

UNIVERSITY OF AARHUS  
DEPARTMENT OF MATHEMATICS



ISSN: 1397-4076

# THE GENERIC GRÖBNER WALK

by K. Fukuda, A. N. Jensen N. Lauritzen and R. Thomas

Preprint Series No.: 1

January 2005

2005/01/24

*Ny Munkegade, Bldg. 530  
DK-8000 Aarhus C, Denmark*

*<http://www.imf.au.dk>  
[institut@imf.au.dk](mailto:institut@imf.au.dk)*

# The generic Gröbner walk

K. Fukuda,<sup>\*</sup> A. N. Jensen,<sup>†</sup> N. Lauritzen,<sup>‡</sup> R. Thomas<sup>§</sup>

February 2, 2005

## Abstract

The Gröbner walk is an algorithm for conversion between Gröbner bases for different term orders. It is based on the polyhedral geometry of the Gröbner fan and involves tracking a line between cones representing the initial and target term order. An important parameter is explicit numerical perturbation of this line. This usually involves both time and space demanding arithmetic of integers much larger than the input numbers. In this paper we show how the explicit line may be replaced by a formal line using Robbiano's characterization of group orders on  $\mathbb{Q}^n$ . This gives rise to the generic Gröbner walk involving only Gröbner basis conversion over facets and computations with marked polynomials. The infinite precision integer arithmetic is replaced by term order comparisons between (small) integral vectors. This makes it possible to compute with infinitesimal numbers and perturbations in a consistent way without introducing unnecessary long integers. The proposed technique is closely related to the lexicographic (symbolic) perturbation method used in optimization and computational geometry.

## 1 Introduction

Let  $R = k[x_1, \dots, x_n]$  denote the polynomial ring in  $n$  variables over a field  $k$ . Gröbner basis computations in  $R$  tend to be very expensive for certain term orders (like the lexicographic order). Therefore it often pays to compute Gröbner bases for "easier" term orders and convert them into Gröbner bases for the desired term order. For zero-dimensional ideals this can be accomplished by the FGLM-algorithm [6]. For general ideals the Gröbner walk algorithm [3] can be applied.

Let  $\prec_1$  and  $\prec_2$  be term orders on  $R$ . The usual Gröbner walk proceeds from the reduced Gröbner basis  $G$  for  $I$  over  $\prec_1$  by tracking a line  $\omega(t) = (1-t)\omega_0 + t\tau_0$ ,  $0 \leq t \leq 1$ , where  $\omega_0$  and  $\tau_0$  are vectors in the respective Gröbner cones  $C_{\prec_1}(I)$  and

---

<sup>\*</sup>Institute for Operations Research, ETH Zürich, Ch-8092, Switzerland,  
fukuda@ifor.math.ethz.ch

<sup>†</sup>Institut for Matematiske Fag, Aarhus Universitet, DK-8000 Århus, Denmark,  
ajensen@imf.au.dk

<sup>‡</sup>Institut for Matematiske Fag, Aarhus Universitet, DK-8000 Århus, Denmark, niels@imf.au.dk

<sup>§</sup>Department of Mathematics, University of Washington, Seattle, WA 98195, USA,  
thomas@math.washington.edu

$C_{\prec_2}(I)$  of  $I$ . At  $t = 0$  the Gröbner basis is known. The line  $\omega(t)$  is tracked through the Gröbner fan of  $I$  and Gröbner bases are computed at common faces of successive Gröbner cones. At  $t = 1$  we reach the reduced Gröbner basis for  $I$  over  $\prec_2$ .

The efficiency of the Gröbner walk rests on clever choices of  $\omega_0$  and  $\tau_0$ . A choice of  $\omega_0$  and  $\tau_0$  on low dimensional faces of Gröbner cones may lead to very heavy Gröbner basis calculations along  $\omega(t)$ . Often (but not always) it pays to choose  $\omega_0$  and  $\tau_0$  generically inside  $C_{\prec_1}(I)$  and  $C_{\prec_2}(I)$  and ensure that  $\omega(t)$  only intersects common faces of low codimension on its way to the target term order  $\prec_2$ .

The initial reduced Gröbner basis  $G$  over  $\prec_1$  makes it possible to compute an interior point in  $C_{\prec_1}(I)$ . Computing an interior point in the target cone  $C_{\prec_2}(I)$  is considerably more difficult, since we do not know the reduced Gröbner basis over  $\prec_2$  in advance. Tran [11] approached this problem using general degree bounds on polynomials in Gröbner bases. The general degree bounds in Tran’s approach may lead to integral weight vectors with 10,000-digit entries in representing a lexicographic interior point in the case of polynomials of degree 10 in 10 variables.

In this paper we give an algorithm where the line  $\omega(t)$  is replaced by a (formal) line  $\Omega(t)$  between suitably chosen perturbations given by  $\prec_1$  and  $\prec_2$  and  $I$ . It turns out that the numerical dependence on  $I$  disappears in our algorithm and that  $\Omega(t)$  may be viewed as a line which can be used for all ideals in the Gröbner walk from  $\prec_1$  to  $\prec_2$ . The formal line has the property that its initial and target points are always in the interior of the Gröbner cones. Furthermore the common faces that  $\Omega(t)$  intersect are all facets.

Tracking  $\Omega(t)$  gives a “Buchberger-like” Gröbner walk algorithm, where one only needs to compute with marked polynomials and term orders. On smaller examples the algorithm can easily be carried out by hand (cf. §5). The preliminary computational experience with a few larger examples seems quite promising (cf. §6).

An understanding of our algorithm requires a firm grip on the usual Gröbner walk algorithm. Therefore §2 and §3 recalls and proves fundamental results for the usual Gröbner walk using which we transition to the generic Gröbner walk in §4.

The basic technique we propose to avoid explicit perturbation is not quite new. The key idea of implicit (symbolic) perturbation was proposed by Charnes in 1952 to make Dantzig’s simplex method for linear programming finite. The method is now known as the lexicographic perturbation method, see [2, page 34], and used by many reliable implementations of the simplex method. In computational geometry, similar symbolic perturbation schemes are used to treat input data points in  $\mathbb{R}^n$  as if they were in general position, see [5, page 14].

## 2 Preliminaries

In this section we recall the basics of convex polyhedral cones. We emphasize a crucial result from the theory of group orders (Lemma 2.1) and recall the construction of the (restricted) Gröbner fan.

### 2.1 Cones and fans

A *convex polyhedral cone* is a set

$$C(v_1, \dots, v_r) = \mathbb{R}_{\geq 0}v_1 + \dots + \mathbb{R}_{\geq 0}v_r \subseteq \mathbb{R}^n$$

where  $v_1, \dots, v_r \in \mathbb{R}^n$ . In the following a *cone* will refer to a convex polyhedral cone. The dual of a cone  $C \subseteq \mathbb{R}^n$  is

$$C^\vee = \{\omega \in \mathbb{R}^n \mid \langle \omega, v \rangle \geq 0, \text{ for every } v \in C\}.$$

The dual of a cone is a cone and the intersection of two cones is a cone. The *dimension* of a cone is the dimension of the linear subspace it spans. For a vector  $u \in \mathbb{R}^n$  we let  $u^\perp = \{x \in \mathbb{R}^n \mid \langle u, x \rangle = 0\}$ . A face  $F \subseteq C$  of a cone  $C$  is a subset  $F = u^\perp \cap C$ , where  $u \in C^\vee$ . Faces of codimension one in  $C$  are called *facets*.

A collection  $\mathcal{F}$  of cones and their faces is called a *fan* if for every  $C_1, C_2 \in \mathcal{F}$  we have  $C_1 \cap C_2 \in \mathcal{F}$  and  $C_1 \cap C_2$  is a common face of  $C_1$  and  $C_2$ .

### 2.2 Rational group orders on $\mathbb{Q}^n$

Let  $(A, +)$  be an abelian group. Recall that a *group order*  $\prec$  on  $A$  is a total order  $\prec$  on  $A$  such that

$$x \prec y \implies x + z \prec y + z$$

for every  $x, y, z \in A$ .

Let  $\omega = (\omega_1, \dots, \omega_n) \subset \mathbb{Q}^n$  be a  $\mathbb{Q}$ -vector space basis for  $\mathbb{Q}^n$ . Then we get a group order  $\prec_\omega$  on  $\mathbb{Q}^n$  given by  $u \prec_\omega v$  if and only if

$$(\langle \omega_1, u \rangle, \dots, \langle \omega_n, u \rangle) <_{\text{lex}} (\langle \omega_1, v \rangle, \dots, \langle \omega_n, v \rangle),$$

where  $<_{\text{lex}}$  refers to the lexicographic order on  $\mathbb{Q}^n$ . We call such a group order *rational*. To describe arbitrary group orders on  $\mathbb{Q}^n$  similarly, one needs a more general setup including real vectors (see [9]). To ease the exposition we will restrict ourselves to rational group orders. A group order refers to a rational group order in the following. For a rational  $\epsilon > 0$  we put

$$\omega_\epsilon = \omega_1 + \epsilon\omega_2 + \dots + \epsilon^{n-1}\omega_n.$$

The following well known lemma plays a key role in the generic Gröbner walk.

**Lemma 2.1** *Let  $\omega = (\omega_1, \dots, \omega_n) \subset \mathbb{Q}^n$  be a  $\mathbb{Q}$ -basis. Suppose that  $F \subset \mathbb{Q}^n$  is a finite set of non-zero vectors with  $0 \prec_\omega v$  for  $v \in F$ . Then there exists  $0 < \delta \in \mathbb{Q}$  such that  $\langle \omega_\epsilon, v \rangle > 0$  for every  $v \in F$  and  $\epsilon \in \mathbb{Q}$  with  $0 < \epsilon < \delta$ .*

*Proof.* We prove this by induction on  $n$ . The case  $n = 1$  is clear. For  $n > 1$  we may find  $0 < \delta_0 \in \mathbb{Q}$  such that

$$\langle \omega_{n-1} + \epsilon \omega_n, v \rangle > 0$$

for every  $v \in F$  with  $\langle \omega_{n-1}, v \rangle > 0$  and  $\epsilon \in \mathbb{Q}$  with  $0 < \epsilon < \delta_0$ . Therefore  $0 \prec_{\omega'} v$  for  $\omega' = (\omega_1, \dots, \omega_{n-2}, \omega_{n-1} + \epsilon \omega_n)$  for every  $v \in F$  if  $0 < \epsilon < \delta_0$ .

By induction there exists  $0 < \delta_1 \in \mathbb{Q}$  such that  $\langle \omega'_\epsilon, v \rangle > 0$  for every  $v \in F$  and  $\epsilon \in \mathbb{Q}$  with  $0 < \epsilon < \delta_1$ . Putting  $\delta = \min(\delta_0, \delta_1)$  we get  $\langle \omega_\epsilon, v \rangle > 0$  for every  $v \in F$  and  $\epsilon \in \mathbb{Q}$  with  $0 < \epsilon < \delta$ .  $\square$

A group order  $\prec$  on  $\mathbb{Q}^n$  is called a term order if  $0 \prec v$  for every  $v \in \mathbb{N}^n$ . This is equivalent to  $0 \prec e_i$  where  $e_i$  denotes the  $i$ -th canonical basis vector for  $i = 1, \dots, n$ . As a consequence of Lemma 2.1 we get the following corollary.

**Corollary 2.2** *Let  $F \subset \mathbb{Q}^n$  be a finite set of positive vectors for the group order  $\prec$  i.e.  $v \succ 0$  for every  $v \in F$ . Then there exists  $\omega \in \mathbb{Q}^n$  such that*

$$\langle \omega, v \rangle > 0$$

for every  $v \in F$ . If  $\prec$  is a term order, we may assume that  $\omega$  has positive coordinates.

## 2.3 The Gröbner fan

Let  $R = k[x_1, \dots, x_n]$  denote the ring of polynomials in  $n$  variables over a field  $k$ . It is convenient to view  $R$  as the semigroup ring  $k[\mathbb{N}^n]$ . We briefly recall the construction of the (restricted) Gröbner fan (cf. [8]) for an arbitrary ideal in  $R$ .

Fix a group order  $\prec$  on  $\mathbb{Q}^n$ . For a polynomial  $f = \sum_{v \in \mathbb{N}^n} a_v x^v \in R$  we let  $\text{supp}(f) = \{v \in \mathbb{N}^n \mid a_v \neq 0\}$  and  $\text{in}_\prec(f) = a_u x^u$ , where  $u = \max_\prec \text{supp}(f)$ . For a vector  $\omega \in \mathbb{R}^n$  we let  $\text{in}_\omega(f)$  denote the sum of terms  $a_v x^v$  in  $f$  maximizing the  $\omega$ -weight  $\langle \omega, v \rangle$ . We call  $f$   $\omega$ -homogeneous if  $f = \text{in}_\omega(f)$ . To an ideal  $I \subseteq R$  we associate the ideals  $\text{in}_\prec(I) = \langle \text{in}_\prec(f) \mid f \in I \setminus \{0\} \rangle$  and  $\text{in}_\omega(I) = \langle \text{in}_\omega(f) \mid f \in I \rangle$ . These ideals may be viewed as deformations of the original ideal  $I$ . The *initial ideal*  $\text{in}_\prec(I)$  is generated by monomials. This does not hold for  $\text{in}_\omega(I)$  in general (unless  $\omega$  is chosen generically).

Now define

$$\partial_\prec(f) = \{u - u' \mid u' \in \text{supp}(f) \setminus \{u\}\} \subset \mathbb{Z}^n,$$

where  $a_u x^u = \text{in}_\prec(f)$ . For a finite set  $F \subseteq R$  of polynomials we let

$$\partial_\prec(F) = \bigcup_{f \in F} \partial_\prec(f)$$

and

$$\begin{aligned} C_\prec(F) &= C(\partial_\prec(F))^\vee \cap \mathbb{R}_{\geq 0}^n \\ &= \{\omega \in \mathbb{R}_{\geq 0}^n \mid \langle \omega, v \rangle \geq 0, v \in \partial_\prec(f), f \in F\}. \end{aligned}$$

Notice that  $\dim C_\prec(F) = n$  by Corollary 2.2 and that

$$C_\prec(F) = \{\omega \in \mathbb{R}_{\geq 0}^n \mid \text{in}_\prec(\text{in}_\omega(f)) = \text{in}_\prec(f) \text{ for every } f \in F\}.$$

A *Gröbner basis* for  $I$  over  $\prec$  is a finite set of polynomials  $G = \{g_1, \dots, g_r\} \subseteq I$  such that

$$\langle \text{in}_{\prec}(g_1), \dots, \text{in}_{\prec}(g_r) \rangle = \text{in}_{\prec}(I).$$

The Gröbner basis  $G$  is called *minimal* if none of  $g_1, \dots, g_r$  can be left out and *reduced* if the coefficient of  $\text{in}_{\prec}(g_i)$  is 1 and  $\text{in}_{\prec}(g_i)$  does not divide any of the terms in  $g_j$  for  $i \neq j$  and  $i, j = 1, \dots, r$ . A reduced Gröbner basis is uniquely determined. Minimal Gröbner bases exist for arbitrary group orders. However, Gröbner bases over arbitrary group orders do not necessarily generate the ideal (as opposed to Gröbner bases over term orders). Similarly, the reduced Gröbner basis is only guaranteed to exist for term orders.

To define the Gröbner fan we now specialize to the case where  $\prec$  is a term order. The *Gröbner cone*  $C_{\prec}(I)$  of an ideal  $I$  over  $\prec$  is defined as  $C_{\prec}(G)$ , where  $G$  is the reduced Gröbner basis of  $I$  over  $\prec$ . The *Gröbner fan* of  $I$  is defined as the set of cones  $C_{\prec}(I)$  along with their faces, where  $\prec$  runs through all term orders. This is a finite collection of cones [10, Theorem 1.2] and one may prove that it is a fan (Propositions 2.3 and 2.4 in [10] give a proof assuming non-negative weight vectors). The following proposition shows that  $C_{\prec}(I)$  is the largest cone among  $C_{\prec}(G)$ , where  $G$  is a Gröbner basis for  $I$  over  $\prec$ .

**Proposition 2.3** *Let  $G$  be a (not necessarily reduced) Gröbner basis for  $I$  over  $\prec$ . Then*

$$C_{\prec}(G) \subseteq C_{\prec}(I).$$

*Proof.* Transforming  $G$  into a minimal Gröbner basis  $G'$  by omitting certain polynomials in  $G$  clearly leads to an inclusion  $C_{\prec}(G) \subseteq C_{\prec}(G')$ . Transforming  $G'$  into the reduced Gröbner basis proceeds by a sequence of reduction steps: suppose that  $f_i, f_j \in G'$  and that a term  $x^v$  in  $f_j$  is divisible by  $\text{in}_{\prec}(f_i)$ . Then  $f_j$  is replaced by  $f'_j = f_j - (x^v / \text{in}_{\prec}(f_i))f_i$ . This reduction may introduce “new” monomials which are not present in  $f_j$ . More precisely if  $w \in \text{supp}(f'_j)$ , then  $w \in \text{supp}(f_j)$  or  $w = v - u + u'$ , where  $a_u x^u = \text{in}_{\prec}(f_i)$  and  $u' \in \text{supp}(f_i)$ . In the latter case we get  $w' - w = (w' - v) + (u - u')$ , where  $a_{w'} x^{w'} = \text{in}_{\prec}(f_j)$ . Let  $G''$  denote the Gröbner basis obtained by replacing  $f_j$  with  $f'_j$ . Then  $C(\partial_{\prec}(G')) \supseteq C(\partial_{\prec}(G''))$  and thereby  $C_{\prec}(G') \subseteq C_{\prec}(G'')$ . Since the reduced Gröbner basis is obtained using a finite number of these reduction steps we have proved the inclusion.  $\square$

For a specific term order one may have infinitely many cones given by different minimal Gröbner bases. As an example consider the ideal  $I = \langle x, y \rangle \subset k[x, y]$ . If  $n$  is a positive natural number then  $G_n = \{x - y^n, y\}$  is a minimal Gröbner basis for  $I$  over the lexicographic order  $\prec$  with  $x \succ y$ . In this case

$$C_{\prec}(I) \supsetneq C_{\prec}(G_1) \supsetneq C_{\prec}(G_2) \supsetneq \dots$$

### 3 The Gröbner walk

We outline the basic idea of the Gröbner walk [3] and give a new lifting step using reduction modulo the known Gröbner basis.

Let  $\prec_1$  and  $\prec_2$  be term orders and  $I$  an ideal in  $R$ . Suppose that we know the reduced Gröbner basis  $G$  for  $I$  over  $\prec_1$ . If

$$\omega \in C_{\prec_1}(I) \cap C_{\prec_2}(I)$$

lies on the common face of the two Gröbner cones, then  $G_\omega = \{\text{in}_\omega(g) \mid g \in G\}$  is the reduced Gröbner basis for  $\text{in}_\omega(I)$  over  $\prec$ . Now a “lifting” of  $G_\omega$  to a Gröbner basis for  $I$  over  $\prec_2$  is required. The procedure for this is based on Proposition 3.2 below. It involves a Gröbner basis computation for  $\text{in}_\omega(I)$  over  $\prec_2$ . The point is that if  $F = C_{\prec_1}(I) \cap C_{\prec_2}(I)$  is a high dimensional face (like a facet) and  $\omega$  is in the relative interior of  $F$ , the ideal  $\text{in}_\omega(I)$  is close to a monomial ideal and this Gröbner basis computation becomes very easy.

Given a term order  $\prec$  and a vector  $\omega \in \mathbb{R}_{\geq 0}^n$  we define the new term order  $\prec_\omega$  by  $u \prec_\omega v$  if and only if  $\langle u, \omega \rangle < \langle v, \omega \rangle$  or  $\langle u, \omega \rangle = \langle v, \omega \rangle$  and  $u \prec v$ . We record the following well known lemma.

**Lemma 3.1** [10, Proposition 1.8] *Let  $I \subseteq R$  be any ideal and  $\omega \in \mathbb{R}_{\geq 0}^n$ . Then*

$$\text{in}_\prec(\text{in}_\omega(I)) = \text{in}_{\prec_\omega}(I).$$

The lifting step (Proposition 3.2(ii) below) in the following proposition is different from the lifting step in the usual Gröbner walk [10, Subroutine 3.7].

**Proposition 3.2** *Let  $I \subseteq R$  be an ideal and  $\prec_1, \prec_2$  term orders on  $R$ . Suppose that  $G$  is the reduced Gröbner basis for  $I$  over  $\prec_1$ . If  $\omega \in C_{\prec_1}(I) \cap C_{\prec_2}(I)$ , then*

(i) *The reduced Gröbner basis for  $\text{in}_\omega(I)$  over  $\prec_1$  is  $G_\omega = \{\text{in}_\omega(g) \mid g \in G\}$ .*

(ii) *If  $H$  is the reduced Gröbner basis for  $\text{in}_\omega(I)$  over  $\prec_2$ , then*

$$\{f - f^G \mid f \in H\}$$

*is a minimal Gröbner basis for  $I$  over  $\prec_{2\omega}$ . Here  $f^G$  is the unique remainder obtained by dividing  $f$  modulo  $G$ .*

(iii) *The reduced Gröbner basis for  $I$  over  $\prec_{2\omega}$  coincides with the reduced Gröbner basis for  $I$  over  $\prec_2$ .*

*Proof.* Given a term order  $\prec$  and a vector  $\omega \in C_\prec(I)$ , the reduced Gröbner bases for  $I$  over  $\prec$  and  $\prec_\omega$  agree. This proves (iii) and (i) taking Lemma 3.1 into consideration. Suppose that  $f$  is an  $\omega$ -homogeneous polynomial (cf. §2.3) in  $\text{in}_\omega(I)$ . Using the division algorithm in computing the unique remainder  $f^G$ , we keep reducing terms with the same  $\omega$ -weight as the terms in  $f = \text{in}_\omega(f)$ . Since  $\text{in}_{\prec_1}(\text{in}_\omega(g)) = \text{in}_{\prec_1}(g)$  for  $g \in G$  and  $f^G = 0$ , we see that all terms in  $f^G$  will have  $\omega$ -weight strictly less than the terms in  $f$ . Therefore

$$\text{in}_\omega(f) = \text{in}_\omega(f - f^G).$$

Now suppose that  $\{f_1, \dots, f_s\}$  is the reduced Gröbner basis for  $\text{in}_\omega(I)$  over  $\prec_2$ . In particular we get that  $f_i$  is  $\omega$ -homogeneous for  $i = 1, \dots, s$ . Then

$$\begin{aligned} \text{in}_{\prec_2\omega}(I) &= \text{in}_{\prec_2}(\text{in}_\omega(I)) = \langle \text{in}_{\prec_2}(f_1), \dots, \text{in}_{\prec_2}(f_s) \rangle \\ &= \langle \text{in}_{\prec_2}(\text{in}_\omega(f_1)), \dots, \text{in}_{\prec_2}(\text{in}_\omega(f_s)) \rangle \\ &= \langle \text{in}_{\prec_2}(\text{in}_\omega(f_1 - f_1^G)), \dots, \text{in}_{\prec_2}(\text{in}_\omega(f_s - f_s^G)) \rangle \\ &= \langle \text{in}_{\prec_2\omega}(f_1 - f_1^G), \dots, \text{in}_{\prec_2\omega}(f_s - f_s^G) \rangle. \end{aligned}$$

This proves that  $\{f_1 - f_1^G, \dots, f_s - f_s^G\} \subseteq I$  is a (minimal) Gröbner basis for  $I$  over  $\prec_{2\omega}$ .  $\square$

Proposition 3.2 may be turned into a Gröbner basis conversion algorithm as shown in the following section.

### 3.1 Conversion along a line

A natural approach to Gröbner basis conversion is to trace the line between vectors in different Gröbner cones and update Gröbner bases successively using Proposition 3.2. This process is called the Gröbner walk [3]. A good reference for this procedure is [4, §4], which inspired the following. We sketch the first step of the Gröbner walk. The succeeding steps of the Gröbner walk are similar. Suppose that  $\omega_0 \in C_{\prec_1}(I)$ ,  $\tau_0 \in C_{\prec_2}(I)$  and that  $G$  is the reduced Gröbner basis for  $I$  over  $\prec_1$ . Here  $\prec_1$  and  $\prec_2$  are rational term orders (cf. §2.2) given by  $\mathbb{Q}$ -bases  $\omega = (\omega_1, \dots, \omega_n)$  and  $\tau = (\tau_1, \dots, \tau_n)$  respectively. Then we consider the line

$$\omega(t) = (1 - t)\omega_0 + t\tau_0, \quad 0 \leq t \leq 1$$

in the Gröbner fan of  $I$  from  $\omega_0$  to  $\tau_0$ . Initially we know the reduced Gröbner basis at  $\omega(0) = \omega_0$  (being  $G$ ). Consider the “last”  $\omega' = \omega(t')$  in  $C_{\prec_1}(I) = C_{\prec_1}(G)$ . To be more precise  $t'$  satisfies

1.  $0 \leq t' < 1$
2.  $\omega(t) \in C_{\prec_1}(I)$  for  $t \in [0, t']$  and  $\omega(t' + \epsilon) \notin C_{\prec_1}(I)$  for every  $\epsilon > 0$ .

If no such  $t'$  exists then  $G$  is the reduced Gröbner basis over  $\prec_2$ . If  $t'$  exists  $\omega(t')$  is on a proper face of  $C_{\prec_1}(I)$  and  $v \in \partial(G)$  exists with  $\langle \omega(t' + \epsilon), v \rangle < 0$  for  $\epsilon > 0$ . This implies that  $\langle \tau_0, v \rangle < \langle \omega_0, v \rangle$  and hence  $\langle \tau_0, v \rangle < 0$ .

This indicates the procedure for finding  $t'$  given  $G$ . For  $v \in \partial(G)$  satisfying  $\langle \tau_0, v \rangle < 0$  we solve  $\langle \omega(t), v \rangle = 0$  for  $t$  giving

$$t_v = \frac{\langle \omega_0, v \rangle}{\langle \omega_0, v \rangle - \langle \tau_0, v \rangle}.$$

Then  $t'$  is the minimal among these  $t_v$ . In this case  $\omega' = \omega(t')$  lies on a proper face  $F$  of  $C_{\prec_1}(I)$  and clearly

$$\omega' \in C_{\prec_{2\omega'}}(I).$$

Now we use  $\prec_{2\omega'}$  as the term order  $\prec_2$  in Proposition 3.2. The point is that we only need the target term order  $\prec_2$  to compute a Gröbner basis for  $\text{in}_{\omega'}(I)$  (not the

notational beast  $\prec_{2\omega'}$ ). The reason for this is that the Buchberger algorithm in this case solely works with  $\omega'$ -homogeneous polynomials and ties are broken with  $\prec_2$ .

To prove that we actually enter a new Gröbner cone we need to show that  $t' > 0$  (cf. [4], §5, (5.3) Lemma). In the initial step it may happen that  $t' = 0$ . But if this is the case we may assume (in the following step of the Gröbner walk) that  $G$  is the reduced Gröbner basis over  $\prec = \prec_{2\omega'}$ . Since  $\tau_0 \in C_{\prec_2}(I)$  is non-zero we may use  $\tau_0$  as the first vector in a  $\mathbb{Q}$ -basis representing  $\prec_2$ . In this case assume that  $t' = 0$ . This means that we can find  $v \in \partial(G)$  with  $\langle \omega', v \rangle = 0$  and  $\langle \tau_0, v \rangle < 0$  contradicting that  $G$  is a Gröbner basis over  $\prec$ .

We have outlined the procedure for tracking the line  $\omega(t)$  through the Gröbner fan detecting when  $\omega(t)$  leaves a cone. The salient point of the generic Gröbner walk is that this calculation can be done formally by choosing certain generically perturbed  $\omega_0$  and  $\tau_0$  given by  $\prec_1$  and  $\prec_2$ .

Here are the steps of the usual Gröbner walk algorithm with the modified lifting step. Recall that a marked polynomial is a polynomial with a distinguished term, which is the initial term with respect to a term order  $\prec$ . For a marked polynomial  $f$ ,  $\partial(f)$  is defined in the natural way (cf. the definition of  $\partial_{\prec}(f)$  in §2.3). A marked Gröbner basis over a term order  $\prec$  is a Gröbner basis over  $\prec$  with all initial terms (with respect to  $\prec$ ) marked. For a marked Gröbner basis we let  $\partial(G) = \cup_{f \in G} \partial(f)$ .

**INPUT:** Marked reduced Gröbner basis  $G$  for  $I$  over a term order  $\prec_1$ , a term order  $\prec_2$  along with  $\omega_0 \in C_{\prec_1}(I)$  and  $\tau_0 \in C_{\prec_2}(I)$ .

**OUTPUT:** Reduced Gröbner basis for  $I$  over  $\prec_2$ .

- (i)  $t = -\infty$ .
- (ii) **Compute\_last\_t.** If  $t = \infty$  output  $G$  and halt.
- (iii) Compute generators  $\text{in}_{\omega}(G) = \{\text{in}_{\omega}(g) \mid g \in G\}$  for  $\text{in}_{\omega}(I)$  as

$$\text{in}_{\omega}(g) = a^u x^u + \sum_{v \in S_g} a_v x^v,$$

where  $S_g = \{v \in \text{supp}(g) \setminus \{u\} \mid t_{u-v} = t\}$  and  $a_u x^u$  is the marked term of  $g \in G$ .

- (iv) Compute reduced Gröbner basis  $H$  for  $\text{in}_{\omega}(I)$  over  $\prec_2$  and mark  $H$  according to  $\prec_2$ .

- (v) Let

$$H' = \{f - f^G \mid f \in H\}.$$

Use marking of  $H$  to mark  $H'$ .

- (vi) Autoreduce  $H'$  and put  $G = H'$ .
- (vii) Repeat from (ii).

**Compute\_last\_t:**

1. Let  $V := \{v \in \partial(G) \mid \langle \omega_0, v \rangle \geq 0 \text{ and } \langle \tau_0, v \rangle < 0 \text{ and } t \leq t_v\}$ , where

$$t_v = \frac{\langle \omega_0, v \rangle}{\langle \omega_0, v \rangle - \langle \tau_0, v \rangle}.$$

2. If  $V = \emptyset$ , put  $t = \infty$  and return.
3. Let  $t := \min\{t_v \mid v \in V\}$  and return.

## 4 The generic Gröbner walk

In this section we show how certain generic choices of  $\omega_0$  and  $\tau_0$  from §3 lead to the generic Gröbner walk algorithm. The crucial point is that step (3) of the procedure **Compute\_last\_t** can be carried out formally using  $\omega_0$  and  $\tau_0$  from well defined perturbations given the term orders  $\prec_1$  and  $\prec_2$ .

For an ideal  $I \subseteq R$  we let  $\partial(I) \subseteq \mathbb{Q}^n$  denote the union of  $\partial_{\prec}(G)$ , where  $G$  runs through the finitely many reduced Gröbner bases for  $I$ . Let  $\prec_1$  and  $\prec_2$  be two term orders given by  $\mathbb{Q}$ -bases  $\omega = (\omega_1, \dots, \omega_n)$  and  $\tau = (\tau_1, \dots, \tau_n)$  of  $\mathbb{Q}^n$  respectively. Observe that  $\omega_\eta$  and  $\tau_\eta$  are in the interior of the Gröbner cones  $C_{\prec_1}(I)$  and  $C_{\prec_2}(I)$  respectively for sufficiently small positive  $\eta$ . This follows from Lemma 2.1. Now define

$$C_{\prec_1, \prec_2} = \{v \in \mathbb{R}^n \mid 0 \prec_1 v \text{ and } v \prec_2 0\}.$$

Here  $\prec_1, \prec_2$  are extended to group orders on  $\mathbb{R}^n$  using  $\omega$  and  $\tau$ .

**Example 4.1** *Suppose that  $\prec_1$  is degree (reverse) lexicographic order and  $\prec_2$  lexicographic order with  $y \prec_{1,2} x$ . Then choosing  $\omega = ((1, 1), (0, -1))$  and  $\tau = ((1, 0), (0, 1))$ , we get  $0 \prec_1 v$  implies  $(0, 0) <_{lex} (v_1 + v_2, -v_2)$  and  $v \prec_2 0$  implies  $(v_1, v_2) <_{lex} (0, 0)$ . Intersecting the regions yielded gives (see Figure 1)*

$$C_{\prec_1, \prec_2} = \{(x, y) \in \mathbb{R}^2 \mid x + y > 0, x < 0\}.$$

To fully understand the choice of  $\delta$  and  $\epsilon$  in the following we encourage the reader to compare with the computations in (\*) and (\*\*) below. Define

$$M_\tau = \{\langle \tau_i, u \rangle v \mid i = 1, \dots, n; u, v \in \partial(I)\}.$$

Corollary 2.2 shows that there exists sufficiently small positive  $\delta$  such that

$$u \prec_1 v \iff \langle \omega_\delta, u \rangle < \langle \omega_\delta, v \rangle \tag{1}$$

for  $u, v \in M_\tau$ . Suppose that  $\delta$  satisfies (1). Now put

$$N_\delta = \{\langle \omega_\delta, u \rangle v \mid u, v \in \partial(I)\}.$$

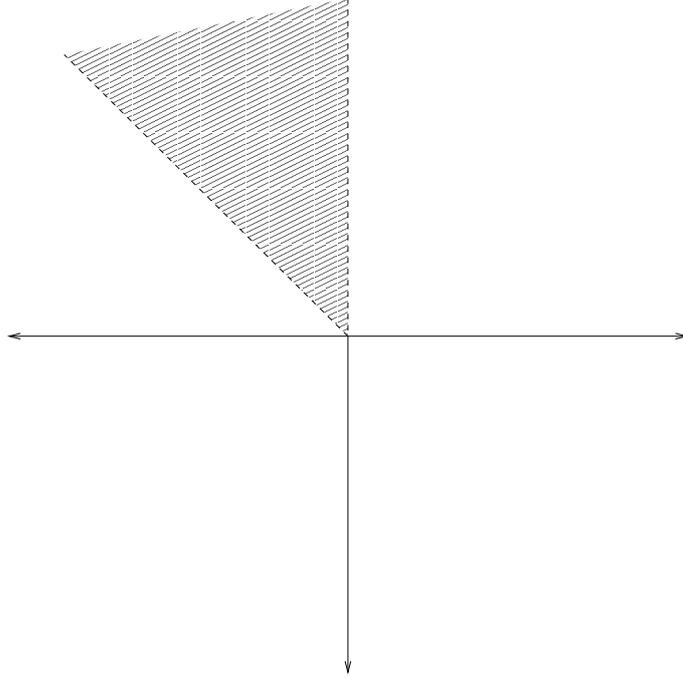


Figure 1:  $C_{\prec_1, \prec_2}$  for  $\prec_1 = \text{degrevlex}$  and  $\prec_2 = \text{lex}$

Again by Corollary 2.2 we know that there exists sufficiently small positive  $\epsilon$  such that

$$u \prec_2 v \iff \langle \tau_\epsilon, u \rangle < \langle \tau_\epsilon, v \rangle \quad (2)$$

for  $u, v \in N_\delta$ . Suppose now that we pick  $\delta$  according to (1) and  $\epsilon$  according to (2). If  $v \in \partial(I) \cap C_{\prec_1, \prec_2}$  we put

$$t_v = \frac{\langle \omega_\delta, v \rangle}{\langle \omega_\delta, v \rangle - \langle \tau_\epsilon, v \rangle} = \frac{1}{1 - \frac{\langle \tau_\epsilon, v \rangle}{\langle \omega_\delta, v \rangle}}.$$

If  $u, v \in \partial(I) \cap C_{\prec_1, \prec_2}$  then  $\langle \omega_\delta, u \rangle, \langle \omega_\delta, v \rangle > 0$  and

$$\begin{aligned} t_u < t_v & \iff (*) \\ \frac{\langle \tau_\epsilon, u \rangle}{\langle \omega_\delta, u \rangle} < \frac{\langle \tau_\epsilon, v \rangle}{\langle \omega_\delta, v \rangle} & \iff \\ \langle \tau_\epsilon, \langle \omega_\delta, v \rangle u \rangle < \langle \tau_\epsilon, \langle \omega_\delta, u \rangle v \rangle & \iff \\ \langle \omega_\delta, v \rangle u \prec_2 \langle \omega_\delta, u \rangle v & \end{aligned}$$

To evaluate  $\prec_2$  above we see that

$$\begin{aligned} \langle \tau_i, \langle \omega_\delta, v \rangle u \rangle < \langle \tau_i, \langle \omega_\delta, u \rangle v \rangle & \iff (**) \\ \langle \omega_\delta, \langle \tau_i, u \rangle v \rangle < \langle \omega_\delta, \langle \tau_i, v \rangle u \rangle & \iff \\ \langle \tau_i, u \rangle v \prec_1 \langle \tau_i, v \rangle u & \end{aligned}$$

for  $i = 1, \dots, n$ . Let  $T$  denote the matrix whose rows are  $\tau_1, \dots, \tau_n$ . By choosing  $\delta$  and  $\epsilon$  generically as above it follows that

$$t_u < t_v \iff Tuv^t \prec_1 Tvu^t$$

where  $\prec_1$  above refers to the lexicographic extension of  $\prec_1$  on  $\mathbb{Z}^n$  to  $\mathbb{Z}^n \times \dots \times \mathbb{Z}^n$ . Here,  $Tuv^t$  and  $Tvu^t$  are  $n \times n$  matrices and we need to compare their rows. Notice that the comparison between  $t_u$  and  $t_v$  does not involve  $\delta$  and  $\epsilon$  but only the term orders  $\prec_1$  and  $\prec_2$ . This leads us to define the *facet preorder*  $\prec$  by

$$u \prec v \iff t_u < t_v \iff Tuv^t \prec_1 Tvu^t \quad (3)$$

for  $u, v \in \partial(I) \cap C_{\prec_1, \prec_2}$ .

**Example 4.2** *Continuing the setup in Example 4.1, if  $u = (u_1, u_2)$  and  $v = (v_1, v_2)$ , then*

$$T = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and the facet preorder  $\prec$  is given by

$$u \prec v \iff (u_1v \prec_1 v_1u) \vee ((u_1v = v_1u) \wedge (u_2v \prec_1 v_2u)).$$

If  $t_u = t_v$  then  $Tuv^t = Tvu^t$  and  $uv^t = vu^t$  since  $T$  is an invertible matrix. The identity  $uv^t = vu^t$  implies that  $u$  and  $v$  are collinear. Since  $u$  and  $v$  lie in the same half space,  $u$  is a positive multiple of  $v$ .

This has the nice consequence that the line  $\omega(t)$  between  $\omega_\delta$  and  $\tau_\epsilon$  intersects the cones in the Gröbner fan in dimension  $\geq n - 1$ . Consider the typical situation, where  $v \in C = C(v, v_1, \dots, v_m)$  is chosen to minimize  $t_v$  as in the Gröbner walk. Then  $\omega(t_v)$  is on a proper face  $F$  of  $C^\vee$ . Since  $t_v = t_u$  implies that  $u$  is a positive multiple of  $v$  for  $u \in \{v_1, \dots, v_m\}$ , we conclude that  $\dim F = n - 1$  i.e.  $F$  is a facet.

The facet preorder  $\prec$  defined in (3) may be inserted in the classical Gröbner walk algorithm giving the *generic Gröbner walk algorithm* completely removing the numerical dependence on the line  $\omega(t)$ . Below,  $-\infty(\infty)$  denotes a vector strictly smaller (larger) than the vectors in  $\partial(I) \cap C_{\prec_1, \prec_2}$ .

**INPUT:** Marked reduced Gröbner basis  $G$  for  $I$  over a term order  $\prec_1$  and a term order  $\prec_2$  (the facet preorder  $\prec$  is given as in (3) using  $\prec_1$  and  $\prec_2$ ).

**OUTPUT:** Reduced Gröbner basis for  $I$  over  $\prec_2$ .

(i)  $w = -\infty$ .

(ii) **Compute\_last\_w.** If  $w = \infty$  output  $G$  and halt.

(iii) Compute generators  $\text{in}_\omega(G) = \{\text{in}_\omega(g) \mid g \in G\}$  for  $\text{in}_\omega(I)$  as

$$\text{in}_\omega(g) = a^u x^u + \sum_{v \in S_g} a_v x^v,$$

where  $S_g = \{v \in \text{supp}(g) \setminus \{u\} \mid u - v \prec w, w \prec u - v\}$  and  $a_u x^u$  is the marked term of  $g \in G$ .

(iv) Compute reduced Gröbner basis  $H$  for  $\text{in}_\omega(I)$  over  $\prec_2$  and mark  $H$  according to  $\prec_2$ .

(v) Let

$$H' = \{f - f^G \mid f \in H\}.$$

Use marking of  $H$  to mark  $H'$ .

(vi) Autoreduce  $H'$  and put  $G = H'$ .

(vii) Repeat from (ii).

### Compute\_last\_w:

1. Let  $V := \{v \in \partial(G) \cap C_{\prec_1, \prec_2} \mid w \prec v\}$ .
2. If  $V = \emptyset$ , put  $w = \infty$  and return.
3. Let  $w := \min_{\prec} \{v \mid v \in V\}$  and return.

## 4.1 Variations on the generic Gröbner walk

Several variations on the generic Gröbner walk are possible. In many cases generators for an ideal are given which form a natural Gröbner basis with respect to a specific weight vector. This happens for example in implicitization problems with polynomials  $y_1 - f_1, \dots, y_m - f_m$ , where  $f_i$  are polynomials in  $x_1, \dots, x_n$  for  $i = 1, \dots, m$ . These polynomials form a Gröbner basis over a vector  $\omega$  assigning zero weights to  $x_1, \dots, x_n$  and positive weights to  $y_1, \dots, y_m$ . In this case one only needs to work with  $\omega$  and perturbations  $\tau_\epsilon$  of the target vector. One may also truncate the facet preorder  $\prec$  (to get a *face preorder*) using only parts  $(\omega_1, \dots, \omega_p)$  and  $(\tau_1, \dots, \tau_q)$  of the  $\mathbb{Q}$ -bases  $\omega$  and  $\tau$ . This leads to an analogue of the perturbation degree  $(p, q)$ -walk defined in [1].

## 5 An introductory example

We illustrate the generic Gröbner walk by a detailed example in the two dimensional case. For a given polynomial  $f \in R$  we let  $L_G(f) = f - f^G$ , where  $G$  is a marked Gröbner basis (markings are underlined). Let  $\prec_1$  denote degree (reverse) lexicographic order and  $\prec_2$  lexicographic order with  $y \prec_{1,2} x$ . The facet preorder  $\prec$  is given as in Example 4.2. Consider the ideal

$$I = \langle x^2 - y^3, x^3 - y^2 - x \rangle \subset \mathbb{Q}[x, y].$$

Initially we put

$$G = \{\underline{y^3} - x^2, \underline{x^3} - y^2 - x\},$$

where the initial terms over  $\prec_1$  are marked. Clearly  $G$  is the reduced Gröbner basis for  $I$  over  $\prec_1$ . The Gröbner cone is given by

$$C_{\prec_1}(I) = C(\{(-2, 3)\} \cup \{(3, -2)\})^\vee \cap \mathbb{R}_{\geq 0}^2.$$

In this case  $(3, -2) \notin C_{\prec_1, \prec_2}$  and  $V = \{(-2, 3)\}$ . So the first facet ideal is  $\langle \underline{y^3} - x^2, x^3 \rangle$ . The reduced Gröbner basis for this ideal over  $\prec_2$  is  $\{\underline{x^2} - y^3, xy^3, y^6\}$  and the lifting step is given by

$$\begin{aligned} L_G(x^2 - y^3) &= x^2 - y^3 \\ L_G(xy^3) &= xy^3 - y^2 - x \\ L_G(y^6) &= y^6 - xy^2 - x^2. \end{aligned}$$

Our new marked reduced Gröbner basis is

$$G = \{\underline{x^2} - y^3, \underline{xy^3} - y^2 - x, \underline{y^6} - xy^2 - y^3\}.$$

Since  $w = (-2, 3) \prec (-1, 4)$  it follows that  $V = \{(-1, 4)\}$  and the next facet ideal is  $\langle x^2, xy^3, \underline{y^6} - xy^2 \rangle$  with reduced Gröbner basis  $\{x^2, \underline{xy^2} - y^6, y^7\}$  over  $\prec_2$ . Since

$$\begin{aligned} L_G(x^2) &= x^2 - y^3 \\ L_G(xy^2 - y^6) &= xy^2 - y^6 + y^3 \\ L_G(y^7) &= y^7 - y^4 - y^2 - x \end{aligned}$$

our new marked reduced Gröbner basis is

$$G = \{\underline{x^2} - y^3, \underline{xy^2} - y^6 + y^3, \underline{y^7} - y^4 - y^2 - x\}.$$

Since  $w = (-1, 4) \prec (-1, 7)$  we get  $V = \{(-1, 7)\}$  and the next facet ideal is  $\langle x^2, xy^2, \underline{y^7} - x \rangle$  with reduced Gröbner basis  $(y^9, \underline{x} - y^7)$  over  $\prec_2$ . Here

$$\begin{aligned} L_G(y^9) &= y^9 - 2y^6 - y^4 + y^3 \\ L_G(x - y^7) &= x - y^7 + y^4 + y^2. \end{aligned}$$

The new marked reduced Gröbner basis is

$$G = \{\underline{y^9} - 2y^6 - y^4 + y^3, \underline{x} - y^7 + y^4 + y^2\}.$$

Since  $V = \emptyset$  in this case, the generic Gröbner walk halts and  $G$  is the reduced Gröbner basis for  $I$  over  $\prec_2$ .

## 6 Preliminary computational experience

In this section we report briefly on computations using an experimental implementation **gw** of the generic Gröbner walk converting from degree reverse lexicographic order to lexicographic order. We have used **C++** with tools from the standard template library (a polynomial is for example implemented using the associative container **map** from integer vectors sorted by the term order to elements of the

field). This is certainly not optimal for larger computations, where the bucket representation of polynomials [12] should be used. Our field is the rational numbers implemented using the GMP package [7]. We work with polynomials with rational coefficients and not normalized integral coefficients (here a further improvement is available). More experienced computer algebra programmers are encouraged to work out effective implementations of our algorithm. The few results given here only serve to illustrate that a rather naive implementation shows promise.

We have selected three examples from [11]. The timings below are for a 1GHz Pentium (3 year old Dell notebook) with 500MB running Red Hat 9 Linux. Tran reported timings from a 233MHz Intel processor with 144MB running Red Hat 5 Linux with his deterministic Gröbner walk algorithm. Needless to say it is difficult if not impossible to compare timings across different computer architectures and implementations. We are slightly optimistic though. It seems that the term order comparisons in the generic Gröbner walk algorithm matches up with the explicit rational arithmetic in Tran's implementation (we do not expect the rational vectors in Tran's implementation to become large on these relatively small examples).

**Example 6.1** ([11], **Example 3.2**) *Target order  $\prec$  is lexicographic with  $x \succ y \succ z \succ w$ .*

$$\begin{aligned}
&8w^2 + 5wx - 4wy + 2wz + 3w + 5x^2 + 2xy - 7xz \\
&\quad - 7x + 7y^2 - 8yz - 7y + 7z^2 - 8z + 8, \\
&3w^2 - 5wx - 3wy - 6wz + 9w + 4x^2 + 2xy - 2xz \\
&\quad + 7x + 9y^2 + 6yz + 5y + 7z^2 + 7z + 5, \\
&- 2w^2 + 9wx + 9wy - 7wz - 4w + 8x^2 + 9xy - 3xz \\
&\quad + 8x + 6y^2 - 7yz + 4y - 6z^2 + 8z + 2, \\
&7w^2 + 5wx + 3xy - 5wz - 5w + 2x^2 + 9xy - 7xz + 4x \\
&\quad - 4y^2 - 5yz + 6y - 4z^2 - 9z + 2.
\end{aligned}$$

*Time for conversion: gw: 0.50s (Tran: 5.33s).*

**Example 6.2** ([11], **Example 3.3**) *Target order  $\prec$  is lexicographic with  $x \succ y \succ z$ .*

$$\begin{aligned}
&16 + 3x^3 + 16x^2z + 14x^2y^3, \\
&6 + y^3z + 17x^2z^2 + 7xy^2z^2 + 13x^3z^2.
\end{aligned}$$

*Time for conversion: gw: 21.84s (Tran: 91.07s).*

**Example 6.3** ([11], **Example 3.4**) *Target order  $\prec$  is lexicographic with  $x \succ y \succ z$ .*

$$\begin{aligned}
&15 + 10x^2y^2 + 13yz + 14xy^2z + 8x^2yz^2 + 11xy^3z^2, \\
&\quad 5 + 4xy + 8y^2, \\
&\quad 16x^3 + 19y + 4x^2y.
\end{aligned}$$

*Time for conversion: gw: 0.09s (Tran: 0.93s).*

## References

- [1] B. Amrhein, O. Gloor, and W. Küchlin. On the Walk. *Theoret. Comput. Sci.* **187** (1997), 179–202.
- [2] V. Chvatal. *Linear Programming*. W.H.Freeman and Company, 1983.
- [3] S. Collart, M. Kalkbrenner, and D. Mall. Converting bases with the Gröbner walk. *J. Symbolic Comp.* **6** (1997), 209–217.
- [4] D. Cox, J. Little, D. O’Shea. Using Algebraic Geometry, 2. edition. §5 is available from <http://mathcs.holycross.edu/~little/Pubs.html>.
- [5] M. de Berg, M. van Kreveld, M. Overmars, and O. Schwarzkopf. *Computational Geometry: Algorithms and Applications*. Springer-Verlag, Berlin, Germany, 2nd edition, 2000.
- [6] J. Faugère, P. Gianni, D. Lazard and T. Mora. Efficient computation of zero-dimensional ideal Gröbner bases by change of ordering. *J. Symbolic Comp.* **16** (1993), 329–344.
- [7] T. Granlund, GNU Multiple Precision Arithmetic Library 4.1.4. September 2004. Available from <http://swox.com/gmp/>.
- [8] T. Mora and L. Robbiano. The Gröbner fan of an ideal. *J. Symbolic Comp.* **6** (1988), 183–208.
- [9] L. Robbiano. Term orderings on the polynomial ring. Proceedings of EUROCAL 85. *Springer Lec. Notes Comp. Sci.* **204** (1985), 513–517.
- [10] B. Sturmfels. Gröbner Bases and Convex Polytopes. University Lecture Series **8**, Amer. Math. Soc., Providence, RI, 1996.
- [11] Q. Tran. A fast algorithm for Gröbner basis conversion and its applications. *J. Symbolic Comp.* **30** (2000), 451–467.
- [12] T. Yan. The geobucket data structure for polynomials. *J. Symbolic Comp.* **25** (1998), 285–293