k+1}$ . Suppose there exists no such  $k$ . Then there exists an index  $i \in I$  such that for all  $j \in \mathbf{N}$  there exists a  $m \in \mathbf{N}$  such that the ideal  $\langle \bigcup_{f \in F_j} T_i(f)lt_i(f) \rangle$  in  $k[T_i]$  is strictly contained in  $\langle \bigcup_{f \in F_{j+m}} T_i(f)lt_i(f) \rangle$ . By Remark 2.4 this is not possible.

**EXAMPLE 3.2.** Let  $<, f, g$  be as in Example 3.1 and let  $J$  be the ideal generated by  $f$  and  $g$ . Then

$$\begin{aligned} T_1(f)lt_1(f) \cap T_1(g)lt_1(g) &= T_1 \cdot x_1^3 x_2^2, \\ T_2(f)lt_2(f) \cap T_2(g)lt_2(g) &= T_2 \cdot x_1 x_2^3, \\ S(1, f, g, x_1^3 x_2^2) &= x_1 x_2^2 f - x_1^2 g = 2x_1^2 x_2^3 - x_1^2 x_2, \\ S(2, f, g, x_1 x_2^3) &= x_2^2 f - 2x_2 g = x_1^2 x_2^2 - 2x_2^2. \end{aligned}$$

Using Example 3.1 we get

$$\begin{aligned} \text{rem}(S(1, f, g, x_1^3 x_2^2), \{f, g\}) &= 0, \\ \text{rem}(S(2, f, g, x_1 x_2^3), \{f, g\}) &= -x_1 x_2 - 2x_2^2. \end{aligned}$$

Hence  $\{f, g\}$  is not a Gröbner basis of  $J$ . Let  $h := x_1 x_2 + 2x_2^2$ . Then  $lt(h) = lt_2(h) = x_2^2$ ,  $lt_1(h) = x_1 x_2$ ,  $T_1(h) = T_1 \cdot x_1$ , and  $T_2(h) = T_2$ . Now

$$\begin{aligned} T_1(f)lt_1(f) \cap T_1(h)lt_1(h) &= T_1 \cdot x_1^2 x_2, \\ T_2(f)lt_2(f) \cap T_2(h)lt_2(h) &= T_2 \cdot x_1 x_2^3, \\ T_1(g)lt_1(g) \cap T_1(h)lt_1(h) &= T_1 \cdot x_1^3 x_2^2, \\ T_2(g)lt_2(g) \cap T_2(h)lt_2(h) &= T_2 \cdot x_1 x_2^3, \end{aligned}$$

and the remainders of  $S(1, f, h, x_1^2 x_2)$ ,  $S(2, f, h, x_1 x_2^3)$ ,  $S(1, g, h, x_1^3 x_2^2)$  and  $S(2, g, h, x_1 x_2^3)$  after division by  $\{f, g, h\}$  are zero. Hence  $\{f, g, h\}$  is a Gröbner basis of  $J$ .

**REMARK 3.1.** Gröbner bases can also be defined for submodules of finite-dimensional free  $K[x]$ -modules [see for example Becker and Weispfenning (1993) or Pauer (1991)]. Their computation can either be reduced to the computation of Gröbner bases of ideals [(Becker and Weispfenning, 1993), chapter 10.4] or be done directly (Pauer, 1991). For the sake of simplicity of presentation we considered here only the case of ideals. We

indicate now how the basic definitions can be generalized to the case of submodules. The extension to this case of the propositions and their proofs is straightforward.

Let  $q$  be a positive integer and denote by  $W$  the free  $K[x]$ -module  $K[x]^q$ . Denote by  $\{e_1, \dots, e_q\}$  the standard-basis of  $W$  and  $U := \{te_i \mid t \in T, 1 \leq i \leq q\}$ . Then  $U$  is a  $K$ -basis of  $W$ , hence the vectors in  $W$  can uniquely be written in the form  $\sum_{u \in U} c_u u$ ,  $c_u \in K$ . Let  $(T_i)_{i \in I}$  be a conic decomposition of  $T$ . Let  $U_i := \{te_j \mid t \in T_i, 1 \leq j \leq q\}$ ,  $i \in I$ . A “generalized term order” on  $U$  for  $(T_i)_{i \in I}$  is a total order on  $U$  such that

- (i)  $e_i$  is the smallest element in  $\{te_i \mid t \in T\}$ ,  $1 \leq i \leq q$ ,
- (ii)  $r < s$  implies  $rt < st$ , for all  $i \in I$ ,  $s \in U_i$ ,  $t \in T_i$ , and  $r \in U$ .

Let  $<$  be a generalized term order on  $U$  for  $(T_i)_{i \in I}$  and let  $f = \sum_{u \in T} c_u u$  be a non-zero polynomial in  $K[x]$ ,  $c_u \in K$ . Then we define

$$\begin{aligned} \text{supp}(f) &:= \{u \in U \mid c_u \neq 0\}. \\ \text{lt}(f) &:= \max \text{supp}(f). \\ T_i(f) &:= \{t \in T \mid \text{lt}(tf) \in U_i\}, 1 \leq i \leq n. \\ \text{If } t \in T_i(f), \text{ then } \text{lt}_i(f) &:= \frac{\text{lt}(tf)}{t}. \end{aligned}$$

A finite subset  $G$  of an submodule  $J$  of  $W$  is a “Gröbner basis of  $J$ ” if and only if  $0 \notin G$  and

$$\{\text{lt}(f) \mid f \neq 0, f \in J\} = \bigcup_{g \in G, i \in I} T_i(g)\text{lt}_i(g).$$

#### 4. Application of Gröbner Basis Theory to the Modelling Problem

In this section we will propose a procedure that allows to check whether a homogeneous linear partial difference equation with constant coefficients provides an unfalsified model for a set of observations.

Suppose that  $\Delta$  is a subset of  $\mathbf{N}^n$ . Consider first the form

$$\langle \cdot, \cdot \rangle_\Delta : K[x_1, \dots, x_n]^q \times (K^q)^\Delta \longrightarrow K$$

that is defined in the following way:

Let  $v \in (K^q)^\Delta$  and let  $f \in K[x_1, \dots, x_n]^q$  be a polynomial row. If  $\text{supp}(f) \not\subseteq \{x^i \mid i \in \Delta\}$ , then we let  $\langle f, v \rangle_\Delta := 0$ . If  $\text{supp}(f) \subseteq \{x^i \mid i \in \Delta\}$  and if

$$f = \sum_{i \in \Delta} f_i x^i,$$

with  $f_i \in K^q$ , then we let

$$\langle f, v \rangle_\Delta := \sum_{i \in \Delta} \langle f_i, v(i) \rangle,$$

where  $\langle -, - \rangle$  is the standard scalar-product on  $K^q$ .

The first step for the solution of our problem is provided by the following proposition whose proof can be found in (Oberst, 1990).

**PROPOSITION 4.1.** *Consider two homogeneous linear partial difference equations with constant coefficients  $R_1 w = 0$  and  $R_2 w = 0$ , where  $R_1 \in K[x_1, \dots, x_n]^{l_1 \times q}$  and  $R_2 \in$*

$K[x_1, \dots, x_n]^{l_2 \times q}$ . Then  $\ker R_1 = \ker R_2$  if and only if there exists polynomial matrices  $X_1, X_2$  of suitable dimensions such that  $R_1 = X_2 R_2$  and  $R_2 = X_1 R_1$ .

In other words: the difference equations  $R_1 w = 0$  and  $R_2 w = 0$  have the same set of solutions if and only if the  $K[x_1, \dots, x_n]$ -module generated by the rows of  $R_1$  and the  $K[x_1, \dots, x_n]$ -module generated by the rows of  $R_2$  coincide. Therefore, in verifying whether a model represented by a difference equation  $Rw = 0$ ,  $R \in K[x_1, \dots, x_n]^{l \times q}$ , is unfalsified, the polynomial matrix  $R$  can be modified in such a way that the module generated by its rows remains unchanged. The following proposition shows that, when the set of generators of this module is a Gröbner basis with respect to a generalized term order  $<$ , the check can be done easily. The only restriction is that the proposition considers only data that are supported on subsets  $\Delta$  of  $\mathbf{N}^n$  having the following special property:

$a \in \Delta$  and  $x^b < x^a$  implies  $b \in \Delta$ . We say in this case that  $\Delta$  is a  $<$ -saturated subset of  $\mathbf{N}^n$ . Note that  $\Delta$  is  $<$ -saturated if and only if there exists  $s \in \mathbf{N}^n$  such that  $\Delta = \{k \in \mathbf{N}^n \mid x^k < x^s\}$ .

**PROPOSITION 4.2.** *Let  $R \in K[x_1, \dots, x_n]^{l \times q}$ ,  $v_1, \dots, v_m \in (K^q)^\Delta$ , and let  $M$  be the  $K[x_1, \dots, x_n]$ -module generated by the rows  $r_1, \dots, r_l$  of  $R$ . Choose a generalized term order  $<$  on  $T$  and extend it to  $\{te_j \mid t \in T, 1 \leq j \leq q\}$  by*

$$se_i < te_j \text{ if and only if } s < t \text{ or } (s = t \text{ and } i < j)$$

(cf. Remark 3.1). Let  $lt(M) := \{lt(r) \mid r \in M, r \neq 0\}$ . We assume that  $\{r_1, \dots, r_l\}$  is a Gröbner basis of  $M$  with respect to the generalized term order  $<$  and that  $\Delta \subseteq \mathbf{N}^n$  is  $<$ -saturated. Then the following assertions are equivalent:

- 1  $\ker(R)$  is an unfalsified model of  $v_1, \dots, v_m \in (K^q)^\Delta$ .
- 2 For all  $u \in \Delta$  and  $h \in \{1, \dots, q\}$  such that  $x^u e_h \in lt(M)$ , there are  $t \in T$  and  $k \in \{1, \dots, l\}$  such that  $lt(tr_k) = x^u e_h$  and  $\langle tr_k, v_i \rangle_\Delta = 0$ ,  $1 \leq i \leq m$ .

**PROOF.** (1  $\Rightarrow$  2) Trivial.

(2  $\Rightarrow$  1) Without loss of generality we can assume that  $m = 1$ . Let  $v := v_1$ . We want to construct recursively  $w \in \ker(R)$  such that  $w|_\Delta = v$ . For  $u \in \Delta$  we define  $w(u) := v(u)$ . Now let  $u \notin \Delta$  and suppose that we have determined  $w(s)$  for all  $s$  with  $x^s < x^u$ . Suppose moreover that we have already determined the first  $h - 1$  components of the vector  $w(u) = (w(u)_1, w(u)_2, \dots, w(u)_q)$ . We want to construct  $w(u)_h$ . There are two cases:

1.  $x^u e_h \notin lt(M)$ . In this case we assign  $w(u)_h$  arbitrarily.
2.  $x^u e_h \in lt(M)$ . By definition of Gröbner bases there exist  $k \in \{1, \dots, l\}$  and a term  $t \in T$  such that  $lt(tr_k) = x^u e_h$ . Then let  $w(u)_h$  be the unique element in  $K$  such that

$$\langle tr_k, w \rangle_{\mathbf{N}^n} = 0.$$

Note that  $w(u)_h$  is well defined by the induction hypothesis.

Now we will show that  $w$  obtained in this way satisfies the requirements, i.e.  $w \in \ker(R)$  and  $w|_\Delta = v$ . First it is clear that  $w|_\Delta = v$ . Therefore we only have to show that  $w \in \ker(R)$  or, equivalently, that

$$\langle r, w \rangle_{\mathbf{N}^n} = 0,$$

for all  $r \in M$ . We will show this by induction. Suppose this is true for all  $r \in M$  such that  $lt(r) < e_h x^u$  and show that the same is true for all  $r \in M$  such that  $lt(r) = e_h x^u$ . If  $u \in \Delta$ , then by (2) there are  $t \in T$  and  $k \in \{1, \dots, l\}$  such that  $lt(tr_k) = x^u e_h$  and

$$\langle tr_k, v \rangle_{\mathbf{N}^n} = \langle tr_k, v \rangle_{\Delta} = 0.$$

If  $u \notin \Delta$  then by the construction above there are  $t \in T$  and  $k \in \{1, \dots, l\}$  such that  $lt(tr_k) = x^u e_h$  and

$$\langle tr_k, v \rangle_{\mathbf{N}^n} = 0.$$

In both cases there exists  $a \in K$  such that  $lt(r + atr_k) < x^u e_h$  and by induction we have

$$\langle r + atr_k, w \rangle_{\mathbf{N}^n} = 0.$$

Hence

$$\langle r, w \rangle_{\mathbf{N}^n} = \langle r + atr_k, w \rangle_{\mathbf{N}^n} - a \langle tr_k, w \rangle_{\mathbf{N}^n} = a \langle tr_k, w \rangle_{\mathbf{N}^n} = 0.$$

The procedure that allows to verify whether a difference equation is an unfalsified model can be expressed in the following way:

Suppose we are given a homogeneous linear partial difference equation with constant coefficients  $Rw = 0$ ,  $R \in K[x_1, \dots, x_n]^{l \times q}$ , and a finite family of observations  $v_1, \dots, v_m \in (K^q)^\Delta$ , where  $\Delta$  is a subset of  $\mathbf{N}^n$  that is saturated with respect to a generalized term order  $<$ .

1. Compute a Gröbner basis  $g_1, \dots, g_h$  of the module generated by the rows of  $R$  and consider the difference equation  $\bar{R}w = 0$ , where  $\bar{R}$  is the polynomial matrix whose rows are  $g_1, \dots, g_h$ . Then by Proposition 4.1,  $Rw = 0$  provides an unfalsified model for  $v_1, \dots, v_m$  if and only if  $\bar{R}w = 0$  provides an unfalsified model for  $v_1, \dots, v_m$ .
2. If  $\Delta$  is a finite subset of  $\mathbf{N}^n$ , then the conditions in assertion (2) of 4.2 can be easily verified in a finite number of steps.

EXAMPLE 4.1. Consider the generalized term order  $<$  defined in Example 3.2. Then the set

$$\Delta := \{(\alpha_1, \alpha_2) \in \mathbf{N}^2 \mid \alpha_1 \leq 2, \alpha_2 \leq 2\}$$

is  $<$ -saturated. Let

$$R := \begin{bmatrix} x_1^2 + 2x_1x_2 \\ x_1x_2^2 + x_2 \\ x_1x_2 + 2x_2^2 \end{bmatrix}$$

be a polynomial matrix in  $\mathbf{Q}[x_1, x_2]^{3 \times 1}$ . As we have seen in Example 3.2, the rows of  $R$  form a Gröbner basis with respect to the generalized term order  $<$ . Consider the trajectories  $v_1$  and  $v_2$  in  $\mathbf{Q}^\Delta$  defined in this way

$$\begin{aligned} v_1(0,0) &= 0, v_1(1,0) = 1, v_1(2,0) = 4, v_1(0,1) = -2, v_1(1,1) = -2, v_1(2,1) = -4, \\ v_1(0,2) &= 1, v_1(1,2) = 2, v_1(2,2) = 2, \\ v_2(0,0) &= 0, v_2(1,0) = 1, v_2(2,0) = -4, v_2(0,1) = -2, v_2(1,1) = 2, v_2(2,1) = -4, \\ v_2(0,2) &= -1, v_2(1,2) = 2, v_2(2,2) = 0. \end{aligned}$$

Let  $M$  be the ideal generated by the three polynomials that form  $R$ . Then the set of all  $u \in \Delta$  such that  $x^u \in lt(M)$  is  $\{(2,0), (2,1), (2,2), (1,2), (0,2)\}$ . Hence by Proposition 4.2 there are only 5 conditions to check in order to verify whether  $\ker(R)$  is an unfalsified model for  $v_1$  or  $v_2$ . Hence we easily see that  $\ker(R)$  is an unfalsified model for  $v_1$ , but

not for  $v_2$ , since

$$\langle x_1(x_1x_2^2 + x_2), v_2 \rangle_{\Delta} = 2.$$

Notice that if

$$R' := \begin{bmatrix} x_1^2 - 4x_2^2 \\ x_1x_2 + 2x_2^2 \\ x_2^3 - 1/2x_2 \end{bmatrix},$$

then  $R'$  and  $R$  provide partial difference equations with the same set of solutions. Moreover the rows of  $R'$  form a Gröbner basis with respect to the lexicographical term order. It is easy to verify that assertion (2) in Proposition 4.2 is true for the rows of  $R'$  and  $v_2$ . This shows that if we want to apply Proposition 4.2 we really need a Gröbner basis with respect to the generalized term order  $<$ .

### References

- Antoulas, A.C., Willems, J.C. (1991). A behavioral approach to linear exact modeling. *IEEE Trans. Automatic Control* **AC-38**, 1776–1802.
- Becker, T., Weispfenning, V. (1993). *Gröbner Bases*. Springer-Verlag.
- Buchberger, B. (1984). A critical-pair completion algorithm for finitely generated ideals in rings. In: *Symposium Rekursive Kombinatorik, Münster (FRG)*. In: *Lectures Notes in Computer Science*. Number 171 Springer-Verlag. pp. 137–161.
- Buchberger, B. (1985). Gröbner bases: An algorithmic method in polynomial ideal theory. In: *Multidimensional Systems Theory* (N. K. Bose, Ed.). pp. 184–232. D. Reidel.
- Heij, C. (1992). Exact modelling and identifiability of linear systems. *Automatica* **28**, 325–344.
- Oberst, U. (1990). Multidimensional constant linear systems. *Acta Applicandae Mathematicae* **20**, 1–175.
- Oberst, U. (1993). On the minimal number of trajectories determining a multidimensional system. *Math. of Control, Signals, and Systems* **6**, 264–288.
- Pauer, F. (1991). Gröbner Basen und ihre Anwendungen. In: *Jahrbuch Überblicke Mathematik* (S. Chat-terji et al., Ed.). pp. 127–149. Vieweg Verlag.
- Petkovsek, M. (1990). Finding Closed-form Solutions of Difference Equations by Symbolic Methods. PhD thesis. School of Computer Science, Carnegie Mellon University.
- Sakata, S. (1988). Finding a minimal set of linear recurring relations capable of generating a given two-dimensional array. *J. Symbolic Computation* **5**, 321–337.
- Stifter, S. (1988). A generalization of reduction rings. *Journal of Symbolic Computation* **4**, 351–364.
- Willems, J.C. (1986). From time series to linear system, part I: Finite dimensional linear time invariant systems. *Automatica* **22**, 561–580.
- Zampieri, S. (1994). Exact modelling of scalar 2D arrays. *Kybernetika* **30**, 129–140.