Journal of Symbolic Computation 55 (2013) 19–29

Contents lists available at SciVerse ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Characterization of relative Gröbner bases

Christian Dönch

RISC, Johannes Kepler University Linz, A-4040 Linz, Austria

ARTICLE INFO

Article history:
Received 6 October 2012
Accepted 3 March 2013
Available online 15 March 2013

Keywords:
Relative Gröbner bases
Relative reduction
Symmetry of relative Gröbner bases
Characterization of relative Gröbner bases

ABSTRACT

We present a characterization of relative Gröbner bases and provide a result on the preservation of a relative Gröbner basis under changes of the involved orderings. Furthermore, we show that computing a relative Gröbner basis amounts to determining a finite basis of an ideal in a possibly non-Noetherian ring. We also provide an example where the method suggested by Zhou and Winkler for computing a relative Gröbner basis does not terminate.

1. Introduction

Dealing with polynomial rings in computer algebra is strongly connected to the concept of Gröbner bases. This is due to the fact that they are understood to provide a possibility of performing algorithms suitable for most essential computations in polynomial rings. One particular application is the computation of Hilbert polynomials of graded and filtered modules over polynomial rings. However a big drawback is the time complexity which in the worst case can be doubly exponential in the number of variables of the system of equations in concern. In fact, the complexity depends on the term order used for the computations. Levin (2007) introduced the notion of Gröbner bases with respect to several orderings as means of computing multivariate dimension polynomials associated with filtered D-modules. Relative Gröbner bases are a generalization of Gröbner bases taking into account two admissible orders. They were introduced by Zhou and Winkler (2008) in order to compute bivariate dimension polynomials associated with modules over rings of difference-differential operators. They also showed that the complexity for computing a relative Gröbner basis has to be at least as high as the maximum of the complexities of computing a Gröbner basis with respect to one of the two orders in concern but could not provide any upper bound. Nevertheless by now they are used as the main tool for the algorithmic computation of bivariate dimension polynomials.

E-mail address: cdoench@risc.jku.at.
URL: http://www.risc.jku.at/home/cdoench.

0747-7171/$ – see front matter
http://dx.doi.org/10.1016/j.jsc.2013.03.003

Several algorithms have been developed for transforming a given Gröbner basis with respect to a particular term order to a Gröbner basis with respect to a different term order with the motivation that in certain cases it is faster to compute a Gröbner basis with respect to an admissible order $\prec$ and then converting it to a Gröbner basis with respect to some other admissible order $\prec'$ than to directly compute a Gröbner basis with respect to $\prec'$. Two notable approaches are the FGLM algorithm (Faugère et al., 1993) and the Gröbner walk (Collart et al., 1997). For the Gröbner walk one uses a result regarding the preservation of a Gröbner basis under changes of admissible orders within the interior of one Gröbner cone (Collart et al., 1997, Lemma 2.2).

The Gröbner walk algorithm relies essentially on the following characterization of Gröbner bases: a subset G of a polynomial ideal I is a Gröbner basis of I if and only if the ideals generated by the leading terms of G and I, respectively, coincide (e.g. Winkler, 1996, Theorem 8.3.4). We prove a similar result for relative Gröbner bases inspired by the definition of Gröbner bases with respect to several orderings as provided by Levin (2007).

In this paper we present the following new results on relative Gröbner bases without which the theory of such bases developed by Zhou and Winkler (2008) cannot be considered as a complete one: 1) Characterization of relative Gröbner bases in terms of divisibility in certain multiplicative monoids (Theorem 12); 2) Conditions under which changes of admissible orders do not change a relative Gröbner basis (Theorem 10); 3) Analysis of the problem of termination of the algorithm provided by Zhou and Winkler for computing relative Gröbner bases and presenting an example where this algorithm does not terminate (Example 14). We also prove the property of symmetry of relative Gröbner bases (Lemma 8).

The paper is organized as follows. In the preliminary section we introduce basic notation and recall the notions of relative Gröbner bases provided by Zhou and Winkler (2008) and Gröbner bases with respect to several orderings in the sense of Levin (2007). In the next section we provide a result on the preservation of a relative Gröbner basis under change of orders. In Section 4 we give a characterization of relative Gröbner bases similar to a well known characterization of Gröbner bases. From the obtained characterization it is uncertain whether a relative Gröbner basis always exists. We provide an example for an ideal I and two admissible orders $\prec, \prec'$ such that the algorithm provided by Zhou and Winkler for computing a $\prec$-Gröbner basis of I relative to $\prec'$ does not terminate and show that in fact there cannot exist any $\prec$-Gröbner basis of I relative to $\prec'$.

2. Preliminaries

Throughout the paper $\mathbb{N}$ denotes the set of non-negative integers. Let K be a field of characteristic 0 and let $X = \{x_1, \ldots, x_n\}$. By $[X]$ we denote the set of terms in the indeterminates $x_1, \ldots, x_n$, i.e., using multi-index notation

$$[X] := \left\{ x^k \;\middle|\; x = (x_1, \ldots, x_n),\ k \in \mathbb{N}^n \right\}.$$

Definition 1. Let $\prec$ be a total order on $[X]$ such that for all $k, l, m \in \mathbb{N}^n$ we have

(i) $1 \preccurlyeq x^k$, and
(ii) $x^k \prec x^l \Rightarrow x^{k+m} \prec x^{l+m}$.

Then $\prec$ is called an *admissible order*.

Every nonzero element f of the free K module $K[X]$ generated by $[X]$ has a unique representation of the form

$$f = a_1\lambda_1 + \cdots + a_d\lambda_d \tag{1}$$

for some nonzero elements $a_1, \ldots, a_d \in K$ and some distinct elements $\lambda_1, \ldots, \lambda_d \in [X]$.

Method 1 Zhou's and Winkler's method for computing relative Gröbner bases

IN: $G = \{g_1, \ldots, g_\mu\}$, $\prec$ and $\prec'$
OUT: $G'' = \{g''_1, \ldots, g''_\nu\}$ a $\prec$-Gröbner basis of I relative to $\prec'$
1: $G' := G$
2: **while** there exist $f, g \in G'$ such that $S_{\prec'}(f, g)$ is $\prec'$-reducible to $r \neq 0$ modulo G' **do**
3: $G' := G' \cup \{r\}$
4: **end while**
5: $G'' := G'$
6: **while** there exist $f, g \in G''$ such that $S_{\prec}(f, g)$ is $\prec$-reducible to $r \neq 0$ modulo G'' relative to $\prec'$ **do**
7: $G'' := G'' \cup \{r\}$
8: **end while**
9: **return** G''

Fig. 1. Zhou's and Winkler's method for computing relative Gröbner bases.

Let $\prec$ be an admissible order on $[X]$, and $f \in K[X] \setminus \{0\}$ of the form (1). Then the *leading term* $\mathrm{lt}_\prec(f)$ of f with respect to $\prec$ is defined by

$$\mathrm{lt}_\prec(f) := \max_\prec\{\lambda_1, \ldots, \lambda_d\},$$

and its coefficient in f is called the *leading coefficient* $\mathrm{lc}_\prec(f)$ of f with respect to $\prec$.

For the concept of relative reduction and relative Gröbner bases see also Zhou and Winkler (2008). Levin's notion of reduction and Gröbner bases with respect to several orderings is closely related (Levin, 2007).

Definition 2. Let $f, h_1, \ldots, h_p, r \in K[X], g_1, \ldots, g_p \subseteq K[X] \setminus \{0\}$, and let $\prec$, $\prec'$ be two admissible orders such that

(i) $f = h_1 g_1 + \cdots + h_p g_p + r$,
(ii) $h_i = 0$ or $\mathrm{lt}_\prec(h_i g_i) \preccurlyeq \mathrm{lt}_\prec(f)$ for $i = 1, \ldots, p$, and
(iii) $r = 0$ or $\mathrm{lt}_\prec(r) \preccurlyeq \mathrm{lt}_\prec(f)$ such that

$$\mathrm{lt}_\prec(r) \notin \left\{\mathrm{lt}_\prec(\lambda g_i) \;\middle|\; \mathrm{lt}_{\prec'}(\lambda g_i) \preccurlyeq' \mathrm{lt}_{\prec'}(r),\ \lambda \in [X],\ i = 1, \ldots, p\right\}.$$

If $r \neq f$ we say that f is *$\prec$-reducible to r modulo $\{g_1, \ldots, g_p\}$ relative to $\prec'$*.

Definition 3. Let $I \subseteq K[X]$ be an ideal, $G \subseteq I \setminus \{0\}$ finite and let $\prec, \prec'$ be admissible orders such that every $f \in I$ is $\prec$-reducible to 0 modulo G relative to $\prec'$. Then G is called *$\prec$-Gröbner basis of I relative to $\prec'$*. If no confusion is possible we say that G is a *relative Gröbner basis*.

Definition 4. Let $f, g \in K[X] \setminus \{0\}$ and let $\prec$ be an admissible order. The *S-polynomial* $S_\prec(f, g)$ of f and g with respect to f is defined as

$$S_\prec(f, g) := \frac{\mathrm{lcm}(\mathrm{lt}_\prec(f), \mathrm{lt}_\prec(g))}{\mathrm{lt}_\prec(f)} \frac{f}{\mathrm{lc}_\prec(f)} - \frac{\mathrm{lcm}(\mathrm{lt}_\prec(f), \mathrm{lt}_\prec(g))}{\mathrm{lt}_\prec(g)} \frac{g}{\mathrm{lc}_\prec(g)},$$

where lcm denotes the *least common multiple*.

Zhou and Winkler (2008, Theorem 3.4) also provide a method which – if it terminates – computes relative Gröbner bases given by any basis for I and two admissible orders $\prec$, $\prec'$. A similar approach is used by Levin (2007, Theorem 3.10) for Gröbner bases with respect to several orderings.

Theorem 5. *Let $I \trianglelefteq K[X]$ be an ideal, $\prec$, $\prec'$ two admissible orders and G a finite basis for I. If Method* 1, *given in Fig.* 1, *terminates, it computes a $\prec$-Gröbner basis of I relative to $\prec'$.*

The proof of the following lemma is similar to the corresponding one for Gröbner bases (e.g. Winkler, 1996, Theorem 8.3.4). Zhou and Winkler (2008, Proposition 3.1) proved (i) $\Rightarrow$ (ii), (iii).

Lemma 6. *Let $I \trianglelefteqslant K[X]$ be an ideal and $G \subseteq I$ a finite basis for I. Let $\prec$ and $\prec'$ be two admissible orders. The following are equivalent*:

(i) *G is a $\prec$-Gröbner basis of I relative to $\prec'$,*
(ii) *every $f \in I$ is $\prec$-reducible to 0 modulo G relative to $\prec'$,*
(iii) *every $0 \neq f \in I$ is $\prec$-reducible modulo G relative to $\prec'$.*

Let $X_1, \ldots, X_p$ be a partition of $\{x_1, \ldots, x_n\}$ in p disjoint subsets. For reasons of convenience we assume that there exist $n_1, \ldots, n_p \in \mathbb{N}$ such that $n_1 + \cdots + n_p = n$ and $X_i = \{x_{1+\sum_{j=1}^{i-1} n_j}, \ldots, x_{\sum_{j=1}^{i} n_j}\}$.

For $\lambda = x_1^{k_1} \cdots x_n^{k_n} \in [X]$ and $1 \leqslant i \leqslant p$ define $\operatorname{ord}_i(\lambda) := \sum_{x_j \in X_i} k_j$ and call it the *i-order* of λ. The *total order* of λ is given by $\operatorname{ord}(\lambda) := \sum_{j=1}^{n} k_j$.

Define p orderings $\prec_1, \ldots, \prec_p$ on $[X]$ by

$$\begin{aligned}\lambda = x_1^{k_1} \cdots x_n^{k_n} \prec_i x_1^{l_1} \cdots x_n^{l_n} = \mu \\ :\Leftrightarrow \quad \big(&\operatorname{ord}_i(\lambda), \operatorname{ord}(\lambda), \operatorname{ord}_1(\lambda), \ldots, \operatorname{ord}_{i-1}(\lambda), \operatorname{ord}_{i+1}(\lambda), \ldots, \operatorname{ord}_p(\lambda), \\ &k_{n_1+\cdots+n_{i-1}+1}, \ldots, k_{n_1+\cdots+n_i}, k_1, \ldots, k_{n_1+\cdots+n_{i-1}}, k_{n_1+\cdots+n_i+1}, \ldots, k_n\big) \\ <_{\text{lex}} \big(&\operatorname{ord}_i(\mu), \operatorname{ord}(\mu), \operatorname{ord}_1(\mu), \ldots, \operatorname{ord}_{i-1}(\mu), \operatorname{ord}_{i+1}(\mu), \ldots, \operatorname{ord}_p(\mu), \\ &l_{n_1+\cdots+n_{i-1}+1}, \ldots, l_{n_1+\cdots+n_i}, l_1, \ldots, l_{n_1+\cdots+n_{i-1}}, l_{n_1+\cdots+n_i+1}, \ldots, l_n\big).\end{aligned}$$

Let us consider $p-1$ new symbols $z_2, \ldots, z_p$ and let Γ be the free commutative semigroup given by

$$\Gamma := \left\{x_1^{k_1} \cdots x_n^{k_n} z_2^{l_2} \cdots z_p^{l_p} \;\middle|\; k_1, \ldots, k_n, l_2, \ldots, l_p \in \mathbb{N}\right\}.$$

For $0 \neq f \in K[X]$ and $i \in \{2, \ldots, p\}$ let $d_i(f) := \operatorname{ord}_i(\operatorname{lt}_{\prec_i}(f)) - \operatorname{ord}_i(\operatorname{lt}_{\prec_1}(f))$ and define $\tilde{\rho} : K[X] \to \Gamma$ by

$$\tilde{\rho}(f) := z_2^{d_2(f)} \cdots z_p^{d_p(f)} \operatorname{lt}_{\prec_1}(f).$$

Definition 7. (See Levin, 2007.) Let I be an ideal in $K[X]$ and let $G \subseteq I$ be finite. Then G is called a *Gröbner basis of I with respect to $\prec_1, \ldots, \prec_p$* if for any $0 \neq f \in I$ there exists $g \in G$ such that $\tilde{\rho}(g) | \tilde{\rho}(f)$.

3. Change of orders

A crucial point in the theory of Gröbner bases is the computational complexity. A lot of effort has been put into the development of algorithms allowing for faster Gröbner basis computations and in algorithms for converting a given Gröbner basis with respect to some admissible order $\prec$ into a Gröbner basis with respect to a different order $\prec'$. In fact, such a conversion is not a continuous process because Gröbner bases are preserved under a moderate change of order. Our first goal in this section is to provide a similar result for relative Gröbner bases. To this end we need the following lemma.

Lemma 8. *Let $I \trianglelefteqslant K[X]$ be an ideal and let $G = \{g_1, \ldots, g_r\} \subseteq I$ be finite. Let $\prec$ and $\prec'$ be two admissible orders. Then G is a $\prec$-Gröbner basis of I relative to $\prec'$ if and only if G is a $\prec'$-Gröbner basis of I relative to $\prec$.*

Proof. Suppose G is a $\prec$-Gröbner basis of I relative to $\prec'$ and let $f_0 \in I$. Then by Lemma 6 f_0 is $\prec$-reducible to 0 modulo G relative to $\prec'$, i.e., there exist $s \in \mathbb{N}$ and $f_1, \ldots, f_s \in K[X]$ such that for all $i = 1, \ldots, s$ the polynomial f_{i-1} is $\prec$-reducible to f_i modulo G relative to $\prec'$ in one step and there exist at least one $i_0 \in \{1, \ldots, s\}$ and $j \in \{1, \ldots, r\}$ with

(i) $\operatorname{lt}_{\prec'}(f_0) = \operatorname{lt}_{\prec'}(f_{i_0}) = \operatorname{lt}_{\prec'}(\frac{\operatorname{lt}_{\prec}(f_{i_0})}{\operatorname{lt}_{\prec}(g_j)} g_j)$, and
(ii) $\operatorname{lt}_{\prec}(\frac{\operatorname{lt}_{\prec}(f_{i_0})}{\operatorname{lt}_{\prec}(g_j)} g_j) = \operatorname{lt}_{\prec}(f_{i_0}) \preccurlyeq \operatorname{lt}_{\prec}(f_0)$.

Hence, f_0 is $\prec'$-reducible modulo G relative to $\prec$ and we conclude that G is a $\prec'$-Gröbner basis of I relative to $\prec$. The opposite implication follows similarly and the lemma is proved. □

A crucial point in the Gröbner walk is a result on the preservation of an autoreduced Gröbner basis under changes of admissible orders within the interior of one Gröbner cone (Collart et al., 1997, Lemma 2.2). The following example illustrates the use of this result for the computation of relative Gröbner bases.

Example 9. Let $\prec_0, \prec_1, \prec_2$, and $\prec_3$ be admissible orders on $[X]$ and $I \trianglelefteq K[X]$ an ideal such that there exists a finite $\prec_0$-Gröbner basis $\emptyset \neq G \subseteq K[X]$ of I relative to $\prec_1$ satisfying for every $g \in G$ the conditions

(i) $\mathrm{lt}_{\prec_0}(g) = \mathrm{lt}_{\prec_2}(g)$, and
(ii) $\mathrm{lt}_{\prec_1}(g) = \mathrm{lt}_{\prec_3}(g)$.

By Zhou and Winkler (2008, Proposition 3.1) G is a Gröbner basis of I with respect to $\prec_0$ and $\prec_1$. By Collart et al. (1997, Lemma 2.2) it follows that G is a Gröbner basis of I with respect to $\prec_2$ and $\prec_3$. Zhou and Winkler state that from this it cannot be concluded that G is a $\prec_2$-Gröbner basis of I relative to $\prec_3$. However, in order to compute a $\prec_2$-Gröbner basis of I relative to $\prec_3$ we can skip the first while-loop of Method 1 and in line 5 set $G'' = G$. From conditions (i) and (ii) it follows that for any $g_i, g_j \in G$ we have $S_{\prec_0}(g_i, g_j) = S_{\prec_2}(g_i, g_j)$ but it is not always true that $\mathrm{lt}_{\prec_0}(S_{\prec_0}(g_i, g_j)) = \mathrm{lt}_{\prec_2}(S_{\prec_2}(g_i, g_j))$ and $\mathrm{lt}_{\prec_1}(S_{\prec_2}(g_i, g_j)) = \mathrm{lt}_{\prec_3}(S_{\prec_2}(g_i, g_j))$. Therefore we still have to execute the second while-loop of Method 1. □

The following theorem addresses the situation of Example 9 and shows that in fact we can also skip the second while-loop of Method 1 under the given conditions.

Theorem 10. *Let $\prec_0, \prec_1, \prec_2, \prec_3$ be admissible orders on $[X]$ and let $G = \{g_1, \ldots, g_r\} \subseteq K[X]$ be a $\prec_0$-Gröbner basis relative to $\prec_1$ such that for all $i \in \{1, \ldots, r\}$ we have*

$$\mathrm{lt}_{\prec_0}(g_i) = \mathrm{lt}_{\prec_2}(g_i),$$
$$\mathrm{lt}_{\prec_1}(g_i) = \mathrm{lt}_{\prec_3}(g_i).$$

Then G is a $\prec_2$-Gröbner basis relative to $\prec_3$.

Proof. Suppose G is a $\prec_0$-Gröbner basis relative to $\prec_1$ and let $f_0 \in \langle G \rangle$. Hence, f_0 is $\prec_0$-reducible to some $f_1 \in \langle G \rangle$ modulo G relative to $\prec_1$, i.e., there exist $\lambda_0 \in [X]$, $i_0 \in \{1, \ldots, r\}$ such that

$$\mathrm{lt}_{\prec_0}(\lambda_0 g_{i_0}) = \mathrm{lt}_{\prec_0}(f_0),$$
$$\mathrm{lt}_{\prec_1}(\lambda_0 g_{i_0}) \preccurlyeq_0 \mathrm{lt}_{\prec_1}(f_0).$$

We have to distinguish the following two cases:

$\mathrm{lt}_{\prec_0}(f_0) = \mathrm{lt}_{\prec_2}(f_0)$: Because of $\mathrm{lt}_{\prec_0}(\lambda_0 g_{i_0}) = \mathrm{lt}_{\prec_2}(\lambda_0 g_{i_0})$ we get that f_0 is $\prec_2$-reducible modulo G relative to $\prec_1$.

$\mathrm{lt}_{\prec_0}(f_0) \prec_2 \mathrm{lt}_{\prec_2}(f_0)$: We obtain $f_1 \in \langle G \rangle$ by removing $\mathrm{lt}_{\prec_0}(f_0)$ from f_0 and inserting finitely many terms which are strictly smaller than $\mathrm{lt}_{\prec_0}(f_0)$ with respect to $\prec_0$ and $\prec_2$ and which are not bigger than $\mathrm{lt}_{\prec_1}(f_0)$ with respect to $\prec_1$. Since G is a $\prec_0$-Gröbner basis relative to $\prec_1$ after finitely many steps – say s – we obtain $f_s \in \langle G \rangle$ such that $\mathrm{lt}_{\prec_0}(f_s) = \mathrm{lt}_{\prec_2}(f_s)$ and there exist $\lambda_s \in [X]$, $i_s \in \{1, \ldots, r\}$ such that

$$\mathrm{lt}_{\prec_2}(\lambda_s g_{i_s}) = \mathrm{lt}_{\prec_0}(\lambda_s g_{i_s}) = \mathrm{lt}_{\prec_0}(f_s) = \mathrm{lt}_{\prec_2}(f_s),$$
$$\mathrm{lt}_{\prec_1}(\lambda_s g_{i_s}) \preccurlyeq_0 \mathrm{lt}_{\prec_1}(f_s) \preccurlyeq_0 \mathrm{lt}_{\prec_1}(f_0).$$

So f_0 is $\prec_2$-reducible modulo g_{i_s} relative to $\prec_1$.

Since in any case f_0 is $\prec_2$-reducible modulo G relative to $\prec_1$ it follows that G is a $\prec_2$-Gröbner basis relative to $\prec_1$. Then by Lemma 8 G is a $\prec_1$-Gröbner basis relative to $\prec_2$. Applying a similar argument as before we obtain that G is a $\prec_3$-Gröbner basis relative to $\prec_2$ and again by Lemma 8 we conclude that G is a $\prec_2$-Gröbner basis relative to $\prec_3$. □

Example 9 *(Continued).* By Theorem 10 the set G is a $\prec_2$-Gröbner basis of I relative to $\prec_3$. □

4. Gröbner bases, Levin's Gröbner bases with respect to several orderings and relative Gröbner bases

The following well-known theorem (e.g. Winkler, 1996, Theorem 8.3.4) characterizing Gröbner bases has several applications. For us it is interesting because it is used for proving the correctness of the Gröbner walk.

Theorem 11. *Let $\prec$ be an admissible order on $[X]$, $I \trianglelefteq K[X]$ an ideal and $G \subseteq I$ finite. Then G is a Gröbner basis for I if and only if $\langle \mathrm{lt}_\prec(I)\rangle = \langle \mathrm{lt}_\prec(G)\rangle$.*

Something similar appears in the notion of Gröbner bases with respect to several orderings as provided by Levin (2007).

Relative Gröbner bases are more general regarding the possible term orders but more restrictive in the sense that they only take into account two of them. The characterization we suggest shows that from a structural point of view they are slightly more complicated than Levin's Gröbner bases with respect to several term orderings.

Let $\prec$, $\prec'$ be two admissible orders on $[X]$. Due to a result by Robbiano (1985) there exist $m \in \{1,\dots,n\}$ and $U \in \mathbb{R}^{n\times m}$ such that

$$\begin{aligned}\alpha : \big([X], \prec'\big) &\to \big(\mathbb{R}^s, <_{\mathrm{lex}}\big),\\ x^k &\mapsto kU\end{aligned}$$

is an injective homomorphism. Note that for $\lambda, \mu \in [X]$ we have

$$\alpha(\lambda\mu) = \alpha(\lambda) + \alpha(\mu).$$

Let us consider a new symbol z and let

$$\begin{aligned}[X,z]_U &:= \big\{x^k z^{kU} \;\big|\; k \in \mathbb{N}^n\big\},\\ \overline{[X,z]_U} &:= \big\{x^k z^l \;\big|\; k \in \mathbb{N}^n,\ l \in \mathbb{Z}^n U,\ 0 \leqslant_{\mathrm{lex}} l - kU\big\}.\end{aligned}$$

For $l_1, l_2 \in \mathbb{Z}^n U$ define $z^{l_1} z^{l_2} = z^{l_1+l_2}$ and $z^{l_1} x^k = x^k z^{l_1}$. Then $[X,z]_U$ and $\overline{[X,z]_U}$ can be considered as multiplicative monoids.

Define $\rho : K[X] \to \overline{[X,z]_U}$ by

$$\rho(f) := \mathrm{lt}_\prec(f) z^{\alpha(\mathrm{lt}_{\prec'}(f))}.$$

Theorem 12. *Let $G = \{g_1,\dots,g_r\} \subseteq K[X]$ be finite, $I := {}_{K[X]}\langle G\rangle$ and let $\prec$, $\prec'$ be two admissible orders on $[X]$. The following are equivalent*:

(i) *G is a $\prec$-Gröbner basis of I relative to $\prec'$,*
(ii) $\rho(I) \subseteq \overline{[X,z]_U}\,\rho(G)$,
(iii) $\overline{[X,z]_U}\,\rho(I) = \overline{[X,z]_U}\,\rho(G)$,
(iv) ${}_{K\overline{[X,z]_U}}\langle\rho(I)\rangle = {}_{K\overline{[X,z]_U}}\langle\rho(G)\rangle$.

Proof. "(i) ⇒ (ii)": Let G be a $\prec$-Gröbner basis of I relative to $\prec'$. Then every $0 \neq f \in I$ is $\prec$-reducible relative to $\prec'$, i.e., there exist $\lambda \in [X]$, $g \in G$ such that

(i) $\mathrm{lt}_{\prec}(\lambda g) = \mathrm{lt}_{\prec}(f)$, and
(ii) $\mathrm{lt}_{\prec'}(\lambda g) \preccurlyeq' \mathrm{lt}_{\prec'}(f)$.

Hence, $\alpha(\lambda) + \alpha(\mathrm{lt}_{\prec'}(g)) \leqslant_{\mathrm{lex}} \alpha(\mathrm{lt}_{\prec'}(f))$ and we obtain

$$\lambda z^{\alpha(\mathrm{lt}_{\prec'}(f)) - \alpha(\mathrm{lt}_{\prec'}(g))} \in \overline{[X,z]_U}.$$

On the other hand

$$\begin{aligned}\lambda z^{\alpha(\mathrm{lt}_{\prec'}(f)) - \alpha(\mathrm{lt}_{\prec'}(g))} \rho(g) &= \lambda z^{\alpha(\mathrm{lt}_{\prec'}(f)) - \alpha(\mathrm{lt}_{\prec'}(g))} \mathrm{lt}_{\prec}(g) z^{\alpha(\mathrm{lt}_{\prec'}(g))} \\ &= \mathrm{lt}_{\prec}(f) z^{\alpha(\mathrm{lt}_{\prec'}(f))} \\ &= \rho(f)\end{aligned}$$

and we conclude $\rho(I) \subseteq \overline{[X,z]_U}\rho(G)$.

"(ii) $\Rightarrow$ (iii)": From $\rho(I) \subseteq \overline{[X,z]_U}\rho(G)$ we get $\overline{[X,z]_U}\rho(I) \subseteq \overline{[X,z]_U}\rho(G)$. Conversely from $I \supseteq G$ we obtain $\overline{[X,z]_U}\rho(I) \supseteq \overline{[X,z]_U}\rho(G)$ and conclude $\overline{[X,z]_U}\rho(I) = \overline{[X,z]_U}\rho(G)$.

"(iii) $\Rightarrow$ (iv)": From $\overline{[X,z]_U}\rho(I) = \overline{[X,z]_U}\rho(G)$ we obtain

$$\begin{aligned}{}_{K\overline{[X,z]_U}}\langle \rho(I)\rangle &= {}_{K\overline{[X,z]_U}}\langle \overline{[X,z]_U}\rho(I)\rangle \\ &= {}_{K\overline{[X,z]_U}}\langle \overline{[X,z]_U}\rho(G)\rangle \\ &= {}_{K\overline{[X,z]_U}}\langle \rho(G)\rangle.\end{aligned}$$

"(iv) $\Rightarrow$ (i)": Suppose ${}_{K\overline{[X,z]_U}}\langle \rho(I)\rangle = {}_{K\overline{[X,z]_U}}\langle \rho(G)\rangle$ and let $0 \neq f \in I$. Then $\rho(f) \in \rho(I)$ and there exist $h_1, \ldots, h_r \in K\overline{[X,z]_U}$ such that

$$\rho(f) = \sum_{i=1}^{r} h_i \rho(g_i).$$

In fact, since $\rho(f)$ and all the $\rho(g)$ are monomials there exists a particular $g \in G$ such that $\rho(f) = h_g \rho(g)$ for some monomial $h_g \in \overline{[X,z]_U}$. Then $h_g = \lambda z^l$ for some $\lambda = x^k z^{kU} \in [X,z]_U$ and $0 \leqslant_{\mathrm{lex}} l \in \mathbb{Z}^n U$. Hence, $\mathrm{lt}_{\prec}(f) = x^k \mathrm{lt}_{\prec}(g)$ and

$$\begin{aligned}z^{\alpha(\mathrm{lt}_{\prec'}(f))} &= z^l z^{kU} z^{\alpha(\mathrm{lt}_{\prec'}(g))} \\ &= z^l z^{\alpha(x^k) + \alpha(\mathrm{lt}_{\prec'}(g))} \\ &= z^l z^{\alpha(\mathrm{lt}_{\prec'}(x^k g))},\end{aligned}$$

i.e., $\alpha(\mathrm{lt}_{\prec'}(x^k g)) \leqslant_{\mathrm{lex}} \alpha(\mathrm{lt}_{\prec'}(f))$ which implies $\mathrm{lt}_{\prec'}(x^k g) \preccurlyeq' \mathrm{lt}_{\prec'}(f)$. We conclude that f is $\prec$-reducible modulo G relative to $\prec'$ which is equivalent to G being a $\prec$-Gröbner basis relative to $\prec'$. □

Remark 13. Zhou and Winkler (2008) proved the correctness of Method 1 but did not discuss its computational cost. On one hand, looking at the method it is obvious that computing a relative Gröbner basis is at least as expensive as computing a Gröbner basis. On the other hand, it seems as if a relative Gröbner basis is some sort of 'extended' Gröbner basis and its computation should not be much more costly than that of a Gröbner basis. In fact, Theorem 12 provides a better understanding of the computational cost of Method 1 by showing that computing a relative Gröbner basis for the ideal I in $K[X]$ also means computing a basis for the ideal ${}_{K\overline{[X,z]_U}}\langle \rho(I)\rangle$ in $K\overline{[X,z]_U}$. Since $K\overline{[X,z]_U}$ is not necessarily Noetherian it is by no means obvious that for every ideal $I \subseteq K[X]$ there exists a finite basis of ${}_{K\overline{[X,z]_U}}\langle \rho(I)\rangle$. Hence, Theorem 12 explains why for certain examples Method 1 does not terminate.

Example 14. Consider the two admissible orders $\prec = \mathrm{lex}(x_3 > x_1 > x_2)$ and $\prec' = \mathrm{grevlex}(x_3, x_2, x_1)$ on $[x_1, x_2, x_3]$, i.e., they are given by

$$x_1^{a_1} x_2^{a_2} x_3^{a_3} \prec x_1^{b_1} x_2^{b_2} x_3^{b_3} \quad :\Leftrightarrow \quad (a_3, a_1, a_2) <_{\mathrm{lex}} (b_3, b_1, b_2),$$

and

$$x_1^{a_1} x_2^{a_2} x_3^{a_3} \prec' x_1^{b_1} x_2^{b_2} x_3^{b_3} \quad :\Leftrightarrow \quad (a_1 + a_2 + a_3, -a_1, -a_2) <_{\mathrm{lex}} (b_1 + b_2 + b_3, -b_1, -b_2).$$

The leading terms with respect to $\prec$ and $\prec'$ will be underlined and dotted underlined, respectively. For $i \in \mathbb{N}$ let

$$G_i = \left\{ f_0 := \dot{x_1^3 x_2^2} + \underline{x_1^4 x_2},\ f_1 := \dot{x_2^3 x_3^2} + \underline{x_1 x_2^2 x_3^2} \right\}$$
$$\cup \left\{ g_j := \dot{x_1^{3+4j} x_2 x_3} + \underline{x_2^{2+4j} x_3^2} \mid j = 0, \ldots, i \right\}.$$

The remainder of this example consists of three parts:

(i) we show that Method 1 does not terminate if we try to compute a $\prec$-Gröbner basis of $I := \langle f_0, g_0 \rangle$ relative to $\prec'$,
(ii) we show that there cannot exist any $\prec$-Gröbner basis of I relative to $\prec'$ – making termination of Method 1 impossible, and
(iii) we use Theorem 12 in oder to understand why there cannot exist any $\prec$-Gröbner basis of I relative to $\prec'$.

(i) We start by showing the non-termination of Method 1 for the given situation. It can be easily verified (e.g. using Maple) that G_0 is a Gröbner basis of I with respect to $\prec'$. We use the method provided by Zhou and Winkler (2008) (see Theorem 5) for computing a $\prec$-Gröbner basis of I relative to $\prec'$. For every $i \in \mathbb{N}$ the S-polynomial of f_0 and g_i with respect to $\prec$ is given by

$$S(f_0, g_i) = x_2^{1+4i} x_3^2 f_0 - x_1^4 g_i = \underline{x_1^3 x_2^{3+4i} x_3^2} - \dot{x_1^{7+4i} x_2 x_3}.$$

Then for every $0 \leqslant j \leqslant i$ we have

(a) $\mathrm{lt}_{\prec}(x_1^3 x_2^{1+4(i-j)} g_j) = \mathrm{lt}_{\prec}(\dot{x_1^{6+4j} x_2^{2+4(i-j)} x_3} + \underline{x_1^3 x_2^{3+4i} x_3^2}) = \mathrm{lt}_{\prec}(S(f_0, g_i))$, and
(b) $\mathrm{lt}_{\prec'}(S_{\prec}(f_0, g_i)) = x_1^{7+4i} x_2 x_3 \prec' x_1^{6+4j} x_2^{2+4(i-j)} x_3 = \mathrm{lt}_{\prec'}(x_1^3 x_2^{1+4(i-j)} g_j)$.

Hence, $S(f_0, g_i)$ is not $\prec$-reducible modulo $\{g_0, \ldots, g_i\}$ relative to $\prec'$. Furthermore it is not $\prec$-reducible modulo f_0. Nevertheless we have

(a) $\mathrm{lt}_{\prec}(x_1^2 x_2^{1+4i} f_1) = \mathrm{lt}_{\prec}(\dot{x_1^2 x_2^{4+4i} x_3^2} + \underline{x_1^3 x_2^{3+4i} x_3^2}) = \mathrm{lt}_{\prec}(S(f_0, g_i))$, and
(b) $\mathrm{lt}_{\prec'}(x_1^2 x_2^{1+4i} f_1) = x_1^2 x_2^{4+4i} x_3^2 \prec' x_1^{7+4i} x_2 x_3 = \mathrm{lt}_{\prec'}(S(f_0, g_i))$.

Hence, $S(f_0, g_i)$ is $\prec$-reducible modulo f_1 relative to $\prec'$ to

$$S(f_0, g_i) - x_1^2 x_2^{1+4i} f_1 = -\dot{x_1^{7+4i} x_2 x_3} - \underline{x_1^2 x_2^{4+4i} x_3^2} =: h_1.$$

It is immediate that h_1 is not $\prec$-reducible modulo f_0. Furthermore for every $0 \leqslant j \leqslant i$ we have

(a) $\mathrm{lt}_{\prec}(x_1^2 x_2^{2+4(i-j)} g_j) = x_1^2 x_2^{4+4i} x_3^2 = \mathrm{lt}_{\prec}(h_1)$, and
(b) $\mathrm{lt}_{\prec'}(h_1) = x_1^{7+4i} x_2 x_3 \prec' x_1^{5+4j} x_2^{3+4(i-j)} x_3 = \mathrm{lt}_{\prec'}(x_1^2 x_2^{2+4(i-j)} g_j)$.

So h_1 is not $\prec$-reducible modulo $\{g_0, \ldots, g_i\}$ relative to $\prec'$. Nevertheless we have

(a) $\mathrm{lt}_\prec(x_1x_2^{2+4i}f_1) = \mathrm{lt}_\prec(\underset{\cdots\cdots}{x_1x_2^{5+4i}x_3^2} + \underline{x_1^2x_2^{4+4i}x_3^2}) = \mathrm{lt}_\prec(h_1)$, and

(b) $\mathrm{lt}_{\prec'}(x_1x_2^{2+4i}f_1) = x_1x_2^{5+4i}x_3^2 \prec' x_1^{7+4i}x_2x_3 = \mathrm{lt}_{\prec'}(h_1)$.

Hence, h_1 is $\prec$-reducible modulo f_1 relative to $\prec'$ to

$$h_1 + x_1x_2^{2+4i}f_1 = -\underset{\cdots\cdots}{x_1^{7+4i}x_2x_3} + \underline{x_1x_2^{5+4i}x_3^2} =: h_2.$$

It is immediate that h_2 is not $\prec$-reducible modulo f_0. Furthermore for every $0 \leqslant j \leqslant i$ we have

(a) $\mathrm{lt}_\prec(x_1x_2^{3+4(i-j)}g_j) = x_1x_2^{5+4i}x_3^2 = \mathrm{lt}_\prec(h_2)$, and

(b) $\mathrm{lt}_{\prec'}(h_2) = x_1^{7+4i}x_2x_3 \prec' x_1^{4+4j}x_2^{4+4(i-j)}x_3 = \mathrm{lt}_{\prec'}(x_1x_2^{3+4(i-j)}g_j)$.

So h_2 is not $\prec$-reducible modulo $\{g_0, \ldots, g_i\}$ relative to $\prec'$. Nevertheless we have

(a) $\mathrm{lt}_\prec(x_2^{3+4i}f_1) = \mathrm{lt}_\prec(\underset{\cdots\cdots}{x_2^{6+4i}x_3^2} + \underline{x_1x_2^{5+4i}x_3^2}) = \mathrm{lt}_\prec(h_2)$, and

(b) $\mathrm{lt}_{\prec'}(x_2^{3+4i}f_1) = x_2^{6+4i}x_3^2 \prec' x_1^{7+4i}x_2x_3 = \mathrm{lt}_{\prec'}(h_2)$.

Hence, h_2 is $\prec$-reducible modulo f_1 relative to $\prec'$ to

$$h_2 - x_2^{3+4i}f_1 = -\underset{\cdots\cdots}{x_1^{7+4i}x_2x_3} - \underline{x_2^{6+4i}x_3^2} = -g_{i+1}.$$

It is immediate that g_{i+1} is not $\prec$-reducible modulo $\{f_0, f_1\}$. Furthermore for every $0 \leqslant j \leqslant i$ we have

(a) $\mathrm{lt}_\prec(x_2^{4+4(i-j)}g_j) = x_2^{6+4i}x_3^2 = \mathrm{lt}_\prec(g_{i+1})$, and

(b) $\mathrm{lt}_{\prec'}(g_{i+1}) = x_1^{7+4i}x_2x_3 \prec' x_1^{3+4j}x_2^{5+4(i-j)}x_3 = \mathrm{lt}_{\prec'}(x_2^{4+4(i-j)}g_j)$.

So g_{i+1} is not $\prec$-reducible modulo $\{g_0, \ldots, g_i\}$ relative to $\prec'$.

Hence, the method provided by Zhou and Winkler (2008) will not terminate on this example. Nevertheless it could still be the case that there exists a $\prec$-Gröbner basis of I relative to $\prec'$ but the provided method cannot compute it.

(ii) In the following we show that no $\prec$-Gröbner basis of I relative to $\prec'$ exists. Suppose there exists an element $0 \neq h \in I$ such that infinitely many g_i are $\prec$-reducible modulo h relative to $\prec'$. Then $\mathrm{lt}_\prec(h) = x_2^{a_1}x_3^{a_2}$ and $\mathrm{lt}_{\prec'}(h) = x_1^{b_1}x_2^{b_2}x_3^{b_3}$, i.e.,

$$\begin{pmatrix} a_1 + a_2 \\ 0 \\ 1 \end{pmatrix} \leqslant_{\mathrm{lex}} \begin{pmatrix} b_1 + b_2 + b_3 \\ -b_1 \\ -b_2 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} b_3 \\ b_1 \\ b_2 \end{pmatrix} \leqslant_{\mathrm{lex}} \begin{pmatrix} a_2 \\ 0 \\ a_1 \end{pmatrix}.$$

Since infinitely many g_i are $\prec$-reducible modulo h relative to $\prec'$ we also have

$$\begin{pmatrix} b_1 + b_2 + 2 + 4i - a_1 + b_3 + 2 - a_2 \\ -b_1 \\ -b_2 - 2 - 4i + a_1 \end{pmatrix} \leqslant_{\mathrm{lex}} \begin{pmatrix} 5 + 4i \\ -3 - 4i \\ -1 \end{pmatrix}$$

for infinitely many $i \in \mathbb{N}$. We have to distinguish several cases:

$a_1 + a_2 < b_1 + b_2 + b_3$: Then $4 + 4i < b_1 + b_2 + b_3 - a_1 - a_2 + 4 + 4i \leqslant 5 + 4i$, i.e., $b_1 + b_2 + b_3 - a_1 - a_2 = 1$. Then we have $-b_1 \leqslant -3 - 4_i$, i.e., $b_1 \geqslant 3 + 4i$. This can obviously not happen for infinitely many $i \in \mathbb{N}$.

$a_1 + a_2 = b_1 + b_2 + b_3$: We distinguish further
$0 < -b_1$: Then $b_1 < 0$ which is not possible.
$0 = -b_1$: Then $-1 \leqslant -b_2$, i.e., $b_2 \leqslant 1$.
$b_2 = 0$: Then $b_3 = a_1 + a_2$ and $b_3 \leqslant a_2$.
$b_3 < a_2$: Then $a_1 < 0$ which is not possible.
$b_3 = a_2$: Then $a_1 = 0$, i.e., $h = cx_3^{a_2} +$ lower terms with respect to $\prec$ and $\prec'$ for some $0 \neq c \in K$. Since G_0 is a $\prec'$-Gröbner basis of I we see that h is not $\prec'$-reducible, i.e., $h \notin I$.
$b_2 = 1$: Then $b_3 = a_1 + a_2 - 1$ and $b_3 \leqslant a_2$.
$b_3 < a_2$: Then $b_3 = a_2 - 1$ and $a_1 = 0$, i.e., $h = c_1 x_3^{b_3+1} + c_2 x_2 x_3^{b_3} +$ lower terms with respect to $\prec$ and $\prec'$ for some $0 \neq c_1, c_2 \in K$. Again since G_0 is a $\prec'$-Gröbner basis of I we see that h is not $\prec'$-reducible, i.e., $h \notin I$.
$b_3 = a_2$: Then $1 = b_2 \leqslant a_1 = 1$, i.e., $h = cx_2 x_3^{b_3} +$ lower terms with respect to $\prec$ and $\prec'$ for some $0 \neq c \in K$. Again since G_0 is a $\prec'$-Gröbner basis of I we see that h is not $\prec'$-reducible, i.e., $h \notin I$.

Hence, there cannot exist any $\prec$-Gröbner basis of I relative to $\prec'$.

Zhou and Winkler (2008) proved the correctness of Method 1 showing that if it terminates it returns a relative Gröbner basis. Since for the given example no $\prec$-Gröbner basis relative to $\prec'$ exists Method 1 cannot terminate.

(iii) We conclude this example by applying Theorem 12 in order to understand why there cannot exist any $\prec$-Gröbner basis of I relative to $\prec'$. From part (i) we know that $\{g_j \mid j = 0, \ldots, \infty\} \subseteq I$. Hence,

$$\left\{\rho(g_j) = x_2^{2+4j} x_3^2 z^{(5+4j,-3-4j,-1)} \;\middle|\; j = 0, \ldots, \infty\right\} \subseteq \rho(I) \subseteq_{K[\overline{X,z}]_U} \langle \rho(I) \rangle.$$

From part (ii) we know that there does not exist any $0 \neq h \in I$ such that infinitely many g_i are $\prec$-reducible modulo h relative to $\prec'$. In other words: there does not exist any $\lambda \in \rho(I)$ dividing infinitely many $\rho(g_i)$. Since $\rho(I)$ contains only monomials the ideal ${}_{K[\overline{X,z}]_U}\langle \rho(I) \rangle$ is a monomial ideal. We conclude that there does not exist any $\mu \in {}_{K[\overline{X,z}]_U}\langle \rho(I) \rangle$ such that any term of μ divides infinitely many $\rho(g_i)$. Hence, the ideal ${}_{K[\overline{X,z}]_U}\langle \rho(I) \rangle$ cannot possess a finite basis. In particular, ${}_{K[\overline{X,z}]_U}\langle \rho(I) \rangle$ cannot possess a finite basis which is a subset of $\overline{[X, z]_U}$. By Theorem 12 this is the reason why there cannot exist any $\prec$-Gröbner basis of I relative to $\prec'$. □

5. Conclusion

We have shown that relative Gröbner bases are symmetric with respect to the given term orders. We have used this property in order to obtain a result concerning the preservation of a relative Gröbner basis under changes of admissible orders which leave the leading terms of the elements of the relative Gröbner basis in concern unaltered. Furthermore we have presented a characterization of relative Gröbner bases resembling a well known characterization of Gröbner bases. From this characterization it has turned out to be questionable whether a relative Gröbner basis always exists. We have presented a counterexample. Despite the fact that currently relative Gröbner bases are the most used tool for the algorithmic computation of bivariate dimension polynomials in contrast to Levin's Gröbner bases with respect to several orderings the worst-case complexity of relative Gröbner bases is not bounded.

Acknowledgements

The research was funded by the Austrian Science Fund (FWF): project P20336-N18 (DIFFOP). This research was partially supported by the Austrian Science Fund (FWF): W1214-N15, project DK11.

References

Collart, S., Kalkbrener, M., Mall, D., 1997. Converting bases with the Gröbner walk. J. Symbolic Comput. 24 (3–4), 465–469.

Faugère, J.C., Gianni, P., Lazard, D., Mora, T., 1993. Efficient computation of zero-dimensional Gröbner bases by change of ordering. J. Symbolic Comput. 16 (4), 329–344.
Levin, A.B., 2007. Gröbner bases with respect to several orderings and multivariable dimension polynomials. J. Symbolic Comput. 42 (5), 561–578.
Robbiano, L., 1985. Term orderings on the polynomial ring. In: EUROCAL'85, vol. 2. In: Lecture Notes in Comput. Sci., vol. 204. Springer, Berlin, pp. 513–517.
Winkler, F., 1996. Polynomial Algorithms in Computer Algebra. Springer, Wien, New York.
Zhou, M., Winkler, F., 2008. Computing difference-differential dimension polynomials by relative Gröbner bases in difference-differential modules. J. Symbolic Comput. 43 (10), 726–745.