RISC-Linz
Research Institute for Symbolic Computation
Johannes Kepler University
A-4040 Linz, Austria, Europe

Linear algebra methods for the transformation of Gröbner bases

Giovanna RODA

(December 20, 1995)

RISC-Linz Report Series No. 95-54

Supported by: University of Bologna, Italy

Linear algebra methods for the transformation of Gröbner bases

G. Roda
Research Institute for Symbolic Computation
Johannes Kepler Universität A-4010 Linz
e-mail: groda@risc.uni-linz.ac.at

December 20, 1995

Abstract

A solution to the problem of converting a Gröbner basis between different orderings for a given ideal is known for the zero-dimensional case. We show how to solve this problem for one-dimensional ideals in two variables by using the same linear algebra techniques that are exploited in the existing algorithm.

For ideals in more than two variables we describe two other known approaches that also use linear algebra.

1 Introduction

In a paper published in 1993 ([5]) Faugère, Gianni, Lazard and Mora showed that for zero-dimensional polynomial ideals it is possible to obtain Gröbner bases with respect to any admissible ordering from any given Gröbner basis by means of linear algebra.

This transformation method (also known as the FGLM algorithm) reduces the problem of constructing any Gröbner basis to the easier problem of constructing a Gröbner basis with respect to a degree-compatible ordering. Since the transformation method was shown to have polynomial complexity, the new method reduces the time complexity for constructing Gröbner bases for zero-dimensional ideals to $d^{O(n^2)}$, where d is the maximum degree and n the number of variables of the input polynomials.

The FGLM algorithm is based on the fact that the ring of classes of polynomials modulo a zero-dimensional ideal is finitely generated as a vector space. The difficulty that arises when considering positive-dimensional ideals comes from the fact that such vector space is not finitely generated.

For bivariate ideals we detected situations in which it is possible to group together infinitely many elements of the basis of the vector space and work with just a finite number of them. For these cases we show how to modify the FGLM algorithm in order to be able to transform Gröbner bases of one-dimensional bivariate ideals into Gröbner bases with respect to the pure lexicographic ordering.

For multivariate positive-dimensional ideals, several other approaches that generalize the FGLM algorithm are known. First of all, it is always possible to compute the Gröbner basis of an ideal with respect to a sequential term ordering by using linear algebra and the knowledge of any other basis of the ideal. Starting from this observation, Mora and Licciardi ([8]) propose to perform a sequence of transformations to sequential orderings until an ordering equivalent to the target one is obtained.

Kapur and Saxena ([7]) propose to perform a sequence of transformations increasing at each step a finite set of terms. The algorithm will terminate when the set of terms contains all terms of the polynomials in the target basis.

Section 2 shows some examples where one needs transformations of Gröbner bases between different orderings.

After introducing some notation (Section 3), we describe in Section 4 the FGLM algorithm for zero-dimensional ideals.

In Section 5 we present our method for one-dimensional ideals in two variables.

In Section 6 we describe the other known approaches for multivariate positive-dimensional ideals.

2 Applications

Our main motivation for studying generalizations of the FGLM algorithm is the computation of standard bases in rings of formal power series. For ideals in these rings there is a method (due to Mora [11]) for computing standard bases with respect to degree-compatible orderings (see also [1] and [12]) but no algorithm is known for lexicographic orderings.

Another application of the transformation of Gröbner bases is the computation of the kernel of a polynomial homomorphism

$$\phi : K[y_1, \ldots, y_m] \longrightarrow K[x_1, \ldots, x_n]$$

given by $\phi(y_i) = f_i$, $i = 1, \ldots, m$. The kernel is given by

$$< y_1 - f_1, \ldots, y_m - f_m > \cap K[y_1, \ldots, y_m]$$

(see [6] and [14] for applications).

It is easy to see that $G := \{y_1 - f_1, \ldots, y_m - f_m\}$ is a reduced Gröbner basis with respect to any ordering such that $\{x_1, \ldots, x_n\} \ll \{y_1, \ldots, y_m\}$ (i. e. such that every term containing at least one of the y_i is bigger than any term containing only x_i's). Hence the computation of the kernel can be done

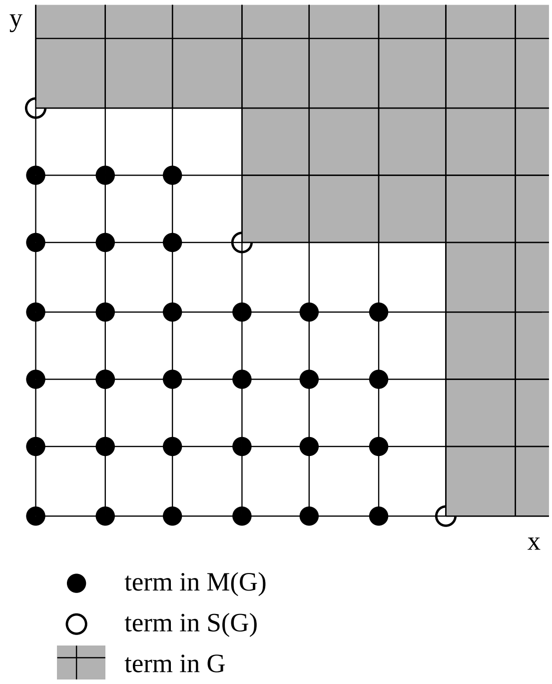

Figure 1: $S(G)$ and $M(G)$ in the case of two variables

by transforming G into a Gröbner basis with respect to an ordering such that $\{y_1, \ldots, y_m\} \ll \{x_1, \ldots, x_n\}$.

The kernel of a polynomial homomorphism provides also a canonical basis for the ring of invariants under the action of a finite group (see [16]).

3 Notation

Let K be a field. Throughout this paper we will use the notations $K[\underline{x}]$ and $K[x_1, \ldots, x_n]$ interchangeably for the ring of polynomials in n variables over K.

The reader is assumed to be familiar with the theory of Gröbner bases (see [2], [3], [4], [10]).

In this paper we will use the word *term* for any product of powers of the x_i's and the word *monomial* for any product of the form ct, where $c \in K$ (the *coefficient* of ct) and t is a term.

If t is a term of the form $x_1^{d_1} x_2^{d_2} \ldots x_n^{d_n}$ we will denote by $deg(t, x_i) := d_i$ the *degree of* t *in* x_i and by $deg(t) := d_1 + d_2 + \ldots + d_n$ the *degree of* t. For a polynomial $p \in K[\underline{x}]$ we will denote by $deg(p)$ the maximum among the degrees of its terms.

From now on we will assume that every Gröbner basis is *reduced*, i. e. that each of its polynomials is

- monic
- irreducible with respect to all other polynomials in the basis

Given an admissible term ordering $<_a$, we will call *leading term* of a polynomial p (and denote it by $lt_{<_a}(p)$ or $lt(p)$ if there is no ambiguity) the highest term with respect to $<_a$ that appears in p.

Note that if $p \in G$ and G is a reduced Gröbner basis then $lt(p)$ cannot divide any other term appearing in the basis but itself.

Let G be a Gröbner basis for an ideal $I \subset K[\underline{x}]$. Two sets of terms (see Figure 1 for the two-variable case) can be canonically associated to G:

$S(G) := \{lt(g) |\ g \in G\}$ the *staircase* of G

$M(G) := \{t |\ t$ term s.t. $lt(g)$ does not divide t for every g $\in G\}$

For these two sets the following properties hold:

- $S(G)$ is a basis for $< \{lt(f) |\ f \in I\} >$
- $M(G)$ is a canonical basis of the vector space $K[\underline{x}]/I$ (i. e. the vector space generated by $M(G)$ is isomorphic to $K[\underline{x}]/I$)
- I is zero-dimensional if and only if $M(G)$ is finite
- I is zero-dimensional if and only if $S(G)$ contains a pure power of x_i for every variable x_i

Given a set $F \subset K[\underline{x}]$ denote by $T(F)$ the set of all terms appearing in the polynomials of F. If $G \subset K[\underline{x}]$ is a Gröbner basis denote by $RT_G(F)$ the set of all terms appearing in the normal forms with respect to G of the polynomials of F. Note that G is a Gröbner basis of the ideal I if and only if $RT_G(I) = M(G)$. The elements of $RT_G(f)$, $f \in K[\underline{x}]/I$, are sometimes called *coordinates* of f with respect to G in order to emphasize the vector space structure of $K[\underline{x}]/I$.

4 The FGLM algorithm

Let $<_1$ and $<_2$ be two admissible term orderings. Given a zero-dimensional ideal $I \subset K[\underline{x}]$, let G_1 denote its Gröbner basis with respect to $<_1$ and G_2 its Gröbner basis with respect to $<_2$.

Assume that we are given G_1; we want to find a transformation that produces G_2 without having to apply Buchberger's algorithm.

The idea is the following. We consider terms in increasing order with respect to $<_2$, starting from 1 (the smallest term). Three cases can occur, as shown in Figure 2 where we have drawn $S(G_2)$ and $M(G_2)$.

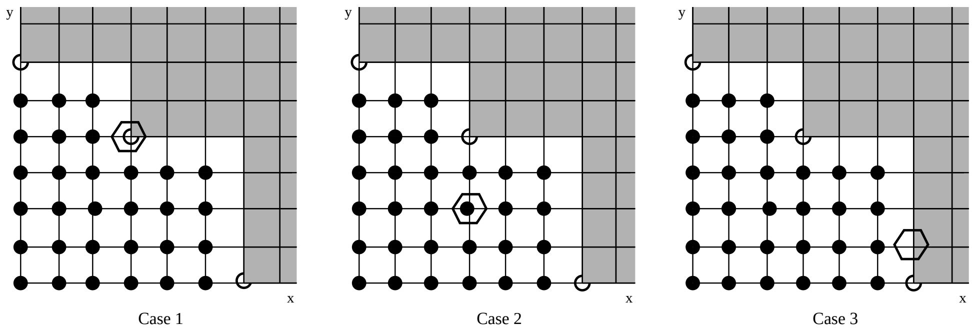

Figure 2: The three cases that occur in the FGLM algorithm

In case 1 the term belongs to $S(G_2)$; in case 2 it belongs to $M(G_2)$; in case 3 it is a strict multiple of an element of $S(G_2)$.

We initialize three sets NewBasis, Staircase and MBasis to the empty set and enlarge them iteratively. These three sets will be contained respectively in G_2, $S(G_2)$ and $M(G_2)$ throughout the algorithm and coincide with them upon its termination.

For each term we must decide whether it gives rise to case 1,2 or 3: in case 1 we find the polynomial whose leading term is the one that we are considering and add it to NewBasis updating at the same time Staircase, in case 2 we add the term to MBasis and in case 3 we do nothing.
For each term t considered in the algorithm we have

NewBasis $= G_2 \setminus \{g \in G_2 | g <_2 t\}$,
Staircase $= S(G_2) \setminus \{s \in S(G_2) | s <_2 t\}$,
MBasis $= M(G_2) \setminus \{s \in M(G_2) | s <_2 t\}$.

Hence these three sets suffice for deciding cases 1,2, and 3.

Case 3 can be detected by checking whether the term t is of the form ss_1, where $s \in$ Staircase and $s_1 \neq 1$ is a term. For the other cases we do the following:

- if the coordinates of t with respect to G_1 are linearly dependent from the coordinates with respect to G_1 of the elements of MBasis then we are in case 1 and the dependency relation gives the new polynomial to be added to NewBasis;

- if the coordinates of t with respect to G_1 are linearly independent from the coordinates with respect to G_1 of the elements of MBasis then we are in case 2 and we add the term to MBasis.

Define the following functions:

normal_form, a function that gives the normal form of a term with respect to a Gröbner basis;

first (resp. *second*), a function that gives the first (resp. second) coordinate of (μ_1, μ_2) for each pair (μ_1, μ_2) in a list of pairs;

cons, a function that appends an element to the end of a list;

next_term, a function that given a term t and a term ordering $<_a$ returns the smallest term with respect to $<_a$ in the set

$$\{s >_a t | \ s \text{ is not multiple of any element of Staircase}\}$$

or "NIL" if the above set is empty.

Algorithm 1 (FGLM)

Input: $<_1$, $<_2$, admissible term orderings
G_1, the reduced Gröbner basis of an ideal I with respect to $<_1$
Output: NewBasis, the reduced Gröbner basis of I with respect to $<_2$

```
MBasis := [ ]; Staircase := [ ]; NewBasis := [ ]; Term := 1;
while Term ≠ NIL do
    Vector := normal_form(G_1,Term);
    if there exists a linear relation:
    Vector +∑_{μ∈ MBasis} c_μ second(μ) = 0
    then
        Polynom := Term+∑_{μ∈ MBasis} c_μ first(μ)
        NewBasis := cons(Polynom,NewBasis);
        Staircase := cons(Term,Staircase);
    else
        MBasis := cons([Term,Vector],MBasis)
    Term := next_term(Term,<_2);
```

Termination of the algorithm is guaranteed by the fact that only the terms that are not strict multiples of elements of $S(G_2)$ are considered. Since I is zero-dimensional there are at most finitely many such terms.

For a proof of correctness and termination of the above algorithm we refer to the original paper by Faugère, Gianni, Lazard and Mora ([5]).

5 Ideals of dimension 1 in two variables

For positive-dimensional ideals the FGLM algorithm is non-terminating since it considers infinitely many terms which all give rise to case 2 and augments at each step MBasis.

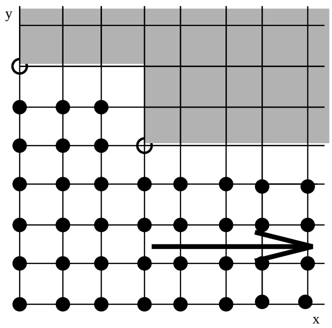

Figure 3: The big arrow shows the terms that make the FGLM algorithm non terminating

Let $K[x, y]$ be the ring of polynomials in the two variables x and y and let $I \subset K[x, y]$ be an ideal of dimension 1.

Let $<_1$ denote any admissible term ordering. In this section we will examine the case in which one wants to transform a Gröbner basis G_1 of I with respect to $<_1$ into a Gröbner basis G_2 with respect to $<_2$, the pure lexicographic ordering with $x < y$.

Our main idea will be best understood by looking at a picture. Let the situation be as in Figure 3, where we have drawn $S(G_1)$ and $M(G_1)$. In this example the FGLM algorithm will immediately get into an infinite loop by considering the terms $1, x, x^2, x^3, \ldots$ which are linearly independent modulo G_1 and lexicographically smaller than any other term containing y.

Now, we would like to avoid considering such an infinite set of terms. If we stop at some point - let's say at a certain degree D - we might risk to miss later some dependency relation involving an x^k for $k > D$.

The idea is the following: once we know that for some integer $m \geq 1$ all terms in the set $S := \{tx^k | \; t = 1, y, y^2, \ldots y^m, \; k = 0, 1, 2, \ldots\}$ are linearly independent and reduced modulo G_1 we just do not consider any of these terms. But later, when looking for a linear dependency relation we will behave as if they had been already examined and added to MBasis.

So, instead of looking for coefficients c_μ satisfying

$$normal\_form(G_1, t) + \sum_{\mu \in \mathrm{MBasis}} c_\mu second(\mu) = 0$$

we will look for coefficients c_μ and c_ν such that

$$normal\_form(G_1, t) + \sum_{\mu \in \mathrm{MBasis}} c_\mu second(\mu) = \sum_{\nu \in S} c_\nu \nu$$

Once we find such a relation we will add to NewBasis the polynomial

$$t + \sum_{\mu \in \text{MBasis}} c_\mu first(\mu) - \sum_{\nu \in S} c_\nu \nu$$

Still, we might run into an infinite loop if all x-multiples of y^{m+1} (modulo G_1) are linearly independent from the terms in S.

Definition 5.1 *Let G be a Gröbner basis in $K[x,y]$. Let $t_1 = x^{k_1}y^{h_1}$ and $t_2 = x^{k_2}y^{h_2}$ be respectively the smallest and the biggest terms in $S(G)$ with respect to the pure lexicographic ordering with $x < y$. Then we say that G has* distance $d_x(G) := h_1$ from the x-axis *and* distance $d_y(G) := k_2$ from the y-axis.

For a Gröbner basis $G \subset K[x,y]$ with respect to a degree-compatible ordering the sum $d_x(G) + d_y(G)$ is equal to the coefficient of the term of degree 1 in the Hilbert function.

Algorithm 2 (modified FGLM for two variables)

Input: $<_1$, an admissible ordering
G_1, the reduced Gröbner basis of an ideal $I \subset K[x,y]$ with $d_y(G_1) = 0$
Output: NewBasis, the reduced Gröbner basis of I with respect to $<_2$
(the pure lexicographic ordering with $x < y$)

MBasis := [ ]; Staircase := [ ]; NewBasis := [ ]; Minterm := *min*(G_1);
Term := MinTerm;
while Term $\neq$ NIL **and** $<$NewBasis$>\neq< G_1 >$ **do**
  if Term is not a multiple of some element of Staircase **then**
    Vector := *normal_form*(G_1,Term);
    if there exists a linear relation:
      Vector $+\sum_{\mu\in \text{ MBasis}} c_\mu\ second(\mu) + \sum_{\nu<_2 \text{Minterm}} c_\nu \nu = 0$
    then
      Polynom := Term$+\sum_{\mu\in \text{ MBasis}} c_\mu\ first(\mu) + \sum_{\nu<_2 \text{Minterm}} c_\nu \nu$
      NewBasis := *cons*(Polynom,NewBasis);
      Staircase := *cons*(Term,Staircase);
    else
      MBasis := *cons*([Term,Vector],MBasis);
  if Terms a multiple of y **then return**(NewBasis);
  Term := *next_term*(Term,$<_2$);

Where the functions *normal_form*, *first* (resp. *second*), *cons*, and *next_term* are defined as in Section 4 and

min is a function that returns the $<_2$-smallest term in $S(G_1)$

Lemma 5.1 *Let I be an ideal in $K[x,y]$ and G_1 be a Gröbner basis for I. Let $<_2$ be the pure lexicographic ordering with $x<y$ and G_2 the Gröbner basis of I with respect to $<_2$. Let t_2 be the biggest term with respect to $<_2$ in $S(G_1)$.*

Then if every term in $T(G_1)\setminus\{t_2\}$ is smaller than t_2 with respect to $<_2$, $d_x(G_2)=d_x(G_1)$.

Proof Let t_1 be the smallest term with respect to $<_2$ in $S(G_1)$. Observe first of all that $d_x(G_2)\geq d_x(G_1)$, otherwise there would be a polynomial $g\in G_2$ with $lt_{<_2}(g)<_2 t_1$ that reduces to zero modulo G_1. But this is impossible since $T(g)\subset M(G_1)$.

Assume now that every term in $T(G_1)\setminus\{t_2\}$ is smaller than t_2 with respect to $<_2$. Denote by p_k the normal form with respect to G_1 of t_1x^k for $k=0,1,\dots$ and set $W_j:=\{p_k|\ k=0,1,\dots j\}$, $S_1:=\{t\in M(G_1)|\ t<_2 t_1\}$.

If $d_x(G_2)>d_x(G_1)$ this means that for every $j=0,1,\dots$ the set $W_j\cup S_1$ is linearly independent. This implies that p_j contains at least one term $t\notin S_1$ for all j.

Now we claim that for every $k=0,1,\dots$ and for every $t\in T(p_k)$

$$deg(t,y)<2deg(t_2,y)-deg(t_1,y) \tag{1}$$

Let $S_2:=\{t\in M(G_1)|\ deg(t,y)<2deg(t_2,y)-deg(t_1,y)\}$. Then we have a contradiction since there should be infinitely many linear combinations of terms of $S_2\setminus S_1$ that are linearly independent.

Let us now prove (1).

Let $t\in RT_{G_1}(t_1x^k)=T(p_k)$. We will prove that (1) holds for t by induction on k. If $k=0$, for every $t\in RT_{G_1}(t_1)$ we know by hypothesis that $t<_2 t_2$ and hence (1) holds. Let (1) be true for every term in $RT_{G_1}(t_1x^k)$ and consider $t\in RT_{G_1}(t_1x^{k+1})$.

Note that if x is reducible modulo G_1 then $t_1=x$ (otherwise G_1 would be trivial) and $t_2=t_1$ or $t_2=y^m$ for some m and in both cases the claim is easy to prove.

Therefore we can assume that x is irreducible modulo G_1. Write $t_1x^{k+1}=(t_1x^k)x$. If p_kx is irreducible modulo $G-1$ then the claim is true since by the induction hypothesis

$$deg(p_k,y)<2deg(t_2,y)-deg(t_1,y)$$

and $deg(p_k,y)=deg(p_kx,y)$.

If p_kx is reducible modulo G_1, let us prove the claim by induction on the length of a reduction of p_kx by G_1.

Let $p_kx\longrightarrow_{G_1} p\longrightarrow_g p*$ for some $g\in G_1$. By induction hypothesis

$$deg(p,y)<2deg(t_2,y)-deg(t_1,y)$$

Let t be the term in p such that $t=t'lt(g)$. If $deg(t',y)<deg(t_2,y)-deg(t_1,y)$ then we're done since $deg(g,y)\leq deg(t_2,y)$.

On the other hand it cannot be that $deg(t', y) \geq deg(t_2, y) - deg(t_1, y)$

Otherwise t must be a multiple of t_2 and we can reduce t by always choosing the polynomial in G_1 with highest degree in y. It is easy to see that the result of such a reduction is a polynomial whose terms have degree in y bounded by $2deg(t_2, y) - deg(t_1, y)$. But since the normal form of a polynomial with respect to a Gröbner basis is unique, also in this case the claim is proven.□

Proposition 5.1 *Algorithm 2 is correct.*

Proof For proving correctness of the algorithm we will proceed by showing some properties that are invariant for the *while*-loop:

(a) the elements of MBasis are linearly independent modulo the ideal generated by G_1

(b) the elements of NewBasis are in the ideal I

(c) the elements of Staircase are the leading terms of the elements of NewBasis

(d) each term which does not appear neither in MBasis nor in Staircase is either a multiple of some element of Staircase or it is smaller than Minterm with respect to $<_2$

(e) all terms that are smaller than Minterm with respect to $<_2$ are in $M(G_2)$

(only (d) and (e) are new with respect to the proof of the original algorithm, but we will prove all points for the sake of completeness)

(a) Suppose that there is a linear combination

$$p = \sum_{\mu \in \text{ MBasis}} c_\mu first(\mu)$$

that is equal to 0 modulo the ideal generated by G_1. This means that $normal\_form(p) = 0$. But

$$\begin{aligned} normal\_form(p) &= normal\_form(\sum_{\mu \in \text{ MBasis}} c_\mu first(\mu)) \\ &= \sum_{\mu \in \text{ MBasis}} c_\mu second(\mu) \end{aligned}$$

But this is impossible because every time there is such a linear dependence relation the current term (the biggest with respect to $<_2$ in the above sum) is put in Staircase and not in MBasis.

(b) If p is a polynomial in NewBasis then it must be of the form

$$t + \sum_{\mu \in \text{ MBasis}} c_\mu \, first(\mu) + \sum_{\nu <_2 \text{ Minterm}} c_\nu \nu$$

and we know that a new polynomial is added to NewBasis if and only if

$$normal\_form(t) + \sum_{\mu \in \text{ MBasis}} c_\mu \, second(\mu) + \sum_{\nu <_2 \text{ Minterm}} c_\nu \nu = 0$$

But the left hand side is $normal\_form(p)$ since $normal\_form(\nu) = \nu$ for $\nu <_2$ Minterm, hence $p \in I$.

(c) This is clear since we consider terms in increasing order with respect to $<_2$ and each polynomial added to NewBasis is a sum of the curren term plus some previously considered terms and possibly some terms that are smaller with respect to $<_2$ than any considered term.

(d) Let t be any term that is neither in MBasis nor in Staircase and assume $t \geq_2$ Minterm. If $deg(t, y) = deg(\text{Minterm}, y)$ then $deg(t, x) > deg(\text{Minterm}, x)$ and t is a multiple of Minterm. If Minterm has been put in Staircase we're done. Otherwise there exists an x-multiple of Minterm that appeared in ListOfNexts and has not been put in Staircase. Therefore such term must be a multiple of an element of Staircase.

Now, in order to prove the assertion by induction, assume that it is true for every term s such that $deg(s, y) = m > deg(\text{Minterm}, y)$.

Let t be a term such that $deg(t, y) = m+1$. Then $t = st_1$ with $deg(s, y) = m$ and it's easy to check that the assertion holds for t.

(e) This should be clear from Lemma 5.1.

By combining all previous points, we know that $NewBasis$ is a Gröbner basis of I with respect to $<_2$. Moreover, by construction none of its terms can be multiple of a leading term other than itself.

Now, by Lemma 5.1 $d_x(G_2) = d_x(G_1)$. Termination of the algorithm is now ensured by Lemma 5.1 since $d_x(G_2) = d_x(G_1)$ and from the fact that the algorithm stops once $<$NewBasis$>=< G_1 >$. □

Remark 5.1 *Let I be a one-dimensional ideal in $K[x, y]$ and L be the linear transformation of coordinates defined by $x' = x + \lambda y$, $y' = y$, $\lambda \in K$. Then, if K is algebraically closed, for almost all values of λ (those that are not roots of a suitable polynomial) L puts I in Noether normal position with respect to x, y (see [9]). Let f be one of the generators of I and write f as $f_0 + f_1 + \cdots + f_d$ where $d := deg(f)$ and f_i is homogeneous of degree d. If f' is the polynomial f after the transformation L then the coefficient of y'^d in f' is $f_d(-\lambda, 1)$. So, if we choose λ so that $f_d(-\lambda, 1) \neq 0$ then the transformed ideal will have a monic polynomial in y whose degree in y is equal to its total degree. Hence by applying a linear transformation as above we can always obtain a Gröbner basis G with respect to a total degree ordering and such that $d_y(G) = 0$.*

6 Positive dimensional ideals

6.1 Sequential orderings and sequences of transformations

An admissible term ordering $<_a$ is called *sequential* if for every term t there are only finitely many terms s such that $s <_a t$.

Example 6.1 *Let* $w := (w_1, \ldots, w_n)$ *be a vector of positive integers and let* $t := x_1^{d_1} x_2^{d_2} \ldots x_n^{d_n}$. *The number* $deg_w(t) = w_1 d_1 + w_2 d_2 + \cdots + w_n d_n$ *is called the* weighted degree *of* t *and it induces a partial ordering* $<_w$ *on the set of terms.*

Any term ordering containing $<_w$ *is sequential.*

Given a Gröbner basis it is possible to transform it into a Gröbner basis with respect to a sequential term ordering by a straightforward modification of the FGLM algorithm (just substitute the line

"**while** Term $\neq$ NIL **do**"

with the line

"**while** Term $\neq$ NIL **and** <NewBasis>$\neq< G_1 >$ **do**").

It is easy to see that for such orderings the FGLM algorithm finds all polynomials of the transformed basis in a finite number of steps. Hence termination is ensured when one checks if the ideal generated by NewBasis is equal to the ideal generated by G_1 every time a polynomial is added to NewBasis. The check can be done by comparing Hilbert functions.

This property of sequential orderings is proven in a paper by Licciardi and Mora ([8], Prop. 1) and also proposed as an exercise in the book by Becker and Weispfenning ([2], Ex. 9.11, p. 433).

Remark 6.1 *In [15], Stanley gives a proof (Thm 2.1, p. 59) that constructs the set of reduced terms of a Gröbner basis with respect to the inverse lexicographic ordering. The method presented is not yet an algorithm because one would need to have another Gröbner basis in order to decide linear independence of terms, but it already contains the main idea of transformation to sequential orderings.*

In order to solve the problem of transforming a basis to a non-sequential ordering, Licciardi and Mora propose to perform successive (partial) FGLM transformations to sequential orderings updating the weights. Termination of this process is guaranteed by the finiteness of the Gröbner fan of an ideal ([13]).

Definition 6.1 *Let* $I \subset K[\underline{x}]$ *be an ideal,* $<_1$ *and* $<_2$ *two term-orderings, and* G_1 *the Gröbner basis of* I *with respect to* $<_1$. *Then* $<_1$ *is equivalent to* $<_2$ *with respect to* I *if* $lt_{<_1}(g) = lt_{<_2}(g)$ *for every* $g \in G_1$.

Note that if $<_1$ *is equivalent to* $<_2$ *with respect to* I *then* G_1 *is also the Gröbner basis of* I *with respect to* $<_2$.

Given a non-sequential ordering it is always possible to find a sequential ordering equivalent to it. Let $<_1$, G_1, I be as in the definition above with $<_1$ non-sequential. Then the problem of finding a sequential ordering equivalent to $<_1$ is solved once one finds a vector $w := (w_1, \ldots, w_n)$ of integers such that for every $g \in G_1$

$$deg_w(lt_{<_1}(g)) > deg_w(t) \text{ for every } t \in T(g - lt <_2 (g)).$$

This is an *integer programming* problem that can also be solved by means of Gröbner bases (see [16]).

Assume that one is given a Gröbner basis G_1 with respect to an ordering $<_1$ induced by the weight vector $w := (w_1, \ldots, w_n)$ and wants to find the basis G_2 with respect to a non-sequential ordering $<_2$. Then the following algorithm will deliver G_2 and a sequential ordering $<_2'$ equivalent to $<_2$.

Algorithm 3 (partial transformations to sequential orderings)

Input: $<_1$, $<_2$, admissible term orderings
w, weight vector inducing $<_1$
G_1, the reduced Gröbner basis of an ideal I with respect to $<_1$
Output: NewBasis, the reduced Gröbner basis of I with respect to $<_2$
$<_2'$, a sequential ordering equivalent to $<_2$ with respect to I

NewBasis := G_1; Weight := w; $<_2'$:= $<_1$;
Polys := *extraneous_polys*(G_1,$<_2$,$<_2'$);
while Polys $\neq$ [ ] **do**
    [Weight,$<_2'$] := *update*($<_2$,Polys);
    MBasis := [ ]; Staircase := [ ]; NewBasis := [ ]; Term := 1;
    while Term $\neq$ NIL **and** $<$NewBasis$>\neq< G_1 >$ **and** Polys = [ ] **do**
        Vector :=*normal_form*(G_1,Term);
        if there exists a linear relation:
        Vector $+\sum_{\mu\in \text{ MBasis}} c_\mu \; second(\mu) = 0$
        then
            Polynom := Term$+\sum_{\mu\in \text{ MBasis}} c_\mu \; first(\mu)$
            if Term $\neq lt_{<_2}$(Polynom) **then**
                Polys := [Polynom];
            else
                NewBasis := *cons*(Polynom,NewBasis);
                Staircase := *cons*(Term,Staircase);
        else
            MBasis := *cons*([Term,Vector],MBasis);
        Term := *next_term*(Term,$<_2'$);

Where the following new functions are defined:

update, a function that given a term-orderings $<_a$ and and a set of polynomials P returns a weight vector w and a term-ordering $<_w$ induced by w such that for every $p \in P$ $lt_{<_w}(p) = lt_{<_a}(p)$.

extraneous_polys, a function that given a set of polynomials P and two term-orderings $<_a$ and $<'_a$ returns the set $\{p \in P | \ lt_{<_a}(p) \neq lt_{<'_a}(p)\}$

In order to show that the above algorithm is correct, it is enough to prove that after finitely many steps the ordering $<'_2$ is equivalent to $<_2$ with respect to I. One should show that the orderings considered during the algorithm are not equivalent with respect to I; then according to ([13]) there can be only finitely many such orderings.

The inner while-loop is certainly terminating when $<'_2$ is not equivalent to $<_2$ because a polynomial p satisfying $lt_{<'_2}(p) \neq lt_{<_2}(p)$ will be found in finitely many steps since $<'_2$ is sequential. When $<'_2$ is equivalent to $<_2$ the inner loop will compute the Gröbner basis with respect to $<_2$ according to the previously described algorithm of transformation to sequential orderings.

6.2 Incrementing finite sets of terms

Kapur ans Saxena in [7] propose an approach to Gröbner bases conversion that also uses sequences of transformations.

Let G_1, G_2 another be as in the previous subsection. The idea is to run the FGLM algorithm picking up the terms from a finite set T. This clearly ensures termination, but if the initial T does not contain $T(G_2)$ then the algorithm will output the basis of a smaller ideal.

In order to obtain the full basis G_2 they propose to perform a sequence of transformations incrementing after each the set T. Also here, after each transformation it is necessary to check whether the transformed basis generates the same ideal as the input one.

Roughly, the algorithm can be described in the following way:

Step 0 choose a small degree d (e. g. $d = 1$);

Step 1 let NewBasis be the set of all the linear relations among the terms of degree d that are equal to zero modulo G_1;

Step 2 if $<$NewBasis$>\neq< G_1 >$ repeat Step 1 with a bigger degree d but considering only those terms of degree d which are not multiples of elements of $\{t | \ t = lt_{<_2}(f), \ f \in NewBasis\}$;

Step 1 is finite, since it just considers finitely many terms. Since there exists a D such that $deg(g) \leq D$ for every $g \in G_2$, when $d = D$ Step 2 will compute the desired basis G_2.

References

[1] T. Becker. Stability and Buchberger criterion for standard bases in power series rings. *Journal of Pure and Applied Algebra*, 66:219–227, 1990.

[2] T. Becker, V. Weispfenning, and H. Kredel. *Gröbner Bases*. Springer-Verlag, 1993.

[3] B. Buchberger. Gröbner bases: an algorithmic method in polynomial ideal theory. In N. K. Bose, editor, *Recent trends in multidimensional system theory*, pages 184–232. Springer-Verlag, 1985.

[4] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms*. Springer-Verlag, 1992.

[5] J. C. Faugère, P. Gianni, D. Lazard, and T. Mora. Efficient Computation of Zero-Dimensional Gröbner Basis by Change of Ordering. *Journal of Symbolic Computation*, 16(4):329–344, 1993.

[6] P. Gianni, B. Trager, and G. Zacharias. Gröbner bases and primary decomposition of ideals. *Journal of Symbolic Computation*, 1988.

[7] D. Kapur and T. Saxena. An algorithm for converting a degree Gröbner basis to a lexicographic Gröbner basis. Technical report, Department of Computer Science, University at Albany, State University of New York, 1994.

[8] S. Licciardi and T. Mora. Implicitization of hypersurfaces and curves by the Primbasissatz and basis conversion. In *ISSAC '94*, pages 191–196. ACM press, 1994.

[9] A. Logar. A computational proof of the Noether normalization lemma. In T. Mora, editor, *AAECC 6*, pages 259–273. Springer-Verlag, 1988.

[10] B. Mishra. *Algorithmic Algebra*. Springer-Verlag, 1993.

[11] F. Mora. Seven variations on standard bases. Technical report, University of Genova, Italy, 1988.

[12] T. Mora, G. Pfister, and C. Traverso. An introduction to the tangent cone algorithm. *Issues in Robotics*, 1993.

[13] T. Mora and L. Robbiano. The Gröbner fan of an ideal. *Journal of Symbolic Computation*, 6(2 - 3):183–208, 1988.

[14] D. Shannon and M. Sweedler. Using Gröbner Bases to determine algebra membership, split surjective algebra homomorphisms and determine birational equivalence. *Journal of Symbolic Computation*, 6(2-3):267–274, 1988.

[15] R. P. Stanley. Hilbert functions of graded algebras. *Advances in Mathematics*, 28:57–83, 1978.

[16] B. Sturmfels. *Algorithms in Invariant Theory.* Texts and Monographs in Symbolic Computation. Springer-Verlag, 1993.