AAECC **9**, 271–291 (1999)

AAECC
Applicable Algebra in
Engineering, Communication
and Computing
© Springer-Verlag 1999

Gröbner Bases for Ideals in Laurent Polynomial Rings and their Application to Systems of Difference Equations

Franz Pauer[1], Andreas Unterkircher[2]

[1]Institut für Mathematik, Universität Innsbruck, Technikerstrasse 25, A-6020 Innsbruck, Austria, (e-mail: Franz.Pauer@uibk.ac.at)
[2]Institut für Umformtechnik, ETH Zürich, Tannenstrasse 3, CH-8092 Zürich, Switzerland, (e-mail: unterkir@ifu.bepr.ethz.ch)

Received: January 20, 1997

Abstract. We develop a basic theory of Gröbner bases for ideals in the algebra of Laurent polynomials (and, more generally, in its monomial subalgebras). For this we have to generalize the notion of term order. The theory is applied to systems of linear partial difference equations (with constant coefficients) on $\mathbb{Z}^n$. Furthermore, we present a method to compute the intersection of an ideal in the algebra of Laurent polynomials with the subalgebra of all polynomials.

Keywords: Laurent polynomial ring, groebner basis, generalized term order, partial difference equation

1 Motivation and Introduction

Let R be a commutative noetherian ring (e. g. a field, $\mathbb{Z}$ or $\mathbb{Z}_m$), Γ a set, let R^Γ be the R-module of all maps from Γ to R, and let $R^{(\Gamma)}$ be the R-submodule of all maps from Γ to R with finite support. There is a natural nondegenerate bilinear form

$$\langle -, - \rangle : R^{(\Gamma)} \times R^\Gamma \longrightarrow R, \quad (f, g) \longmapsto \sum_{i \in \Gamma} f(i)g(i) \ .$$

Let $<$ be a well-order on Γ. (Then every strictly descending sequence in Γ is finite). For $0 \neq f \in R^{(\Gamma)}$ we define the “degree of f”

$$deg(f) := \max\{\, i \in \Gamma \mid f(i) \neq 0 \,\}$$

and the "leading coefficient of f"

$$lc(f) := f(deg(f)) .$$

For $\emptyset \neq M \subseteq R^{(\Gamma)}$ let

$$deg(M) := \{ deg(f) \mid f \in M, f \neq 0 \}$$

and

$$M^{\perp} := \left\{ g \in R^{\Gamma} \mid \langle f, g \rangle = 0, \text{ for all } f \in M \right\} .$$

Obviously $M^{\perp}$ is an R-submodule of R^{Γ}.

Definition 1.1 *Let $\{0\} \neq W \leq R^{(\Gamma)}$ be a submodule of $R^{(\Gamma)}$. Then a family $(v_i)_{i \in deg(W)}$ in W is a "triangular basis of W" if and only if $deg(v_i) = i$ and $lc(v_i) = 1$, for all $i \in deg(W)$.*

Remark 1.1 It is clear that every triangular basis is an R-basis of W. If R is a field, then there always exists a triangular basis of W. Nevertheless, in general it is not possible to compute actually such a basis.

Proposition 1.1 *Let W be an R-subspace of $R^{(\Gamma)}$. Assume that there is a triangular basis $(v_i)_{i \in deg(W)}$ of W. Then the map*

$$r : W^{\perp} \longrightarrow R^{\Gamma \setminus deg(W)}, \quad g \longmapsto g|_{\Gamma \setminus deg(W)}$$

is an R-linear isomorphism.
Let $(e_i)_{i \in \Gamma}$ be the standard basis of $R^{(\Gamma)}$ and let $h \in R^{\Gamma \setminus deg(W)}$. Then $g := r^{-1}(h)$ can be computed recursively as follows:
Let m be the smallest element in Γ.
If $m \in deg(W)$, then $g(m) = 0$, else $g(m) = h(m)$.
Let $i > m$ and suppose that $g(j)$ has already been computed for all $j < i$.
If $i \in deg(W)$, then $g(i) = \langle e_i - v_i, g \rangle$, else $g(i) = h(i)$.

Proof. Let $w \in W^{\perp}$ such that $r(w) = 0$. Suppose $w \neq 0$. Let j be the smallest element in the support of w. Then $j \in deg(W)$ and $w(j) = \langle v_j, w \rangle = 0$. Contradiction. Hence r is injective.

Let $i \in \Gamma$ and $\Delta := \{ j \in \Gamma \mid j < i, (e_i - v_i)(j) \neq 0 \}$. Then Δ is finite. Since $lc(v_i) = 1$ we have $\langle e_i - v_i, g \rangle = \langle e_i - v_i, \sum_{j \in \Delta} g(j) e_j \rangle$, hence the recursive definition (with respect to the well-order $<$) of $g \in R^{\Gamma}$ given above is correct.

It remains to show that $g \in W^{\perp}$. If not, then the set

$$\left\{ j \in deg(W) \mid \langle v_j, g \rangle \neq 0 \right\}$$

would not be empty. Let i be its smallest element. Then

$$0 \neq \langle v_i, g \rangle = \langle e_i - e_i + v_i, g \rangle = \langle e_i, g \rangle - \langle e_i - v_i, g \rangle = g(i) - g(i) = 0 .$$

Contradiction. □

Now we consider important special cases of the situation above: Let Γ be a submonoid of $(\mathbb{Z}^n, +)$, for instance $\Gamma = \mathbb{Z}^{n-m} \times \mathbb{N}^m,\ \mathbb{Z}^n,\ \mathbb{N}^n$. In this case $R^{(\Gamma)}$ can be considered as the (monomial) subalgebra $R[x^i; i \in \Gamma]$ generated by the set $\left\{ x^i = x_1^{i_1} \dots x_n^{i_n} \mid i \in \Gamma \right\}$ in the algebra $R[x_1, \dots, x_n, x_1^{-1}, \dots, x_n^{-1}]$ of Laurent polynomials. We then write $\sum_{i \in \Gamma} f(i) x^i \in R[x^i; i \in \Gamma]$ instead of $f \in R^{(\Gamma)}$.

Let $W \leq R[x^i; i \in \Gamma]$ be an ideal generated by elements $f_1, \dots, f_k \in R[x^i; i \in \Gamma]$. Then the set $\left\{ x^i f_j \mid i \in \Gamma, 1 \leq j \leq k \right\}$ is a system of generators of the R-module W. Hence

$$W^{\perp} = \left\{ g \in R^{\Gamma} \mid \forall i \in \Gamma,\ \forall j,\ \langle x^i f_j, g \rangle = 0 \right\}$$

$$= \left\{ g \in R^{\Gamma} \mid \forall i \in \Gamma,\ \forall j,\ \sum_{s \in \Gamma} f_j(s) g(s+i) = 0 \right\},$$

i.e. $W^{\perp}$ is the set of solutions of the system of difference equations

$$\sum_{s \in \Gamma} f_j(s) g(s+i) = 0, \quad 1 \leq j \leq k,\ i \in \Gamma$$

(where $g \in R^{\Gamma}$ is the unknown function).

We extend this to a slightly more general situation: Let$B$ be a finite set, let Γ' be a submonoid of $(\mathbb{Z}^n, +)$, and let $\Gamma := \Gamma' \times B$. Then $R^{(\Gamma)}$ can be considered as the free $R[x^i; i \in \Gamma']$ -module $V := \bigoplus_{b \in B} R[x^i; i \in \Gamma']\, b$. We then write $\sum_{i \in \Gamma', b \in B} f(i, b) x^i b \in V$ instead of $f \in R^{(\Gamma)}$.

Let $W \leq V$ be an $R[x^i; i \in \Gamma']$ -submodule of V, generated by elements $f_1, \dots, f_k \in V$. Then the set $\left\{ x^i f_j \mid i \in \Gamma', 1 \leq j \leq k \right\}$ is a system of R-module generators of W. Hence

$$W^{\perp} = \left\{ g \in R^{\Gamma} \mid \forall i \in \Gamma',\ \forall j,\ \sum_{s \in \Gamma'} \sum_{d \in B} f_j(s, d) g(s+i, d) = 0 \right\},$$

i.e. $W^{\perp}$ is the set of solutions of the system of difference equations

$$\sum_{(s,d) \in \Gamma} f_j(s, d) g(s+i, d) = 0, \quad 1 \leq j \leq k,\ i \in \Gamma'$$

(where $g \in R^{\Gamma} \cong (R^B)^{\Gamma'}$ is the unknown function).

If R is a field, Proposition 1.1 reduces the problem of solving this system of difference equations to the problem of computing $deg(W)$ and a triangular basis of W. If $\Gamma = \mathbb{N}^n$ (or $\mathbb{N}^n \times B$) and $<$ is a term order, this can be done by computing a Gröbner basis of W. This was first observed and applied by U. Oberst in [4]. The case $\Gamma = \mathbb{Z}^n$ was treated in [11] and in [10]. The method there was to consider the algebra of Laurent polynomials $R[x_1, \dots, x_n, x_1^{-1}, \dots, x_n^{-1}]$ as the factor algebra

$$R[x_1, \dots, x_n, y_1, \dots, y_n] / \langle x_1 y_1 - 1, \dots, x_n y_n - 1 \rangle$$

and to compute a Gröbner basis of the inverse image of the ideal W in

$$R[x_1, \dots, x_n, y_1, \dots, y_n] .$$

The aim of this paper is to present a direct method: we define Gröbner bases with respect to generalized term orders for ideals in the algebra of Laurent polynomials (and, more generally, in its finitely generated monomial subalgebras). For the sake of completeness we do not restrict ourselves to the case of coefficient fields, but admit coefficients in a commutative noetherian ring R. Of course, if we want to compute Gröbner bases, we have to assume additionally that we can solve linear equations over R, i.e. for given elements $r, r_1, r_2, \dots, r_k \in R$ we should be able to decide if r is an R-linear combination of $r_1, r_2, \dots, r_k$, and if so, to compute a parameter form of the affine subspace $\{s \in R^k \mid \sum_{i=1}^{k} r_i s_i = r\}$ of R^k.

Gröbner bases for ideals in the algebra of Laurent polynomials over $\mathbb{Z}$ have first been considered in [8], Chapter 10.7. There they were defined with respect to a specified well-order on the set of Laurent-monomials. Our approach extends an idea of S. Zampieri, who introduced generalized term orders on the set of monomials in a polynomial ring in view of applications to the modelling problem in system theory [6]. Gröbner bases for monomial subalgebras of polynomial rings have been studied in [9], Chapter 11. A slightly more general situation (monomial algebras with no non-constant invertible elements) has been treated in [7], Chapter 3.

Let R be a commutative noetherian ring, let T be a finitely generated submonoid of the group $\{x^i \mid i \in \mathbb{Z}^n\}$ of power-products in the ring of Laurent polynomials $R[x_1, \dots, x_n, x_1^{-1}, \dots, x_n^{-1}]$, and let $R[T]$ be a subalgebra generated by T. In Section 2 we define generalized term orders on T and Gröbner bases (with respect to them) for submodules of finite-dimensional free $R[T]$-modules. We present a method to compute the intersection of an ideal in the ring of Laurent polynomials with the subring of all polynomials. (This answers a question of G. Traverso). In Section 3 we formulate and prove an analogon of Buchberger's Algorithm for the computation of Gröbner bases. In Section 4 several examples are discussed, among them those given in [10] and [11]. For the latter our method yields the results without essential computations.

We assume the reader to be familiar with the theory of Gröbner bases with respect to term orders (see [2], [1] or [3]).

2 Gröbner Bases with Respect to Generalized Term Orders

Let R be a commutative noetherian ring, let $n \in \mathbb{N}_{>0}$, and let

$$R[x, x^{-1}] := R[x_1, \dots, x_n, x_1^{-1}, \dots, x_n^{-1}]$$

be the commutative ring of Laurent polynomials over R. The set

$$\left\{ x^i := x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \mid i \in \mathbb{Z}^n \right\}$$

of power-products (or terms) in $R[x, x^{-1}]$is a group, isomorphic to $\mathbb{Z}^n$.

Let T be a finitely generated submonoid of $\left\{ x^i \mid i \in \mathbb{Z}^n \right\}$, e.g. $T = \left\{ x^i \mid i \in \mathbb{Z}^n \right\}$ or $T = \left\{ x^i \mid i \in \mathbb{Z}^m \times \mathbb{N}^{n-m} \right\}$.

Definition 2.1 (conic decomposition) *A "conic decomposition" of T is a finite family $(T_i)_{i \in I}$ of finitely generated submonoids of T, such that*
for each $i \in I$ the group generated by T_i contains T,
for each $i \in I$ the monoid T_i contains only one invertible element, and

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

Example 2.1 Let $T := \left\{ x^i \mid i \in \mathbb{Z}^n \right\}$ and let D be the set of all maps from $\{1, \dots, n\}$ to $\{-1, 1\}$. For $d \in D$ define

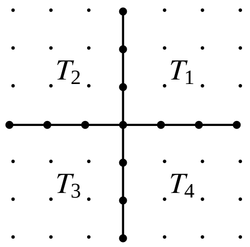
$$T_d := \left\{ x_1^{d(1)m_1} x_2^{d(2)m_2} \dots x_n^{d(n)m_n} \mid m_1, \dots, m_n \in \mathbb{N} \right\}.$$

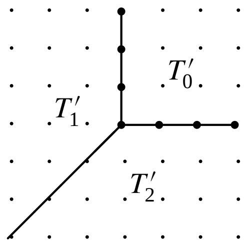
Then $(T_d)_{d \in D}$ is a conic decomposition of T.

Example 2.2 Let $T_0' := \left\{ x^i \mid i \in \mathbb{N}^n \right\}$ and let T_j' be the monoid generated by

$$\{x_1^{-1} x_2^{-2} \dots x_n^{-1}\} \cup \{x_1, x_2, \dots, x_n\} \setminus \{x_j\},$$

$1 \leq j \leq n$. Then $(T_j')_{0 \leq j \leq n}$ is a conic decomposition of $T := \left\{ x^i \mid i \in \mathbb{Z}^n \right\}$. The following figures illustrate the conic decompositions defined above for $n = 2$:





Notation. For a submonoid S of $\left\{ x^i \mid i \in \mathbb{Z}^n \right\}$ let

$$R[S] := \left\{ \sum_{s \in S} c_s s \mid c_s \in R \right\} \subseteq R[x, x^{-1}]$$

be the subalgebra of $R[x, x^{-1}]$ generated by S. (If we use the notation $\sum_{s \in S} c_s s$ we always assume that only finitely many c_s are not zero). Then $R[S]$ is the "monomial algebra defined by S".

Let V be a finite-dimensional free $R[T]$-module with basis B and let $U := \{tb \mid t \in T,\ b \in B\}$. If $(T_i)_{i\in I}$ is a conic decomposition of T, let $U_i := \{tb \mid t \in T_i,\ b \in B\}$, $i \in I$.
(If $V = R[T]$ and $B = \{1\}$, then $U_i = T_i$, for all $i \in I$).

Definition 2.2 (generalized term order) *Let $(T_i)_{i\in I}$ be a conic decomposition of T. A "generalized term order" on U for $(T_i)_{i\in I}$ is a total order $<$ on U such that*

b is the smallest element in $\{tb \mid t \in T\}$, for all $b \in B$,

and

$r < s$ implies $tr < ts$, for all $i \in I$, $s \in U_i$, $t \in T_i$, and $r \in U$.

Remark 2.1 If $|I| = 1$ and $T = \left\{x^i \mid i \in \mathbb{N}^n\right\}$, then T is a (trivial) conic decomposition of T. In this case any generalized term order is a term order.

Remark 2.2 Let $(T_i)_{i\in I}$ be a conic decomposition of T, $V = R[T]$, and $B = \{t\}$, where t is an invertible element of T. Then $U_i = tT_i$ and t is the minimal element in $T = U$ with respect to every generalized term order for $(T_i)_{i\in I}$.

The following Lemma shows how to construct a generalized term order on T and on U.

Lemma 2.1 *Let $(T_i)_{i\in I}$ be a conic decomposition of T and let $S := \{1\}$ or $S := T_j$ for some $j \in I$. Let $<_G$ be a total group order on $G := \left\{x^i \mid i \in \mathbb{Z}^n\right\}$ such that 1 is the smallest element in S and let $<_B$ be a total order on B. Let $f : T \longrightarrow \mathbb{Q}_{\geq 0}$ be a function fulfilling the following conditions:*

1. *for all $t \in T \setminus S$: $f(t) > 0$,*
2. *for all $s, t \in T$: $f(st) \leq f(s) + f(t)$,*
3. *for all $i \in I$: $f|_{T_i}$ is a monoid-homomorphism.*

Then the order $<_T$ defined by

$$r <_T s :\Longleftrightarrow f(r) < f(s) \text{ or } (f(r) = f(s) \text{ and } r <_G s),$$

for all $r, s \in T$, is a generalized term order on T for $(T_i)_{i\in I}$.
The order defined by

$$rb <_U sc :\Longleftrightarrow r <_T s \text{ or } (r = s \text{ and } b <_B c),$$

for all $r, s \in T$, $b, c \in B$, is a generalized term order on U for $(T_i)_{i\in I}$.

Proof. Conditions 1 and 3 for f imply that 1 is the smallest element in T. Let $r \in T$, $i \in I$, $s, t \in T_i$ such that $r <_T s$. Then

$$f(r) < f(s) \text{ or } f(r) = f(s) \text{ and } r <_G s.$$

In the first case we have

$$f(rt) \leq f(r) + f(t) < f(s) + f(t) = f(st)$$

hence $rt <_T st$. In the second case we have

$$f(rt) \leq f(r) + f(t) = f(s) + f(t) = f(st) \text{ and } rt <_G st$$

(since $<_G$ is a group order), hence $rt <_T st$. □

Example 2.3 Let $(T_d)_{d\in D}$ be the conic decomposition defined in Example 2.1. Define

$$f(x_1^{i_1}x_2^{i_2}\dots x_n^{i_n}) := |i_1| + |i_2| + \dots + |i_n|$$

and
$x_1^{i_1}x_2^{i_2}\dots x_n^{i_n} <_G x_1^{j_1}x_2^{j_2}\dots x_n^{j_n}$ if and only if $(i_1, i_2, \dots, i_n)$ is lexicographically smaller than $(j_1, j_2, \dots, j_n)$. Then $<_T$ (defined by f and $<_G$) is a generalized term order on T for $(T_d)_{d\in D}$.

Example 2.4 Let $(T_j)_{0\leq j\leq n}$ be the conic decomposition defined in Example 2.2. Define

$$f(x_1^{i_1}x_2^{i_2}\dots x_n^{i_n}) := i_1 + \dots + i_n - (n+1)\min\{0, i_1, i_2, \dots, i_n\}$$

and define $<_G$ as in Example 2.3. Then $<_T$ is a generalized term order on T for $(T_j)_{0\leq j\leq n}$.

Example 2.5 Let $(T_j)_{0\leq j\leq n}$ and $<_G$ be as in Example 2.4. Define

$$f(x_1^{i_1}x_2^{i_2}\dots x_n^{i_n}) := -\min\{0, i_1, i_2, \dots, i_n\}.$$

Then $<_T$ is a generalized term order on T for $(T_j)_{0\leq j\leq n}$. All elements of T_0 are smaller than any element of $T \setminus T_0$.

Lemma 2.2 *(see [6], 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 $\mathbb{Z}[T_i]$ is strictly increasing. Since the monoid T_i is finitely generated, the ring $\mathbb{Z}[T_i]$ is noetherian. This yields the assertion. □

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 $f = \sum_{u\in U} c_u u$ be a non-zero element in V, $c_u \in R$. Then we define*
$supp(f) := \{u \in U \mid c_u \neq 0\}$ (the "support of f"),
$lt(f) := \max supp(f)$ (the "leading term of f"),
$lc(f) := c_{lt(f)}$, (the "leading coefficient of f"),
$lm(f) := lc(f)lt(f)$ (the "leading monomial of f"), and
$T_i(f) := \{t \in T \mid lt(tf) \in U_i\}$, $i \in I$.

Definition 2.4 (Gröbner basis) *Let W be an $R[T]$-submodule of V and G a finite subset of $W \setminus \{0\}$.*
Then G is a Gröbner basis of W (with respect to a conic decomposition $(T_i)_{i\in I}$ of T and a generalized term order $<$ on U) if and only if for all $i \in I$ the $R[T_i]$-module

$$_{R[T_i]}\langle\, lm(f);\ f \neq 0,\ f \in W,\ lt(f) \in U_i\,\rangle$$

is generated by

$$\{\, lm(tg);\ g \in G,\ t \in T_i(g)\,\}.$$

Example 2.6 Let $f \in V \setminus \{0\}$ and $W := R[T]f$. If R is a domain, then $\{\, f\,\}$ is a Gröbner basis of W (with respect to every generalized term order). But for $R := \mathbb{Z}_4$, $V := \mathbb{Z}_4[x_1]$, $f := \overline{2}x_1 + \overline{1}$, and $W := \mathbb{Z}_4[x_1]f$, the set $\{\, f\,\}$ is not a Gröbner basis of W, since $\overline{2}f = \overline{2} \in W$.

Proposition 2.1 *Let G be a Gröbner basis of an ideal W in $R[x_1, \dots, x_n, x_1^{-1}, \dots, x_n^{-1}]$ with respect to the generalized term order $<_T$ defined in Example 2.5. For $g \in R[x_1, \dots, x_n, x_1^{-1}, \dots, x_n^{-1}]$ let $t(g) \in T$ be the uniquely determined power-product such that*

$$\bigcap_{s\in supp(g)} s^{-1}T_0 = t(g)T_0\,.$$

Then $\{t(g)g | g \in G\}$ is a Gröbner basis of $W \cap R[x_1, \dots, x_n]$.

Proof. Let $f \in W$. Since $<_T$ is the order defined in Example 2.5, $lt(f) \in T_0$ implies $supp(f) \subseteq T_0$, i.e. $f \in R[x_1, \dots, x_n]$. Hence

$$_{R[x_1,\dots,x_n]}\langle lm(f);\ f \neq 0, f \in W, lt(f) \in T_0\rangle$$
$$= {}_{R[x_1,\dots,x_n]}\langle lm(f);\ f \neq 0, f \in W \cap R[x_1, \dots, x_n]\rangle.$$

Let $t \in T_0(g)$ and $g \in G$. Then $lt(tg) \in T_0$ and $supp(tg) \subseteq T_0$. Therefore

$$t \in \bigcap_{s\in supp(g)} s^{-1}T_0$$

and there is an $u \in T_0$ such that $t = t(g)u$. Hence $\{lm(tg);\ g \in G, t \in T_0(g)\}$ and $\{lm(t(g)g);\ g \in G\}$ generate the same ideal in $R[x_1, \dots, x_n]$. □

Remark 2.3 Proposition 2.1 yields a method to compute generators of the ideal $W \cap R[x_1, \dots, x_n]$, see Example 4.1.

Lemma 2.3 *(See [6] , Lemma 2.1 and Lemma 2.2)*
1. Let N be a finite subset of T and let $i \in I$. Then there is a $p \in T_i$ such that $pN \subseteq T_i$.
2. Let $0 \neq f \in V$, $s, t \in T_i(f)$, and let $u, v \in supp(f)$ such that $lt(tf) = tu \in U_i$, $lt(sf) = sv \in U_i$. Then $u = v$.

Proof. 1. The group generated by T_i contains T, hence for every $t \in N$ there are $r_t, s_t \in T_i$ such that $r_t^{-1}s_t = t$. Then take $p := \prod_{t \in N} r_t \in T_i$.
2. Since $u, v \in supp(f)$, $tv \le tu$ and $su \le sv$. Choose $p \in T_i$ such that $pu,\ pv \in U_i$ and $ps,\ pt \in T_i$ (see 1). Then

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

and

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

Hence

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

This implies

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

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

Definition 2.5 *Let* $0 \ne f \in V$, $i \in I$ *and* $t \in T_i(f)$. *Then define*

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

Remark 2.4 By Lemma 2.3, $lt_i(f)$ is well-defined (i.e. 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 $p.supp(f) \subseteq U_i$ (cf. Lemma 2.3). Then $lt(pf) \in U_i$ and $lt_i(f) = \frac{lt(pf)}{p}$.

For the computation of the sets $T_i(f)$ see chapter 4.

3 Buchberger's Algorithm for Generalized Term Orders

We maintain the notations of Section 2 and fix a conic decomposition $(T_i)_{i \in I}$ of T and a generalized term order $<$ on U.

Definition 3.1 *Let* F *be a finite subset of* $V \setminus \{0\}$ *and let* $0 \ne (h_f)_{f \in F}$ *be a family in* $R[T]$. *Then*

$$u_F((h_f)_{f \in F}) := max \left\{ tv \mid (t, v) \in \bigcup_{f \in F} (supp(h_f) \times supp(f)) \right\}\ .$$

Remark 3.1 Consider two families $0 \ne (h_f)_{f \in F}$, $0 \ne (h'_f)_{f \in F}$ in $R[T]$. Let $u := u_F((h_f)_{f \in F})$ and $u' := u_F((h'_f)_{f \in F}$. Then

$$u_F((h_f + h'_f)_{f \in F}) \le max\{u, u'\}\ .$$

(If $u \ne u'$, then $u_F((h_f + h'_f)_{f \in F}) = max\{u, u'\}$).

If $u \in U_i$ and $t \in T_i$, then

$$u_F((th_f)_{f \in F}) = tu \in U_i \, .$$

If $u' \in U_i$, $u < u'$ and $t \in T_i$, then

$$u_F((th_f)_{f \in F}) < tu' \, .$$

If $c \in R$ and $(ch_f)_{f \in F} \neq 0$, then $u_F((ch_f)_{f \in F}) \leq u$. (If c is not a zero-divisor in R, then $u_F((ch_f)_{f \in F}) = u$).

Proposition 3.1 *Let F be a finite subset of $V \setminus \{0\}$ and let $g \in V$. Then there is a family $(h_f)_{f \in F}$ in $R[T]$such that*

$$(h_f)_{f \in F} = 0 \text{ or } u_F((h_f)_{f \in F}) = lt(g)$$

and

$$g = \sum_{f \in F} h_f f \quad \text{or} \quad lm(g - \sum_{f \in F} h_f f) \notin \bigcup_{i \in I} {}_{R[T_i]}\langle lm(tf);\, f \in F, t \in T_i(f)\rangle \ .$$

The family $(h_f)_{f \in F}$ can be computed as follows ("Division algorithm"):

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

While there are $c_f \in R$, $t_f \in T$ such that $lm(g) = \sum_{f \in F} c_f lm(t_f f)$, replace h_f by $h_f + c_f t_f$ and g by $g - \sum_{f \in F} c_f t_f f$.

(Note that this "algorithm" is effective only under the hypothesis that we can solve linear equations over R).

Proof. We only have to show that the algorithm above terminates after a finite number of steps. But since in each step $lt(g - \sum_{f \in F} c_f t_f f) < lt(g)$, this follows from Lemma 2.2 . □

Definition 3.2 *Let F, g, h_f be as in the proposition above. Then $rem(g, F) := g - \sum_{f \in F} h_f f$ is "a remainder on division of g by F".*
(It is clear that $rem(g, F)$ is not uniquely determined by g and F).

Proposition 3.2 *Let W be a non-zero submodule of V .*
1. W contains a Gröbner basis.
2. Let G be a Gröbner basis of W. Then $f \in V$ is an element of W if and only if a remainder (or all remainders) on division of f by G is zero.
3. Each Gröbner basis of W generates the $R[T]$-module W.

Proof. 1. For all $i \in I$ choose a finite subset E_i of $\{lm(f) \mid f \neq 0, f \in W, lt(f) \in U_i\}$ which generates the $R[T_i]$-submodule ${}_{R[T_i]}\langle lm(f);\, 0 \neq f, f \in W, lt(f) \in U_i\rangle$. Then

$$\left\{ f \in W \mid lm(f) \in \bigcup_{i \in I} E_i \right\}$$

is a Gröbner basis of W.
2. follows from Proposition 3.1.
3. follows from 2. □

Remark 3.2 Let $i \in I$ and let $E \subseteq V \setminus \{0\}$. Then

$$\bigcap_{g \in E} {}_{R[T_i]}\langle lt(tg);\ t \in T_i(g)\rangle = \{0\}$$

if and only if there are elements $f, g \in E$ such that $lt_i(f) = lt_i(f)^*b, lt_i(g) = lt_i(g)^*c$, where $lt_i(f)^* \in T, lt_i(g)^* \in T, b \in B, c \in B$ and $b \neq c$.

Proposition 3.3 *Let G be a finite subset of $V \setminus \{0\}$ and let W be the $R[T]$-submodule of V generated by G. For $i \in I$ and $E \subseteq G$ let $S(i, E)$ be a finite system of generators of the R-module*

$$\left\{ (c_g)_{g\in E} \in R^E \mid \sum_{g \in E} c_g lc_i(g) = 0 \right\}$$

and let $U(i, E) \subseteq U_i$ be a finite system of generators of the $R[T_i]$-module

$$\bigcap_{g \in E} {}_{R[T_i]}\langle lt(tg);\ t \in T_i(g)\rangle$$

(i.e. $U(i, E) = \emptyset$ or $\bigcap_{g\in E} T_i(g)lt_i(g) = T_i.U(i, E)$).
Then the following assertions are equivalent:
(1) G is a Gröbner basis of W.
(2) For all $i \in I$, for all $E \subseteq G$ such that $U(i, E) \neq \emptyset$, for all $s = (s_g)_{g\in G} \in S(i, E)$, and for all $v \in U(i, E)$:

$$rem\left(\sum_{g\in E} s_g \frac{v}{lt_i(g)} g, G\right) = 0\,.$$

(Here $\frac{v}{lt_i(g)}$ means $\frac{v^*}{lt_i(g)^*}$, where v^* and $lt_i(g)^*$ are the power-products in $R[T]$ with $v^*b = v$ and $lt_i(g)^*b = lt_i(g)$, for some $b \in B$, see Remark 3.2).

Proof. (1) $\Rightarrow$ (2) : Since $\sum_{g\in E} c_s \frac{v}{lt_i(g)} g$ is an element of W, the assertion follows from Proposition 3.2.
(2) $\Rightarrow$ (1) : Let $f \in W$, $f \neq 0$. We have to show

$$lm(f) \in \bigcup_{i\in I} {}_{R[T_i]}\langle lm(tg);\ g \in G, t \in T_i(g)\rangle\ .$$

Since W is generated by G, we have

$$f = \sum_{g\in G} h_g g\,,$$

for some $h_g \in R[T]$.
Let $u := u_G((h_g)_{g\in G})$. We choose the family $(h_g)_{g\in G}$ such that u is minimal, i.e. if

$$f = \sum_{g\in G} h'_g g$$

then $u \leq u_G((h'_g)_{g\in G})$.
Let $j \in I$ be such that $u \in U_j$and let

$$E := \left\{ g \in G \mid \text{ there is a } p(g) \in supp(h_g) \text{ such that } p(g)lt_j(g) = u \right\} .$$

Then E is not empty and for all $g \in E$ we have $p(g) \in T_j(g)$. Let $c_g \in R$ be the coefficient of h_g at $p(g)$. If $c_g lc_j(g) \neq 0$, then $lm(h_g g) = c_g lc_j(g)u$, otherwise $h_g g = 0$ or $lt(h_g g) < u$. It is clear that $lt(f) \leq u$.
If $lt(f) = u$, then

$$E' := \left\{ g \in E \mid lt(h_g g) = u \right\}$$

is not empty and

$$lm(f) = \sum_{g\in E'} lm(h_g g) = \sum_{g\in E'} c_g lm(p(g)g) \in {}_{R[T_j]}\langle lm(tg); g \in G, t \in T_j(g)\rangle .$$

Hence it remains to show that $lt(f)$ cannot be smaller than u.
If $lt(f) < u$, then

$$\sum_{g\in E} c_g lc_i(g) = 0.$$

Hence there is a family $(d_s)_{s\in S(j,E)}$ in R such that

$$(c_g)_{g\in G} = \sum_{s\in S(j,E)} d_s s ,$$

i.e. for all $g \in E$, $c_g = \sum_{s\in S(j,E)} d_s s_g$. For $g \in E$ define $\overline{h}_g := c_g p(g)$, for $g \in G \setminus E$ let $\overline{h}_g := 0$. Then

$$f = \sum_{g\in G} h_g g = \sum_{g\in G} (h_g - \overline{h}_g)g + \sum_{g\in E} \overline{h}_g g$$

and

$$u_G((h_g - \overline{h}_g)_{g\in G}) < u .$$

Now consider

$$\sum_{g\in E} \overline{h}_g g = \sum_{g\in E} c_g p(g)g = \sum_{s\in S(j,E)} d_s \sum_{g\in E} s_g p(g)g .$$

For $g \in E$ we have $p(g)lt_j(g) = u \in U_j$ and $p(g) \in T_j(g)$, thus $u \in \bigcap_{g\in E} T_j(g)lt_j(g)$. Hence there are $v \in U(j, E) \subseteq U_j$ and $r \in T_j$ such that $r.v = u$. Let $q(g) \in T_j(g)$ be such that $v = q(g)lt_j(g)$, i.e.

$$q(g) = \frac{v}{lt_j(g)} .$$

Then

$$r \cdot q(g)lt_j(g) = r \cdot v = u = p(g)lt_j(g) ,$$

hence $p(g) = r \cdot q(g)$ and

$$\sum_{g\in E} \overline{h}_g g = \sum_{s\in S(j,E)} d_s r \sum_{g\in E} s_g q(g)g .$$

By (2), for every $s \in S(j, E)$ there is a family $(k_{g,s})_{g\in G}$ in $R[T]$such that

$$\sum_{g\in E} s_g q(g)g = \sum_{g\in G} k_{g,s} g$$

and

$$u_G((k_{g,s})_{g\in G}) = lt\left(\sum_{g\in E} s_g q(g)g\right) =: w(s) .$$

For all $g \in E$ we have $lt(q(g)g) = v \in U_j$ and moreover $\sum_{g\in E} s_g lc_j(g) = 0$. Hence $w(s) < v \in U_j$. Since $r \in T_j$, this implies

$$u_G((rk_{g,s})_{g\in G}) < r \cdot v = u \in U_j$$

(see Remark 3.1). Thus

$$\sum_{g\in E} \overline{h}_g g = \sum_{g\in G} \left(\sum_{s\in S(j,E)} d_s r k_{g,s}\right) g ,$$

and

$$u_G\left(\left(\sum_{s\in S(j)} d_s r k_{g,s}\right)_{g\in G}\right) < u$$

(see Remark 3.1). For all $g \in G$ let

$$h'_g := (h_g - \overline{h}_g) + \sum_{s\in S(j,E)} d_s r k_{g,s} ,$$

then

$$u_G((h'_g)_{g\in G}) < u \text{ and } f = \sum_{g\in G} h'_g g ,$$

which contradicts the minimality of u. □

Proposition 3.4 *Let R be a principal ideal domain (e.g. a field). Let G be a finite subset of $V \setminus \{0\}$ and let W be the $R[T]$-submodule of V generated by G. For $i \in I$ and $f, g \in G$ let $U(i, f, g) \subseteq U_i$ be a finite system of generators of the $R[T_i]$-module*

$$_{R[T_i]}\langle lt(tf);\ t \in T_i(f)\rangle \cap {}_{R[T_i]}\langle lt(tg);\ t \in T_i(g)\rangle$$

(i.e. $U(i, E) = \emptyset$ or $T_i(f)lt_i(f) \cap T_i(g)lt_i(g) = T_i.U(i, f, g)$) and let $L_i(f, g)$ be a least common multiple of $lc_i(f)$ and $lc_i(g)$. For $v \in U(i, f, g)$ define

$$S(i, f, g, v) := \frac{L_i(f, g)}{lc_i(f)} \frac{v}{lt_i(f)} f - \frac{L_i(f, g)}{lc_i(g)} \frac{v}{lt_i(g)} g \in W\ .$$

Then the following assertions are equivalent:
(1) G is a Gröbner basis of W.
(2) For all $i \in I$, for all $f, g \in G$, and for all $v \in U(i, f, g)$

$$rem(S(i, f, g, v), G) = 0\ .$$

Proof. Let $E \subseteq G$ be a subset with at least two elements and let $\left\{ \delta_g \mid g \in E \right\} \subseteq R^E$ be the standard-basis of R^E. If R is a principal ideal domain, then $\left\{ \frac{L_i(f,g)}{lc_i(f)} \delta_f - \frac{L_i(f,g)}{lc_i(g)} \delta_g \mid f, g \in E \right\}$ is a finite system of generators of

$$\left\{ (c_g)_{g \in E} \in R^E \mid \sum_{g \in E} c_g lc_i(g) = 0 \right\}$$

(see for example [5], Lemma 3.4). Hence Proposition 3.4 is a Corollary of Proposition 3.3 . □

Proposition 3.5 (Buchberger's Algorithm) *Let G be a finite subset of $V \setminus \{0\}$ and let W be the $R[T]$ -submodule generated by G. For $i \in I$ and $E \subseteq G$ let $S(i, E)$ be a finite system of generators of the R-module*

$$\left\{ (c_g)_{g \in E} \in R^E \mid \sum_{g \in E} c_g lc_i(g) = 0 \right\} \text{ and}$$

let $U(i, E) \subseteq U_i$ be a finite system of generators of the $R[T_i]$-module

$$\bigcap_{g \in E} {}_{R[T_i]}\langle lt(tg);\ t \in T_i(g)\rangle$$

(i.e. $U(i, E) = \emptyset$ or $\bigcap_{g \in E} T_i(g)lt_i(g) = T_i.U(i, E)$).

By the following algorithm a Gröbner basis of W can be computed:
$G_0 := G$,
$G_{j+1} := G_j \cup (\{rem(\sum_{g \in E} s_g \frac{v}{lt_i(g)} g, G_j) | i \in I,\ E \subseteq G_j,\ s \in S(i, E),$ $v \in U(i, E)\} \setminus \{0\}$.
If $G_{j+1} = G_j$, then G_j is a Gröbner basis of J.

Proof. By Proposition 3.3 we only have to show that there is a $k \in \mathbb{N}$ such that $G_k = G_{k+1}$. Suppose there is no such k. Then there is an index $i \in I$ such that for all $j \in \mathbb{N}$ there is a $m \in \mathbb{N}$ such that the $R[T_i]$-submodule $\langle lm(tg);\ g \in G_j, t \in T_i(g)\rangle$ of $\bigoplus_{b \in B} R[T_i]b$ is strictly contained in $\langle lm(tg);\ g \in G_{j+m}, t \in T_i(g)\rangle$. Since $R[T_i]$ is noetherian, this is not possible. □

4 Examples

Let F be a finite subset of $V \setminus \{0\}$. In order to compute a Gröbner basis of the submodule generated by F, we first have to determine the sets $T_i(f)$, for all $i \in I$, $f \in F$. For that purpose we use the facts that

$$T = \bigcup_{i \in I} T_i(f)$$

and

$$T_i.T_i(f) = T_i(f), \text{ for all } i \in I,$$

as well as the following two lemmas.

Lemma 4.1 *Let $(T_i)_{i \in I}$ be a conic decomposition of T such that*

$${}_{gr}\langle T_i \cap T_j\rangle \cap T_i = T_i \cap T_j$$

for all $i, j \in I$. (Here ${}_{gr}\langle T_i \cap T_j\rangle$ is the subgroup of $\{x^i | i \in \mathbb{Z}^n\}$ generated by $T_i \cap T_j$). Let $f \in V$ and $i, j \in I$ such that $T_i(f) \cap T_j(f) \neq \emptyset$. Then

$$lt_i(f) = lt_j(f) \textit{ and}$$

$$t \in T_i(f),\ s \in T_i \cap T_j,\ st \in T_i(f) \cap T_j(f) \textit{ imply } t \in T_j(f).$$

Proof. From $T_i(f) \cap T_j(f) \neq \emptyset$ and the uniqueness of $lt_i(f)$ and $lt_j(f)$ we get $lt_i(f) = lt_j(f) =: l$.
Now $lt(tf) = tl \in T_i$ and $lt(stf) = stl \in T_i \cap T_j$. We have to show that $tl \in T_j$.
Let $v := stl$, then $tl = s^{-1}v \in {}_{gr}\langle T_i \cap T_j\rangle \cap T_i = T_i \cap T_j$. Thus $tl \in T_j$. □

Lemma 4.2 *Let $f \in R[T]$ and let $(T_i)_{i \in I}$ be a conic decomposition of T. If there exists a subset $\emptyset \neq J \subseteq I$ such that*

$$\bigcap_{j \in J} T_j = \{1\} \textit{ and } \bigcap_{j \in J} T_j(f) \neq \emptyset$$

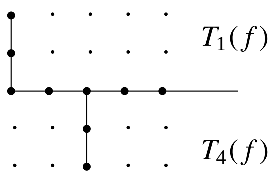
then

$$f \in T \textit{ and } \bigcap_{j \in J} T_j(f) = \{f^{-1}\}.$$

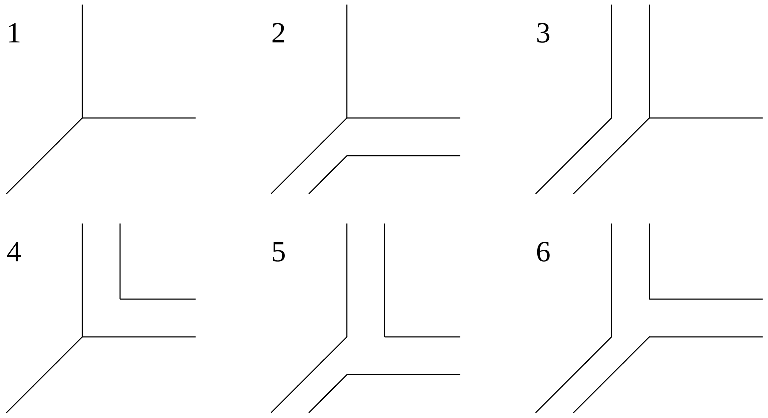
Proof. Let $t \in \bigcap_{j\in J} T_j(f)$. Then $lt(tf) \in \bigcap_{j\in J} T_j = \{1\}$. Since 1 is the smallest element in T, we have $tf = 1$ and $t = f^{-1}$. □

Remark 4.1 The conic decompositions defined in Examples 2.1 and 2.2 fulfill the condition in Lemma 4.1.

Hence, if we take for instance the generalized term order defined in Example 2.3 (with $n = 2$), the following case cannot occur: $T_1(f) = T_1,\ T_4(f) = T_4.x_1^2$.



Remark 4.2 Let $T := \{x^i | i \in \mathbb{Z}^2\}$ and let $<$ be the generalized term order with respect to (T_0, T_1, T_2) defined in Example 2.4. Using Lemma 4.1 it is easy to see that the $T_i(f)$'s are always generated by one element and that only six different cases for $(T_0(f), T_1(f), T_2(f))$ can occur:



Moreover, the intersections $\bigcap_{g\in E} T_i(g).lt_i(g)$ (cf. Proposition 3.3) are generated by one element, i.e. the sets $U(i, E)$ contain only one element. Consequently Buchberger's algorithm for this generalized term order is particularly simple.

The following algorithm computes $T_0(f)$, $T_1(f)$ and $T_2(f)$ for $f \in R[T]$. For $s = x_1^{i_1} x_2^{i_2} \in T$ let $e_k(s) := i_k,\ k = 1, 2$.

Algorithm

Input: $f \in R[T]$

Output: $T_0(f), T_1(f), T_2(f)$

If f is a monomial then

```
    $T_0(f) = T_0.f^{-1}$, $T_1(f) = T_1.f^{-1}$, $T_2(f) = T_2.f^{-1}$ (Case 1). END
For $k = 1$ to 2 do
    $m_k := -\min(\{e_k(s) | s \in supp(f)\} \cup \{0\})$
$t := x_1^{m_1} x_2^{m_2}$
While ($t \in T_0(f)$) do
    $t := t.x_1^{-1} x_2^{-1}$
$t := t.x_1 x_2$
While ($t \in T_0(f)$) do
    $t := t.x_1^{-1}$
$t := t.x_1$
While ($t \in T_0(f)$) do
    $t := t.x_2^{-1}$
$t := t.x_2$
If $t \in T_1(f)$ then
    $T_0(f) = T_0.t,\ T_1(f) = T_1.t,\ T_2(f) = T_2.(t.x_2^{-1})$ (Case 2). END
If $t \in T_2(f)$ then
    $T_0(f) = T_0.t,\ T_1(f) = T_1.(t.x_1^{-1}),\ T_2(f) = T_2.t$ (Case 3). END
If $t.x_1^{-1} x_2^{-1} \notin T_1(f)$ then
    $T_0(f) = T_0.t,\ T_1(f) = T_1.(t.x_1^{-1}),\ T_2(f) = T_2.(t.x_1^{-1} x_2^{-1})$ (Case 5). END
If $t.x_1^{-1} x_2^{-1} \notin T_2(f)$ then
    $T_0(f) = T_0.t,\ T_1(f) = T_1.(t.x_1^{-1} x_2^{-1}),\ T_2(f) = T_2.(t.x_2^{-1})$ (Case 6). END
$T_0(f) = T_0.t,\ T_1(f) = T_1.(t.x_1^{-1} x_2^{-2}),\ T_2(f) = T_2.(t.x_1^{-1} x_2^{-1})$ (Case 4). END
End of Algorithm.
```

For the conic decomposition defined in Example 2.1 the analogous algorithm is slightly more complicated (in this case the $T_i(f)$'s may be generated by more than one element) but still not costly.

Example 4.1 We compute a Gröbner basis with respect to the generalized term order defined in Example 2.5 of the ideal W generated by $f := x_1^{-2} x_2^{-2} + x_2^2$ and $g := x_1 x_2^{-3} + x_1 x_2$ in $\mathbb{Q}[x_1, x_2, x_1^{-1}, x_2^{-1}]$.

Let $F = \{f, g\}$.

Now
$lt(f) = x_1^{-2} x_2^{-2} \in T_1 \cap T_2$;
$lt_0(f) = x_2^2,\ T_0(f) = T_0 \cdot x_1^2 x_2^2;\ lt_1(f) = x_1^{-2} x_2^{-1},\ T_1(f) = T_1 \cdot x_1 x_2$;
$lt_2(f) = x_1^{-2} x_2^{-1},\ T_2(f) = T_2 \cdot x_1 x_2$;
$lt(g) = x_1 x_2^{-3} \in T_2$.

Since $lt(g) \in T_2(f) \cdot lt_2(f)$ we may replace g by
$-rem(g, \{f\}) = x_1^3 x_2 - x_1 x_2 =: h_1$ and F by $\{f, h_1\}$.

Since

$lt(h_1) = x_1^3 x_2 \in T_0$;
$lt_0(h_1) = x_1^3 x_2,\ T_0(h_1) = T_0 \cdot x_1^{-1} x_2^{-1};\ lt_1(h_1) = x_1 x_2,\ T_1(h_1) = T_1 \cdot x_1^{-2} x_2^{-1}$;
$lt_2(h_1) = x_1^3 x_2,\ T_2(h_1) = T_2 \cdot x_1^{-1} x_2^{-1}$.

Now

$T_0(f) \cdot lt_0(f) \cap T_0(h_1) \cdot lt_0(h_1) = T_0 \cdot x_1^2 x_2^4,\ S(0, f, h_1, x_1^2 x_2^4) = 1 + x_2^4 =: h_2$,
$T_1(f) \cdot lt_1(f) \cap T_1(h_1) \cdot lt_1(h_1) = T_1 . x_1^{-1} x_2$,
$S(1, f, h_1, x_1^{-1} x_2) = x_1^{-3} x_2^{-3} + x_1 x_2 =: h_2, rem(h_2, F) = h_2$;

We have
$lt(h_2) = x_2^4 \in T_0 \cap T_1$,
$lt_0(h_2) = x_2^4,\ T_0(h_2) = T_0;\ lt_1(h_1) = x_2^4,\ T_1(h_2) = T_1$;
$lt_2(h_2) = 1,\ T_2(h_2) = T_2 \cdot x_2^{-1}$ and $T_0(h_2) lt_0(h_2) \cap T_0(h_1) lt_0(h_1) =$
$T_0 \cdot x_1^2 x_2^4,\ S(0, h_1, h_2, x_1^2 x_2^4) = -x_2^4 - x_1^2 = -h_2 + 1 - x_1^2$.

Let $h_3 := x_1^2 - 1$ and $F := \{f, h_1, h_2, h_3\}$.

All further S-polynomials reduce to 0. Thus the set

$$G := \{x_1^{-2} x_2^{-2} + x_2^2, x_1^3 x_2 - x_1 x_2, x_2^4 - 1, x_1^2 - 1\}$$

is a Gröbner basis of W and

$$\{x^m | m \in \mathbb{Z}^2\} \setminus \bigcup_{0 \le i \le 2, g \in G} T_i(g) lt_i(g) \ = \ \{x^m | m \in \Delta\},$$

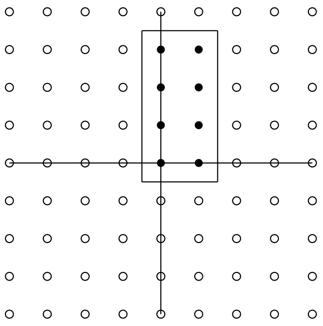
where $\Delta = \{(0,0), (1,0), (0,1), (1,1), (0,2), (1,2), (0,3), (1,3)\}$.

Hence for all $y : \ \Delta \to \mathbb{Q}$ there is a unique solution $z : \ \mathbb{Z}^2 \to \mathbb{Q}$ of the system of difference equations

$$z(-2 + s_1, -2 + s_2) + z(s_1, 2 + s_2) = 0$$

$$z(1 + s_1, -3 + s_2) + z(1 + s_1, 1 + s_2) = 0\ ,$$

for all $(s_1, s_2) \in \mathbb{Z}^2$, such that $z|_\Delta = y$ (see chapter 1).



By Proposition 2.1 the set $\{x_1^2 x_2^2 f, x_1^3 - x_1 x_2, x_2^4 + 1, x_1^2 - 1\}$ is a Gröbner basis of $W \cap \mathbb{Q}[x_1, x_2]$. The reduced Gröbner basis of $W \cap \mathbb{Q}[x_1, x_2]$ is $\{x_2^4 + 1, x_1^2 - 1\}$.

Example 4.2 We compute a Gröbner basis with respect to the generalized term order defined in Example 2.3 of the ideal generated by $f := x_1^{-1}x_2 + x_2$ and $g := x_1^{-2}x_2^{-1} + x_1$ in $\mathbb{Q}[x_1, x_2, x_1^{-1}, x_2^{-1}]$.

Let $F := \{f, g\}$.

We get
$lt(f) = x_1^{-1}x_2 \in T_2$;
$lt_1(f) = x_2,\ T_1(f) = T_1 \cdot x_1x_2^{-1}$; $lt_2(f) = x_1^{-1}x_2,\ T_2(f) = T_2 \cdot x_2^{-1}$;
$lt_3(f) = x_1^{-1}x_2,\ T_3(f) = T_3 \cdot x_2^{-1}$; $lt_4(f) = x_2,\ T_4(f) = T_4 \cdot x_1x_2^{-1}$;
$lt(g) = x_1^{-2}x_2^{-1} \in T_3$;
$lt_1(g) = x_1,\ T_1(g) = T_1 \cdot x_1 \cup T_1 \cdot x_2$; $lt_2(g) = x_1^{-2}x_2^{-1},\ T_2(g) = T_2 \cdot x_1^{-1}x_2$;
$lt_3(g) = x_1^{-2}x_2^{-1},\ T_3(g) = T_3 \cdot 1$; $lt_4(g) = x_1,\ T_4(g) = T_4 \cdot x_1$.

Since $lt(g) \in T_3(f).lt_3(f)$ we replace g by $rem(g, \{f\}) = x_2^{-1} - 1 =: g'$ and F by $\{f, g'\}$. Now
$lt(g') = x_2^{-1} \in T_3 \cap T_4$;
$lt_1(g') = -1,\ T_1(g') = T_1.x_2$; $lt_2(g') = -1,\ T_2(g') = T_2.x_2$;
$lt_3(g') = x_2^{-1},\ T_3(g') = T_3.1$; $lt_4(g') = x_2^{-1},\ T_4(g') = T_4.1$;
$rem(f, \{g'\}) = x_1^{-1} + 1$ and $\{x_1^{-1} + 1, x_2^{-1} - 1\}$ is a Gröbner basis.

Example 4.3 (compare [10] , section 5) Let $T := \{x^i | i \in \mathbb{Z}^2\}$, $V := \mathbb{R}[T]^2$ and let $\{e_1, e_2\}$ be the standard basis of V. We extend the generalized term order $<$ on T defined in Example 2.3 to a generalized term order $<_U$ on $U = \{te_i \mid t \in T,\ i = 1, 2\}$:

$$pe_i <_U qe_j \ :\Leftrightarrow\ p < q \text{ or } [\ p = q \text{ and } i < j\ ]$$

$$\text{for all } p, q \in \mathbb{R}[x_1, x_2, x_1^{-1}, x_2^{-1}],\ i, j \in \{1, 2\}.$$

Let W be the $\mathbb{R}[T]$-submodule generated by

$$g_1 = \begin{pmatrix} 2x_1x_2^{-1} + x_2 + x_2^{-1} \\ x_1^{-1}x_2 - x_1 \end{pmatrix} \text{ and } g_2 = \begin{pmatrix} x_1x_2^2 - 1 \\ x_1^2x_2^{-1} - x_2^{-1} + 2 \end{pmatrix}.$$

We obtain
$lt(g_1) = 2x_1x_2^{-1} \cdot e_1 \in T_4$;
$lt_1(g_1) = -x_1 \cdot e_2,\ T_1(g_1) = T_1 \cdot x_1x_2$;
$lt_2(g_1) = x_1^{-1}x_2 \cdot e_2,\ T_2(g_1) = T_2 \cdot x_1^{-1} \cup T_2 \cdot x_2$;
$lt_3(g_1) = x_2^{-1} \cdot e_1,\ T_3(g_1) = T_3 \cdot x_1^{-1}x_2^{-1}$;
$lt_4(g_1) = 2x_1x_2^{-1} \cdot e_1,\ T_4(g_1) = T_4 \cdot 1$;

$lt(g_2) = x_1^2x_2^{-1} \cdot e_2 \in T_4$;
$lt_1(g_2) = x_1x_2^2 \cdot e_1,\ T_1(g_2) = T_1 \cdot x_1^{-1}x_2$;
$lt_2(g_2) = x_1x_2^2 \cdot e_1,\ T_2(g_2) = T_2 \cdot x_1^{-2}$;
$lt_3(g_2) = -x_2^{-1} \cdot e_2,\ T_3(g_2) = T_3 \cdot x_1^{-2}x_2^{-1}$;
$lt_4(g_2) = x_1^2x_2^{-1} \cdot e_2,\ T_4(g_2) = T_4 \cdot x_1^{-1}$;

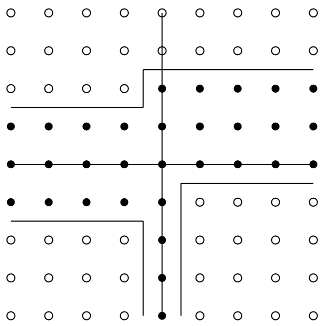
Since

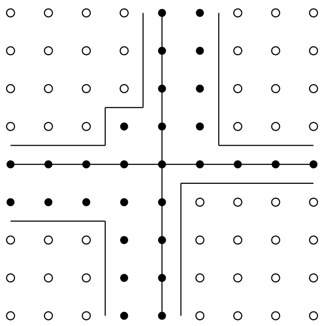
$$_{R[T_i]}\langle lt(tf);\ t \in T_i(f)\rangle \cap {}_{R[T_i]}\langle lt(tg);\ t \in T_i(g)\rangle \ = \ \{0\},$$

the set $U(i, f, g)$ is empty, for $1 \le i \le 4$, hence Proposition 3.4 immediately implies that $\{g_1, g_2\}$ is a Gröbner basis of W.

The following figures illustrate the sets Δ_1 and Δ_2, defined by

$$\{x^m e_j | m \in \mathbb{Z}^2\} \setminus \bigcup_{1\le i\le 4,\ 1\le k\le 2} T_i(g_k) lt_i(g_k) \ = \ \{x^m e_j | m \in \Delta_j\},\ \ j = 1, 2\ .$$





Example 4.4 For a single partial difference equation over $\mathbb{Z}^n$ (given by a Laurent polynomial $f \in \mathbb{R}[x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1}]$) we only have to determine the sets $T_i(f).lt_i(f)$, $i \in I$.

Let $n = 2$ and let $<$ be the generalized term order defined in Example 2.3. Then a set of “initial data” for the difference equation associated to $f := x_1x_2^{-1} + x_1 + x_1^{-1}x_2^{-1} + x_1^{-1}$ ([11], Section 5) is

$$\begin{aligned}&\{m \in \mathbb{Z}^2 | x^m \notin \bigcup_{1\le i\le 4} T_i(f).lt_i(f)\}\\ &\quad = \{(k, 0)|k \in \mathbb{Z}\} \cup \{(0, k)|k \in \mathbb{Z}\} \cup \{(-1, k)|k \in \mathbb{Z}\}.\end{aligned}$$

References

1. Becker, T., Weispfenning, V.: Gröbner Bases. Graduate Texts in Mathematics 141. New York: Springer 1993
2. Buchberger, B.: Gröbner bases: An algorithmic method in polynomial ideal theory. In: N. K. Bose, editor, Multidimensional Systems Theory, pp. 184–232. Dordrecht: Reidel, 1985
3. Eisenbud, D.: Commutative Algebra with a View Toward Algebraic Geometry. Graduate Texts in Mathematics 150. New York: Springer 1995
4. Oberst, U.: Multidimensional constant linear systems. Acta Applicandae Mathematicae **20**, 1–175 (1990)
5. Pauer, F., Pfeifhofer, M.: The Theory of Gröbner Bases. L'Enseignement Mathématique **34**, 215–232 (1988)
6. Pauer, F., Zampieri, S.: Gröbner Bases with respect to Generalized Term Orders and their Application to the Modelling Problem. J. Symbolic Computation **21**, 155–168 (1996)

7. Sakata, S.: Shift Register Synthesis on Convex Cones and Cylinders and Fast Decoding of General One-point AG Codes. Bull. of the University of Electro-Communications, 8(2), 187–203 (1995)
8. Sims, C.: Computation with finitely presented groups. Cambridge University Press 1994
9. Sturmfels, B.: Gröbner Bases and Convex Polytopes. Providence: Am. Math. Soc. 1996
10. Zampieri, S.: A Solution of the Cauchy Problem for Multidimensional Discrete Linear Shift-Invariant Systems. Linear Algebra and its Applications **202**, 143–162 (1994)
11. Zerz, E., Oberst, U.: The Canonical Cauchy Problem for Linear Systems of Partial Difference Equations with Constant Coefficients over the Complete r-Dimensional Integral Lattice $\mathbb{Z}^r$. Acta Applicandae Mathematicae **31**, 249–273 (1993)