Converting Bases with the Gröbner Walk

S. COLLART, M. KALKBRENER AND D. MALL

Department of Mathematics, Swiss Federal Institute of Technology, 8092 Zurich, Switzerland

We present an algorithm which converts a given Gröbner basis of a polynomial ideal I to a Gröbner basis of I with respect to another term order. The conversion is done in several steps following a path in the Gröbner fan of I. Each conversion step is based on the computation of a Gröbner basis of a toric degeneration of I.

1. Introduction

The objective of this note is the presentation of a procedure for converting a given Gröbner basis (Buchberger 1965, 1970) of a polynomial ideal I to a Gröbner basis of I with respect to another term order. This procedure, which we call the Gröbner walk, is completely elementary and does not require any assumptions about the dimension or the number of variables of the ideal.

The Gröbner walk breaks up the conversion problem into several simple steps between adjacent Gröbner bases following a path in the Gröbner fan. Since two term orders leading to adjacent Gröbner bases can be viewed as refinements of a common partial order, these simple transformations can be computed working just with the initial forms with respect to this partial order. Because the initial forms typically involve far fewer terms than the polynomials as a whole, the transformations can be computed cheaply. First experiments seem to indicate that the Gröbner walk performs rather well for large classes of examples.

It is interesting to note that, although the theoretic concepts on which the algorithm is based are neither new nor complicated, it has not been considered before as a candidate for efficient change of basis, even though there has been some interest in Gröbner basis conversion for some time (see for instance Faugère et al. (1993), Traverso (1993), Gianni et al. (1994) and Faugère (1994)). The main reason for the interest in this question is the obvious demand for fast conversion algorithms. For instance, if for some polynomial ideal a Gröbner basis with respect to some elimination order is sought, it may well be more efficient to compute first a Gröbner basis with respect to a total degree order, and then to convert, since total degree bases are generally much faster to compute. More specialised applications which by nature involve basis conversions might for instance be the implicitisation of varieties (Hoffmann (1989), Licciardi and Mora (1994), Kalkbrener (1995)) and the inversion of polynomial isomorphisms.

The authors are indebted to several sources for their inspiration. The article by Faugère et al. (1993) which proposed a solution in the zero-dimensional case motivated the authors to consider the question of basis conversion. The theory of Gröbner fans introduced by Mora and Robbiano (1988) (see also Schwartz (1988)) provided the geometric interpretation essential for the formulation of the algorithm. A dual approach is based on the notion of state polytope and toric degenerations (Bayer and Morrison (1988), Sturmfels (1994), Mall (1995), Collart and Mall (1995)). The authors' own interest in the question of base conversion goes back to 1993 (cf. Collart et al. (1993)). As pointed out to the authors by T. Mora, the idea behind the Gröbner walk was independently used by A. Assi (1993) for computing 'critical tropisms' (see also Alonso et al. (1992a, 1992b)).

The Gröbner walk was first implemented experimentally by the authors in *Mathematica*. More recently, B. Amrhein and O. Gloor (1995) are working with a 'real world' implementation developed at the University of Tübingen based on the Gröbner bases implementation by Windsteiger and Buchberger (1993). The results so far are very encouraging.

2. Gröbner cones

Throughout this paper let I be an ideal in the polynomial ring $A := K[x_1, \ldots, x_n]$, where K is an arbitrary field. The set of terms in the variables $x_1, \ldots, x_n$ is denoted by T^n. Let f be a polynomial in A and G a subset of A. The ideal generated by G is denoted by $\langle G \rangle$. For an admissible term order $\prec$ on T^n the initial monomial of f is denoted by $in_\prec(f)$ and the set $\{in_\prec(g) \mid g \in G\}$ is denoted by $G_\prec$. The reduced Gröbner basis of an ideal I with respect to $\prec$ is denoted by $R_\prec(I)$. The set $\Omega^n := \{(\psi_1, \ldots, \psi_n) \in \mathbb{Q}^n \mid \psi_i \geq 0$ for every $i \in \{1, \ldots, n\}\}$ is called the set of weight vectors. For $\sigma, \tau \in \Omega^n$ we denote the line segment in Ω^n between σ and τ by $\overline{\sigma\tau}$, i.e.

$$\overline{\sigma\tau} := \{(1-a)\,\sigma + a\,\tau \mid 0 \leq a \leq 1\}.$$

Let $\omega = (\omega_1, \ldots, \omega_n) \in \Omega^n$. For a monomial $t = a x_1^{i_1} \cdots x_n^{i_n}$ in A we denote its ω-degree by

$$deg_\omega(t) := \sum_{j=1}^{n} i_j \omega_j.$$

The ω-degree of a non-zero polynomial f, abbreviated $deg_\omega(f)$, is the maximum of the ω-degrees of the monomials which occur in f with non-zero coefficients. The initial form of f with respect to ω, abbreviated $in_\omega(f)$, is the sum of all those monomials in f with maximal ω-degree. Furthermore, $deg_\omega(0) := -1$ and $in_\omega(0) := 0$. A polynomial f is called *ω-homogeneous* if $f = in_\omega(f)$. Note that for $\omega = (1, \ldots, 1)$ this notion coincides with standard homogeneity. For a subset G of A the set $\{in_\omega(g) \mid g \in G\}$ is denoted by G_ω.

For the term order $\prec$ and the weight vector ω we define the term order $(\omega \mid \prec)$ on T^n by

$$t_1\,(\omega \mid \prec)\,t_2 \quad \text{if} \quad deg_\omega(t_1) < deg_\omega(t_2) \quad \text{or} \quad deg_\omega(t_1) = deg_\omega(t_2) \text{ and } t_1 \prec t_2.$$

We say that $\prec$ *refines* ω if $deg_\omega(t_1) < deg_\omega(t_2)$ implies $t_1 \prec t_2$ for $t_1, t_2 \in T^n$. Obviously, $(\omega \mid \prec)$ refines ω.

For sufficiently generic ω the initial ideal $\langle I_\omega \rangle$ is a monomial ideal. In this case there exists a term order $\prec$ such that $\langle I_\prec \rangle = \langle I_\omega \rangle$, and we say that any such vector *represents* the term order $\prec$ for I. The following lemma (see, for instance, Proposition 15.16 in Eisenbud (1995)) gives a criterion whether a weight vector represents a term order for I.

LEMMA 2.1. *Let I be an ideal and $\prec$ a term order. A weight vector ω represents $\prec$ for I if and only if $in_\omega(g) = in_\prec(g)$ for all $g \in R_\prec(I)$.*

Let $C_\prec(I)$ be the topological closure in $\mathbb{Q}^n$ of $\{\omega \in \Omega^n \mid \langle I_\prec \rangle = \langle I_\omega \rangle\}$. This is a convex, polyhedral cone in $\mathbb{Q}^n$ with a non-empty interior called the Gröbner cone of I with respect to $\prec$. The *finite* set $F(I) := \{C_\prec(I) \mid \prec$ a term order$\}$ is called the Gröbner fan of I (see Mora and Robbiano (1988)).

The following lemma, which follows immediately from lemma 2.1, will be used as a termination condition in our basis conversion algorithm.

LEMMA 2.2. *Let I be an ideal and $\prec_1$ and $\prec_2$ be two term orders. Then $C_{\prec_1}(I) = C_{\prec_2}(I)$ if and only if $in_{\prec_1}(g) = in_{\prec_2}(g)$ for every $g \in R_{\prec_1}(I)$.*

As a consequence we obtain that $C_{\prec_1}(I) = C_{\prec_2}(I)$ if and only if $R_{\prec_1}(I) = R_{\prec_2}(I)$. Hence, we can speak about the reduced Gröbner basis of I over the corresponding Gröbner cone.

REMARK 2.3. *Let I be an ideal, $\prec$ a term order and $\omega \in \mathbb{Q}^\ltimes$. Then $\omega \in C_\prec(I)$ if and only if $in_\prec(g) = in_\prec(in_\omega(g))$ for every $g \in R_\prec(I)$.*

The following proposition characterises neighbouring Gröbner cones touched by line segments originating in a given point ω.

PROPOSITION 2.4. *Let ω and τ be two different weight vectors and $\prec$ a term order which refines τ. Then there exists an $\omega' \in \overline{\omega\tau}$ with $\omega' \neq \omega$ such that*

$$\overline{\omega\omega'} \subseteq C_{(\omega\,|\prec)}(I).$$

PROOF. Since $(\omega|\prec)$ refines ω it follows that $\omega \in C_{(\omega\,|\prec)}(I)$. Let $R_{(\omega\,|\prec)}(I) = \{g_1, \dots, g_r\}$ and put $h_i := g_i - in_\omega(g_i)$ for $i = 1, \dots, r$. We can choose a weight vector $\omega_i \in \overline{\omega\tau}$ such that $\omega_i \neq \omega$ and $deg_\psi(u)$ is greater than $deg_\psi(v)$ for every $\psi \in \overline{\omega\omega_i}$, every monomial u in $in_\omega(g_i)$ and every monomial v in h_i. Since $\prec$ refines τ, it follows that $deg_\tau(u)$ is at most $deg_\tau(in_{(\omega\,|\prec)}(g_i))$ for every monomial u in $in_\omega(g_i)$. Thus, $\psi \in \overline{\omega\omega_i}$ implies that $deg_\psi(t)$ is at most $deg_\psi(in_{(\omega\,|\prec)}(g_i))$ for every monomial t in g_i. Therefore, $in_{(\omega\,|\prec)}(in_\psi(g_i)) = in_{(\omega\,|\prec)}(g_i)$. We denote the element of $\{\omega_1, \dots, \omega_r\}$ closest to ω with ω'. Then $\omega' \in \overline{\omega\tau}$ with $\omega' \neq \omega$ and $in_{(\omega\,|\prec)}(in_{\omega'}(g)) = in_{(\omega\,|\prec)}(g)$ for every $g \in R_\prec(I)$. Hence, $\omega' \in C_{(\omega\,|\prec)}(I)$ by remark 2.3, and we are done. □

3. The Gröbner walk

We now present the algorithm for computing the reduced Gröbner basis $R_{\prec_2}(I)$ of I with respect to $\prec_2$, given admissible orders $\prec_1$ and $\prec_2$ and the reduced Gröbner basis $R_{\prec_1}(I) = \{g_1, \dots, g_r\}$. For our purposes we assume that $\prec_1$ and $\prec_2$ are given by sequences $S_{\prec_1}$ and $S_{\prec_2}$ of rational vectors which span $\mathbb{Q}^n$ (see Robbiano (1985)). Note that the first members of $S_{\prec_1}$ and $S_{\prec_2}$, denoted by σ respectively τ, are the unique weight vectors (up to a scalar factor) refined by $\prec_1$, $\prec_2$ respectively.

The Gröbner walk is based on the following strategy: we move on the line segment $\overline{\sigma\tau}$ from σ to τ. Whenever we leave a Gröbner cone C and enter a new cone C' we transform the reduced Gröbner basis over C into the reduced Gröbner basis over C'. The crucial point is that this conversion can be done efficiently without applying Buchberger's algorithm to the reduced Gröbner basis over C. After finitely many conversions we arrive at $C_{\prec_2}(I)$ and obtain the reduced Gröbner basis with respect to $\prec_2$.

More precisely, let ω be the weight vector with

$$\overline{\sigma\omega} = \overline{\sigma\tau} \cap C_{\prec_1}(I).$$

ω can be easily computed from σ, τ and $R_{\prec_1}(I)$ using linear algebra techniques. It follows from proposition 2.4 that after leaving $C_{\prec_1}(I)$ we enter $C_{(\omega\,|\prec_2)}(I)$. We now have to transform $R_{\prec_1}(I)$ into $R_{(\omega\,|\prec_2)}(I)$. This can be done in the following way.

Observe that there is a term order $\prec$ which refines ω such that $C_{\prec}(I) = C_{\prec_1}(I)$. Therefore $in_{\prec}(f) = in_{\prec}(in_{\omega}(f))$ for all $f \in I$ and

$$\langle\langle I_\omega\rangle_\prec\rangle = \langle I_\prec\rangle = \langle R_{\prec_1}(I)_\prec\rangle = \langle (R_{\prec_1}(I)_\omega)_\prec\rangle.$$

Hence, $R_{\prec_1}(I)_\omega$ is a Gröbner basis of $\langle I_\omega\rangle$ with respect to $\prec$. We now convert $R_{\prec_1}(I)_\omega$ to the reduced Gröbner basis $M := \{m_1, \ldots, m_s\}$ of $\langle I_\omega\rangle$ with respect to $(\omega \mid \prec_2)$. Note that this conversion itself can be done with any basis conversion algorithm. Since $m_1, \ldots, m_s$ are ω-homogeneous we can compute ω-homogeneous polynomials $h_{i1}, \ldots, h_{ir}$ with

$$m_i = \sum_{j=1}^{r} h_{ij} in_\omega(g_j) \quad \text{and} \quad deg_\omega(m_i) = deg_\omega(h_{ij} in_\omega(g_j)) \text{ for } j \in \{1, \ldots, r\} \text{ with } h_{ij} \neq 0.$$

Replacing $in_\omega(g_j)$ by g_j we obtain

$$f_i := \sum_{j=1}^{r} h_{ij} g_j \quad \text{and} \quad G := \{f_1, \ldots, f_s\}. \tag{3.1}$$

It immediately follows that $in_\omega(f_i) = m_i$ and therefore

$$\langle I_{(\omega\,|\prec_2)}\rangle = \langle\langle I_\omega\rangle_{(\omega\,|\prec_2)}\rangle = \langle M_{(\omega\,|\prec_2)}\rangle = \langle G_{(\omega\,|\prec_2)}\rangle.$$

Hence, G is a Gröbner basis of I with respect to $(\omega \mid \prec_2)$ which we reduce to $R_{(\omega\,|\prec_2)}(I)$.

Using lemma 2.2 as termination condition we obtain a Gröbner basis with respect to $\prec_2$ after finitely many basis conversions.

4. Implementational issues

The performance of the Gröbner walk depends on many parameters. For instance, the Gröbner basis G obtained in (3.1) is generally not reduced but only minimal (cf. Eisenbud (1995) p. 329). Since all results in this paper hold for minimal Gröbner bases as well the reduction of G would not be necessary for the correctness of the algorithm.

Performing one step in the Gröbner walk we have to compute a Gröbner basis M of a toric degeneration $\langle I_\omega\rangle$ of I. (Proper) toric degenerations are generated by (proper) initial forms of polynomials of I. Therefore, their Gröbner bases are much faster to compute than the original Gröbner bases of I. Furthermore, we can use an arbitrary basis conversion algorithm, for instance the method described in Gianni et al. (1994) instead of Buchberger's algorithm. This is possible because $\langle I_\omega\rangle$ is an ω-homogeneous ideal given by a Gröbner basis.

Another important parameter is the choice of the path since the number of conversion steps and the complexity of each step heavily depend on it. Ideally, the path is in 'general position', and only intersects the walls between cones in codimension one faces. This is because these faces correspond to the most degenerate $\langle I_\omega \rangle$ that are able to bridge adjacent Gröbner cones, involving the fewest terms in their reduced Gröbner bases. In this case a single weight vector, e.g. a weight vector orthogonal to the face, is sufficient to order the monomials during the conversion between the bases of $\langle I_\omega \rangle$. In practice it seems appropriate to vary the starting point and the direction of the path at each step in order to ensure the generality of the position.

For practical applications it is important to know for which classes of polynomial sets the Gröbner walk is superior to other methods. The previous remarks indicate that sets consisting of polynomials with many terms are especially appropriate for the Gröbner walk.

Acknowledgment: We thank an anonymous referee for detailed and helpful suggestions.

References

Alonso, M. E., Mora, T., Niesi, G., Raimondo, M. (1992a). An algorithm for computing analytic branches of space curves at singular points. In *Proc. 1992 Int. Workshop on Mathematics Mechanization*, pp. 135–166. International Academic Publishers.

Alonso, M. E., Mora, T., Niesi, G., Raimondo, M. (1992b). Local parametrization of space curves at singular points. In B. Falcidieno, I. Herman, and C. Pienovi, editors, *Computer Graphics and Mathematics*, pp. 61–90. Springer. Eurographic Seminar Series.

Amrhein, B., Gloor, O. (1995). Experimente mit dem Gröbner walk. In preparation.

Assi, A. (1993). Standard bases, critical tropisms and flatness. *AAECC* **4**, 197–215.

Bayer, D. A., Morrison, I. (1988). Standard bases and geometric invariant theory; I. Initial ideals and state polytopes, *J. Symb. Comp.* **6**, 209–217.

Buchberger, B. (1965). *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* PhD thesis, Univ. Innsbruck, Dept. of Math., Innsbruck, Austria.

Buchberger, B. (1970). Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems. *Aequationes Mathematicae* **4**, 374–383.

Collart, S., Kalkbrener, M., Mall, D. (1993). The Gröbner walk. Preprint.

Eisenbud D. (1995). *Commutative Algebra with a View toward Algebraic Geometry.* Volume 150 of *Graduate Texts in Mathematics*, Springer, New York.

Faugère, J.C. (1994). Résolutions des systèms d' équations algébriques. Thesis, Univ. Paris 6.

Faugère, J.C., Gianni, P., Lazard, D., Mora, T. (1993). Efficient computation of zero-dimensional Gröbner bases by change of ordering. *J. Symb. Comp.* **16**, 329–344.

Gianni, P., Mora, T., Robbiano, L., Traverso, C. (1994). Hilbert functions and Buchberger algorithm. Preprint.

Hoffmann, C.M. (1989). *Geometric and Solid Modeling: An Introduction.* Morgan Kaufmann Publishers Inc.

Kalkbrener, M. (1995). Implicitization by Gröbner basis conversion. Preprint, presented at IMACS'95, Albuquerque, New Mexico.

Licciardi, S., Mora, T. (1994). Implicitization of hypersurfaces and curves by the Primbasissatz and basis conversion. *Proc. ISSAC'94*, pp. 191–196, Oxford, England.

Mall, D. (1995). Gröbner fans and projective schemes. Preprint.

Mora, T., Robbiano, L. (1988). The Gröbner fan of an ideal. *J. Symb. Comp.* **6**, 183–208.

Robbiano, L. (1985). Term orderings on the polynomial ring. *Proc. EUROCAL'85*, pp. 513–517, Linz, Austria.

Schwartz, N. (1988). Stability of Gröbner bases. *J. Pure and Appl. Alg.* **53**, 171–186.

Sturmfels, B. (1994). Gröbner Bases and Polytopes, Lectures presented at the Holiday Symposium at New Mexico State University. Preprint.

Traverso, C. (1993). Computing the Hilbert-Poincaré series of monomial ideals, applications to Gröbner bases. Preprint.

Windsteiger, W., Buchberger, B. (1993). GRÖBNER: a library for computing Gröbner bases based on SACLIB. Technical report RISC-Linz Series 93-72, University of Linz, Austria.