Algorithms for change of orderings in the theory of Gröbner bases

DISSERTATION

zur Erlangung des akademischen Grades

Doktor der technischen Wissenschaften

angefertigt am Institut für Symbolysches Rechnen

Eingereicht von: Giovanna Roda

Beurteilung: Prof. Franz Winkler
Prof. Mirella Manaresi

Linz, April 2004

Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass ich die vorliegende Dissertation selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt bzw. die wörtlich oder sinngemäß entnommenen Stellen als solche kenntlich gemacht habe.

Giovanna Roda

Abstract

Gröbner bases are one of the most significant methods of computer algebra. Its high computational complexity makes the method often unfeasible in practice, and several techniques for its improvement have been investigated. Algorithms for change of orderings reduce the complexity of lexicographic Gröbner bases, that are interesting for many practical applications.

This thesis is concerned with an unified treatment of the Gröbner walk and the FGLM algorihms for change of orderings. The relation between the two algorithms becomes clear in a combination of the two methods that we call FGLM walk.

After a thorough description of the algorithms and their mathematical background, we conclude by comparing their performance on some real examples.

Kurzfassung

Gröbner Basen sind eine der bedeutendsten Methoden der Computeralgebra. Ihre höhe Berechnungskomplexität macht die Methode oft unpraktisch, und mehrere Techniken für Ihre Verbesserung sind untersucht worden. Algorithmen für Ordnungsänderung senken die Komplexität der Berechnung von lexicographischen Gröbner Basen, die für viele Praktische Anwendungen interessant sind.

Diese Dissertation beschäftigt sich mit einer vereinigten Behandlung der Gröbner Walk und FGLM Algorithmen für Ordnungsänderung. Der Zusammenhang zwischen den zwei Algorithmen wird offensichtlich in einer Kombination der zwei methoden die wir FGLM Walk nennen.

Nach einer vollständigen Beschreibung der Algorithmen und deren mathematischen Hintergrund, wir schliessen mit dem Vergleich deren Leistung für einige echte Beispiele.

Aknowledgments

It was not easy to get back to mathematics after seven years spent in the "real world". If I have managed to write this thesis, this I owe to the people who believed in me, supported and encouraged me throughout all these years. My thanks go to my advisor Franz Winkler, from whom I learned Computer Algebra und with whom I had interesting discussion on algorithms for change of orderings. Mirella Manaresi knows me since I took her course in Algebraic Geometry, and she is the one who suggested that I start a PhD after graduating from the University of Bologna. I think that this thesis will be my best thanks to her. To my parents I wish to express a big "grazie di tutto", and that will never be big enough.

Contents

Chapter 1

Preliminaries

1.1 Introduction

Introduced in 1965 by Buchberger, Gröbner bases are a powerful computational method in algebra. Given a system of polynomials in several variables, a Gröbner basis provides a set of canonical representatives for the ideal generated by the polynomials together with an effective method for reducing any given polynomial to its canonical form. Once a Gröbner basis is known, one has a tool for investigating algorithmically several algebraic and geometric properties of the system. Among others, one can decide if the system has finitely many solutions and, if not, what is the dimension of the space of solutions.

Gröbner bases depend on the choice of some special orders on the set of power products called term orderings. Some problems like for instance the elimination of variables from a polynomial system require special term orderings called lexicographic. Since lexicographic orderings make the computation of Gröbner bases particularly hard, algorithms for change of orderings have been devised. These algorithms take as input a Gröbner basis with respect to some ordering that is known to be easier to compute and deliver a Gröbner basis with respect to a prescribed lexicographic ordering.

There exist two methods for change of orderings in the theory of Gröbner bases: the Gröbner walk algorithm and the FGLM algorithm. The first method relies on the properties of a fan of polyhedral cones called the Gröbner fan of an ideal. To each class of term orderings giving rise to

the same Gröbner basis for an ideal corresponds a cone in the fan. Given an initial Gröbner basis, one walks from one cone to another in the fan until the target cone and its corresponding Gröbner basis is reached. The FGLM algorithm works for zero-dimensional ideals and it uses linear algebra methods on the vector space constituted by the classes of reduced polynomials modulo the ideal.

In this manuscript we study the classification of term orderings on the rings of polynomials. Following the characterization given by Robbiano, we enfold Hahn's embedding theorem and give a simple visual representation of term ordering types.

We then introduce partial term orderings and demonstrate some significant properties in relation to Gröbner bases. For this part we mainly follow the work laid out by Collart and Mall. Partial term orderings are the foundations of the Gröbner walk algorithm. We present the algorithm and give a hint for a local complexity analysis as suggested by Kalkbrener.

We then present the algorithm by Faugere, Gianni, Lazard and Mora (FGLM) for zero-dimensional ideals and demostrate how this method can be modified in order to be feasible for positive dimensional ideals.

We conclude by presenting some computations of Gröbner bases done with the two methods. The Gröbner walk shows to be superior to the FGLM algorithm for both zero-dimensional and positive dimensional polynomial systems. For zero-dimensional systems a modification of the FGLM algorithm allows us to present what we believe is a fairer comparison of the two methods and show that in this case their performance is quite similar.

1.2 Outline

In Section 1.3 we introduce the notation and definitions that will be used throughout the rest of the thesis.

Chapter 2 starts with an exposition of the basic notions in the theory of Gröbner bases. In Section 2.3 we present with Robbiano's constructive proof of a theorem by Hahn ([30], see also Erdös ([24]) yielding a representation of term orderings as matrices with real entries. We conclude the section by presenting our result on term ordering types (2.3.1). The rest of Chapter 2 is devoted to the investigation of the properties of partial term

orderings (Sections 2.4 through 2.6). Partial term orderings allow to generalize the notions of homogeneity and quasi-homogeneity of polynomials. We show how the properties of Gröbner bases of quasi-homogeneous ideal hold in this more general setting and give an analogous of the notion of Hilbert function.

In Chapter 3 we start by recalling some notions from convex geometry (Section 3.1) that will be needed in Section 3.2 to define the Gröbner cone of an ideal with respect to a given term ordering. In Section 3.3 we give a definition of the Gröbner fan of an ideal and present a new concise proof of its finiteness.

Section 3.5 deals with implementation issues for improving the performance of the Gröbner walk, as described by Armhrein, Gloor and Küchlin. In Section 3.6 we investigate Kalkbrener's degree bound for adjacent Gröbner bases. This bound allows a local analysis of the complexity of the algorithm.

In Chapter 5 we conclude by comparing the two methods for zero-dimensional and positive dimensional ideals.

1.3 Basic definitions and notation

We summarise here some of the basic definitions and notations that will be used throughout the rest of this thesis.

Let K be a field. By $K[x_1, \ldots, x_n]$ we denote the ring of polynomials in the variables $x_1, \ldots, x_n$ with coefficients in K and by T^n the set

$$\{x_1^{d_1} \cdots x_n^{d_n} \mid d_1, \ldots, d_n \in \mathbb{N}\}$$

of power products (or *terms*) in the variables $x_1, \ldots, x_n$.

A product of the form ct where $c \in K$ and $t \in T^n$ is called a *monomial*.

Given a set $F \subseteq K[x_1, \ldots, x_n]$ we denote by $\langle F \rangle$ the ideal generated by F in $K[x_1, \ldots, x_n]$, that is

$$\langle F \rangle := \{\sum_{f_i \in \Phi} f_i h_i \mid \Phi \text{ is a finite subset of } F,\ h_i \in K[x_1, \ldots, x_n]\}$$

The symbol $\overline{K}$ will denote the algebraic closure of the field K.

By $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ we will denote the sets of natural, integer, rational, and real numbers and by $\mathbb{N}^n$, $\mathbb{Z}^n$, $\mathbb{Q}^n$, and $\mathbb{R}^n$ respectively the sets of their n-tuples. A subscript $+$ close to a set will denote the subset of nonnegative elements of that set, for instance $\mathbb{R}^n_+$ will denote the set of vectors whose coordinates are nonnegative real numbers

$$\mathbb{R}^n_+ := \{(v_1, \ldots, v_n) \mid v_i \in \mathbb{R},\ v_i \geq 0 \text{ for every } i = 1, \ldots, n\}$$

Let K be a field (for instance $K = \mathbb{Q}$, $K = \mathbb{R}$). Then the symbol K^n represents

- the set of points $\{(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in K\}$ called the *affine space* over K
- the *K-vector space* with componentwise addition

  $$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$$

  and scalar multiplication

  $$c(a_1, \ldots, a_n) = (ca_1, \ldots, ca_n)$$

  for every $(a_1, \ldots, a_n)$, $(b_1, \ldots, b_n) \in K^n$, $c \in K$

Given two vectors $v, w \in K^n$, with $v = (v_1, \ldots, v_n)$ and $w = (w_1, \ldots, w_n)$, we denote by $v \cdot w$ the *inner product* (or *dot product*) $v_1w_1 + \ldots + v_nw_n \in K$. For $K = \mathbb{R}$ the space $\mathbb{R}^n$, equipped with the distance function

$$d(p, q) = \sqrt{\sum_{i=1}^{n} (p_i - q_i)^2}$$

defined for every $p = (p_1, \ldots, p_n)$, $q = (q_1, \ldots, q_n) \in \mathbb{R}^n$, is called *Euclidean space*. When dealing with $\mathbb{R}^n$ it should be clear from the context whether we are referring to the affine, vector, or Euclidean space.

Chapter 2

Gröbner bases and term orderings

In this chapter we begin by recalling the basic notions from the theory of Gröbner bases of polynomial ideals. Associated to a polynomial ideal is the vector space of the residue classes modulo the ideal, called the residue class ring, for which Gröbner bases provide a canonical representation.

Gröbner bases are dependent on the choice of particular orderings of polynomials, called term orderings. Following Robbiano, we show how to represent term orderings by suitable matrices and give a full classification of term orderings. By recalling some notions from the theory of ordered groups, we show how the finitely many different types of term orderings may be described as chains of some special subspaces.

By dropping the condition that the order be total, one obtains a wider family of polynomial orderings called partial term orderings. Partial term orderings allow to generalize the notions of quasi-homogeneity - and hence of homogeneity - for polynomials. We demonstrate under which conditions the properties of Gröbner bases of quasi-homogeneous ideals can be carried on in this more general setting.

The results in this chapter constitute the theoretical foundations on which the methods for change of orderings that will be presented in the following chapters are built. Namely, the vector structure of the residue class ring allows to use linear algebra methods in the FGLM algorithm, while the properties of partial term orderings are exploited in the Gröbner walk algorithm.

After recalling some equivalent definitions of Gröbner bases in Section 2.1, in Section 2.2 we show how from any Gröbner bases one may read

off a canonical set of generators for the residue class ring called staircase. In Section 2.3 we demonstrate how the monoid of terms may be embedded into $\mathbb{R}^n$, thus providing a representation of term orderings as classes of matrices with real entries. Furthermore, in 2.3.1 we look at the classification of term orderings within a group-theoretic framework and are able to present a characterization of term ordering types as chains of values. In Section 2.4 we introduce partial term orderings and discuss their basic properties. Partial term ordering allow to generalize the notion of homogeneity. Given a partial term ordering, one may associate to a polynomial ideal a so-called toric degeneration. The main properties of toric deformations are presented in Section 2.5. Finally, in Section 2.6 we discuss Hilbert functions of toric deformations as a natural extension of Hilbert functions of homogeneous and quasi-homogeneous ideals.

Our main sources for this chapter are:

- [44], [43], and [46] for the classification of term orderings
- [18] for the characterization of partial term orderings and toric degenerations

Other sources used throughout the chapter are indicated within each section.

2.1 Gröbner bases

Gröbner bases are special bases of polynomial ideals that allow to reduce any polynomial in the ideal to its canonical representative (normal form). The construction of a Gröbner basis for an ideal requires an ordering on the set of terms that guarantees that the reduction of any polynomial to normal form may be performed in a finite number of steps.

In this section we will define Gröbner bases and state the properties that will be needed later. Methods for the construction of Gröbner bases as well as numerous applications to symbolic computation may be found in the vast literature on the subject.

Gröbner bases were introduced by Buchberger in his Ph.D thesis in 1965 ([11], see also [12, 13]). The theory of Gröbner bases has since then

been widely investigated, together with its applications to algebraic geometry and commutative algebra. The basic theory is presented in several books ([20, 9, 42, 2, 51, 28]). Applications of Gröbner bases to algebraic geometry and commutative algebra are presented in [21] and [38]. See also [47] for the use of Gröbner bases in invariant theory.

Before defining term orderings on the ring of polynomials we will recall the definition of *order relation* on a set.

Let A be a set. A relation $R \subseteq A \times A$ is called

- *reflexive* if $(a, a) \in R$ for every $a \in A$
- *anti-symmetric* if $(a, b) \in R$ and $(b, a) \in R$ imply $a = b$
- *transitive* if $(a, b) \in R$ and $(b, c) \in R$ imply $(a, c) \in R$

Any relation satisfying the three properties above will be called a *partial order* or simply an *order* on the set A. A set A endowed with an order R is called an *ordered set* and denoted by (A, R).

If $R \subseteq A \times A$ is an order and, for every $a, b \in A$, either $(a, b) \in R$ or $(b, a) \in R$ (that is, every two elements of A are comparable with respect to R) then R is called a *total order* on A and we call (A, R) a *totally ordered set*.

A total order $\prec$ on T^n is called *admissible term ordering* or simply *term ordering* if it is well-founded and compatible with the semi-group structure of T^n, that is for all $t, t_1, t_2 \in T^n$

- $1 = x_1^0 \cdots x_n^0 \prec t$
- if $t_1 \prec t_2$ then $tt_1 \prec tt_2$

Given a term-ordering $\prec$ and a polynomial $f \in K[x_1, \ldots, x_n]$ we denote by $supp(f)$ the set of monomials occurring with a non-zero coefficient in the distributive normal form of f and call this set the *support* of f. The greatest monomial in $supp(f)$ with respect to $\prec$ is called *initial monomial* of f with respect to $\prec$ and is denoted by $f_\prec$. If the coefficient of $f_\prec$ is 1 then $f_\prec$ is called the *initial term* or *leading term* of f with respect to $\prec$.

Given a term ordering $\prec$ and a set $F \subseteq K[x_1, \ldots, x_n]$, we denote by $F_\prec$ the set $\{f_\prec \mid f \in F\}$ of the initial monomials of the polynomials in

F . Analogously, for an ideal I, the ideal $\langle I_\prec \rangle$ generated by the initial monomials of the polynomials in I is called the *initial ideal* of I with respect to $\prec$.

Fix a term ordering $\prec$. A finite subset G of non-zero polynomials $G \subseteq I \subseteq K[x_1, \ldots, x_n]$ of an ideal I is a *Gröbner basis* (or *standard basis*) of I with respect to $\prec$ if and only if

$$\langle I_\prec \rangle = \langle G_\prec \rangle$$

that is, the initial ideal of I with respect to $\prec$ is generated by the initial terms of the polynomials in G with respect to $\prec$.

An ideal $I \subseteq K[x_1, \ldots, x_n]$ is called a *monomial ideal* if it is generated by monomials. By Dickson's lemma we know that any monomial ideal in $K[x_1, \ldots, x_n]$ admits a finite basis of monomials. Given a monomial ideal $I = \langle m_1, \ldots, m_r \rangle$, a monomial m belongs to I if and only if m is divisible by some monomial m_j , for $j \in \{1, \ldots, r\}$, in the basis.

Hence, a Gröbner basis can be equivalently defined as a finite set G of non-zero polynomials $G \subseteq I \subseteq K[x_1, \ldots, x_n]$ of an ideal I such that the initial term of any element of I is divisible by one of the initial terms of the polynomials in G.

Given $f, g, h \in K[x_1, \ldots, x_n]$ with $g \neq 0$ and a term ordering $\prec$, we say that f reduces to h modulo g and write

$$f \longrightarrow_g h$$

if and only if $g_\prec$ divides a monomial $m \in supp(f)$ and

$$h = f - \frac{m}{g_\prec}\, g$$

Analogously, if $G \subseteq K[x_1, \ldots, x_n]$, we say that f reduces to h modulo G and write

$$f \longrightarrow_G h$$

if there exists a sequence of reductions

$$f \longrightarrow_{g_{i_1}} h_1 \longrightarrow_{g_{i_2}} h_2 \cdots \longrightarrow_{g_{i_{k-1}}} h_{k-1} \longrightarrow_{g_{i_k}} h$$

with $g_{i_1}, g_{i_2}, \ldots, g_{i_k} \in G$. The polynomial h is called the *remainder* of the division of f by G.

Another characterisation of Gröbner bases is that they are subsets of an ideal containing no zero polynomials and such that every polynomial has a unique remainder with respect to them. This unique remainder of a polynomial f modulo a Gröbner basis G is called the *normal form* of f with respect to G and is denoted by $NF_G(f)$.

A *reduced Gröbner basis* for an ideal I is a Gröbner basis such that

- for every $g \in G$ no monomial in $supp(g)$ is divisible by any of the terms in $G_\prec \setminus \{g_\prec\}$
- for every $g \in G$ the coefficient of of $g_\prec$ is 1, that is $G_\prec \subset T^n$

Note that in our definition of reduced Gröbner basis we require the polynomials in the basis to be monic.

2.2 Residue class rings

The ring of classes of polynomials modulo an ideal may be viewed as a vector space over the field of coefficients. A Gröbner basis of an ideal delivers as a side-product a linearly independent basis for this vector space. The basis consists of all terms contained in a set that is fully determined by the initial terms of the polynomials in the Gröbner basis and is called a *staircase*.

Let $R := K[x_1, \ldots, x_n]$ be the ring of $n-$variate polynomials over the field K and let I be a proper ideal of R. For each $f \in R$ define the *residue class* of f modulo I to be the set $f + I = \{f + g \mid g \in I\}$ and denote by R/I the set of all residue classes. Together with addition and multiplication defined by

- $(f + I)(g + I) = (f + g) + I$
- $(f + I)(g + I) = fg + I$

for every $f, g \in R$, R/I becomes a ring with $1 + I$ as unity and $I = 0 + I$ as zero element.

One can see that the map

$$\begin{array}{rccc} \phi: & R & \longrightarrow & R/I \\ & f & \longrightarrow & f+I \end{array}$$

is a surjective ring homomorphism whose kernel is the ideal I.

R/I may be regarded as a vector space over K by viewing it as an additive abelian group with scalar multiplication

$$c(f+I) = cf + I \text{ for every } c \in K,\ f \in R.$$

Identify terms in T^n with n-tuples of natural numbers through the map log given by

$$\begin{array}{rccc} log: & T^n & \longrightarrow & \mathbb{N}^n \\ & x_1^{d_1} \cdots x_n^{d_n} & \longrightarrow & (d_1, \ldots, d_n) \end{array}$$

Then a *staircase* $S \subseteq \mathbb{N}^n$ is a set with the property that for every $a = (a_1, \ldots, a_n) \in S$, if $b = (b_1, \ldots, b_n) \in \mathbb{N}^n$ is smaller that a coordinatewise, i.e. $b_i \leq a_i$ for every $i = 1, \ldots, n$, then $b \in S$.

Let G be a Gröbner basis for the ideal I. Then the set

$$S(G) = \{t \in T^n \mid t \text{ is not multiple of any of the initial terms in } G\}$$

is a linearly independent vector space basis of R/I. We call $S(G)$ the *staircase of* G.

For every $f \in R$ the terms appearing in the normal form of f with respect to G belong to $S(G)$ and conversely every linear combination of elements of $S(G)$ is the normal form of some polynomial in R with respect to G. Hence, we can express the fact that the K-vector space generated by $S(G)$ is isomorphic to $R/\langle G\rangle$ by saying that $S(G)$ is a *canonical basis* of $R/\langle G\rangle$. The terms in $S(G)$ are sometimes also called *standard terms*.

If G is a reduced Gröbner basis then its leading terms are the minimal elements with respect to the coordinatewise ordering in $\mathbb{N}^n \setminus S(G)$, the complement of $S(G)$ in $\mathbb{N}^n$.

Let $U = \{u_1, \ldots, u_r\}$ be a subset of the set of variables $\{x_1, \ldots, x_n\}$. Then $I \cap K[u_1, \ldots, u_r]$ is an ideal in $K[u_1, \ldots, u_r]$ called the *elimination ideal* of I with respect to U. A set of variables $U \subseteq \{x_1, \ldots, x_n\}$ is called *independent modulo* I if $I \cap K[u_1, \ldots, u_r] = \{0\}$.

Define the *dimension of an ideal* I as

$$dim(I) = max\{|U| \mid U \subseteq \{x_1, \ldots, x_n\} \text{ independent modulo } I\}$$

It can be proven that an ideal I is *zero-dimensional* if and only if $S(G)$ is finite for any Gröbner basis G of I. This implies that I is zero-dimensional if and only if any Gröbner basis G of I contains a polynomial g_i whose leading term is a pure power of x_i for every variable x_i , $i = 1, \ldots, n$. This result is known as the "*shape lemma*" (see also [8]).

2.3 Classification of term orderings

It is useful to have a representation of term orderings in order to get a better insight into their behaviour in relation with Gröbner bases. In this section we will show how to represent term orderings as special matrices with coefficients in $\mathbb{R}^n$. Our exposition is based on Robbiano's work ([44], see also [43]). This topic has been also treated in Chapter 4 of [50].

We will start by identifying in a natural way the set of terms in n variables with the set of n-tuples of natural numbers. We will then show how to embed $\mathbb{N}^n$ as an ordered structure into $\mathbb{Z}^n$, $\mathbb{Q}^n$, and finally $\mathbb{R}^n$ preserving its order. As a result, we are able to represent term orderings as special matrices whose rows are vectors in $\mathbb{R}^n$.

Given two ordered sets A and B, a map $f : A \longrightarrow B$ is *order-preserving* if whenever $a_1 \leq a_2$ in A, then $f(a_1) \leq f(a_2)$ in B.

The set of terms T^n can be identified in a natural way with $\mathbb{N}^n$ through the map log introduced in Section 2.2.

One can see that log is an isomorphism between the multiplicative semigroup T^n and the additive semigroup $\mathbb{N}^n$. Hence we can identify every term ordering on $\mathbb{T}^n$ with an ordering $<$ on $\mathbb{N}^n$.

Let us now regard $\mathbb{Z}^n$ as the group generated by $\mathbb{N}^n$. Then an ordering $<$ on $\mathbb{N}^n$ uniquely extends to a total group ordering on $\mathbb{Z}^n$ such that $\mathbb{N}^n$ is positive.

Let $q = (q_1, \ldots, q_n) \in \mathbb{Q}^n$. Then one can always find an $m \in \mathbb{N}_+ \setminus \{0\}$ such that

$$mq = (mq_1, \ldots, mq_n) \in \mathbb{Z}^n$$

In this way any total ordering $<$ on the group $\mathbb{Z}^n$ uniquely extends to the total group ordering on $\mathbb{Q}^n$ defined by $q > 0$ if and only if $mq > 0$.

We will now show how to embed $\mathbb{Q}^n$ into $\mathbb{R}^n$ as ordered groups.

Let G be a $\mathbb{Q}$ -subvectorspace of $\mathbb{Q}^n$ of dimension r and denote by $G_{\mathbb{R}}$ the $\mathbb{R}$ -subvectorspace of $\mathbb{R}^n$ generated by G .

Let $G^+ = \{g \in G \mid g > 0\}$ and $G^- = \{g \in G \mid g < 0\}$.

Denote by I_G the subset of $G_{\mathbb{R}}$ of all elements $p \in G_{\mathbb{R}}$ such that, for every open neighborhood U_p of p in $\mathbb{R}^n$, $U_p \cap G^+$ and $U_p \cap G^-$ are non-empty.

Then I_G is a subvectorspace of $G_{\mathbb{R}}$ of dimension $r - 1$ (think of $G_{\mathbb{R}}$ as the real line, I_G as the 0 element).

Given $v \in \mathbb{R}^n$ denote by $d(v)$ the dimension of the $\mathbb{Q}$ -subvectorspace of $\mathbb{R}$ spanned by the coordinates of v. We call $d(v)$ the *rational dimension* of v.

Denote by $U(G)$ the half-line which is orthogonal to I_G and such that $U(G) \cap G \subseteq G^-$. Then $d(v)$ is constant on the set of nonzero multiples of v, in particular on $U(G)$.

A base $\{v_1, \ldots, v_r\}$ of $G_{\mathbb{R}}$ as $\mathbb{R}$ -vectorspace can be chosen in such a way that $v_1, \ldots, v_r \in \mathbb{Q}^n$. Hence, if we write a vector $v \in G_{\mathbb{R}}$ as $\sum_{i=1}^{r} \lambda_i v_i$ with $\lambda_i \in \mathbb{R}$, it is clear that the vector space spanned over $\mathbb{Q}$ by its coordinates is contained in the vector space spanned by $\lambda_1, \ldots, \lambda_r$ and therefore the rational dimension of v can be at most r (the dimension of G).

Example Let $v = (\sqrt{2}, 1, 0)$. Then $v = \sqrt{2}(1, 0, 0) + (0, 1, 0)$ and the rational dimension of v is $d(v) = 2$. Let G be the $\mathbb{Q}$ -subvectorspace of $\mathbb{Q}^3$ of dimension 2 generated by $(1, 0, 0)$, $(0, 1, 0)$. Then cleary any vector $v \in G_{\mathbb{R}}$ can have at most rational dimension 2 . //

Let G , $G_{\mathbb{R}}$ be as before and $u_1, \ldots, u_s \in G_{\mathbb{R}}$. Denote for short with u the array $(u_1, \ldots, u_s)$. Define

$$\begin{array}{rccc} deg_u : & \mathbb{Q}^n & \longrightarrow & \mathbb{R}^s \\ & v & \longrightarrow & (v \cdot u_1, \ldots, v \cdot u_s) \end{array}$$

where $v \cdot u_i$ denotes the inner product of v and u_i.

The map deg_u is called the u *-multi-degree map*.

Endow $\mathbb{R}^s$ with the lexicographic ordering defined by $(a_1, \ldots, a_s) > 0$ if and only if the first non-zero coordinate a_i is positive. Then the u -multi-degree map gives an ordering on $\mathbb{Q}^n$ which is in general partial as the following example shows.

Example Let $u = (u_1, u_2)$ where $u_1 = (0, 1, 0)$, $u_2 = (0, 0, 1)$ and let $v = (1, 0, 0)$. We can't decide if $v > 0$ according to the u -multi-degree, in fact $v \cdot u_1 = v \cdot u_2 = 0$. //

In order to get a total ordering on $\mathbb{Q}^n$ we will need to make the map deg_u injective. Then deg_u becomes an injective order homomorphism between $\mathbb{Q}^n$ into $\mathbb{R}^s$ as ordered groups.

Set $G_1 = \mathbb{Q}^n$, $r_1 = n$, the dimension of $\mathbb{Q}^n$. Let I_{G_1} be the subvectorspace of G_1 defined as before as the set of the elements $p \in G_1$ which have a positive and a negative element of $(G_1)_{\mathbb{R}}$ in every open neighborhood. Choose a vector u_1 on the half-line $U(G_1)$ contained in $G_1 \setminus I_{G_1}$. Let $d_1 = d(u_1)$ be the rational dimension of u_1 . For a vector $v \in G_1 \setminus I_{G_1}$ we have $vu_1 = 0$ if and only if $u_1 = 0$. This is because $u_1 \in U(G_1) \subseteq G_1 \setminus I_{G_1}$.

Now we have to take care of what happens on I_{G_1} .

Let $G_2 = I_{G_1} \cap \mathbb{Q}^n$. Note that G_2 is a $\mathbb{Q}$ -subvectorspace of $\mathbb{Q}^n$ of dimension $r_2 = r_1 - d_1 = n - d_1$.

Repeat the argument above with I_{G_2} and get a vector u_2 of rational dimension d_2 . Note that since the rational dimensions are positive integers, and at each step the rational dimension decreases, this procedure will eventually stop.

In the end we have a set of orthogonal vectors $u_1, \ldots, u_s$ such that $d(u_1) + \cdots + d(u_s) = n$.

We have now enough notions to provide a characterisation of term orderings.

Let $\sim$ be the equivalence relation on the set of real vectors given by $v_1 \sim v_2$ if $d(v_1) = d(v_2)$ and there exists $\lambda \in \mathbb{R}^+$ such that $v_2 = \lambda v_1$.

Then it is clear that the above construction yields the same ordering if we substitute u_i with an equivalent vector, hence we will consider the equivalence class $[u_i]$ in place of u_i .

Finally, let $\prec$ be a term ordering on $\mathbb{K}[x_1, \ldots, x_n]$. Then $\prec$ is given by the following data:

- the type of $\prec$, an integer s with $1 \leq s \leq n$
- the partition type of $\prec$, i.e. a partition $(d_1, \ldots, d_s)$ of n
- an element $([u_1], \ldots, [u_s])$ of classes of real vectors such that for every $i = 1, \ldots, s$, if G_{i-1} is the $\mathbb{Q}$ -subvectorspace of $\mathbb{Q}^n$ orthogonal to $(u_1, \ldots, u_{i-1})$, then $u_i \in G_{i-1}$.

Example The *pure lexicographic ordering* is defined as the term ordering $\prec_{plex}$ such that

$$t_1 \prec_{plex} t_2$$

whenever $t_1 = x_1^{a_1} \cdots x_n^{a_n}$, $t_2 = x_1^{b_1} \cdots x_n^{b_n}$ and for the smallest i such that $b_i \neq a_i$, the difference $b_i - a_i$ is positive. Then $\prec_{lex}$ is of type n and partition type $(1, 1, \ldots, 1)$ and it can be represented by the vectors $([e_1], \ldots, [e_n])$, the rows of the identity matrix

$$\begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & 0 \\ 0 & 0 & \ldots & 1 \end{pmatrix}$$

The *total degree reverse lexicografic ordering* $\prec_{grevlex}$ is given by

$$t_1 \prec_{grevlex} t_2$$

whenever $t_1 = x_1^{a_1} \cdots x_n^{a_n}$, $t_2 = x_1^{b_1} \cdots x_n^{b_n}$ are such that either

$$a_1 + \cdots + a_n < b_1 + \cdots + b_n \text{ (that is, } deg(t_1) < deg(t_2))$$

or $deg(t_1) = deg(t_2)$ and if i is the biggest index for which for $b_i \neq a_i$, then $b_i - a_i$ is negative.

This is also an ordering of type n and partition type $(1, 1, \ldots, 1)$ and its vectors are represented by the rows of the matrix

$$\begin{pmatrix} 1 & 1 & \dots & 1 & 1 \\ 0 & 0 & \dots & 0 & -1 \\ 0 & 0 & \dots & -1 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & -1 & 0 & \dots & 0 \end{pmatrix}$$

//

2.3.1 Hahn's embedding theorem

The classification of term orderings may be regarded as a special case of Hahn's embedding theorem (see for instance [29], Th. 4.D, p. 73) for abelian lattice-ordered groups. In this framework term ordering types may be defined as chains of values in lattice-ordered groups and have a simple visual characterisation. The following material is from [46].

Let G be an abelian group written additively, ordered by $\leq$. A subset $C \subseteq G$ is called a *convex subgroup* of G if for all $g \in G$ and $c_1, c_2 \in C$

$$c_1 \leq g \leq c_2 \text{ implies } g \in C$$

It can be proven that the set of convex subgroups of G is totally ordered by inclusion and that the union of any family of convex subgroups of G is itself a convex subgroup of G. Observe that $\{0\}$ is a convex subgroup of G for every group G.

By applying Zorn's lemma one can see that for every $g \in G \setminus \{0\}$ there exists a convex subgroup $V \subseteq G$ such that $g \in G \setminus V$ and such that V is maximal with this property. This subgroup is called a *value* of g in G. The set of all values of g is denoted by $\Gamma(g)$ and the set of all values of all $g \in G \setminus \{0\}$ by $\Gamma(G)$.

Since we will consider only abelian groups, in the following when we speak of a group we will implicitely assume it is abelian.

Lemma The coarsest admissible order on $\mathbb{N}^n$ is the "divides" order relation.

Proof Let $\preceq$ be any admissible order on T^n and $t_1, t_2 \in T^n$ such that $t_1 \neq t_2$ and $t_1 \mid t_2$. Write $t_1 = x_1^{\alpha_1} \dots x_n^{\alpha_n}$ and $t_2 = x_1^{\beta_1} \dots x_n^{\beta_n}$. We will show that t_1 and t_2 must be comparable with respect to $\preceq$ and that $t_1 \preceq t_2$, thus proving that "divides" is the coarsest admissible order on T^n.

Observe that $t = \frac{t_2}{t_1} = (x_1^{\beta_1 - \alpha_1} \dots x_n^{\beta_n - \alpha_n}) \in T^n$ since $\beta_i - \alpha_i \geq 0$ in $\mathbb{N}^n$ for every $i = 1, \dots, n$. Since $\preceq$ is admissible we have $1 \preceq t$ from the well-foundedness property and $t_1 \preceq tt_1$ from the compatibility with the semigroup structure of T^n. But $tt_1 = t_2$, hence we have found the desired relation. //

Observe that the "divides" order relation on T^n is the coordinatewise order on $\mathbb{N}^n$ and that its embedding in $\mathbb{Z}^n$ (resp. $\mathbb{Q}^n$) is the coordinatewise order in $\mathbb{Z}^n$ (resp. $\mathbb{Q}^n$).

Hence, classifying orders on $\mathbb{Q}^n$ is the same as classifying refinements of the coordinatewise order.

Denote by $\preceq_c$ the coordinatewise order on $\mathbb{Q}^n$ and let $\mathbb{Q}^n$ be ordered by $\preceq_c$. Then the set of values $\Gamma(\mathbb{Q}^n)$ has a simple characterisation as will be shown in the next lemma.

Lemma All convex subgroups of $\mathbb{Q}^n$, regarded as ordered group with $\preceq_c$, are the subspaces of $\mathbb{Q}^n$, regarded as the Euclidean space, of the form

$$\{(a_1, \dots, a_n) \in \mathbb{Q}^n \mid c_1 a_1 = 0, \dots, c_n a_n = 0,\ c_i \in \{0, 1\}\}$$

Proof We prove the statement by induction on n.

For $n = 1$, the only convex subgroups of $\mathbb{Q}$ are $\mathbb{Q} = \{a \in \mathbb{Q} \mid ca = 0,\ c = 0\}$ itself and $\{0\} = \{a \in \mathbb{Q} \mid ca = 0,\ c = 1\}$, hence the statement holds.

Assume that the statement holds for $n - 1$ and consider the projection map

$$\begin{array}{rcl} p_j : \mathbb{Q}^n & \longrightarrow & \mathbb{Q}^{n-1} \\ (a_1, \dots,\ a_{j-1}, a_j, a_{j+1}, \dots, a_n) & \longrightarrow & (a_1, \dots, a_{j-1}, a_{j+1}, \dots, a_n) \end{array}$$

For every $1 \leq j \leq n$, p_j is a linear map and it is order-preserving, in particular it preserves convexity. Let C be a convex subgroup of $\mathbb{Q}^n$. Then

its projection under p_j is a convex subgroup of $\mathbb{Q}^{n-1}$ and by induction hypothesis must be of the form

$$\{(a_1, \ldots, a_{n-1}) \in \mathbb{Q}^{n-1} \mid c_1 a_1 = 0, \ldots, c_{n-1} a_{n-1} = 0,\ c_i \in \{0, 1\}\}$$

Note that for $c_i = 0$ for all $i = 1, \ldots, n-1$ we have $\mathbb{Q}^{n-1}$ and for $c_i = 1$ for all $i = 1, \ldots, n-1$ we have $\{0\}$ as convex subgroups of $\mathbb{Q}^{n-1}$.

Without loss of generality we can assume that there exists $k \in \{1, \ldots, n-1\}$ such that, up to a permutation of variables, every element in $p_j(C)$ is of the form $(a_1, \ldots, a_k, 0, \ldots, 0)$, that is

$$p_j(C) = \{(a_1, \ldots, a_{n-1}) \in \mathbb{Q}^{n-1} \mid a_i = 0 \text{ for } 0 \leq i \leq k\}$$

Then every element of C is of the form

$$a = (a_1, \ldots, a_k, 0, \ldots, 0, a_j, 0, \ldots, 0)$$

If $a_j = 0$ for every $a \in C$ then C has the desired form. Otherwise, assume that there exist $\xi_1, \ldots, \xi_k, \xi_j \in \mathbb{Q}$ not all zero such that

$$\xi_1 a_1 + \cdots + \xi_k a_k + \xi_j a_j = 0$$

for every $a = (a_1, \ldots, a_k, 0, \ldots, 0, a_j, 0, \ldots, 0) \in C$. But then we have a contradiction.

In fact, one can always choose $b_1, \ldots, b_k, b_j \in \mathbb{Q}$ such that

$$\xi_1 b_1 + \cdots + \xi_k b_k + \xi_j b_j \neq 0$$

Then $(b_1, \ldots, b_k, 0, \ldots, 0) \in p_j(C)$ but $(b_1, \ldots, b_k, 0, \ldots, 0, b_j, 0, \ldots, 0) \notin C$. Therefore it must be $\xi_1 = \ldots = \xi_k = 0$. Then C may be either of the form

$$C = \{(a_1, \ldots, a_n) \in \mathbb{Q}^n \mid a_i = 0 \text{ for } 0 \leq i \leq k,\ a_j = 0\}$$

or

$$C = \{(a_1, \ldots, a_n) \in \mathbb{Q}^n \mid a_i = 0 \text{ for } 0 \leq i \leq k\}$$

thus proving the claim. //

Let $\alpha \subseteq \{1, \ldots, n\}$ and denote by S_α the subspace of $\mathbb{Q}^n$ given by

$$S_\alpha = \{(a_1, \ldots, a_n) \in \mathbb{Q}^n \mid a_i = 0 \text{ for every } i \in \alpha\}$$

We have shown that the set of values $\Gamma(\mathbb{Q}^n)$ of $\mathbb{Q}^n$ endowed with the $\preceq_c$ ordering is exactly the collection of the $2^n - 1$ values S_α as α varies among the non-empty subsets of $\{1, \ldots, n\}$

$$\Gamma(\mathbb{Q}^n) = \{S_\alpha \mid \alpha \subseteq \{1, \ldots, n\},\ \alpha \neq \emptyset\}$$

Lemma 3.1.2, p. 32 from [29] states that in an ordered group the set of all convex subgroups is a chain. Hence, in order to refine $\preceq_c$ on $\mathbb{Q}^n$ one needs to form chains within the set of values such that the inclusion relations between any two subspaces are preserved.

Note that such chains have maximal length n.

Also note that the subspace $\{0\} = S_{\{1,2,\ldots,n\}}$ must be convex for every term ordering because of the well-foundedness condition. Hence, every chain defining a term ordering must contain the $\{0\}$ value.

We call the chain of values of the term ordering $\prec$ the *type* of $\prec$.

Let $m \leq n$ and $\alpha_i \subseteq \{1, \ldots, n\}$ for $i = 1, \ldots, k$ and

$$(S_{\alpha_1}, S_{\alpha_2}, \ldots, S_{\alpha_m})$$

be the ascending chain of values defining a term ordering type. Then we must have $\alpha_1 = \{1, \ldots, n\}$ and $\alpha_{i+1} \subset \alpha_i$ for every $i = 1, \ldots, m-1$.

We can encode the type into an $m \times n$ matrix

$$\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \cdots \\ \alpha_m \end{pmatrix} = \begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_{m1} & \alpha_{m2} & \ldots & \alpha_{mn} \end{pmatrix}$$

where, for every $j = 2, \ldots, m$, α_{jk} is the k-th coordinate of α_j for $k \leq |\alpha_j|$, 0 otherwise.

Let $a(n)$ be the number of term ordering types. A combinatorial argument gives

$$a(n) = \sum_{k=1}^{n} \begin{pmatrix} n \\ k \end{pmatrix} a(n-k)$$

that evaluates asymptotically to $\frac{1}{2} \frac{n!}{log(2)^{(n+1)}}$.

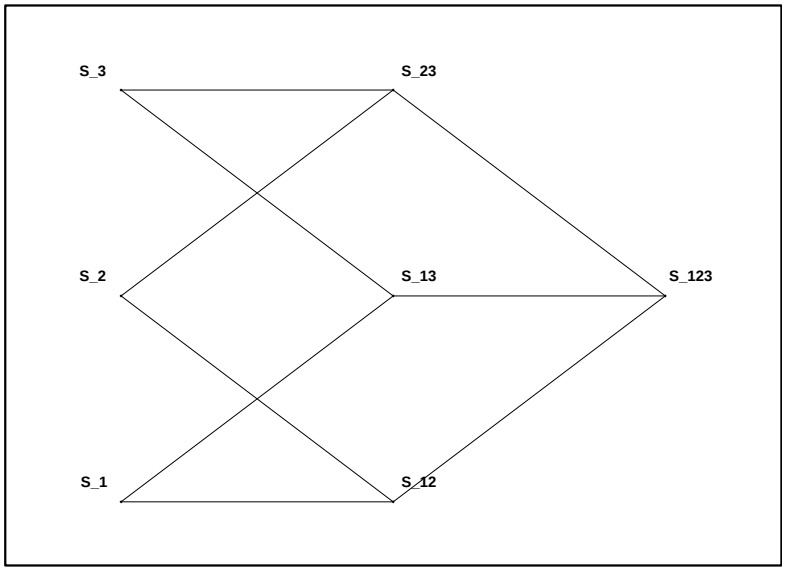


Figure 2.1: values in $\mathbb{Q}^3$

Example Let $n = 3$. Then the set of values of $\mathbb{Q}^n$ endowed with the $\preceq_c$ ordering is

$$S_{\{1\}}, S_{\{2\}}, S_{\{3\}}, S_{\{1,2\}}, S_{\{1,3\}}, S_{\{2,3\}}, S_{\{1,2,3\}} = \{0\}$$

The partial ordering on $\Gamma(\mathbb{Q}^3)$ is shown by a graph in Figure 2.1 where the edges represent inclusion.

We have 13 different term ordering types on T^3 corresponding to the chains of values

$3-chains$	$2-chains$	$1-chain$
$S_{\{1\}} \subset S_{\{1,2\}} \subset \{0\}$	$S_{\{1\}} \subset \{0\}$	$\{0\}$
$S_{\{1\}} \subset S_{\{1,3\}} \subset \{0\}$	$S_{\{2\}} \subset \{0\}$	
$S_{\{2\}} \subset S_{\{1,2\}} \subset \{0\}$	$S_{\{3\}} \subset \{0\}$	
$S_{\{2\}} \subset S_{\{2,3\}} \subset \{0\}$	$S_{\{1,2\}} \subset \{0\}$	
$S_{\{3\}} \subset S_{\{1,3\}} \subset \{0\}$	$S_{\{1,3\}} \subset \{0\}$	
$S_{\{3\}} \subset S_{\{2,3\}} \subset \{0\}$	$S_{\{2,3\}} \subset \{0\}$	

By applying the definition of convexity, one can verify that the 3-chains correspond to pure lexicographic orderings on all three variables, whereas 2-chains correspond to orderings where one variable is compared lexicographically to the other two. The 1-chain $\{0\}$ corresponds to archimedean orderings. //

The term ordering types described here as chains of values encode the type (length of the chain) and the partition type (dimensions of the subspaces) described before.

2.4 Some properties of partial term orderings

An ordering on the set of terms that is not necessarily total but that satisfies the properties of compatibility with the semigroup structure of T^n and of well-foundedness is called a partial term ordering. Clearly every term ordering is a refinement of a partial term ordering. Given a partial term ordering $\lhd$, a polynomial is called $\lhd$-homogeneous if all of its monomials belong to the same layer with respect to $\lhd$. This notion of $\lhd$-homogeneity generalizes the customary notions of homogeneity and quasi-homogeneity.

An order relation on T^n (not necessarily a total one) is called *admissible partial term ordering* or simply *partial term ordering* if it is well-founded and compatible with the semi-group structure of T^n.

As shown in the previous section, any term ordering $\prec$ can be represented by some special finite sequence $\Omega = (\omega_1, \ldots, \omega_s)$ of weight vectors $\omega_i \in \mathbb{R}^n_+$ with nonnegative real coordinates through the multi-degree map

$$\begin{array}{rccc} deg_\Omega : & \mathbb{Q}^n & \longrightarrow & \mathbb{R}^s \\ & v & \longrightarrow & (v \cdot \omega_1, \ldots, v \cdot \omega_s) \end{array}$$

by prescribing

$$t_1 \prec t_2 \text{ if and only if } deg_\Omega(log(t_1)) <_{lex} deg_\Omega(log(t_2))$$

where $<_{lex}$ is the canonical lexicographic ordering on $\mathbb{R}^n$.

Conversely, any Ω-sequence gives rise to a partial term ordering that will be denoted by $\lhd_\Omega$ or shortly by $\lhd$ when Ω is clear from the context. Recall that $\lhd_\Omega$ is total if and only if the map deg_Ω is injective.

A term ordering arising from an Ω-sequence will be called a *representable admissible partial term ordering*.

Remark that any representable admissible partial term ordering contains the "divides" order relation on T^n. In fact, given the partial term ordering $\lhd_\Omega$ with $\Omega = (\omega_1, \ldots, \omega_s)$, whenever $t_1 \mid t_2$, if we write $log(t_1) =$

$(\alpha_1, \ldots, \alpha_n)$ and $log(t_2) = (\beta_1, \ldots, \beta_n)$, we have $log(t_1) - log(t_2) = (\alpha_1 - \beta_1, \ldots, \alpha_n - \beta_n)$ with $\alpha_i - \beta_i \leq 0$ for every $i = 1, \ldots, n$. But then the scalar product

$$(log(t_1) - log(t_2)) \cdot \omega_j \leq 0$$

for every $j = 1, \ldots, s$ since $\omega_j \geq 0$ and $log(t_1) - log(t_2)$ is a vector whose coordinates are all ≤ 0. Hence $t_1 \lhd_\Omega t_2$.

From now on when we talk about partial term orderings we will always assume that they are representable unless otherwise stated.

Example Let $n = 3$ and T^n be the set of terms in the variables x, y, z. Let $\Omega = ((1,1,1),(1,0,0))$. Then

$$x^{a_1}y^{a_2}z^{a_3} \lhd x^{b_1}y^{b_2}z^{b_3}$$

if and only if $a_1 + a_2 + a_3 < b_1 + b_2 + b_3$ or $a_1 + a_2 + a_3 = b_1 + b_2 + b_3$ and $a_1 < b_1$.

The ordering $\lhd$ is partial since for instance the terms y and z are incomparable. Note that $\lhd$ is a refinement of the usual partial ordering "deg" given by comparing the degrees of terms. While for instance all terms of degree 2 $\{x^2, y^2, z^2, xy, xz, yz\}$ form one layer with respect to "deg" in T^3, $\lhd$ partitions this layer into the three subsets $\{x^2\}$, $\{xy, xz\}$, and $\{y^2, z^2, yz\}$. //

Let us recall some notions from the theory of ordered sets (an exhaustive treatment of the theory can be found for instance in [22]).

Let (A, R) be an ordered set. A *chain* $C \subseteq A$ is a totally ordered subset of A, that is for every $a,\ b \in C$ either $(a, b) \in R$ or $(b, a) \in R$.

An *antichain* $C \subseteq A$ is a subset of A such that no two elements of C are comparable with respect to R, that is for every $a,\ b \in C$, $(a, b) \in R$ if and only if $a = b$.

A *filter* $Q \subseteq A$ is a subset of A such that for every $b \in Q$ and for every $a \in A$, if $(b, a) \in R$ then $a \in Q$.

If $B \subseteq A$ we denote by $\uparrow B := \{a \in A \mid$ there exists $b \in B$ s. t. $(b, a) \in R\}$ the smallest filter containing B. Remark that $\uparrow B = B$ if and only if B is a filter. If $B = \{b\}$ is a singleton we denote by $\uparrow b$ the set $\{a \in A | (b, a) \in R\}$.

An ordered set (A, R) satisfies the *descending chain condition* if there do not exist infinite chains $C \subseteq A$ where $C = \{a_1, a_2, \ldots\}$ such that $(a_{i+1}, a_i) \in R$ for every $i \in \mathbb{N}$.

Lemma Let (A, R) be an ordered set satisfying the descending chain condition. Then the following properties are equivalent

1. every filter can be written as a finite union $\bigcup_{i=1}^{k} \uparrow a_i$ with $a_i \in A$ such that $\{a_1, \ldots, a_k\}$ is an antichain
2. the set of filters of A satisfies the ascending chain condition with respect to inclusion
3. every nonempty collection of filters admits at least one maximal element with respect to inclusion
4. in A there are no infinite antichains
5. every subset of A admits a finite number of minimal elements

Proof 1⇒2 Let I_λ be an ascending chain of filters. Then their union is also a filter that we denote by $I = \cup I_\lambda$. Since by 1 I admits a finite system of generators, there exists an index Λ such that all generators of I are contained in I_Λ. Therefore $I = I_\Lambda$ and the chain becomes stationary.

2⇒3 Let I_1 be an element of a nonempty collection of filters of A. If I_1 is maximal, then the assertion is proven. Otherwise let I_2 be a filter properly containing I_1. By repeating the same argument one obtains an ascending chain of filters that by 2 has to terminate with the desired maximal element.

3⇒4 Let $\{a_1, a_2, \ldots\}$ be an antichain. The collection of filters $\uparrow \{a_1\}$, $\uparrow \{a_1, a2\}$, $\ldots$ must have by 3 a maximal element and since $\uparrow \{a_1\} \subset \uparrow \{a_1, a2\} \subset \ldots$ there must exist $k \in \mathbb{N}$ such that $\{a_1, a_2, \ldots, a_k\}$ is maximal and the antichain cannot contain any further elements.

4⇒5 The set of minimal elements is an antichain and it is a nonempty set since the descending chain condition holds.

5⇒1 Let Q be a filter and let $\{a_1, \ldots, a_k\}$ be its minimal elements. Let $P := \bigcup_{i=1}^{k} \uparrow a_i = \uparrow \{a_1, \ldots, a_k\}$. Then $P \subseteq Q$. Let $b \in Q \setminus \{a_1, \ldots, a_k\}$ a non minimal element. Then there exists $z_1 \in Q$ such that $(z_1, b) \in R$. If z_1

is minimal then $z_1 \in \{a_1, \ldots, a_k\}$ thus $b \in P$. Otherwise let $z_2 \in Q$ be such that $(z_1, b) \in R$ and so on. Eventually one will have to stop because the set $\{y, z_1, z_2, \ldots\}$ admits a minimal element. Hence $Q \subseteq P$. //

An ordered set (A, R) for which the descending chain condition holds and that satisfies the previous equivalent properties is called *noetherian*.

The property of T^n (respectively $\mathbb{N}^n$) with the partial order "divides" (respectively the natural order) being noetherian is known as Dickson's lemma. A proof of the lemma may be found for instance in [9], p. 163, Corollary 4.48, or in [51], p. 186, Theorem 8.3.2.

The following lemma tells us that any order refining a noetherian order is itself noetherian (the proof of this property is proposed as an exercise in [9], p. 160, Exercise 4.41).

Lemma Let (A, R) be a noetherian ordered set and let R' be an order relation on A such that $R \subseteq R'$. Then (A, R') is also noetherian.

Proof We start by showing that the descending chain condition holds for R'. By contradiction, let $C = \{a_1, a_2, \ldots\} \subseteq A$ such that $(a_{i+1}, a_i) \in R'$ for every $i \in \mathbb{N}$ be an infinite descending chain. Since (A, R) is noetherian, C admits a finite number of minimal elements with respect to R. Let $\{b_{j_1}, \ldots, b_{j_m}\} \subseteq C$ be such set of minimal elements with $j_1 < \cdots < j_m$. Then for every $j > j_m$we have $(a_{j+1}, a_j) \in R'$ and $(a_{j+1}, a_j) \notin R$, otherwise we would contradict the property of minimality. But then $\{a_j, a_{j+1}, \ldots\}$ is an infinite antichain in (A, R) and this is not possible since (A, R) is noetherian.

We now need to prove one of the equivalent conditions of the previous lemma. We show that (A, R') does not contain any infinite antichain. By contradiction, let $C = \{a_1, a_2, \ldots\} \subseteq A$ be an infinite antichain with respect to R'. As before, let $\{b_{j_1}, \ldots, b_{j_m}\} \subseteq C$ the finite of minimal elements with respect to R. But then, for every $a_i \in C$, there exists j_k such that $(b_{j_k}, a_i) \in R$ and since $R \subseteq R'$ it also holds $(b_{j_k}, a_i) \in R'$, hence C is not an antichain with respect to R'. //

We already observed that any partial term ordering $\lhd$ is a refinement of

the "divides" order relation on T^n, hence every partial term ordering $\lhd$ is noetherian.

A partial term ordering $\lhd$ partitions T^n and therefore KT^n into maximal antichains or $\lhd$-*layers* that are strictly ordered by $\lhd$.

Hence we can generalize the concept of quasi-homogeneity (and of homogeneity as a special case of quasi-homogeneity) to that of $\lhd$-homogeneity. Note that whenever $\lhd$ is total, the $\lhd$-layers of $T^n$are finite since each layer contains homogeneous (resp. quasi-homogeneous) forms of the same degree (resp. weighted degree). When considering partial term orderings, the $\lhd$-layers of T^n may be infinite.

A polynomial $f \in K[x_1, \ldots, x_n]$ is called $\lhd$-*homogeneous* if all terms in $supp(f)$ belong to the same $\lhd$-layer. Any polynomial f can be uniquely decomposed into a sum of $\lhd$-homogeneous segments $f_1, f_2, \ldots, f_m$ such that

$$f = f_1 + f_2 + \cdots + f_m$$

with $f_1 \lhd f_2 \lhd \cdots \lhd f_m$.

Note that for the singleton $\Omega = (\omega)$ $\lhd$-homogeneity coincides with quasi-homogeneity with respect to the weight vector ω. If in addition ω is the vector $(1, 1, \ldots, 1)$ then we have the classical definition of homogeneity.

For a polynomial $f \in K[x_1, \ldots, x_n]$ denote by $f_\lhd$ the sum of all monomials in $supp(f)$ that belong to the maximal segment of f with respect to $\lhd$. This is the $\lhd$-*initial segment* of f and it coincides with the initial monomial of f whenever $\lhd$ is total (and hence a term ordering).

Example Let $n = 3$, T^n be the set of terms in the variables x, y, z, and $\Omega = ((1, 0, 1), (1, 0, 0))$.

Then the polynomial

$$f = 3xz^3 - x^5 + 2x^3yz + 3x^4z + 2x^4 - 2y^2z^3$$

is already decomposed into $\lhd_\Omega$-segments since all of its terms are incomparable with respect to deg_Ω.

Since $deg_\Omega(xz^3) = (4, 1)$, $deg_\Omega(x^5) = (5, 5)$, $deg_\Omega(x^3yz) = (4, 3)$, $deg_\Omega(x^4z) = (5, 4)$, $deg_\Omega(x^4) = (4, 4)$, and $deg_\Omega(y^2z^3) = (3, 3)$ we can order the $\lhd_\Omega$-

segments by sorting the Ω-degrees lexicographically obtaining

$$f = -x^5 + 3x^4z + 2x^4 + 2x^3yz + x^2z^2 + 3xz^3 - 2y^2z^3$$

where $-x^5$ is the maximal $\lhd_\Omega$-segment in f. //

Example Let $n = 3$, T^3 the set of terms in the variables x, y, z, and $\Omega = ((1,1,2),(1,1,0))$. Then $f = f_1 + f_2$ where $f_1 = y^3z^2 + 2x^2y^5$, $f_2 = 3x^5y^2 + x^4yz$ is the decomposition of f into $\lhd_\Omega$-segments where $deg_\Omega(f_1) = (7,5)$ and $deg_\Omega(f_2) = (7,2)$ and f_1 is the maximal $\lhd_\Omega$-segment in f. //

For a set $F \subseteq K[x_1, \ldots, x_n]$ denote by $F_\lhd$ the set $\{f_\lhd \mid f \in F\}$.

An ideal $I \subseteq K[x_1, \ldots, x_n]$ is $\lhd$-*homogeneous* if for all $f \in I$, the $\lhd$-homogeneous decomposition $f = f_1 \lhd \cdots \lhd f_m$ of f satisfies $f_i \in I$ for all $i = 1, \ldots, m$. This is equivalent to saying that I admits a basis of $\lhd$-homogeneous polynomials.

For a partial term ordering $\lhd_\Omega$ represented by a sequence $\Omega = (\omega)$ consisting of one single vector, we will denote for short by $f_\omega := f_{\lhd_\Omega}$ (respectively $F_\omega := F_{\lhd_\Omega}$) the ω-homogeneous initial form of a polynomial f (respectively the set of initial ω-homogeneous initial forms of the polynomials in the set F) with respect to $\lhd_\Omega$ in accordance with the usual notations for quasi-homogeneity.

2.5 Partial term orderings and Gröbner bases

Given a partial term ordering $\lhd$, the $\lhd$-initial forms of polynomials in an ideal I generate its $\lhd$-initial ideal. Whenever $\lhd$ is total - and hence a term ordering - the $\lhd$-initial ideal of I corresponds to its initial ideal. Since $\lhd$-initial ideals generalize the notion of initial ideals, it makes sense to investigate how to generalize properties of initial ideals for this broader family of ideals.

In this section we demonstrate some significant properties of $\lhd$-initial ideals. In particular, we show how from the Gröbner basis of an ideal one may read off a Gröbner basis of its $\lhd$-initial ideal, whenever the term ordering is a refinement of $\lhd$.

The properties of Gröbner bases and partial term orderings have been investigated by Collart and Mall (see [15],[16], and[17], [18]). In our exposition we follow [18].

Given an ideal $I \subseteq K[x_1, \ldots, x_n]$ and a partial term order $\lhd$ on T^n, the *toric degeneration of I with respect to* $\lhd$ is the ideal $\langle I_\lhd \rangle = \langle \{ f_\lhd \mid f \in I \} \rangle$. The collection of all toric degenerations of I is called the *toric complex* of I. This terminology comes from [18], where the authors briefly explain how these objects are related to the theory of toric varieties.

Gröbner bases of toric degenerations allow a characterization that is similar to that of Gröbner bases of initial ideals. In order to present the main result of this section, we need to state some more properties of partial term orderings.

Given partial term orderings $\lhd_1, \lhd_2, \ldots, \lhd_r$ we define the *concatenation ordering* as the ordering obtained by comparing first according to $\lhd_1$, then to $\lhd_2$, etc. and denote it by $(\lhd_1 \mid \lhd \mid \ldots \mid \lhd_r)$. If $\prec$ is a term ordering then, given a partial term ordering $\lhd$, the term ordering $(\lhd \mid \prec)$ is said to *refine* $\lhd$.

An ideal I is called $\lhd$-*homogeneous* if for every $f \in I$, if $f = f_1 + \cdots + f_m$ is the $\lhd$-homogeneous decomposition of f, then $f_i \in I$ for every $i = 1, \ldots, m$.

Let $I \subseteq K[x_1, \ldots, x_n]$ be an ideal, and $\lhd, \lhd_1, \lhd_2$ partial term orderings. Then the following are some basic properties of $\lhd$-homogeneity:

- I is $\lhd$-homogeneous if and only if it has a set of $\lhd$-homogeneous generators
- I is $(\lhd_1 \mid \lhd_2)$-homogeneous if and only if it is both $\lhd_1$-homogeneous and $\lhd_2$-homogeneous

Let $(\lhd \mid \lhd')$ be a concatenation of term orderings on T^n. Then for any polynomial $f \in K[x_1, \ldots, x_n]$ taking the initial term with respect to $\lhd'$ of the $\lhd$-inital segment of f is the same as taking the $(\lhd \mid \lhd')$-initial segment of f since $(\lhd \mid \lhd')$ refines $\lhd$, that is

$$f_{(\lhd \mid \lhd')} = (f_\lhd)_{\lhd'}$$

For a set F of polynomials $F \subseteq K[x_1, \ldots, x_n]$ we have similarly

$$F_{(\lhd \mid \lhd')} = (F_\lhd)_{\lhd'}$$

Note that, if $(\lhd \,|\prec)$ is a term ordering on T^n refining $\lhd$, where $\prec$ is a term ordering, then for any polynomial $f \in K[x_1, \ldots, x_n]$ taking the initial term with respect to $(\lhd \,|\prec)$ of the $\lhd$-inital segment of f is the same as taking the $(\lhd \,|\prec)$ of f since $(\lhd \,|\prec)$ refines $\lhd$, that is

$$(f_\lhd)_{(\lhd|\prec)} = f_{(\lhd|\prec)} = (f_\lhd)_\prec$$

If F is any subset of polynomials $F \subseteq K[x_1, \ldots, x_n]$ then similarly

$$(F_\lhd)_{(\lhd|\prec)} = F_{(\lhd|\prec)} = (F_\lhd)_\prec$$

Let $\lhd$ be a partial term ordering on $K[x_1, \ldots, x_n]$. Thes a set of polynomials $G \subseteq K[x_1, \ldots, x_n]$ is called *meager* with respect to $\lhd$ if for every $g, g' \in G$ onr has either $g_\lhd \lhd g'_\lhd$ or $g'_\lhd \lhd g_\lhd$, that is, no two $\lhd$-initial segments of polynomials in G lie in the same $\lhd$-layer.

Proposition Let $I \subseteq K[x_1, \ldots, x_n]$ be an ideal and $\lhd$ and $\lhd'$ partial term orderings on T^n. Then the initial ideal of I with respect to $(\lhd \mid \lhd')$ is equal to the initial ideal of I with respect to $\lhd'$ of the the $\lhd$-initial ideal of I, that is

$$\langle I_{(\lhd|\lhd')} \rangle = \langle (\langle I_\lhd \rangle)_{\lhd'} \rangle$$

Proof A proof of this may be found in [18], Proposition 2.4. The proof is based on the fact that for every ideal I there exists a finite meager set $G \subset I$ such that every $f \in \langle I_\lhd \rangle$ can be written as a sum of initial segments of elements of G. //

Proposition Let $\lhd$ be a partial term ordering on T^n represented by Ω and $I \subseteq K[x_1, \ldots, x_n]$ be an ideal. Let $\prec$ be any term ordering on T^n. Then

1. if G is the reduced Gröbner basis of I with respect to $(\lhd \,|\prec)$ then $G_\lhd$ is a Gröbner basis of $\langle I_\lhd \rangle$ with respect to $(\lhd \,|\prec)$
2. there exists $\omega \in \mathbb{R}^n_+$ such that $\langle I_\lhd \rangle = \langle I_\omega \rangle$

3. I is $\lhd$-homogeneous if and only if all of its reduced Gröbner bases are

4. $I = \langle I_\lhd \rangle$ if and only if I is $\lhd$-homogeneous

Proof 1. For proving (1) we will use the basic property of refinements of partial term orderings mentioned at the beginning of this section.

Recall that, by the basic properties of Gröbner bases, G is a Gröbner basis of I with respect to a term ordering if and only if the initial terms of G generate the initial ideal of I with respect to the given term ordering. Hence we can write $\langle G_{(\lhd|\prec)} \rangle = \langle I_{(\lhd|\prec)} \rangle$ since G is by definition a Gröbner basis of I with respect to $(\lhd|\ \prec)$.

What we need to prove is that $(G_\lhd)_{(\lhd|\prec)}$ generates $\langle (\langle I_\lhd \rangle)_{(\lhd|\prec)} \rangle$. But this follows from the fact that $(\langle I_\lhd \rangle)_{(\lhd|\prec)} = I_{(\lhd|\prec)}$ and $(G_\lhd)_{(\lhd|\prec)} = G_{(\lhd|\prec)}$

2. In order to prove (2) we will use induction on the number of vectors in the sequence Ω.

If $\Omega = (\omega)$ then ω is the required vector.

Let (2) hold for any sequence of $k-1$ vectors $\Omega' = (\omega_1, \ldots, \omega_{k-1})$ and let ω' be the vector such that $\langle I_{\lhd_{\Omega'}} \rangle = \langle I_{\omega'} \rangle$. Let $\omega_k \in \mathbb{R}^n_+$ be a weight vector and $\Omega'' = (\omega_1, \ldots, \omega_{k-1}, \omega_k)$. What we need to show is that there exists an $\omega'' \in \mathbb{R}^n_+$ such that $\langle I_{\lhd_{\Omega''}} \rangle = \langle I_{\omega''} \rangle$. Let $\prec$ a term ordering refining $\lhd_{\Omega''}$ and G the reduced Gröbner basis of I with respect to $\prec$. According to (1), $G_{\lhd_{\Omega''}}$ is a Gröbner basis of $\langle I_{\lhd_{\Omega''}} \rangle$ with respect to $\prec$ and we can write $\langle I_{\lhd_{\Omega''}} \rangle = \langle G_{\lhd_{\Omega''}} \rangle$. Then if we provide a ω'' such that $\langle G_{\lhd_{\Omega''}} \rangle = \langle G_{\omega''} \rangle$ we have completed the proof of the induction step.

Let $g \in G$, $t_1, t_2 \in supp(g)$ and let $a = log(t_1)$, $\beta = log(t_2)$ and let $t_1 \lhd_{(\omega'|\omega_k)} t_2$. According to the definition of multi-degree, $t_1 \lhd_{(\omega'|\omega_k)} t_2$ if and only if $(\omega'\alpha, \omega_k\alpha) <_{lex} (\omega'\beta, \omega_k\beta)$. Set $\omega'' = \omega' + \varepsilon\omega_k$ for some $\varepsilon \in \mathbb{R}_+ \setminus \emptyset$. We will prove that one can always find such an ε for which $t_1 \lhd_{(\omega'|\omega_k)} t_2$ if and only if $t_1 \lhd_{\omega''} t_2$.

By definition of ω'' , $t_1 \lhd_{\omega''} t_2$ if and only if $(\omega' + \varepsilon\omega_k)\alpha < (\omega' + \varepsilon\omega_k)\beta$.

If $\omega'\alpha < \omega'\beta$ then denote their difference by $\lambda = \omega'\beta - \omega'\alpha \in \mathbb{R}_+ \setminus \emptyset$. Take ε such that the inequality $\varepsilon\omega_k\alpha < \lambda + \varepsilon\omega_k\beta$ holds, that is $\varepsilon(\omega_k\alpha - \omega_k\beta) < \lambda$. If $\omega_k\alpha - \omega_k\beta$ then any positive ε will do, otherwise one can always find a positive ε such that $\varepsilon < \frac{\lambda}{\omega_k\alpha - \omega_k\beta}$.

If $\omega'\alpha = \omega'\beta$ then $\omega_k\alpha < \omega_k\beta$ and any positive ε satisfies the inequality

$(\omega' + \varepsilon\omega_k)\alpha < (\omega' + \varepsilon\omega_k)\beta$.

By repeating the same argument for all pairs of terms in $supp(g)$ and for every $g \in G$ one has an $\varepsilon \in \mathbb{R}_+ \setminus \emptyset$ and a weight vector $\omega'' = \omega' + \varepsilon\omega_k$ such that $\langle G_{\lhd_{\Omega''}} \rangle = \langle G_{\omega''} \rangle$.

3. If I is $\lhd$-homogeneous then it admits a basis of $\lhd$-homogeneous polynomials. Let G be a reduced Gröbner basis of I. If $g \in G$ and g is not $\lhd$-homogeneous, then since $g \in I$ and I is $\lhd$-homogeneous, every $\lhd$-homogeneous component of g belongs to I. But this means that g is reducible with respect to G, and this means that G is not reduced. But then every reduced Gröbner basis G contains only $\lhd$-homogeneous polynomials.

Conversely, assume that every reduced Gröbner basis of I is $\lhd$-homogeneous. Let $G = \{g_1, \ldots, g_r\}$ be a reduced Gröbner basis of I and let $f \in I$ be $\lhd$-homogeneous. Then we can write

$$f = \sum_{i=1}^{r} h_i g_i$$

for some polynomials $h_1, \ldots, h_r$ not necessarily $\lhd$-homogeneous. For every i, let $h_i = \sum_{j=1}^{k_i} h_{ij}$ be the decomposition of h_i into $\lhd$-homogeneous segments. Then we can write

$$f = \sum_{i=1}^{r} (\sum_{j=1}^{k_i}) g_i$$

Hence, since every $\lhd$-homogeneous segment of f is in I, the ideal I is $\lhd$-homogeneous.

4. If $I = \langle I_\lhd \rangle$ then I is $\lhd$-homogeneous by (3).

Conversely, if I is $\lhd$-homogeneous, by hypothesis all $\lhd$-homogeneous components of f are in I for every $f \in I$ and therefore $f \in \langle I_\lhd \rangle$ and $I \subseteq \langle I_\lhd \rangle$. In order to prove the other inclusion, observe that every $g \in \langle I_\lhd \rangle$ can be written as $\sum_i h_i (f_i)_\lhd$ with $f_i \in I$. Then, since $(f_i)_\lhd \in I$, it follows that $g \in I$. //

2.6 Partial term orderings and Hilbert functions

In this section we define an analogous Hilbert functions for $\lhd$-homogeneous ideals as a generalization of Hilbert functions of homogeneous ideals. For an ideal that is not homogeneous, one may define the affine Hilbert function. It is known (see for instance [20], p. 448, Prop. 4) that if $\prec$ is a degree-compatible term ordering then the Hilbert function of an ideal equals the Hilbert function of its initial ideal with respect to $\prec$, and hence it can be read off from a Gröbner basis with respect to $\prec$. An analogous property also holds for partial term orderings that are refinements of a weight vector with positive coordinates.

Our results are derived from [18], [35], [45].

A *$\mathbb{Z}$-graded ring* is a ring R that admits a direct sum decomposition (as an abelian group)

$$R = \bigoplus_{i \in \mathbb{Z}} R_i$$

such that if $r_i \in R_i$ and $r_j \in R_j$, then $r_i r_j \in R_{i+j}$.

One can define gradings by arbitrary groups, but for now the definition of $\mathbb{Z}$-grading will suffice. Hence in the following we will mean $\mathbb{Z}$-graded every time we talk about *graded*.

A module M over a graded ring R is *graded* if it can be written as a direct sum

$$M = \bigoplus_{i \in \mathbb{Z}} M_i$$

such that if $m_i \in M_i$ and $m_j \in M_j$ then $m_i m_j \in M_{i+j}$.

The ring of polynomials $K[x_1, \ldots, x_n]$ together with the usual degree "deg" is graded since every polynomial can be written as a sum of homogeneous forms. This is called the *standard grading* of the ring of polynomials. If we set

$$K[x_1, \ldots, x_n]_{=s} := \{f \in K[x_1, \ldots, x_n] \mid f \text{ homogeneous of degree } s\}$$

then we can write

$$K[x_1, \ldots, x_n] = \bigoplus_{s \in \mathbb{Z}} K[x_1, \ldots, x_n]_{=s}$$

where $K[x_1, \ldots, x_n]_{=0} = K$, the ring of coefficients, and $K[x_1, \ldots, x_n]_{=s} = \emptyset$ for $s < 0$.

Similarly, one can equip $K[x_1, \ldots, x_n]$ with the grading given by any *weighted degree* given by a weight vector $v \in \mathbb{R}^n_+$ with positive coordinates.

Consider now a homogeneous ideal $I \subseteq K[x_0, x_1, \ldots, x_n]$. One can regard $K[x_0, x_1, \ldots, x_n]/I$ as a K-module. Given a Gröbner basis G of I we even have a basis of $K[x_0, x_1, \ldots, x_n]/I$ as vector space over K. The set

$$S(G) = \{t \in T^{n+1} \mid t \text{ not multiple of any of the leading terms in } G\}$$

generates $K[x_0, x_1, \ldots, x_n]/I$ as a vector space over K and is called the staircase of G (see Section 2.2).

The vector spaces $(K[x_0, x_1, \ldots, x_n]/I)_{=s}$ of forms of degree s yield a grading on $K[x_0, x_1, \ldots, x_n]/I$

$$K[x_0, x_1, \ldots, x_n]/I = \bigoplus_{s \in \mathbb{Z}} (K[x_0, x_1, \ldots, x_n]/I)_{=s}$$

Define the *Hilbert function* of a graded K-module as

$$H(M, s) := dim_K M_s$$

Observe that if $K[x_0, x_1, \ldots, x_n]$ is equipped with the standard grading then

$$\begin{aligned} dim_K(K[x_0, x_1, \ldots, x_n]/I)_{=s} &= dim_K K[x_0, x_1, \ldots, x_n]_{=s}/I_{=s} \\ &= dim_K K[x_0, x_1, \ldots, x_n]_{=s} - dim_K I_{=s} \\ &= \begin{pmatrix} n+s \\ s \end{pmatrix} - dim_K I_{=s} \end{aligned}$$

where $dim_K K[x_1, \ldots, x_n]_{=s} = \begin{pmatrix} n+s \\ s \end{pmatrix}$ is the number of terms of degree s in $n+1$ variables.

Example

Let $I = \langle x^3 + y^3 + z^3 \rangle \subseteq K[x, y, z]$. Consider the standard grading and order the terms so that $x^3 > y^3 > z^3$. Then

i	generators of M_i as K-vectorspace	$dim_K M_i$
0	$\{1\}$	1
1	$\{x, y, z\}$	3
2	$\{x^2, xy, xz, y^2, yz, z^2\}$	6
3	$\{x^2y, x^2z, xy^2, xyz, xz^2, y^3, y^2z, yz^2, z^3\}$	9
4	$\{x^2y^2, x^2yz, x^2z^2, xy^3, xy^2z, xyz^2, xz^3, y^4, y^3z, y^2z^2, yz^3, z^4\}$	12
...	...	...

Counting terms of degree s that are multiples of x^3 is the same as counting terms of degree $s - 3$. Hence for $s \geq 3$ we have $dim_k I_{=s} = \begin{pmatrix} 3+s-4 \\ s-3 \end{pmatrix}$ and $H(K[x, y, z]/I, s) = \begin{pmatrix} 3+s-1 \\ s \end{pmatrix} - \begin{pmatrix} 3+s-4 \\ s-3 \end{pmatrix}$.

If we add the line x to the ideal I we know by Bezout's theorem that a line and a cubic curve meet in 3 points in the projective space. Observe that $K[x, y, z]/\langle x^3 + y^3 + z^3, x \rangle \cong K[y, z]/\langle y^3 + z^3 \rangle$ and the Hilbert function is

s	0	1	2	3	4	...
$H(K[y, z]/\langle y^3 + z^3 \rangle, s)$	1	2	3	3	3	...

The fact that for any $s \geq 2$ the Hilbert function is a constant is a consequence of the well-known result that for a big enough s the Hilbert function can be expressed as a polynomial in s called the *Hilbert polynomial* whose degree is the dimension of the variety of I. //

If $I \subseteq K[x_1, \ldots, x_n]$ is not a homogeneous ideal then the set of polynomials of total degree s is not a K-module since it is not closed under addition. We can instead consider the K-module $(K[x_1, \ldots, x_n]/I)_{\leq s}$ of polynomials of degree $\leq s$ and define the *affine Hilbert function* as

$$^a H(M, s) := dim_K M_{\leq s}$$

If one denotes by I^h the homogenization of the ideal I then the affine and projective Hilbert functions satisfy the equality

$$^aH(K[x_1,\ldots,x_n]/I,s) = H(K[x_0,x_1,\ldots,x_n]/I^h,s)$$

This and other properties of Hilbert functions are presented in Chapter 9 of [20]. We will just recall here those properties which provide a method for its computation.

In the projective case, the Hilbert function of a homogeneous ideal coincides with the Hilbert function of its initial ideal ideal that is

$$H(K[x_0,x_1,\ldots,x_n]/I,s) = H(K[x_0,x_1,\ldots,x_n]/\langle I_\prec\rangle,s)$$

for any term ordering $\prec$ and I homogeneous. A proof of this property can be found in [20], p.452, Prop. 9.

In the affine case we need to consider term orderings that are compatible with the degree, that is those term orderings $\prec$ such that $t_1 \prec t_2$ implies $deg(t_1) \leq deg(t_2)$. Call such orderings *graded*.

Then for $I \subseteq K[x_1,\ldots,x_n]$ not necessarily homogeneous we can write

$$^aH(K[x_1,\ldots,x_n]/I,s) =^a H(K[x_1,\ldots,x_n]/\langle I_\prec\rangle,s)$$

for any graded term ordering $\prec$. For a proof of this fact see [20], p. 448, Prop. 4.

We now want to investigate the behaviour of the Hilbert function of initial ideals with respect to partial term orderings.

Let $\lhd$ be a partial term ordering arising from an Ω-sequence. We have seen in Section 2.4 that any polynomial $f \in K[x_1,\ldots,x_n]$ can be uniquely decomposed into a sum of $\lhd$-homogeneous segments $f_1, f_2, \ldots, f_m$ such that $f = f_1 \lhd + f_2 \lhd + \cdots + \lhd f_m$.

Let $\Omega = (\omega_1,\ldots,\omega_m)$ with $\omega_i \in \mathbb{R}^n_+$ for every $i = 1,\ldots,m$, $m \leq n$. If we set

$$K[x_1,\ldots,x_n]_{=_\lhd w} := \{f \in K[x_1,\ldots,x_n] |\ f \text{ homogeneous of } \Omega\text{-degree } w\}$$

for $w \in \mathbb{Z}^m$ then we can write

$$K[x_1,\ldots,x_n] = \bigoplus_{w\in\mathbb{Z}^m} K[x_1,\ldots,x_n]_{=_\lhd w}$$

In fact, let $w_1, w_2 \in \mathbb{Z}^m$ and $f_1, f_2 \in K[x_1, \ldots, x_n]$ Ω-homogeneous such that $w_1 = deg_\Omega(f_1)$ and $w_2 = deg_\Omega(f_2)$. Then one can see that $deg_\Omega(f_1 f_2) = deg_\Omega(f_1) + deg_\Omega(f_2) = w_1 + w_2$. Also, if $deg_\Omega(f_1) = deg_\Omega(f_2)$ then $deg_\Omega(f_1 + f_2) = deg_\Omega(f_1) = deg_\Omega(f_2)$.

Let $I_{=_\lhd w} = I \cap K[x_1, \ldots, x_n]_{=_\lhd w}$. Remark that $(K[x_1, \ldots, x_n]/I)_{=_\lhd w} = K[x_1, \ldots, x_n]_{=_\lhd w}/I_{=_\lhd w}$, but in general $(K[x_1, \ldots, x_n]/I)_{=_\lhd w}$ is not finite. To see this, consider for instance the ideal $\langle x_1 \rangle$ and the partial term ordering given by $\omega = (1, 0, \ldots, 0)$ in $K[x_1, \ldots, x_n]$. Then for every $(d_1, \ldots, d_n) \in \mathbb{N}^n$ we have $deg_\omega(x_1^{d_1} \cdots x_n^{d_n}) = (d_1, 0, \ldots, 0)$, therefore for every $w = (w_1) \in \mathbb{Z}^1$ the vector space $K[x_1, \ldots, x_n]_{=_\lhd w}/I_{=_\lhd w}$ is infinite.

Lemma Let $\lhd$ be a the partial term represented by $\Omega = (\omega_1, \ldots, \omega_m)$. Then, whenever $\omega_1 = (\omega_{11}, \ldots, \omega_{1n}) \in \mathbb{R}^n_+$ satisfies $\omega_{1i} > 0$ for every $i = 1, \ldots, n$, the vector space $K[x_1, \ldots, x_n]_{=_\lhd w}/I_{=_\lhd w}$ has finite dimension for every $(w_1, \ldots, w_m) \in \mathbb{Z}^m$.

Proof Let $t = x_1^{d_1} \cdots x_n^{d_n}$ with $(d_1, \ldots, d_n) \in \mathbb{N}^n$ and $w = (w_1, \ldots, w_m) \in \mathbb{Z}^m$. Then if we prescribe $deg_\Omega(t) = w = (w_1, \ldots, w_m)$, the equation $\omega_{01} d_1 + \cdots + \omega_{0n} d_n = w_1$ has finitely many solutions $(d_1, \ldots, d_n)$ in $\mathbb{Z}^n$ and hence in $\mathbb{N}^n$. //

Since we are not interested in infinite dimensional vector spaces, we assume from now on that the first vector in Ω has positive coordinates.

Let $\lhd$ be a partial term ordering represented by Ω, I be a $\lhd$-homogeneous ideal and $(K[x_0, x_1, \ldots, x_n]/I)_{=_\lhd w}$ be the K-module of the Ω-homogeneous forms in $(K[x_0, x_1, \ldots, x_n]/I)$ of Ω-degree w. Then, as in the case of homogeneous ideals, one can compute the dimension of this vector space by computing the dimension of their initial ideals (see Proposition 9, Ch. 9 §3, p. 452 in [20]).

Proposition Let $\Omega = (\omega_0, \omega_1, \ldots, \omega_m)$ be a sequence of vectors $\omega_i \in \mathbb{R}^{n+1}_+$ representing the partial term ordering $\lhd$ on T^{n+1} and let $\prec$ be a term ordering. Assume that $\omega_0 = (\omega_{00}, \omega_{01}, \ldots, \omega_{0n})$ is such that $\omega_{0j} > 0$ for every $j = 0, 1, \ldots n$. If $I \subseteq K[x_0, x_1, \ldots, x_n]$ is a $\lhd$-homogeneous ideal then $K[x_0, x_1, \ldots, x_n]_{=_\lhd w}/I_{=_\lhd w}$ and $K[x_0, x_1, \ldots, x_n]_{=_\lhd w}/(I_\prec)_{=_\lhd w}$ have the same dimension as vector spaces over K.

Proof For $f \in K[x_0, x_1, \ldots, x_n]_{=_\triangleleft w}$ denote by $[f]$ the equivalence class of f in $K[x_0, x_1, \ldots, x_n]_{=_\triangleleft w}/I_{=_\triangleleft w}$.

We want to show that the set

$$C := \{[t] \mid deg_\Omega(t) = w,\ t \text{ not multiple of any of the leading terms in } \langle I_\prec \rangle\}$$

is a basis of the vector space $K[x_0, x_1, \ldots, x_n]_{=_\triangleleft w}/I_{=_\triangleleft w}$.

We know from the previous lemma that C is finite. Denote the elements of C by $[t_1], \ldots, [t_r]$ and choose $h_1, \ldots h_r \in K$ such that $\sum_{i=1}^r h_i[t_i] = [0]$. Then $\sum_{i=1}^r h_i t_i \in I$ and therefore reducible to 0 modulo the Gröbner basis G of I with respect to $\prec$. By definition of C, since $\{t_1, \ldots, t_r\} \in S(G)$, we must have $h_1 = \ldots = h_r = 0$. Hence, C is linearly independent.

We now want to prove that C spans $K[x_0, x_1, \ldots, x_n]_{=_\triangleleft w}/I_{=_\triangleleft w}$.

Let $f \in K[x_0, x_1, \ldots, x_n]_{=_\triangleleft w}$ and f' be its normal form modulo G. Since every polynomial in G is $\triangleleft$-homogeneous, $f' \in K[x_0, x_1, \ldots, x_n]_{=_\triangleleft w}$ and $[f] = [f']$. Hence, C is a basis of $K[x_0, x_1, \ldots, x_n]_{=_\triangleleft w}/I_{=_\triangleleft w}$.

Moreover

$$\begin{aligned}
&dim_K(I \cap K[x_0, x_1, \ldots, x_n]_{=_\triangleleft w}) = \\
&= |K[x_0, x_1, \ldots, x_n]_{=_\triangleleft w}| - |K[x_0, x_1, \ldots, x_n]_{=_\triangleleft w}/I \cap K[x_0, x_1, \ldots, x_n]_{=_\triangleleft w}| \\
&= |K[x_0, x_1, \ldots, x_n]_{=_\triangleleft w}| - |C| \\
&= dim_K(I_{=_\triangleleft w} \cap K[x_0, x_1, \ldots, x_n]_{=_\triangleleft w})
\end{aligned}$$

//

If we drop the condition of $\triangleleft$-homogeneity for I, we need an additional restriction on $\prec$ in order to obtain a similar result. Namely, we require the term ordering $\prec$ to be a refinement of $\triangleleft$. Note that since we require the first vector in Ω to have positive coordinates, whenever $\Omega = (\omega) = (1, \ldots, 1)$, prescribing that $\prec$ be a refinement of $\triangleleft$ is the same as prescribing that $\prec$ be a graded term ordering.

Proposition Let $\Omega = (\omega_1, \ldots, \omega_s)$ be a sequence of vectors $\omega_i \in \mathbb{R}^n_+$ with $\omega_1 = (\omega_{11}, \ldots, \omega_{1n})$ such that $\omega_{1j} > 0$ for every $j = 1, \ldots, n$. Let $\triangleleft$ be the partial term ordering on T^n represented by Ω and let $\prec$ be a term ordering refining $\triangleleft$. Then $(K[x_1, \ldots, x_n]/I)_{=_\triangleleft w}$ and $(K[x_1, \ldots, x_n]/I_\prec)_{=_\triangleleft w}$ have the same dimension as vector spaces over K.

Proof Since Ω gives a grading on $K[x_1, \ldots, x_n]$, $dim(K[x_1, \ldots, x_n]/I)_{=_\lhd w}$ is the Hilbert function of I. Since $\prec$ refines $\lhd$, $\prec$ is graded and we know that the Hilbert function of $I_\prec$ is the same of the Hilbert function of I. //

Chapter 3

The Gröbner Walk

The Gröbner fan of an ideal is a partition of the set of term orderings such that two term orderings belonging to the same element of the partition yield the same oriented reduced Gröbner basis, where oriented means that the leading terms of the polynomials in the basis are marked out.

Gröbner fans were first introduced by Robbiano and Mora in 1988 (see [43]). In their paper they consider the space of real vectors and study the behavior of term orderings that refine the partial term orderings given by these vectors. For a given polynomial ideal, the vectors corresponding to term orderings that yield the same Gröbner basis are contained in a convex subset (cone) of $\mathbb{R}^n$, and this set is polyhedral. Furthermore, the family of all such cones, called the Gröbner fan of the ideal, is finite. The definition of Gröbner fan of an ideal was originally aimed at providing an algorithm for the construction of universal Gröbner bases. These are bases that satisfy the Gröbner property for any term ordering.

The Gröbner fan of an ideal allows to define an algorithm for change of orderings in the theory of Gröbner bases. The algorithm has been presented in 1997 by Collart, Kalkbrener, and Mall ([14]) and is known as the Gröbner walk. The combinatorial properties of Gröbner fans on which the Gröbner walk algorithm is based are also presented in [15],[16], and[17].

Given an initial term ordering one steps on different cones in the fan until the target ordering is reached. Any two cones in the fan have a common face that consists of those partial term orderings that may be refined to term orderings belonging to either one of the two cones. By exploiting the properties of partial orderings on the intersections of cones, one does

not have to compute a whole Gröbner basis at each step. Instead, one just needs to compute the Gröbner basis of a $\lhd$-homogeneous initial ideal and lift it.

The Gröbner walk algorithm has shown to be in many cases less costly than a computation of one single Gröbner basis because, even if stepping on the fan requires the computation of Gröbner bases for several smaller ideals, these are in general easier to compute.

Some implementation issues and improvements of the Gröbner walk algorithm are presented in [5] , [6], and [4], where the problem of determining a path on the fan that minimizes computations is investigated. Even though there is no answer to how to define an optimal path, some criteria have been investigated that result in a better behaviour of the algorithm. By perturbing the path one avoids those points where more than two cones intersect, which correspond to homogeneous ideals that are harder to compute. Empirical results show that perturbation of the path may in many cases improve the performance of the algorithm. The use of perturbation techniques together with the construction of a convenient ordering equivalent to the target one lead to a further speed-up of the algorithm as shown in [49].

In [18], Collart and Mall analyze the relationship between the Gröbner fan and what they call the toric complex of an ideal and are able to provide new insights in this theory. Given a partial term ordering, a toric degeneration of an ideal is the ideal generated by the initial forms of the elements of the ideal with respect to an admissible partial term ordering. The toric complex of an ideal is defined as the collection of all toric degenerations of the ideal.

An thorough complexity analysis of the Gröbner walk algorithm is not yet known. One contribution in this direction has been given by Kalkbrener in [35]. The provided bound on the degrees of polynomials in adjacent Gröbner bases may be used for a local complexity analysis of the algorithm. Two cones are called adjacent if their intersection lies in a facet (that is a proper face of maximal dimension) of both cones. Kalkbrener demonstrates that the maximum degree of one basis can be at most quadratic in the maximum degree of the adjacent basis. Still, a doubly exponential lower bound on the degrees holds for non-adjacent bases.

Based on a result by Huyn ([34]), Kalkbrener shows that for every natural number m there exists a prime ideal P and two reduced Gröbner bases F and G of P such that F has bounded degree and cardinality $O(m)$ and

G has degree and cardinality at least 2^{2^m}. In [36] it is shown how for certain classes of ideals this behaviour may be explained by a conjecture in complexity theory.

Analogous to the notion of Gröbner fan of an ideal is the notion of state polytope of an ideal. Even though we will not present this theory here, we refer to [48] for an introduction to the topic.

After recalling some basic notions from convex geometry in Section 3.1, in Section 3.2 we introduce Gröbner cones for polynomial ideals. In Section 3.3 we demonstrate some properties of Gröbner fans following Robbiano's approach. In Section 3.4 the Gröbner walk algorithm is presented. Section 3.5 illustrates with an example how perturbation methods can speed up the walk. Our computations have been performed with the Gröbner walk implementation (see [3]) in CASA (see [32]). Finally, in Section 3.6 we present Kalkbrener's proof of the degree bound for adjacent Gröbner bases.

3.1 Some notions from convex geometry

In this section we recall some basic notions about convex sets in the Euclidean space and give the definition of polyhedral cones.

For vectors v, w in $\mathbb{R}^n$, viewed as the Euclidean space, denote by $v \cdot w$ the ordinary scalar product $v_1w_1 + \cdots + v_nw_n$ where $v = (v_1, \ldots, v_n)$, $w = (w_1, \ldots, w_n)$. Recall that the Euclidean distance between the points v and w in $\mathbb{R}^n$ equals

$$\|v - w\| = \sqrt{(v - w)^2}$$

and that $\mathbb{R}^n$ is endowed with the standard topology where the open sets are unions of open balls of center $v \in \mathbb{R}^n$ and radius $r \in \mathbb{R}_+$ given by $B(v, r) = \{w \in \mathbb{R}^n \mid \|v - w\| \leq r\}$.

If $V \subseteq \mathbb{R}^n$, the set of all linear combinations with nonnegative coefficients

$$\lambda_1 v_1 + \cdots + \lambda_k v_k$$

where $v_1, \ldots, v_k \in V$ and $\lambda_i \in \mathbb{R}$, $\lambda_i \geq 0$ for every $i = 1, \ldots, k$ is called the *positive hull* of V or the *cone* determined by V . If V is finite then we call the positive hull of V a *polyhedral cone* or simply a *cone.*

A set $V \subseteq \mathbb{R}^n$ is called *convex* if for any two elements $v, w \in V$ with $v \neq w$ the line segment

$$[v, w] := \{\lambda v + (1 - \lambda)w \mid 0 \leq \lambda \leq 1\}$$

is contained in V .

Observe that the cone of any set $V \subseteq \mathbb{R}^n$ is a closed convex set.

One can prove that a cone is polyhedral if and only if it is of the form $\{v \in \mathbb{R}^n \mid Av \leq 0\}$ for some matrix $A \in \mathbb{R}^{m \times n}$ (see [41]). If the cone C is given by $\{v \in \mathbb{R}^n \mid Av \leq 0\}$ then C is determined by a subset $\{v_1, \ldots, v_k\}$ of the set of solutions to the system $My = b$, where M consists of n linearly independent rows of $\begin{pmatrix} A \\ I \end{pmatrix}$ and $b = \pm e_j^T$ for some unit vector e_j.

We say that $v \in V \subseteq \mathbb{R}^n$ is in the *relative interior* of V, $v \in relint\, V$ if v is in the interior of the affine subspace generated by V (that is, there exists an open ball B entirely contained in the affine subspace generated by V and such that $v \in B$). By abuse of language, we call *interior* of a cone its relative interior.

For a fixed $u \in \mathbb{R}^n$, $u \neq 0$, and $\alpha \in \mathbb{R}$, the set $H := \{v \mid v \cdot u = \alpha\}$ is a hyperplane. $H^+ := \{v \mid v \cdot u \geq \alpha\}$ and $H^- := \{v \mid v \cdot u \leq \alpha\}$ are called the *half-spaces bounded by* H.

A hyperplane H is called a *supporting hyperplane* for a closed convex set $K \subseteq \mathbb{R}^n$ if $K \cap H \neq \emptyset$ and $K \subseteq H^+$ or $K \subseteq H^-$. If $K \subseteq H^+$ and $\alpha = 0$ then the origin $0 = (0, \ldots, 0)$ is called an *apex* of K.

Let $A \in \mathbb{R}^{m \times n}$ be the matrix representing the polyhedral cone C as the set $\{v \in \mathbb{R}^n \mid Av \leq 0\} \subseteq \mathbb{R}^n$ and denote by a_i its i-th row. Then C is the intersection of the half-spaces bounded by $H_i^- := \{v \mid v \cdot a_i \leq 0\}$ where the $H_i := \{v \mid v \cdot a_i = 0\}$ are supporting hyperplanes for C.

If H is a supporting hyperplane of the closed convex set K , we call $F := K \cap H$ a face of K.

The *dimension* of a convex set is defined as the dimension of the affine subspace generated by it.

Since a face of the closed convex set K is itself a closed convex set, one can speak about dimension of a face. A *proper face* is a face of dimension d where $0 < d < dim(K)$. A *facet* is a proper face of maximal dimension $d = dim(K) - 1$. A *vertex* is a face of dimension 0 and an *edge* is a face of

dimension 1.

More material on the combinatorics of convex sets can be found in as well as in [25] as well as in [10]. Convex sets are a basic tool in linear programming (see [40]).

3.2 Gröbner cones of an ideal

Say that two term orderings are equivalent if they give rise to the same oriented Gröbner basis. Then the set of real vectors that give rise to equivalent term orderings forms a polyhedral cone.

Let log be the map which associates to every monomial $cx_1^{d_1} \cdots x_n^{d_n}$ the n-tuple of its exponents $(d_1, \ldots, d_n)$. We define the *difference vectors* of f with respect to $\prec$ as

$$\delta_\prec(f) := \{log(f_\prec) - log(m) \mid m \in supp(f),\ m \neq f_\prec,\ m \not| f\}$$

For $F \subseteq K[x_1, \ldots, x_n]$ we define in an analogous way the set of difference vectors of F as the union of the sets of difference vectors of the polynomials in F

$$\delta_\prec(F) := \bigcap_{\delta \in F} \delta_\prec(f) \subseteq \mathbb{Z}^n$$

Example Let $f = 2x^2y + 3xyz + 4y^2 + 5y$ and let $\prec$ be the total degree lexicographic ordering with $x > y > z$. Then $\delta_\prec(f)$ is the set

$$\{(1, 0, -1), (2, -1, 0)\}$$

Note that the vector $(2, 0, 0) = log(2x^2y) - log(5y)$ is not in $\delta_\prec(f)$ since $y \mid x^2y$. //

Example If $G = \{yz^2 + 3t,\ xt^4 - y^3zt - y\}$ and $\prec$ is the total degree lexicographic ordering with $x > y > z > t$ then

$$\delta_\prec(G) = \{(0, 1, 2, -1), (1, -3, -1, 3), (1, -1, 0, 4)\}$$

is the set of difference vectors for G. //

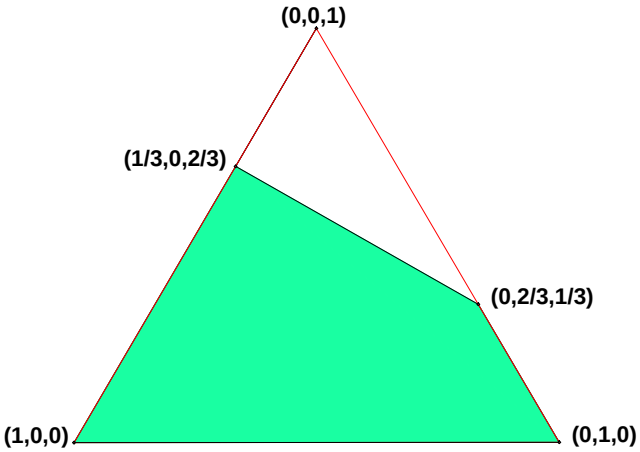


Figure 3.1: Cone of $\{\underline{xz^2},\ \underline{z^4},\ \underline{y^3z^2} - 5z^2,\ \underline{xy^4} - 5xy,\ \underline{x^4y} - 2z^2\}$

Given a set of vectors with real coordinates $V \subseteq \mathbb{R}^n$ denote by V^* the *polar cone* of V, i.e.

$$V^* := \{w \in \mathbb{R}^n \mid w \cdot v \geq 0\, \forall v \in V\}$$

Let $I \subseteq K[x_1, \ldots, x_n]$ be an ideal and G the reduced Gröbner basis of I with respect to a given term ordering $\prec$.

The (*restricted*) *Gröbner cone* of I with respect to $\prec$ is the set

$$C_\prec(I) := \delta_\prec(I)^* \cap \mathbb{R}^n_+$$

where $\mathbb{R}^n_+$ denotes the set of real vectors with non-negative coordinates.

Example Let $F = \{xy^2z^2,\ x^4y + xyz^2 - 2z^2,\ xy^4 - 5xy\}$, let $I \subseteq \mathbb{Q}[x, y, z]$ be the ideal generated by F and let $\prec$ be the total degree reverse lexicographic ordering with $x > y > z$.

We compute

$$G = \{\underline{xz^2},\ \underline{z^4},\ \underline{y^3z^2} - 5z^2,\ \underline{xy^4} - 5xy,\ \underline{x^4y} - 2z^2\}$$

the reduced Gröbner basis of I with respect to $\prec$ where the leading terms are underlined.

Then $\delta_\prec(G) = \{(4, 1, -2)\}$ and the Gröbner cone $C_\prec(I)$ is the set of vectors $\overline{w} = (w_1, w_2, w_3) \in \mathbb{R}^3_+$ satisfying

$$4w_1 + w_2 - 2w_3 \geq 0$$

Figure 3.1 shows the slice of the Gröbner cone of G cut out by the plane $x + y + z = 1$. The slice is a quadrilateral with vertices $(1, 0, 0)$, $(\frac{1}{3}, 0, \frac{2}{3})$, $(0, \frac{2}{3}, \frac{1}{3})$, and $(0, 1, 0)$. //

This one as well as the following drawings of cones' sections have been generated in Maple using the the `convex` package ([27]). A mathematical reference for the package is [52].

Example Let $G = \{\underline{yz^2} + 3t,\ \underline{xt^4} - y^3zt - y\}$ and $\prec$ the total degree lexicographic term ordering with $x > y > z > t$. One can verify that G is a reduced Gröbner basis with respect to $\prec$, hence the cone of the ideal I generated by G with respect to $\prec$ is given by the vectors $\overline{w} = (w_1, w_2, w_3, w_4) \in \mathbb{R}^4_+$ satisfying

$$\begin{cases} w_2 + 2w_3 - w_4 \geq 0 \\ w_1 - 3w_2 - w_3 + 3w_4 \geq 0 \\ w_1 - w_2 + 4w_4 \geq 0 \end{cases}$$

//

3.3 The Gröbner fan of an ideal

The Gröbner fan of an ideal is defined as the collection of all of its Gröbner cones. This collection is finite and its elements are in one-to-one correspondence with the oriented reduced Gröbner bases of the ideal.

We call the *(restricted) Gröbner fan* of an ideal and denote it by $F(I)$ the set

$$F(I) := \{C_\prec(I) \mid \prec \text{ is a term ordering}\}$$

In the next two lemmas we state some interesting properties of Gröbner cones.

Lemma Let G_1 and G_2 be two reduced Gröbner bases of the ideal $I \subseteq K[x_1, \ldots, x_n]$ with respect to the term orderings $\prec_1$ and resp. $\prec_2$. If $(G_1)_{\prec_1} = (G_2)_{\prec_1}$, then $G_1 = G_2$.

Proof We know that G_1 is a Gröbner basis of I with respect to $\prec_1$ if and only if $\langle (G_1)_{\prec_1} \rangle = \langle I_{\prec_1} \rangle$. But then since $(G_1)_{\prec_1} = (G_2)_{\prec_1}$, we also have $\langle (G_2)_{\prec_1} \rangle = \langle I_{\prec_1} \rangle$ and this implies that G_2 is also a Gröbner basis of I with respect to $\prec_1$. Hence $G_1 = G_2$ because of the uniqueness of the reduced Gröbner basis with respect to a given term ordering. //

Note that the converse of the previous lemma is in general not true. In fact there can be two reduced Gröbner bases which are equal as sets of polynomials and yet have different initial ideals. If one views Gröbner bases for an ideal as generating sets of reduction rules, it may occur that two reduced bases given by the same finite set of polynomials can give rise to different systems of reductions.

Call a Gröbner basis *oriented* if the leading terms of its polynomials are marked out. Then the previous lemma states a one-to-one correspondence between the set of oriented reduced Gröbner bases of an ideal and the Gröbner fan of the ideal. For each ideal there exist at most finitely many oriented reduced Gröbner bases since the Gröbner fan is finite. In order to prove that we need a further lemma.

Lemma Let G_1 and G_2 be two reduced Gröbner bases of the ideal $I \subseteq K[x_1, \ldots, x_n]$ with respect to the term orderings $\prec_1$ and, respectively, $\prec_2$. Then, if $(G_1)_{\prec_1} \neq (G_2)_{\prec_2}$, at least one term in $(G_2)_{\prec_2}$ is not divisible by any of the terms in $(G_1)_{\prec_1}$, that is it belongs to $S(G_1)$.

Proof Let $G_1 = \{g_1, \ldots, g_r\}$ and $G_2 = \{h_1, \ldots, h_s\}$. By contradiction, assume that for every $j = 1, \ldots, s$ there exists $t_j \in T^n$ such that $(h_j)_{\prec_2} = t_j(g_{i_j})_{\prec_1}$for some $i_j \in \{1, \ldots, r\}$.

If $t_j = 1$ for every $j \in \{1, \ldots, s\}$ and $r = s$ then we have $G_1 = G_2$ by the previous lemma.

If $t_j = 1$ for every $j \in \{1, \ldots, s\}$ and $r \neq s$ then it cannot be that $s > r$ otherwise G_2 would not be reduced. Let us then assume that $s < r$. Then

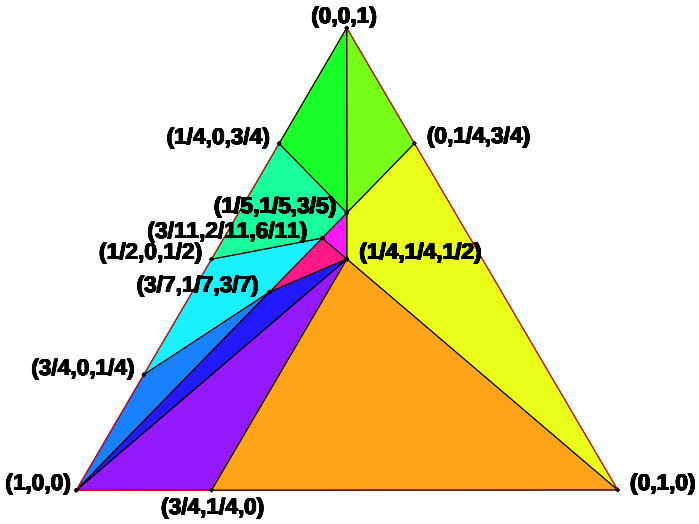


Figure 3.2: The Gröbner fan of $\{x^3 + xz - 2z,\ y^3 - xz\}$

there exists at least one $k \in \{1, \ldots, r\}$ such that $(g_k)_{\prec_1} \neq (h_j)_{\prec_2}$. But then one can prove that $g_k \notin \langle G_2 \rangle$, thus obtaining a contradiction. To prove that, just observe that g_k is irreducible with respect to G_2 by the hypothesis that G_1 is reduced and the assumption that $(G_2)_{\prec_2} \neq (G_1)_{\prec_1}$, i.e. the initial terms in G_2 with respect to $\prec_2$ are a subset of the initial terms of G_1 with respect to $\prec_1$ and hence $S(G_1) \subset S(G_2)$.

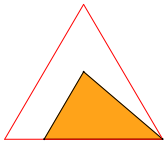
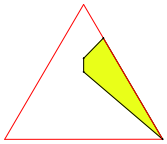
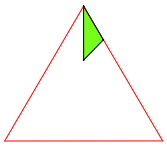
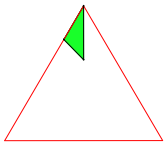
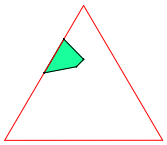
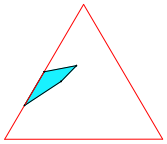
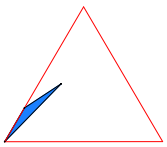
We can therefore assume that there exists a $j \in \{1, \ldots, s\}$ and $1 \neq t_j \in T^n$ such that $(h_j)_{\prec_2} = t_j(g_{i_j})_{\prec_1}$.

But then the polynomial $g_{i_j} \in G_1$ is in $\langle G_1 \rangle$ but not in $\langle G_2 \rangle$ since it is irreducible with respect to $\prec_2$. //

It can be proven that the Gröbner fan of an ideal is finite. For a proof of this result see [43]p. 193, Lemma 2.6.

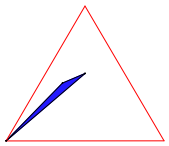
Example

Let $F = \{x^3 + xz - 2z,\ y^3 - xz\}$. Then the Gröbner fan of $I = \langle F \rangle$ consists of the following 11 cones $C_1, \ldots, C_{11}$ where for each cone a matrix representing the term ordering and the reduced Gröbner basis is shown:

Cone	Order matrix	Gröbner basis	Slice of cone
C_1	$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$	$\underline{y^3} - xz$ $\underline{x^3} + xz - 2z$	
C_2	$\begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$\underline{xz} + x^3 + -2z$ $\underline{y^3} + x^3 - 2z$	
C_3	$\begin{pmatrix} 1 & 1 & 3 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$	$\underline{z} - \frac{1}{2}y^3 - \frac{1}{2}x^3$ $\underline{xy^3} + x^4 - 2y^3$	
C_4	$\begin{pmatrix} 1 & 1 & 3 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$	$\underline{z} - \frac{1}{2}y^3 - \frac{1}{2}x^3$ $\underline{x^4} + xy^3 - 2y^3$	
C_5	$\begin{pmatrix} 3 & 2 & 6 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$	$\underline{x^3} + y^3 - 2z$ $\underline{xz} - y^3$ $\underline{z^2} - \frac{1}{2}zy^3 - \frac{1}{2}x^2y^3$	
C_6	$\begin{pmatrix} 2 & 1 & 3 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$\underline{xz} - y^3$ $\underline{x^3} + y^3 - 2z$ $\underline{zy^3} - 2z^2 + x^2y^3$ $\underline{z^3} - \frac{1}{2}z^2y^3 - \frac{1}{2}xy^6$	
C_7	$\begin{pmatrix} 10 & 1 & 5 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$	$\underline{xz} - y^3$ $\underline{xy^6} + z^2y^3 - 2z^3$ $\underline{z^4} - \frac{1}{2}z^3y^3 - \frac{1}{2}y^9$ $\underline{zy^3} - 2z^2 + x^2y^3$ $\underline{x^3} + y^3 - 2z$	

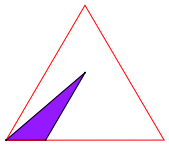
C_8 $\begin{pmatrix} 1 & 1 & 2 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

$\underline{xz} - y^3$
$\underline{x^3} + y^3 - 2z$
$\underline{x^2y^3} + zy^3 - 2z^2$
$\underline{xy^6} + z^2y^3 - 2z^3$
$\underline{z^3y^3} - 2z^4 + y^9$



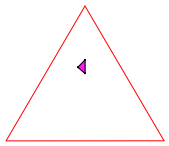
C_9 $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

$\underline{y^9} + z^3y^3 - 2z^4$
$\underline{xz} - y^3$
$\underline{xy^6} + z^2y^3 - 2z^3$
$\underline{x^2y^3} + zy^3 - 2z^2$
$\underline{x^3} + y^3 - 2z$



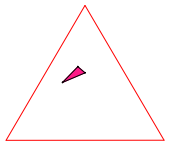
C_{10} $\begin{pmatrix} 1 & 1 & 3 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$

$\underline{x^3} + y^3 - 2z$
$\underline{xz} - y^3$
$\underline{zy^3} - 2z^2 + x^2y^3$



C_{11} $\begin{pmatrix} 3 & 2 & 6 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$

$\underline{xz} - y^3$
$\underline{x^3} + y^3 - 2z$
$\underline{x^2y^3} + zy^3 - 2z^2$
$\underline{z^2y^3} - 2z^3 + xy^6$



//

3.4 The Gröbner walk algorithm

Given a Gröbner basis with respect to a starting term ordering, the Gröbner walk algorithm provides a method for obtaining a Gröbner basis for a given target ordering without having to use Buchberger's algorithm for the whole ideal.

The Gröbner walk algorithm is based on two crucial properties of Gröbner fans:

- since the Gröbner fan is finite one can reach a target ordering in finitely many steps by choosing a distinct cone at each step
- when stepping into a new cone it is not necessary to perform a full Gröbner basis computation, but instead one can compute a Gröbner

basis for a smaller ideal (the initial ideal with respect to some partial term ordering) and then lift it to a Gröbner basis of the new cone by performing polynomial operations

The main result that allows to avoid the computation of a new Gröbner basis when stepping on distinct cones of the Gröbner fan is contained in the following lemma.

Let $\triangleleft$ be a partial term ordering on the set of term T^n. We have seen in Section 2.5 that for every partial term ordering $\triangleleft$ and for every ideal $I \subseteq K[x_1, \ldots, x_n]$ there exists $\omega \in \mathbb{R}^n_+$ such that $\langle I_\triangleleft \rangle = \langle I_\omega \rangle$.

Lemma Let $\prec_1$ and $\prec_2$ be two term orderings whose cones contain a common weight vector ω. Let $G = \{g_1, \ldots, g_r\}$ be the reduced Gröbner basis of I with respect to $\prec_1$ and $H = \{h_1, \ldots, h_s\}$ the reduced Gröbner basis of $\langle I_\omega \rangle$ with respect to $\prec_2$. Then

- $(\forall i \in 1, \ldots, s)\ h_i = \sum_{j=1}^{r} h_{ij} in_\omega(g_j)$ with $h_{i1}, \ldots, h_{ir}$ ω -homogeneous
- $\{f_1, \ldots, f_s\}$ where $f_i = \sum_{j=1}^{r} h_{ij} g_i$ is a Gröbner basis of I with respect to $\prec_2$.

Proof We will start by showing that G_ω is a Gröbner basis of I_ω with respect to $\prec_1$.

According to the preceeding definition of Gröbner basis it suffices to show that $\langle (I_\omega)_{\prec_1} \rangle = \langle (G_\omega)_{\prec_1} \rangle$. Since $\prec_1$ refines ω, for every polynomial f $in_{\prec_1}(in_\omega(f)) = in_{\prec_1}(f)$, therefore $(G_\omega)_{\prec_1} = G_{\prec_1}$ and $(I_\omega)_{\prec_1} = I_{\prec_1}$.

Since G_ω is a Gröbner basis of I_ω with respect to $\prec_1$ we can compute $\omega-$homogeneous polynomials $h_{i1}, \ldots, h_{ir}$ such that $h_i = \sum_{j=1}^{r} h_{ij} in_\omega(g_j)$ and $deg_\omega(h_i) = deg_\omega(h_{ij} in_\omega(g_j))$. Note that the S-polynomial of two ω -homogeneous forms is itself a ω -homogeneous. Also, reducing a ω -homogeneous polynomial by a ω -homogeneous polynomial results in a ω -homogeneous polynomial.

Finally, the set $F = \{f_1, \ldots, f_s\}$ where $f_i = \sum_{j=1}^{r} h_{ij} g_j$ is a Gröbner basis of I with respect to $\prec_2$. In fact $\langle F_{\prec_2} \rangle = \langle I_\omega \rangle_{\prec_2} = \langle I_{\prec_2} \rangle$. //

From proof of the lemma we see that, given two term orderings $\prec_1$ and $\prec_2$, a weight vector ω in the intersection of their cones, and the reduced Gröbner basis G of I with respect to $\prec_1$, the computation of a Gröbner F of I with respect to $\prec_2$ requires the following steps

- extraction of the ω-homogeneous initial forms of the polynomials in G
- computation of a Gröbner basis H of G_ω with respect to $\prec_2$
- computation of the normal forms with respect to G_ω and $\prec_1$of the polynomials in H
- lifting H to a Gröbner basis F with respect to $\prec_2$ by forming linear combinations of the polynomials in G with the h_{ij} as coefficients
- auto-reduce F

Given an ordering $\prec_1$ and the corresponding cone $C_{\prec_1}(I)$ we want to step into a new cone that does not coincide with $C_{\prec_1}(I)$ by choosing an appropriate term ordering $\prec_2$. We have seen in the previous section that the criterion for deciding the equality of two cones is given by

$$C_{\prec_2}(I) = C_{\prec_1}(I)$$

if and only if

$$in_{\prec_2}(g) = in_{\prec_1}(g)$$

for every g in the reduced $\prec_1$-Gröbner basis of I .

Therefore, in order to step out of C_1, it suffices to choose a term ordering $\prec_2$ for which at least one of the initial monomials in G changes.

Assume now we are given a Gröbner basis for the term ordering $\prec_1$ and we want to compute a Gröbner basis with respect to a given term ordering $\prec_2$ by using the properties of the Gröbner fan of the ideal. Assume that we are given vectors $\sigma, \tau \in \mathbb{R}^n_+$ such that $\prec_1$ is a refinement of σ and $\prec_2$ a refinement of τ.

Let ω be a weight vector on the line segment

$$\sigma\tau = \{(1-t)\sigma + t\tau \mid 0 \leq t \leq 1 \text{ where } \sigma,\ \tau \in \Omega^n\}$$

such that

$$t \in \{s \in Q \cap (0,1] \mid in_\omega(g) = in_{\prec_1}(g) + m, m \in supp(g - in_{\prec_1}(g)), deg(m) > 0\}$$

Note that there can be more than one term m satisfying the condition above, hence one can have several ω to choose from. Speaking in terms of cones, one just needs to pick a point on a face of the cone in order to get out of that cone, but no restriction is given neither on the choice of the face nor on the choice of the point. We will see in the next section how the choice of the next weight vector influences the efficiency of the algorithm.

Once we have picked the next weight vector ω, we refine it to a term ordering by taking $\prec_\omega$ as the concatenation of ω and $\prec_2$ (see Section 2.4).

The Gröbner walk algorithm

Input: $\prec_1$ and $\prec_2$ term orderings refining the weight vectors ω and, respectively, τ

G Gröbner basis with respect to $\prec_1$.

Output: G reduced Gröbner basis with respect to $\prec_2$

Loop

1. $G_\omega \longleftarrow$ initials forms of G with respect to ω
2. $\omega \longleftarrow$ next weight vector $\omega + t(\tau - \omega)$
3. if c is undefined then return G
4. $G_\omega \longleftarrow$ Gröbner basis of G_ω with respect to $\prec_\omega := (\omega \mid \prec_2)$
5. $G \longleftarrow$ lift G_ω
6. $G_\omega \longleftarrow$ interreduce G //

3.5 Walking faster

In this section we show how the Gröbner walk algorithm can be modified in order to avoid costly computations. Each step in the algorithm requires the computation of a Gröbner basis for a quasi-homogeneous ideal. Since no optimal path is prescribed by the algorithm, one may at each step perturb the path so that the polynomials in the quasi-homogeneous ideal are as small as possible. In order to keep the intermediate bases as small as possible, the points to avoid are precisely those where more than two cones intersect. At these points, in fact, the quasi-homogeneous initial forms generally consist of more monomials than at point where only two cones intersect.

Path perturbation may be carried out

- globally, by perturbing the initial and final data, as long as one remains within the prescribed cones
- locally, by perturbing the intermediate data even though this might lead to taking more steps

When applying a global perturbation, it is always possible to perturb the final data remaining within the target cone by choosing a special term ordering that depends on the known degree bounds for polynomials in Gröbner bases.

Note that global as well as local perturbation may lead to a walk consisting of more steps, but since at each step computations may be carried out much faster, this strategy results generally in a speedup of the algorithm.

Furthermore, one may speed up the computations of the intermediate Gröbner bases by exploiting the properties of the underlying initial ideals.

3.5.1 Path perturbation

In order to illustrate the technique of path perturbation we will look at an example in three variables in order to be able to visualize the Gröbner fan.

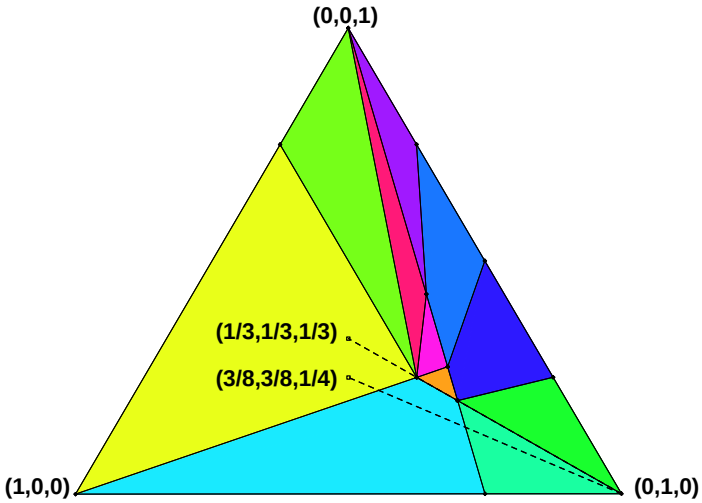


Figure 3.3: Gröbner fan for $I = \langle z^3 - yz - 2y,\ x^3 - yz \rangle$

Example Let $F = \{z^3 - yz - 2y, x^3 - yz\}$ be a set of polynomials. The set F is also the reduced Gröbner basis of $I = \langle F \rangle$ with respect to the total degree reverse lexicographic ordering represented by the matrix $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}$. Assume we want to convert G to a Gröbner basis with respect to the pure lexicographic ordering with $y > x > z$, represented by the matrix $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

In Figure 3.3 the slice of the Gröbner fan of I cut out by the plane $x+y+z = 1$ is pictured. One can see that the cone containing $(1, 1, 1)$ has no common face (except for the apex $(0, 0, 0)$) with any of the two cones containing $(0, 1, 0)$. Furthermore, the segment that joins $(\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$ with $(0, 1, 0)$ goes through two points of intersection of several cones. On the pictured slice, these are the points $(\frac{1}{4}, \frac{1}{2}, \frac{1}{4})$ where 6 cones intersect, and $(\frac{1}{5}, \frac{3}{5}, \frac{1}{5})$ where 5 cones intersect. If one would step out of the initial cone by following the straight path leading from $(\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$ to $(0, 1, 0)$, one would have to compute the following Gröbner bases of quasi-homogeneous ideals:

$$\begin{array}{cll} \langle z^3 - yz,\ x^3 - yz\rangle & \text{corresponding to weight} & (\frac{1}{4}, \frac{1}{2}, \frac{1}{4}) \\ \langle z^3 - 2y + x^3,\ yz,\ yx^3 - 2y^2 + x^3z^3\rangle & \text{corresponding to weight} & (\frac{1}{5}, \frac{3}{5}, \frac{1}{5}) \end{array}$$

If one perturbs the initial weight and takes for instance weight $(\frac{3}{8}, \frac{3}{8}, \frac{1}{4})$ - that one can see is still in the initial cone - then the walk requires the computation of Gröbner bases for the following initial ideals:

$$\begin{array}{cll} \langle z^3 - yz,\ x^3\rangle & \text{corresponding to weight} & (\frac{2}{5}, \frac{2}{5}, \frac{1}{5}) \\ \langle yz + z^3 - 2y,\ x^3 + z^3 - 2y\rangle & \text{corresponding to weight} & (\frac{3}{14}, \frac{9}{14}, \frac{1}{7}) \end{array}$$

Thus, by perturbing the initial weight we have obtained in the first step an ideal that consists of one monomial and one binomial, whereas in the first step of the non-perturbed path we would an ideal generated by two binomials. For the second step there is no gain as far as the number of terms in the generators of the quasi-homogeneous ideal are concerned. //

In general, let M be an $n \times n$ matrix representing a term ordering $\prec$ on T^n and G a Gröbner basis with respect to $\prec$. We will assume that M has entries in $\mathbb{N}_+$(this is not a restriction since it is always possible to find such a matrix for any term ordering). Let $C_\prec$be the cone of $\prec$ for the ideal generated by G. Then $C_\prec$ contains the first row r_1 of M. Then, for ϵ sufficiently small, if we may perturb r_1 by ϵr_2 remaining within the cone. Such an ϵ has to satisfy

$$\tfrac{1}{\epsilon} > tdeg(g)\, max(r_2) \text{ for every } g \in G$$

where $tdeg(g) := max\{\sum_{i=1}^n d_i \mid x_1^{d_1} \cdots x_n^{d_n} \text{is a term in } g\}$ and with $max(r_2)$ we denote the maximum value among the coordinates of r_2.

If r_1 lies on a face F_1 of dimension d of the cone, in general $r_1 + \epsilon r_2$ will lie on a face F_2 of dimension $d+1$ that contains F_1. Perturbing by the third row of M, we get a vector $r_1 + \epsilon r_2 + \epsilon^2 r_3$ that is contained in a $d+3$-dimensional open set of the cone, provided that

$$\tfrac{1}{\epsilon} > tdeg(g)(max(r_2) + max(r_3) \text{ for every } g \in G$$

One can continue in this fashion until a maximally perturbed vector is obtained

$$r_1 + \epsilon r_2 + \epsilon^2 r_3 + \cdots + \epsilon^{n-1} r_n$$

This perturbed vector lies within the cone, and hence does not belong to any other cone.

In a similar way, one may perturb the final weight vector. In our example, one would have to choose a point close to $(0, 1, 0)$. If one chooses a vector with positive entries, then the last step requires a Gröbner basis computation with respect to a degree-compatible ordering, which is easier than the computation of a Gröbner basis with respect to a lexicographic ordering.

The drawback of perturbing the target weight vector is that one does not know in advance how the final cone looks like, hence it might be that the perturbed vector lies outside of the target cone. In this case, one might either undo the perturbation and repeat the last step or proceed on on the perturbed path until the target cone is reached.

For pure lexicographic orderings, Tran ([49]) shows that a weight vector with positive entries that lies within the target cone can always be determined a priori.

Let $\prec$ be the pure lexicographic term ordering with $x_1 < x_2 < \cdots < x_n$ on the ring of polynomials in n variables and let $I \subseteq K[x_1, \ldots, x_n]$ be an ideal. Then, given an upper bound D for the degree of the polynomials in any Gröbner basis of I, one can determine a priori a weight vector whose refinement gives the desired lexicographic ordering. Namely, the weight

$$\omega = (D^{n-1}, D^{n-2}, \ldots, 1)$$

represents the Gröbner cone $C_{\prec}(I)$. Note that if d is the maximum total degree of the polynomials that generate the ideal, then for any Gröbner basis $D = (d^2 + 2d)^{2^{(n-1)}}$ (see [23]). For zero-dimensional ideals the bound is given by $D = d^{O(n)}$.

3.5.2 Exploiting properties of intermediate bases

One of the most costly parts of the Gröbner walk algorithm is the computation of Gröbner bases for initial ideals at each step on the path. There are yet some special properties of these ideals that may be exploited in order to optimize Buchberger's algorithm.

One first observation is that among the generators of the initial ideals there is a higher number of monomials than in random ideals. Since the S-polynomial of two monomials is always 0, one does not need to process such S-polynomials. By creating two distinct lists for monomials and true polynomials, one may furthermore reduce the time for creating critical

pairs. In fact, if the list of true polynomials contains p elements, and the list of monomials q elements, one just needs to form $\frac{p(p-1)}{2} + pq$ critical pairs, skipping $\frac{q(q-1)}{2}$ pairs. Note that since the polynomials in the initial ideals are in general short, their reduction is relatively cheap, hence the creation of critical pairs takes up most of the time in the Gröbner basis computation.

As far as skipping of unnecessary S-polynomials is concerned, just Buchberger's first criterion is useful in this case, while searching for a third polynomial in order to apply the second criterion takes generally more time than reducing the two polynomials.

Due to the presence of monomials among the generators, it is convenient to use those first when carrying out a reduction to normal form. Reducing by a monomial in fact results in a cancellation of the monomial in the polynomial being reduced, thus making the polynomial shorter.

3.6 Degree bound for adjacent Gröbner bases

When two cones in the Gröbner fan are adjacent, the initial ideal corresponding to a weight vector on the ciommon face of the two ideals is not only $\lhd$-homogeneous but it is also quasi-homogeneous. This property allows to construct a bound for polynomials in two Gröbner bases corresponding to adjacent cones. The bound gives a measure of the local complexity of the Gröbner walk algorithm.

Two cones in the Gröbner fan are called adjacent if they have a face in common that has maximal dimension. Then one can prove that the degrees of polynomials in the Gröbner bases on two adjacent cones can not differ too much, namely for any two Gröbner bases G_1, G_2 on adjacent cones in the polynomial ring in n variables, the following inequality holds:

$$deg(G_2) < 2deg(G_1)^2 + (n+1)deg(G_1)$$

This result also explains why the computation of intermediate Gröbner bases is so fast, since one mostly walks on adjacent cones.

For our presentation we follow the article by Kalkbrener ([35]).

The Gröbner walk algorithm requires at each step the computation of a Gröbner basis in a cone that has a face in common with the previous cone,

for which a Gröbner basis is already known. An interesting question to ask is how much the degrees of the polynomials in the two Gröbner bases may differ. Kalkbrener presents a quadratic bound for Gröbner bases of cones whose intersection is a face of maximal dimension.

Let $I \subseteq K[x_1, \ldots, x_n]$ be an ideal and $\prec_1$, $\prec_2$ term orderings such that $C_{\prec_1}(I) \neq C_{\prec_2}(I)$. Then $C_{\prec_1}(I)$ and $C_{\prec_2}(I)$ are called *adjacent* if $C_{\prec_1}(I) \cap C_{\prec_2}(I)$ has dimension $n-1$.

For a set of polynomials $G \subseteq K[x_1, \ldots, x_n]$ denote by

$$deg(G) := max\{deg(g) \mid g \in G\}$$

Let us now state the main result of the paper by Kalkbrener.

Proposition Let G_1 and G_2 be the reduced Gröbner bases of I with respect to $\prec_1$ and $\prec_2$ respectively such that the cones $C_{\prec_1}(I)$ and $C_{\prec_2}(I)$ are adjacent. Then the following inequality holds

$$deg(G_2) < 2deg(G_1)^2 + (n+1)deg(G_1)$$

In the rest of the section we will sketch the main steps of the proof.

Denote by H the hyperplane that contains the common face of $C_{\prec_1}(I)$ and $C_{\prec_2}(I)$. Then H can be represented as the $n-1$ dimensional variety of a linear form

$$a_1\xi_1 + \cdots + a_n\xi_n$$

We first observe that H cannot be a boundary face of the positive orthant of $\mathbb{R}^n$.

Remember that for an ideal I and a term ordering $\prec$, we defined the Gröbner cone of I with respect to $\prec$ as $C_\prec(I) := \delta_\prec(I)^* \cap \mathbb{R}^n_+$. Hence $C_\prec(I)$ is contained in the positive orthant of $\mathbb{R}^n$.

Let F_1 be the $n-1$-dimensional face of $C_{\prec_1}(I)$ that lies in H, F_2 the $n-1$-dimensional face of $C_{\prec_2}(I)$ that lies in H, and $\omega \in F_1 \cap F_2$. Then $H^+ = \{v \in \mathbb{R}^n_+ \mid v \cdot \omega \geq 0\}$ and $H^- = \{v \in \mathbb{R}^n_+ \mid v \cdot \omega \leq 0\}$ are the half-spaces bounded by H and without loss of generality we may assume that $C_{\prec_1}(I) \subseteq H^+$ and $C_{\prec_2}(I) \subseteq H^-$. But then H cannot be a boundary face of the positive orthant of $\mathbb{R}^n$, that is the variety of ξ_j for some $0 \leq j \leq n$. In fact, if H were given by $\xi_j = 0$ then there would exist a vector $\omega =$

$(\omega_1, \ldots, \omega_{j-1}, 0, \omega_{j+1}, \ldots, \omega_n) \in F_1 \cap F_2 \subset \mathbb{R}^n_+$ and since for every $w \in C_{\prec_2}$ we have $w \cdot \omega \leq 0$ then, since $w \in \mathbb{R}^n_+$, it must be $w_i = 0$ for every $i \neq j$, that is $C_{\prec_2}$ has dimension ≤ 1.

Based on this observation we can now prove the following lemma.

Lemma If $C_{\prec_1}(I)$ and $C_{\prec_2}(I)$ are adjacent cones in the fan of the ideal I, then there exists $\omega \in C_{\prec_1}(I) \cap C_{\prec_2}(I)$ with positive coordinates.

Proof Let $a_1\xi_1 + \cdots + a_n\xi_n$ be the linear form defining the $n-1$ dimensional variety H such that $C_{\prec_1}(I) \cap C_{\prec_2}(I) \subseteq H$. Since it cannot be that $a_1 = \cdots = a_n = 0$ because otherwise it would be $H = \mathbb{R}^n$ and $dim(H) = n$, we may assume without loss of generality that $a_n \neq 0$. Let $\omega = (\omega_1, \ldots, \omega_n) \in C_{\prec_1}(I) \cap C_{\prec_2}(I)$. Take $\omega_1 = 1, \ldots, \omega_{n-1} = 1$. Then, since $\omega \in H$, we have $a_1 + \cdots + a_{n-1} + \omega_n a_n = 0$ and since $a_n \neq 0$ we can write $\omega_n = -\frac{a_1 + \cdots + a_{n-1}}{a_n}$. If $\omega_n > 0$ then we have found the desired ω with positive coordinates. Otherwise, let $\omega_n = 0$. Then it must be $a_1 + \cdots + a_{n-1} = 0$. Since it cannot be that $a_1 = \cdots = a_n = 0$ because otherwise H would be the hyperplane $\xi_n = 0$, there must be an $a_j > 0$ for some $1 \leq j \leq n-1$. Assume that $a_{n-1} > 0$ (if $a_{n-1} < 0$ we can always take H to be defined by $-a_1\xi_1 - \cdots - a_n\xi_n$). Then one there exists $\epsilon > 0$ sufficiently small such that $1 - \epsilon a_n > 0$ and $\omega = (1, \ldots, 1, 1 - \epsilon a_n, \epsilon a_{n-1})$ is the desired vector with positive coordinates. //

The hyperplane H containing the common face of the cones $C_{\prec_1}(I)$ and $C_{\prec_2}(I)$ is the variety of $a_1\xi_1 + \cdots + a_n\xi_n$ such that

- $a_1, \ldots, a_n$ are integers
- $gcd(a_1, \ldots, a_n) = 1$
- at least one of the $a_i$is positive
- at least one of the $a_i$is negative

Without loss of generality we may reorder the variables so that there exists $l \in \{1, \ldots, n-1\}$ such that $a_i > 0$ for $1 \leq i \leq l$ and $a_j \leq 0$ for $l+1 \leq j \leq n$.

Let

$$s = \prod_{i=0}^{l} x_i^{a_i} \text{ and } t = \prod_{j=l+1}^{n} x_i^{-a_i}$$

Let $R \subseteq T^n$ be the set of terms that are neither divisible by s nor by t. For every $k \in \mathbb{N}$ and for every $r \in R$ define

$$E_{r,k} = \{rs^i t^{k-i} \mid i \in \{0, \ldots, k\} \text{ and } E_r = \bigcup_{k \in BBN} E_{r,k}$$

Then

- $\bigcup_{r \in R} E_{r,k} = T^n$
- $E_{r_1} \cap E_{r_2} = \emptyset$ for $r_1, r_2 \in R$ with $r_1 \neq r_2$
- for every $r \in R$ the function ψ defined by $\psi(rs^i t^j) = x_0^i x_1^j$ is an order isomorphism between the posete E_r and T^2

By showing that for every $r \in R$ and every $k \in \mathbb{N}$ the set $E_{r,k}$ is an equivalence class, proving the bound for T^n can be reduced to constructing a bound in T^2.

Consider the partial term ordering $\lhd$ given by the vector $\omega \in C_{\prec_1}(I) \cap C_{\prec_2}(I)$ with positive coordinates. Let J be the ideal $I_\lhd = I_\omega$. Then we have $\langle I_{\prec_1} \rangle = \langle J_{\prec_1} \rangle$ and $\langle I_{\prec_2} \rangle = \langle J_{\prec_2} \rangle$. By applying the results from Section 2.6 we know that $(K[x_1, \ldots, x_n]/J)_{=_\lhd w}$, $(K[x_1, \ldots, x_n]/J_{\prec_1})_{=_\lhd w}$, and $(K[x_1, \ldots, x_n]/J_{\prec_2})_{=_\lhd w}$ have the same dimension.

Hence $(K[x_1, \ldots, x_n]/I_{\prec_1})_{=_\lhd w}$ and $(K[x_1, \ldots, x_n]/I_{\prec_2})_{=_\lhd w}$ have the same dimension.

But $(K[x_1, \ldots, x_n]/I_{\prec_1})_{=_\lhd w}$ and $(K[x_1, \ldots, x_n]/I_{\prec_2})_{=_\lhd w}$ are antichains in T^n with respect to the "divides" order relation. Then the bound is proven once one can show that if A and B are antichains in T^nsuch that for every degree $d \in \mathbb{N}$ the number of elements of $\langle A \rangle$ of degree d equals the number of elements of $\langle B \rangle$ of multidegree d

$$deg(B) < 2deg(A)^2 + (n+1)deg(A)$$

Let us look at what happens in the case of antichains in T^2. Let A, B be antichains in T^2 such that for every $d \in \mathbb{N}$

$$\mid \{a \in \langle A \rangle \mid deg_\omega(a) = d\} \mid = \mid \{b \in \langle B \rangle \mid deg_\omega(b) = b\} \mid$$

Let t be the least common multiple of the elements of A. Then $deg(t) \leq 2deg(A)$ and for each $i > 2deg(A)$ the cardinality of $\nabla_d(A) =\mid \{a \in \langle A \rangle \mid deg_\omega(a) = d\} \mid$ is constant. For $i > 2deg(A)$ we have

$$\nabla_d(A) = \nabla_d(B) = \nabla_{d+1}(B) = \cdots$$

This means that there cannot be any term in B of degree greater than $2deg(A)$, otherwise it would be $\nabla_{d+1}(B) < \nabla_d(B)$.

Chapter 4

The FGLM algorithm

The FGLM algorithm is a method for change of orderings by means of linear algebra techniques. The method applies to Gröbner bases of zero-dimensional ideals, that are ideals whose underlying polynomial systems have finitely many common solutions.

When the polynomial system generating a zero-dimensional ideal is in triangular form, one can compute its solutions by solving univariate polynomial equations. Lexicographic orderings yield Gröbner bases with the desired triangular shape, yet they are known to have the worst computational complexity among all term orderings.

By employing the FGLM algorithm, the computation of a lexicographic Gröbner basis may be reduced to the computation of a Gröbner basis with respect to a degree-compatible ordering whose time complexity is known to be $d^{O(n^2)}$, where d is the maximum degree of the input polynomials and n the number of variables.

The FGLM algorithm is based on the observation that polynomials may be regarded as a linear combinations of terms with coefficients in the ground field K. Analogously, the ring of polynomials may be regarded as a vector space of infinite dimension generated by the terms in T^n and with coefficients in K.

This has suggested to use linear algebra techniques to solve problems in the ring of polynomials and led to the algorithm presented in [26], named FGLM after its autors, Faugère, Gianni, Lazard, and Mora.

The residue class ring of an ideal is a vector subspace of the ring of

polynomials. If the polynomials that generate the ideal have finitely many common roots, then the residue class ring of the ideal is finitely generated as a vector space. Whenever the residue class ring of an ideal is finitely generated, the ideal is called *zero-dimensional*.

Any Gröbner basis of an ideal gives as a by-product a set of terms that is a generating set for the residue class ring, viewed as a vector space. This set of terms, called a *staircase*, not only generates the residue class ring but it is also its canonical basis. Reducing a polynomial to its normal form with respect to a Gröbner basis is nothing else than representing the polynomial as combination of terms from the canonical basis.

In the case of a zero-dimensional ideal, the staircase is a finite set. Since finiteness of the staircase does not depend on the ordering chosen for computing the Gröbner basis, it suffices to compute any Gröbner basis to decide if the ideal is zero-dimensional.

The main idea of the FGLM algorithm is to compute a staircase for the new ordering by finding linear dependencies between terms. These dependencies not only give the shape of the new staircase but also yield the polynomials in the new basis. Linear algebra is used to compute dependencies between terms. The finiteness property of the vector space guarantees termination of the algorithm.

The material in this chapter is arranged as follows. In Section 4.1 we present the FGLM algorithm and give an informal proof of its correctness. The finite vector-space structure of the residue class ring allows a detailed complexity analysis of the FGLM algorithm. This is presented in Section 4.2. All material presented in sections 4.1 and 4.2 is derived from [26].

Generalisations of the FGLM algorithm for positive-dimensional ideals have been proposed by Mora and Licciardi ([39]) and by Kapur and Saxena ([37]). Both methods require a sequence of transformations, where each transformation is carried out by means of linear algebra. We discuss these methods in section 4.3.

4.1 The algorithm for zero-dimensional ideals

The FGLM algorithm is an alternative method to the Gröbner walk for change of orderings devised for zero-dimensional polynomial ideals. Given a Gröbner basis with respect to some ordering, the Gröbner basis with

respect to a given target ordering is computed without using Buchberger's algorithm. The polynomials in the new basis are computed by means of linear algebra, by looking for special linear dependencies among polynomials. Termination of the algorithm is guaranteed by the fact that the ideal is zero-dimensional.

The FGLM algorithm for zero-dimensional ideals is based on the following key ideas:

- the residue class ring with respect to an ideal may be viewed as a vector space
- for zero-dimensional ideals, residue class rings are finitely generated and any Gröbner basis provides a canonical vector-space basis
- the elements that are not in the vector-space basis are linearly dependent from the elements in the basis, and the dependency relations give polynomials in the Gröbner basis

In this section we will describe the algorithm in detail. A proof of its correctness may be found in [26].

Let G be a Gröbner basis of an ideal $I \subseteq K[x_1, \ldots, x_n]$. For the sake of conciseness we will denote by $In(G)$ the set of initial terms of G whenever the underlying term ordering is clear from the context. Recall that the set

$$S(G) = \{t \in T^n \mid t \text{ is not a multiple of any term in } In(G)\}$$

is a linearly independent vector space basis of $K[x_1, \ldots, x_n]/\langle G\rangle$ called the *staircase* of G.

Figure 4.1 shows $S(G)$ (not-filled dots) and $In(G)$ (grey-filled dots) for the case of two variables x, y where the coordinates of the points in the grid are pairs of exponents of terms.

Let $I \subseteq K[x_1, \ldots, x_n]$ be an ideal and G its Gröbner basis with respect to some term ordering. Then the following conditions are equivalent

- $S(G)$ is a finite set
- $K[x_1, \ldots, x_n]/\langle G\rangle$ is a finite-dimensional vector space over K
- the variety $V(I)$ over $\overline{K}$, the algebraic closure of K, is a finite set

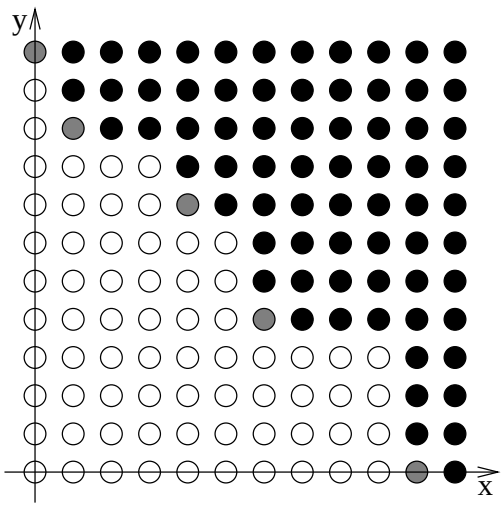


Figure 4.1: Initial terms and staircase

- if G is a Gröbner basis of I then in $In(G)$ there is a monomial of the form $c_i x_i^{d_i}$ for every $i = 1, \ldots, n$

Additionally, the number of elements in $S(G)$ equals the number of points in $V(I)$, counted with their multiplicities.

This result is well-known and will not be proven here. Proofs may be found in [20], [9], or [2].

An ideal is called *zero-dimensional* if it satisfies the conditions above.

Given a polynomial $f \in K[x_1, \ldots, x_n]$, we may reduce it to its normal form with respect to G. Its support will contain terms from $S(G)$, that are irreducible with respect to G. In order to emphasize the vector space structure of $K[x_1, \ldots, x_n]/\langle G \rangle$, the terms appearing in the normal form of f are sometimes called the *coordinates of f with respect to G*.

Let $\prec_1$ and $\prec_2$ be two term orderings and denote by G_1 the reduced Gröbner basis of the ideal I with respect to $\prec_1$, by G_2 the reduced Gröbner basis of I with respect to $\prec_2$.

Assume that the ideal I is zero-dimensional. Given G_1 we will describe a method for obtaining G_2 without having to apply Buchberger's algorithm.

The idea is the following. We consider terms in ascending order with

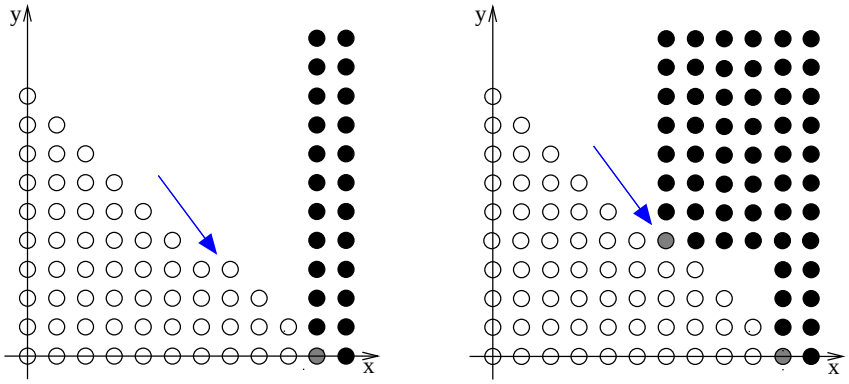


Figure 4.2: The current term is in $S(G_2)$ or in $In(G_2)$

respect to $\prec_2$ starting from 1. At each step one of the three following cases may occur

- the term belongs to $S(G_2)$
- the term belongs to $In(G_2)$
- the term is a multiple of some term in $In(G_2)$

We initialize three sets $NewBasis$, $Initials$, and $Staircase$ to the empty set and enlarge them iteratively. These three sets will at each step be subsets of G_2, $In(G_2)$, and $S(G_2)$, resp., and coincide with them upon termination.

For each term considered, we have to decide to which of the three cases above the term gives rise. This may be decided by searching for a linear dependence relation of the new term from the already processed terms who have ended up in $Staircase$. If no linear dependence is found, the set is added to $Staircase$; if a linear dependence relation is found, we have also found a polynomial to be added to $NewBasis$, and whose initial term with respect to $\prec_2$ is the current term, that goes to augment $Initials$. Terms that are multiples of some term in $Initials$ will not be processed, hence the third case will not occur.

In Figure 4.2 an arrow points at the current term being considered in the algorithm. The terms corresponding to the empty dots have already been processed and added to $Staircase$. Grey dots have been added to $Initials$ and black-filled dots are multiples of some of the $Initials$. The empty areas of the picture correspond to those terms who haven't been processed by the algorithm yet. To the right one can see that, whenever a

term is found that belongs to $In(G_2)$, all of its multiples get marked and won't be considered in the following steps of the algorithm.

For each term t considered at one step in the algorithm we have

- $NewBasis = \{g \in G_2 \mid g_{\prec_2} \prec_2 t\}$
- $Initials = NewBasis_{\prec_2} = \{s \in In(G_2) \mid s_{\prec_2} \prec_2 t\}$
- $Staircase = \{s \in S(G_2) \mid s \prec_2 t\}$

These three sets suffice for deciding if there is a linear dependence relation since we only want to consider terms that are smaller than t with respect to $\prec_2$.

If t is of the form ss_1 for some term in $Initials$, we just step on to the next term.

If not, we reduce t to its normal form with respect to $\prec_1$. If its $\prec_1$-coordinates are linearly dependent from the $\prec_1$-coordinates of the elements in $Staircase$, then we add t to $Initials$ and the dependency relation gives a new polynomial to be added to $NewBasis$. In case no dependency relation is found, the term t is added to $Staircase$.

Denote by $NF(t)$ the normal form of t with respect to $\prec_1$.

The FGLM algorithm

Input: $\prec_1$, $\prec_2$ term orderings

G Gröbner basis with respect to $\prec_1$ such that $G \neq \{1\}$

Output: $NewBasis$ reduced Gröbner basis with respect to $\prec_2$

initialize $NewBasis$and $Initials$ to the empty set, $Staircase$to $\{1\}$

Loop

1. $t \longleftarrow min_{\prec_2}\{s \in T^n \mid t \prec_2 s,\ s \notin \langle Initials\rangle,\ t \neq 1\}$
2. if t is undefined return $NewBasis$
3. $t_1 \longleftarrow NF(t)$

4. if there exists $t_1 + \sum_{\mu \in Staircase} c_\mu NF(\mu) = 0$ then

   (a) $NewBasis \longleftarrow NewBasis \cup \{t + \sum_{\mu \in Staircase} c_\mu \mu\}$

   (b) $Initials \longleftarrow Initials \cup \{t\}$

5. else $Staircase \longleftarrow Staircase \cup \{(t, t_1)\}$ //

Observe that what the algorithm does is to construct monic polynomials that belong to the ideal and such that their leading terms with respect to $\prec_2$ minimally generate $I_{\prec_2}$. Hence the output Gröbner basis is reduced.

Theorem The FGLM algorithm is correct

Proof of correctness Let G_1 be a reduced Gröbner basis for I with respect to $\prec_1$, $\prec_2$ another admissible term ordering. Let $S(G_1) = \{a_1, \ldots, a_{D(I)}\}$ be the staircase of G_1, where D is the dimension of $K[x_1, \ldots, x_n]/I$ as a K-vector space. Let $S(G_2) = \{b_1, \ldots, b_{D(I)}\}$. Then the algorithm constructs a matrix $C = (c_{ki})$ such that

$$b_i = c_{1i}a_1 + \cdots + c_{D(I)i}a_{D(I)}$$

for every $b_i \in S(G_2)$.

We proceed iteratively initializing the sets $NewBasis$ and $Initials$ to the empty set, and $Staircase$to $\{1\}$.

Let now t be the minimum term with respect to $\prec_2$ in the set

$$\{s \in T^n \mid t \prec_2 s \text{ for every } t \in Staircase \cup Initials,\ s \notin \langle Initials \rangle,\ t \neq 1\}$$

Then t must be of the form $x_j b_i$ for some x_j, b_i with $x_j \in \{x_1, \ldots, x_n\}$, $b_i \in Staircase$. In fact, if for every x_j that divides t it would be $\frac{t}{x_j} \in \langle Initials \rangle$, then also t would be in $\langle Initials \rangle$.

Then one of these two cases may occur

1. $t = g_{\prec_2}$ for some $g \in G_2$, t is added to $Initials$ and g is added to $NewBasis$

2. t is added to $Staircase$

Let $T(G_1) = (t_{ijk})$be the tensor defined as

$$t_{ijk} := j\text{-th coordinate w.r.t. } S(G_1) \text{ of } NF_{G_1}(x_i b_k)$$

for $b_k \in S(G_1)$.

We compute he coordinates $c(t) = (c(t)_1, \ldots, c(t)_{D(I)})$ of t as follows

$$\begin{array}{rcl} t = x_i b_j & = & x_j \sum_k c_{kj} a_k \\ & = & \sum_k c_{kj}(x_j a_k) \\ & = & \sum_k c_{ki}(\sum_h t_{jhk} a_h) \\ & = & \sum_h (\sum_k t_{jhk} c_{ki}) a_h \\ & = & \sum_h c(t)_h a_h \end{array}$$

If the vector $c(t)$ is linearly independent from the vectors in C, then we are in case 2 and we have found a new term $t \in Staircase$. Otherwise we obtain a new element $g \in G_2$ from the dependency relation. //

4.2 Complexity analysis

After giving a bound on the size of the input basis, we present an analysis of the FGLM algorithm that shows that its complexity is polynomial in the number n of variables. When taking into account the growth of coefficients, the complexity of the algorithm is polynomial in d^{n^2}, where d is the maximum degree of the polynomials generating the ideal.

The results in this section are derived from [26].

A polynomial time algorithm for computing universal Gröbner bases of zero-dimensional ideals using linear algebra is also presented in [7], where bounds on the degrees of the term in staircases are read off from the properties of certain zonotopes.

4.2.1 Size of the input basis

The FGLM algorithm takes as input a Gröbner basis. For a 0-dimensional ideal in n variables, the size S of any Gröbner basis satisfies the following inequality

$$S \leq D^2 + 2nD$$

where D is the vector-space dimension of $K[x_1, \ldots, x_n]/I$. This bound will be needed later for an overall complexity analysis of the FGLM algorithm.

Let $I \subseteq K[x_1, \ldots, x_n]$ be a zero-dimensional ideal and G be a Gröbner basis of I. We will start by giving some bounds on the size of the input Gröbner basis G. We will assume that G is reduced.

Let D be the number of irreducible terms with respect to G. This number is an invariant of the ideal since it represents the number of common zeros (counted with multiplicity) of the polynomials in the ideal in an algebraic closure of the ground field. Hence we can write $D = D(I)$ to emphasize the fact that this number does not depend on the particular Gröbner basis of the ideal.

Denote by k the number of polynomials in the input Gröbner basis G. Then $k \geq n$ since for every $i = 1, \ldots, n$ there is a polynomial in G whose leading term is of the form $c_i x_i^{d_i}$.

An upper bound for k is $nD(I)$ for any 0-dimensional ideal I. In fact, let d_i be the degree of the univariate polynomial in x_i in the Gröbner basis G for $i = 1, \ldots, n$. Then the exponents of the leading term of any polynomial in G must be contained in the hypercube whose volume is $d_1 d_2 \cdots d_n$ and since $d_i \leq D$ for every i, we have proven that $k \leq nD$.

Now, in order to represent the basis G one needs a representation for

- the basis $S(G)$
- the polynomials in G

Each element in $S(G)$ may be represented by the array of length n of its exponents.

Since we assume G to be reduced, any polynomial $g \in G$ is the sum of its leading term plus a linear combination of elements of $S(G)$. Hence the representation of one polynomial g in the basis requires

- an array of length n (exponents of the initial term)
- an array of length D (coefficients of the remaining terms in $supp(g)$ as linear combinations of elements of $S(G)$)

Hence, the size of the input is bounded above by $nD+k(n+D)$. Remembering that the number of polynomials k is at most nD, one gets the following bound on the size S of the input basis

$$2nD + n^2 \leq S \leq nD^2 + n^2 D + nD$$

In practice, k is at most D (except when D is very small), hence

$$S \leq D^2 + 2nD$$

4.2.2 A polynomial time complexity result

Assuming that operations on the ground field require unit time, we present a complexity analysis of the FGLM algorithm that yields a polynomial result in n and D.

The steps in the FGLM algorithm that contribute to its overall complexity require the following computations

- determining the next term to be processed (line 1)
- computing the normal form of a term (line 3)
- searching for a linear dependency relation among polynomials (line 4)

We present here a complexity analysis assuming that field operations require unit time. With this assumption, the overall complexity is polynomial in n and D.

Next term

In line 1 we want to compute the next term as $min\{s \in T^n | \; t \prec_2 s, \; s \notin \langle Initials \rangle\}$ where t is the previously processed term. In order to provide a good complexity bound, we rewrite the algorithm in a way that shows how the next term may be computed efficiently.

Let us introduce a new set $ListOfNexts$ and a function $InsertNexts$ that, given a term t, inserts into $ListOfNexts$ the products of t by all the variables, sorts $ListOfNexts$ by $\prec_2$, and removes all duplicates.

Let $NextTerm$ be a function returning the smallest term in $ListOfNexts$ with respect to the target ordering. The algorithm then becomes

FGLM algorithm (with management of ListOfNexts)

Input: $\prec_1$, $\prec_2$ term orderings

G Gröbner basis with respect to $\prec_1$ such that $G \neq \{1\}$

Output: $NewBasis$ reduced Gröbner basis with respect to $\prec_2$

initialize $NewBasis$, $Initials$, $Staircase$, $ListOfNexts$ to the empty set, $t = 1$

Loop

1. if t is undefined return $NewBasis$
2. if t is not a multiple of any of the elements in $Initials$
3. $t_1 \longleftarrow NF_{\prec_1}(t)$
4. if there exists $t_1 + \sum_{\mu \in Staircase} c_\mu NF_{\prec_1}(\mu) = 0$ then
   (a) $NewBasis \longleftarrow NewBasis \cup \{t + \sum_{\mu \in Staircase} c_\mu \mu\}$
   (b) $Initials \longleftarrow Initials \cup \{t\}$
5. else
   (a) $Staircase \longleftarrow Staircase \cup \{(t, t_1)\}$
   (b) $InsertNexts(t)$
6. $t \longleftarrow NextTerm$ //

We have already shown that $Initials$ can contain at most nD elements since so does any Gröbner basis of a 0-dimensional ideal. Then in line 2 we need to perform nD comparisons between terms and this would yield a time complexity of $O(nD*nD*n)$ since each comparison takes $O(n)$ time and this step is carried out nD times.

But there is a way of avoiding all these comparisons, namely one has to remember that each term that is added to $ListOfNexts$ is a product of a term in $Staircase$ by a variable. One can then keep track of how many times each term has been inserted in $ListOfNexts$ and replace the test in line 2 by the line

"2. if the number of insertions of t in $ListOfNexts$ is greater than the number of variables in t"

Then this test has a time complexity of $O(n)$ yielding an overall complexity of $O(nD * n)$ since the test is repeated nD times.

Let us now turn to analyse how much time is needed for the management of $ListOfNexts$. This is a list of length at most nD that is merged at each step with a list of length n, requiring $O(nD)$ comparisons of terms (time $O(n)$). Overall, we have $O(nD*n*D) = O(n^2D^2)$, $InsertNexts$ being called D times.

With an implementation of $ListOfNexts$ as efficient priority queue with nD insertions and nD deletions of the least element, the complexity reduces to $O(n^2Dlog(nD))$.

In order to be able to give a polynomial bound for the complexity of the normal form computation, we introduce a new function and show how to compute it by using linear algebra instead of the Buchberger normal form reduction.

Normal form

In line 3 we want to compute $NF(t)$, the normal form of a term t with respect to the Gröbner basis G. Note that the normal forms in line 4 do not need to be computed since they have already been stored as the second coordinates of the elements of $Staircase$.

The term t is the product of some term τ and a variable x_j. Since $\tau_1 := NF(\tau)$ has already been computed, we can use this information when computing $NF(t)$. In fact, since $NF(t) = NF(\tau x_j) = NF(NF(\tau) * NF(x_j))$, when computing the normal form of t is the same as computing normal forms of terms of the form σx_j, where $\sigma \in S(G)$.

Denote by $\sigma_1, \ldots, \sigma_D$ the elements of $S(G)$. Let $T(G) = (t_{ijk})$ be the $n \times D \times D$ tensor whose element t_{ijk} is the j-th coordinate w.r.t. $S(G)$ of $NF(\sigma_i x_k)$. Then in order to compute $T(G)$, $O(nD^3)$ arithmetic operations are needed.

In fact, consider the set $\overline{S(G)} := S(G) \cup \{\sigma x_i |\ \sigma \in S(G),\ i = 1, \ldots, n\}$ containing all terms in the staircase of G plus the terms at the border. Assume that $\overline{S(G)}$ is ordered by $\prec$ (the ordering corresponding to G). We will construct the coordinates vectors t_{i*k} by following the order in which the $\sigma_i x_k$ appear in $\overline{S(G)}$.

Consider the term $\sigma_i x_k$. If $\sigma_i x_k \in S(G)$ then it's already in normal form

and we have

$$t_{ijk} = \begin{cases} 1 \, if \; j = i \\ 0 \, otherwise \end{cases}$$

If $\sigma_i x_k \in In(G)$, then there exists a polynomial $g \in G$ that has $\sigma_i x_k$ as its leading term. Write $g = \sigma_i x_k + \sum_{u=1}^{D} c_u \sigma_u$ and in this case we have

$$t_{ijk} = (-a_1, \ldots, -a_D)$$

The last case to consider is when $\sigma_i x_k \in \overline{S(G)} \setminus (S(G) \cup In(G))$, that is when the term is on the border of the staircase but is not an initial term of any of the polynomials in G. In this case $\sigma_i x_k$ is the product of some variable x_l by a term $\sigma_h x_m$ whose coordinates t_{h*m} have already been computed since $\sigma_h x_m \prec \sigma_h x_m x_l = \sigma_i x_k$. But then $\sigma_i x_k = \sigma_h x_m x_l = x_l \sum_v t_{hvs} \sigma_v = \sum_u \sum_v t_{hvs} t_{vul} b_u$. In this way one has to perform D^2 operations in order to compute t_{i*k}, and since this has to be repeated at most nD times, the complexity of computing $T(G)$ is $O(nD^3)$.

Linear dependency

We are now left with analysing the complexity of searching for a linear dependency relation among polynomials (line 4 in the algorithm).

This is a linear algebra problem that is equivalent to triangularizing a $D \times nD$ matrix, task that can be achieved in time $O(nD^3)$.

4.2.3 Growth of coefficients

For a thorough complexity analysis of the FGLM algorithm it is necessary to take into account the growth of the coefficients. While the linear algebra computations have a complexity that is exponential in n but polynomial in D, the normal form computations introduce a growth that appears to be exponential in nD, even though this has to be proven still.

By introducing a new measure of the problem, E , that is proven to be bounded above by D^n, we are finally able to state that the overall complexity is polynomial in E.

Another bound on the size of the input

We start by introducing a new measure for the size of the problem.

Let $\prec_1$, $\prec_2$ be the term ordering used to compute the input Gröbner basis G, and respectively the target term ordering. We restrict the analysis to the case where $\prec_1$ is a degree ordering (i.e. for terms t_1, t_2, whenever $deg(t_1) < deg(t_2)$, then $t_1 \prec_1 t_2$). This is anyways the case in which the algorithm is mostly useful.

Let E be the number of terms in the new basis that are not greater (with respect to $\prec_1$) than any term in the set

$$\overline{S(G)} := S(G) \cup \{\sigma x_i | \, \sigma \in S(G), \, i = 1, \ldots, n\}$$

Then E is the maximum number of terms that may appear in the normal form computations carried out in the algorithm. As before, let D be the number of irreducible terms with respect to G. Then the following inequality holds

$$D \leq E \leq \left(\begin{array}{c} n+D \\ n \end{array} \right) = \frac{(n+D)!}{n!D!} \leq D^n$$

If the maximal degree of the irreducible terms in $S(G)$ is d, then

$$E \leq \left(\begin{array}{c} n+d+1 \\ n \end{array} \right) = \frac{(n+d+1)!}{n!(d+1)!}$$

The two above bounds are nothing else than the number of terms in n variables of degree at most D and, respectively, $d+1$.

A polynomial result

The growth of coefficients affects the normal form and the linear algebra computations in the algorithm.

The reduction to normal form requires at most E steps, that is the number of terms that may be reduced. It can be shown that a normal form reduction is equivalent to multiplying E matrices by a vector. Since one computes at most E normal forms in the algorithm, the complexity of the normal form computations is $O(E^2)$.

The linear algebra part consists in triangularizing matrices.

Hence, over fields for which polynomial algorithms exist for multiplying and triangularizing matrices, the FGLM algorithm is polynomial. One can show that, for instance, finite fields and the field of rational numbers are polynomial.

4.3 Variations for positive dimensional ideals

The finiteness of the residue class ring is a crucial property because it guarantees termination of the FGLM algorithm for zero-dimensional ideals. The problem with positive dimensional ideals is that one is not dealing anymore with finitely generated vector spaces, hence a workaround is required in order to guarantee the termination of the algorithm. We will describe here two methods that work in positive dimension.

Both methods rely on a sequence of applications of the FGLM algorithm. At each step in the sequence the termination of the algorithm is guaranteed, the output Gröbner basis may yet not be the desired one.

The first method, proposed in [39], works for some special term orderings called sequential, for which there is only a finite number of terms that are smaller than any given term. At each step the input basis is converted to a sequential ordering until the target ordering is reached. We show that this method is very similar to the Gröbner walk. The main difference is that here the intermediate bases are computed with the FGLM algorithm instead of using the technique of lifting bases of initial ideals.

The second method, presented in [37], runs at each step the FGLM algorithm on a finite set of terms. The result is a Gröbner basis of possibly a smaller ideal. At each step the set of terms is incremented until the target basis is obtained. This method will be briefly discussed in 4.3.3.

4.3.1 Conversion to sequential term orderings

A term ordering $\prec$ is called *sequential* if for every term $t \in T^n$ there are at most finitely many terms s such that $s \prec t$.

Recall that an order $\leq$ on a group G (written multplicatively) is called *archimedean* if for every $g_1, g_2 \in G^+ \backslash \{1\}$ there exists $k \in \mathbb{N}$ such that $g_1 \leq g_2^k$.

Next, we prove that for term orderings the archimedean property is equivalent to being sequential.

Proposition Let $\prec$ be a term ordering. Then $\prec$ is sequential if and only if it is archimedean.

Proof If there exist $s, t \in T^n$ such that $s^k \prec t$ for every $k \in \mathbb{N}$ then $\prec$ cannot be sequential.

Assume now that $\prec$ is archimedean. We will prove by induction on n that there cannot exist an infinite set $S \subseteq T^n$ and a term $t \in T^n$ such that $s \prec t$ for every $s \in S$.

For $n = 1$ the only term ordering is the "divide" order relation and for every term $t \in T^1$ we have $t = x_1^k$ for some $k \in \mathbb{N}$ and $|S| = k$.

Assume that every archimedean term ordering in T^{n-1} is sequential. Let $S \subseteq T^n$ be an infinite set of terms such that $s \prec t$ for every $s \in S$. For every $s \in S$ write $s = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$. Denote by s_i the term obtained from s by setting $x_i = 1$ and set $S_i = \{s_i |\ s \in S\}$. The term ordering $\prec$ is archimedean on T^{n-1}. Since s_i divides s for every $s \in S$, we have $s_i \prec s$ and hence $s_i \prec t$ for every $i = 1, \ldots, n$. By the induction hypothesis S_i must be therefore finite for every i.

Since S is infinite there must exist a $j \in \{1, \ldots, n\}$ and a $\overline{s} \in S_j$ such that there are infinitely many $k \in \mathbb{N}$ such that $x_j^k \overline{s} = s \in S$. But this contradicts the hypothesis that $\prec$ is archimedean because if there would exist $m \in \mathbb{N}$ such that $t \prec x_j^m$ then the k satisfying $x_j^k \prec x_j^k \overline{s} \prec t$ would be at most finitely many. //

Sequential orderings are those refining a weight vector whose coordinates are all positive. Observe that for any term ordering it is always possible to find a sequential ordering belonging to its cone. Let in fact $\prec$ be a non-sequential term ordering and G a Gröbner basis with respect to $\prec$. Finding a sequential term ordering in the cone of $\prec$ is the same as finding a weight vector with positive coordinates $\omega = (\omega_1, \ldots, \omega_n) \in \mathbb{Q}_+^n$ with $\omega_i \neq 0$ for every $i = 1, \ldots, n$ and such that $G_\omega = G_\prec$. This is an integer programming problem that can also be solved by means of Gröbner bases (see [19],[47], or [33]).

We now present the algorithm that converts any given Gröbner basis of an ideal to a Gröbner basis with respect to a sequential term ordering. The ideal in question may be positive dimensional. This algorithm is very similar to the FGLM algorithm presented in Section 4.1. Here we need some additional conditions in order to guarantee termination, namely

- the target weight vector has to have positive coordinates
- every a new polynomial is added to $NewBasis$, we check if $NewBasis$ is a Gröbner basis with respect to the target term ordering

Note that the second condition requires a test for the Gröbner property of $NewBasis$ and not a whole Gröbner basis computation. The test may be carried out by reducing S-polynomials.

Let τ be a vector in $\mathbb{Q}^n$ with positive coordinates and denote by $NF(t)$ the normal form of t with respect to $\prec_1$.

FGLM conversion to sequential orderings

Input: $\prec_1$ term ordering refining ω, $\prec_2$ sequential term ordering refining τ

G Gröbner basis with respect to $\prec_1$ such that $G \neq \{1\}$

Output: $NewBasis$, the reduced Gröbner basis with respect to $\prec_2$

initialize $NewBasis$and $Initials$ to the empty set, $Staircase$to $\{1\}$

Loop

1. $t \longleftarrow min_{\prec_2}\{s \in T^n \mid t \prec_2 s,\ s \notin \langle Initials\rangle,\ t \neq 1\}$
2. if t undefined or ($\langle NewBasis\rangle = \langle G\rangle$ and $NewBasis$ is complete) return $NewBasis$
3. $t_1 \longleftarrow NF(t)$
4. if there exists $t_1 + \sum_{\mu \in Staircase} c_\mu NF(\mu) = 0$ then
   (a) $NewBasis \longleftarrow NewBasis \cup \{t + \sum_{\mu \in Staircase} c_\mu \mu\}$
   (b) $Initials \longleftarrow Initials \cup \{t\}$
5. else $Staircase \longleftarrow Staircase \cup \{(t, t_1)\}$ //

From the way we construct $NewBasis$, at each step the polynomials in $NewBasis$ are

- monic
- interreduced with respect to $\prec_2$, i.e. for every $g \in NewBasis$ no term in $supp(g)$ is divisible by any of the terms in $NewBasis_{\prec_2} \setminus \{g_{\prec_2}\}$
- they belong to the ideal I

These properties make $NewBasis$ a subset of the reduced Gröbner basis with respect to $\prec_2$ at each step in the loop. That does not make yet $NewBasis$ the Gröbner basis of the input ideal, in fact it might be that even if $\langle NewBasis \rangle = \langle G \rangle$, still $NewBasis$ might not be complete. The check for completeness my be carried out by reducing all S-polynomials in $NewBasis$ to their normal form with respect to $NewBasis$. As long as there are S-polynomials that do not reduce to 0, one needs to carry on the search for dependencies. Remark that while in Buchberger's algorithm one adds to the basis the S-polynomials that do not reduce to 0, here one does not need to add them to the basis. $NewBasis$ gets enlarged only when a new linear dependency relation is found. At each addition of a new polynomial to $NewBasis$, one checks if one is able to reduce to zero the S-polynomials that couldn't be reduced before, and at the same time adds $\mid NewBasis \mid$ S-polynomials to the list of S-polynomials to be reduced.

The staircase of a positive dimensional ideal is an infinite set. Upon termination, the algorithm delivers just a finite subset of the staircase of $NewBasis$, namely the set

$$\{s \in S(NewBasis) \mid s \prec_2 t \; for \; every \; t \in NewBasis_{\prec_2}\}$$

of all terms in the staircase of $NewBasis$ that are smaller with respect to $\prec_2$ of all $\prec_2$-initial terms of $NewBasis$.

Next, we present a more formal proof of correctness of the algorithm.

Proof of correctness For proving that the FGLM conversion to sequential orderings algorithm is correct we show that it delivers the reduced Gröbner basis of $I = \langle G \rangle$ with respect to $\prec_2$. Notice that the algorithm is the same as the FGLM algorithm for 0-dimensional ideals presented in Section 4.1. Here we require $\prec_2$ to be a sequential ordering and we have an additional test in line 2.

Assume for now that the algorithm terminates. We first prove that the elements in $Staircase$ are linearly independent modulo I. If it would not

be so, then there would be a finite subset $C \subseteq Staircase$ such that the linear combination

$$f = \sum_{t_i \in C} \lambda_i t_i$$

reduces to 0 modulo I. That is,

$$NF(f) = \sum_{t_i \in C} \lambda_i NF(t_i) = 0$$

Without loss of generality, we may assume that $C = \{t_1, \ldots, t_k\}$ with $t_1 \prec_2 t_2 \prec_2 \cdots \prec_2 t_k$, where $\prec_2$ is the target sequential ordering. Since in the loop we consider terms in increasing order with respect to $\prec_2$, by the time t_k is being examined the terms $t_1, t_2 \ldots, t_{k-1}$ have already been added to $Staircase$. But then t_k is added to $Initials$ and not to $Staircase$ because the condition in line 4 of the algorithm is satisfied. Hence the elements in $Staircase$ are linearly independent modulo I.

We now show that the elements in $NewBasis$ belong to I. Every polynomial f that is added to $NewBasis$ is by costruction of the form

$$f = t + \sum_{\mu \in Staircase} c_\mu \mu$$

and it satisfies $NF(t) + \sum_{\mu \in Staircase} c_\mu NF(\mu) = 0$. But

$$NF(f) = NF(t) + \sum_{\mu \in Staircase} c_\mu NF(\mu)$$

and since $NF(f) = 0$, we have $f \in I$.

Finally, since we consider terms in ascending order with respect to $\prec_2$, the terms in $Initials$ are the leading terms with respect to $\prec_2$ of the elements in $NewBasis$.

Now we want to show that every term that is not in $Staircase$ nor in $Initials$ is either

- a multiple of a term in $Initials$
- it is greater with respect to $\prec_2$ than all terms in $Initials$

If t is a term that is processed by the algorithm (line 1) and the condition "($\langle NewBasis \rangle = \langle G \rangle$ and $NewBasis$ is complete)" is not true, then t is

added either to $Initials$or to $Staircase$, hence the statement is in this case true.

The reason why a term t is not processed by the algorithm is either (by the definition of the next term t in line 1) because $t \in \langle Initials \rangle$, and hence is a multiple of a term in $Initials$, or because the condition in line 2 "($\langle NewBasis \rangle = \langle G \rangle$ and $NewBasis$ is complete)" is satisfied and the algorithm returns $NewBasis$ without processing t. But then we know that t is greater with respect to $\prec_2$ than all terms in $Initials$.

We now have to prove that the algorithm terminates. But this follows from the fact that $\prec_2$ is sequential and hence for every term t there are at most a finite number of terms that are smaller than t with respect to $\prec_2$. This implies that in a finite number of steps we obtain a set of polynomials that generates $I_{\prec_2}$ and such that all S-polynomials reduce to 0, hence a reduced Gröbner basis of I with respect to $\prec_2$. Since each polynomial f in $NewBasis$ is monic and by construction none of the monomials in $supp(f)$ is multiple of any of the terms in $Initials$ other than itself, then $NewBasis$ is reduced. //

4.3.2 The FGLM Walk

We have seen how to convert a Gröbner basis of a positive dimensional ideal to a sequential ordering by using a modified FGLM algorithm. We now present an algorithm using that uses sequences of applications of these FGLM conversions to sequential orderings. At each step in the sequence, we convert to a new sequential ordering, and stop once a sequential ordering is found that lies in the same cone of the non-sequential target term ordering. In order to verify whether two term orderings lie in the same cone, it is sufficient to compare the initial terms in the respective Gröbner bases, as shown in Section 3.4.

In this way, we can compute Gröbner bases of positive dimensional ideals with respect to non-sequential orderings by using the FGLM machinery.

Calling this variation the "FGLM walk" points out the fact that this algorithm may be viewed as a Gröbner walk where each conversion is carried out by means of the FGLM algorithm. The additional restriction here is on the choice of the next weight vector, whose coordinates have to be positive in order to guarantee that each term ordering in the sequence of conversions is sequential.

Denote by $NF(t)$ the normal form of t with respect to $\prec_1$. Let $fglm_p$ be a function that, given the reduced Gröbner basis of an ideal I with respect to $\prec_{old}$ and a sequential term ordering $\prec_{new}$, delivers the reduced Gröbner basis of I with respect to $\prec_2$. The algorithm that computes this function has been presented in 4.3.1.

FGLM walk

Input: $\prec_1$ term ordering refining ω, $\prec_2$ term ordering

G reduced Gröbner basis with respect to $\prec_1$ such that $G \neq \{1\}$

Output: $NewBasis$ reduced Gröbner basis with respect to $\prec_2$

initialize $NewBasis$ to G

initialize $\prec_{old}$ to $\prec_1$,

initialize $\prec_{new}$ to $\prec_2$

Loop

1. if $NewBasis_{\prec_{old}} = NewBasis_{\prec_2}$ then return $NewBasis$
2. $\omega \longleftarrow$ next weight vector $\omega + c(\tau - \omega)$ with positive coordinates
3. $\prec_{new} \longleftarrow$ term ordering refining ω
    1. $NewBasis \longleftarrow fglm_p(NewBasis, \prec_{old}, \prec_{new})$
    2. $\prec_{old} \longleftarrow \prec_{new}$

//

4.3.3 Incrementing finite sets of terms

In [37] a variation of the FGLM algorithm that works for positive dimensional ideals is proposed. In order to overcome the problem with the infinite vector space basis of the residue class ring, one works with a finite subset of it, namely the subset given by all terms of degree smaller than a given d.

Given a Gröbner basis G, the algorithm goes as follows

1. choose a degree d
2. let $NewBasis$ be the set of all linear relations modulo G among terms of degree $\leq d$, computed by FGLM
3. if $\langle NewBasis \rangle \neq \langle G \rangle$ repeat step 1 with a new degree bigger than d

This algorithm terminates since there exists $d \in \mathbb{N}$ such that, for every g in the target Gröbner basis, $deg(g) \leq D$. The FGLM computation in step 2 is finite since we are considering finitely many terms. Yet, it does not deliver the target Gröbner basis if the current d is strictly smaller than D, thus requiring another conversion.

Note that nothing is said on how to chose d. Starting with $d = D$ would avoid intermediate computations but it is in most cases not a good choice.

Dealing with degree bounds reminds us of the method proposed in [49], where a Gröbner Walk is performed by choosing a target ordering that depends on the known degree bounds for the new basis. In this case though, choosing an initial degree equal to the known bound for the new basis would make the algorithm very inefficient in most cases, since we would consider more terms than necessary when the bound is not reached.

Chapter 5

Comparison of the two methods

For zero-dimensional ideals there exist implementations of the Gröbner walk and of the FGLM algorithms in Maple. We converted a few Gröbner bases to the pure lexicographic ordering and compared the runtimes of the two algorithms. For all of our examples, the Gröbner walk algorithm performed better (up to 50 times) than the FGLM algorithm. By looking at the steps that required most of the computation time, we noticed that the FGLM algorithm performed much worse than the Gröbner walk whenever most of the runtime was spent on normal form computations. We therefore tried to modify the FGLM algorithm slightly in order to avoid costly normal forms computations. This led to a better runtime for the FGLM algorithm, and even though with our modifications the runtimes of the FGLM algorithm were worse than those of the Gröbner walk, in some cases both algorithms took the same time to terminate. In any case, with our modifications we were able to provide what we claim is a fairer comparison of the two algorithms.

For positive dimensional ideals we compared the Gröbner walk algorithm with what we call the FGLM walk. For vector spaces that do not admit a finite basis, the FGLM algorithm does not terminate in general. It does terminate, though, if one performs a conversion to a sequential term ordering. The Gröbner cone of any given term ordering contains a term ordering that is the refinement of a positive weight vector. By using a sequence of such conversions, we approximate the final term ordering by a positive weight vector until the target term ordering is reached. For positive dimensional ideals the Gröbner walk algorithm was more than one thousand times faster than the FGLM algorithm. This behaviour may be explained by the fact that FGLM conversions require the search for depen-

dencies among families of terms. In the positive dimensional case, these families are very big even when considering sequential term orderings.

We conclude by saying that whereas it might make sense to use sequences of FGLM conversions instead of the Gröbner walk algorithm for zero-dimensional ideals, this does not seem to make any sense for positive dimensional ideals.

All experiments ran on a computer with 1.90GHz Intel Pentium 4 processor under Linux 2.4.10. Times are expressed in seconds.

The polynomial systems that we used for our experiments are listed in Appendix A A. Most of them come from of the benchmark suite for Computer Algebra that is available on the internet (see [1]).

5.1 Zero-dimensional ideals

In this section we compute Gröbner bases for some zero-dimensional polynomial ideals and compare the performance of the Gröbner walk and the FGLM algorithms for these examples. In Section 5.1.1 we use the algorithms that are available in Maple. But the comparison would not be fair since it does not take in account the perturbation of the target weight vector that is implemented in the Gröbner walk algorithm. In order to make the comparison fair, we also introduce a perturbation of the target weight vector in the FGLM algorithm and apply it in sequence. The results of this new comparison are presented in Section 5.1.2. The Gröbner walk algorithm is still faster than the FGLM algorithm, but by a smaller factor.

5.1.1 Comparing the existing algorithms

In order to get an idea of how algorithms for change of ordering perform in practice, we computed Gröbner bases with respect to the pure lexicographic ordering of zero-dimensional polynomial systems using the Gröbner walk and the FGLM algorithms.

The input was a precomputed Gröbner basis with respect to the total degree inverse lexicographic ordering.

The output was a Gröbner basis of the ideal generated by the input basis with respect to the pure lexicographic ordering such that $x_1 > \cdots > x_n$ for the list of variables $[x_1, \ldots, x_n]$.

For each example, we kept track of the total run time as well as of the times required by the most costly steps of each of the two algorithms. These are: construction of weight vectors (including perturbation of the initial and final weights), computation of Gröbner bases of the intermediate quasi-homogeneous initial ideals, and lifting of the bases for the Gröbner walk; normal form, finding linear dependency relations among polynomials, and selection of the current term to be processed for the FGLM algorithm. For the Gröbner walk we also kept track of the number of steps in the path.

We used the implementations that are currently available in Maple: the `GWalk` function (described in [3]) from the CASA package (see [32], also [31]) and the `fglm` function from the `Ore_algebra` package.

The following table contains a a summary of our results. For each system, we listed

- n, the number of variables
- d, the maximum total degree of the generators
- D, the number of irreducible terms with respect to the ideal (see discussion in Section 4.2)
- C, the number of digits of the longest coefficients in the final basis

The third and fourth columns contain the timings obtained when running `GWalk` and `fglm` , the last row contains the ratio of the total runtimes FGLM/GW.

	Info	GW		FGLM		ratio
a1	$n = 3$		11.80		260.57	22
	$d = 5$	$weight$	1.10	$normalf$	101.76	
	$D = 54$	GB	1.86	$nextterm$	.34	
	$C = 202$	$lift$	6.77	$dependency$	158.47	
		$steps$	74			
a2	$n = 3$		.03		.06	2
	$d = 2$	$weight$	.01	$normalf$	.02	
	$D = 4$	GB	0	$nextterm$	0	
	$C = 2$	$lift$	.01	$dependency$	.40	
		$steps$	1			

	Info	GW		FGLM		ratio
a3	$n = 5$		1.64		2.98	2
	$d = 2$	$weight$	.28	$normalf$	.81	
	$D = 16$	GB	.36	$nextterm$	.09	
	$C = 77$	$lift$	.51	$dependency$	2.07	
		$steps$	20			
a4	$n = 2$		.01		.09	9
	$d = 2$	$weight$	0	$normalf$	.07	
	$D = 4$	GB	0	$nextterm$	0	
	$C = 2$	$lift$	0	$dependency$	.02	
		$steps$	1			
a5	$n = 3$		2.07		69.93	34
	$d = 6$	$weight$	.19	$normalf$	68.52	
	$D = 20$	GB	.27	$nextterm$	.50	
	$C = 9$	$lift$	.36	$dependency$	1.36	
		$steps$	23			
a6	$n = 2$	$total$	.01	$total$	.07	7
	$d = 2$	$weight$	0	$normalf$	.04	
	$D = 4$	GB	0	$nextterm$	0	
	$C = 2$	$lift$	0	$dependency$	.03	
		$steps$	1			
a7	$n = 3$	$total$	.03	$total$	.27	9
	$d = 2$	$weight$	.01	$normalf$	.20	
	$D = 8$	GB	.01	$nextterm$	0	
	$C = 7$	$lift$	.01	$dependency$	.07	
		$steps$	4			
a8	$n = 3$	$total$	.17	$total$	.17	1
	$d = 2$	$weight$	.29	$normalf$	.02	
	$D = 8$	GB	.5	$nextterm$	0	
	$C = 19$	$lift$	.01	$dependency$	.14	
		$steps$	6			
a9	$n = 3$	$total$	23.75	$total$	371.86	16
	$d = 5$	$weight$	.86	$normalf$	42.01	
	$D = 40$	GB	4.35	$nextterm$	.10	
	$C = 701$	$lift$	16.88	$dependency$	329.76	
		$steps$	46			

	Info	GW		FGLM		ratio
a10	$n = 2$	$total$	.48	$total$	3.24	7
	$d = 7$	$weight$	.08	$normalf$	1.13	
	$D = 28$	GB	.18	$nextterm$	.02	
	$C = 24$	$lift$	.19	$dependency$	2.09	
		$steps$	18			
a11	$n = 3$	$total$	.12	$total$	.18	2
	$d = 2$	$weight$	.01	$normalf$	.13	
	$D = 8$	GB	.04	$nextterm$	0	
	$C = 24$	$lift$	.03	$dependency$	.05	
		$steps$	6			
a12	$n = 3$	$total$	3.47	$total$	87.07	25
	$d = 4$	$weight$	.30	$normalf$	5.30	
	$D = 24$	GB	.54	$nextterm$	.01	
	$C = 307$	$lift$	2.09	$dependency$	81.76	
		$steps$	27			
a13	$n = 3$	$total$	.02	$total$	.14	7
	$d = 3$	$weight$	0	$normalf$	.10	
	$D = 6$	GB	0	$nextterm$	0	
	$C = 10$	$lift$	.01	$dependency$	.04	
		$steps$	2			
a14	$n = 4$	$total$	4.19	$total$	28.47	7
	$d = 4$	$weight$	.30	$normalf$	3.30	
	$D = 24$	GB	.84	$nextterm$	.7	
	$C = 332$	$lift$	2.36	$dependency$	25.10	
		$steps$	24			
a15	$n = 3$	$total$	.10	$total$	.19	2
	$d = 3$	$weight$	.01	$normalf$	.14	
	$D = 8$	GB	.01	$nextterm$	0	
	$C = 36$	$lift$	.06	$dependency$	.02	
		$steps$	4			
a16	$n = 2$	$total$	0.02	$total$	.14	7
	$d = 4$	$weight$	0	$normalf$	.03	
	$D = 5$	GB	0	$nextterm$	0	
	$C = 2$	$lift$	0.01	$dependency$	.10	
		$steps$	2			

	Info	GW		FGLM		ratio
a17	$n = 3$	$total$	.54	$total$	.84	2
	$d = 4$	$weight$	.10	$normalf$	.47	
	$D = 16$	GB	.13	$nextterm$	.02	
	$C = 16$	$lift$	.10	$dependency$	.35	
		$steps$	16			
a18	$n = 4$	$total$	.44	$total$	16.88	38
	$d = 2$	$weight$	.04	$normalf$	15.42	
	$D = 16$	GB	.20	$nextterm$	.04	
	$C = 96$	$lift$	.19	$dependency$	1.415	
		$steps$	12			
a19	$n = 4$	$total$	.37	$total$	13.74	37
	$d = 2$	$weight$	.05	$normalf$	12.53	
	$D = 16$	GB	.14	$nextterm$	0	
	$C = 96$	$lift$	.15	$dependency$	1.21	
		$steps$	12			
a20	$n = 4$	$total$	5.51	$total$	34.06	6
	$d = 2$	$weight$	0.54	$normalf$	4.63	
	$D = 16$	GB	1.23	$nextterm$	.17	
	$C = 441$	$lift$	2.30	$dependency$	29.26	
		$steps$	19			
a21	$n = 4$	$total$	7.08	$total$	16.35	2
	$d = 4$	$weight$	.84	$normalf$	8.25	
	$D = 16$	GB	2.63	$nextterm$	.27	
	$C = 9$	$lift$	2.16	$dependency$	7.80	
		$steps$	40			
a22	$n = 2$	$total$	.43	$total$	11.43	27
	$d = 11$	$weight$	.12	$normalf$	.84	
	$D = 56$	GB	.08	$nextterm$	.02	
	$C = 50$	$lift$	.15	$dependency$	10.57	
		$steps$	18			
a23	$n = 3$	$total$	3.24	$total$	70.30	22
	$d = 6$	$weight$	.05	$normalf$	68.68	
	$D = 20$	GB	.33	$nextterm$	.01	
	$C = 9$	$lift$	.44	$dependency$	1.61	
		$steps$	23			

	Info	GW		FGLM		ratio
a24	$n = 4$	$total$	6.42	$total$	17.37	3
	$d = 4$	$weight$	.84	$normalf$	9.35	
	$D = 56$	GB	2.05	$nextterm$	.24	
	$C = 9$	$lift$	2.03	$dependency$	7.77	
		$steps$	35			
a25	$n = 4$	$total$	32.77	$total$	695.40	21
	$d = 3$	$weight$	3.75	$normalf$	598.27	
	$D = 73$	GB	3.82	$nextterm$	.62	
	$C = 27$	$lift$	21.78	$dependency$	96.48	
		$steps$	59			
a26	$n = 4$	$total$	4.30	$total$	32.46	8
	$d = 2$	$weight$	0.29	$normalf$	4.10	
	$D = 16$	GB	1.58	$nextterm$	.01	
	$C = 441$	$lift$	2.37	$dependency$	28.35	
		$steps$	19			
a27	$n = 3$	$total$	26.99	$total$	1090.64	40
	$d = 4$	$weight$	2.62	$normalf$	236.61	
	$D = 45$	GB	8.45	$nextterm$	.02	
	$C = 296$	$lift$	14.80	$dependency$	854.01	
		$steps$	61			
a28	$n = 3$	$total$	12.98	$total$	646.38	50
	$d = 5$	$weight$	2.06	$normalf$	526.94	
	$D = 54$	GB	2.17	$nextterm$	.12	
	$C = 194$	$lift$	7.25	$dependency$	119.31	
		$steps$	79			

For these examples the Gröbner walk performed better than the FGLM algorithm up to a factor of 50, even when the walk required several steps. One may also observe that the ratio is generally higher whenever normal form computations make up for most of the runtime of the FGLM algorithm.

5.1.2 A fairer comparison

We saw in the previous section that the FGLM algorithm performs much worse than the Gröbner walk algorithm whenever most of its runtime is spent on normal form computations.

Since it is known that normal form reductions for degree compatible

orderings are faster than for lexicographic orderings, we tried to improve the normal form computation timing in the FGLM algorithm by converting the basis to a degree compatible ordering. We already mentioned in Section 3.5 that one can construct a priori a weight vector that is contained in the target cone. This vector depends on the degree bound for polynomials in the Gröbner bases of the ideal.

Instead of using the bound, we performed a sequence of conversions with the FGLM algorithm with respect to total degree orderings $\prec_1, \prec_2, \ldots$ where $\prec_i$ was a term ordering refining the weight vector

$$\omega_i = (2^{i^{(n-1)}}, 2^{i^{(n-2)}}, \ldots, 1)$$

for $i = 1, 2, \ldots$ until the desired basis was reached. Property (d) of Theorem 2.7 in [43] guarantees that there exists an i big enough such that ω_i is in the interior of the Gröbner cone of $\prec_{plex}$. Denote by $\prec_{lex}$the pure lexicographic ordering with $x_1 > x_2 > \cdots > x_n$. After each transformation we checked if the obtained Gröbner basis G would satify $G_{\prec_i} = G_{\prec_{lex}}$. If not, one more step would be required, and we used G as input for the next conversion, otherwise we were done.

The following table shows the timings obtained by running a sequence of FGLM conversions on some of the previous examples.

	Info	FGLM SEQUENCE		FGLM		ratio
a5	$n = 3$		3.09		69.93	23
	$d = 6$	$normalf$	1.16	$normalf$	68.52	
	$D = 20$	$nextterm$	.03	$nextterm$	.50	
	$C = 9$	$dependency$	1.34	$dependency$	1.36	
		$steps$	5			
a12	$n = 3$		21.08		87.07	4
	$d = 4$	$normalf$	3.59	$normalf$	5.30	
	$D = 24$	$nextterm$	.22	$nextterm$	.01	
	$C = 307$	$dependency$	15.38	$dependency$	81.76	
		$steps$	5			
a18	$n = 4$		2.52		16.88	7
	$d = 2$	$normalf$	.63	$normalf$	15.42	
	$D = 16$	$nextterm$	.19	$nextterm$	.04	
	$C = 96$	$dependency$	1.35	$dependency$	1.415	
		$steps$	4			

	Info	FGLM SEQUENCE		FGLM		ratio
a19	$n = 4$		2.17		13.74	6
	$d = 2$	$normalf$	.60	$normalf$	12.53	
	$D = 16$	$nextterm$	.02	$nextterm$	0	
	$C = 96$	$dependency$	1.44	$dependency$	1.21	
		$steps$	4			
a26	$n = 4$		23.47		32.46	1
	$d = 2$	$normalf$	3.21	$normalf$	4.10	
	$D = 16$	$nextterm$	.16	$nextterm$	.01	
	$C = 441$	$dependency$	16.91	$dependency$	28.35	
		$steps$	4			
a27	$n = 3$		183.31		1090.64	6
	$d = 4$	$normalf$	21.46	$normalf$	236.61	
	$D = 45$	$nextterm$	.80	$nextterm$	.02	
	$C = 296$	$dependency$	151.61	$dependency$	854.01	
		$steps$	6			
a28	$n = 3$		164.82		646.38	4
	$d = 5$	$normalf$	18.66	$normalf$	526.94	
	$D = 54$	$nextterm$	.72	$nextterm$	.12	
	$C = 194$	$dependency$	106.84	$dependency$	119.31	
		$steps$	6			

Based on these timings, it seems that also for the FGLM algorithm it is faster to compute a sequence of intermediate Gröbner bases instead of converting the input basis at once. This may be explained by two facts:

- degree-compatible orderings are used - these orderings make normal forms computations faster
- the cone of the input basis at each step is "close" to the target cone

Note that the Gröbner walk algorithm, as it is implemented in CASA, uses path perturbation (see Section 3.5.1). In particular, the target weight vector is perturbated at the beginning of the algorithm. Once the perturbed target vector is reached, it is checked if the desired Gröbner basis has been obtained (and this is true in most cases). If not, then further steps in the direction of the non-perturbed target vector are carried out. This means that when we computed our examples we almost never converted a basis to a pure lexicogtraphic ordering when using the Gröbner walk algorithm. That's why using a sequence of FGLM conversions instead of the FGLM algorithm makes the comparison a fairer one.

Note also that since we do not set any restriction on the choice of the next weight vector (other than that it has to lie outside of the current cone), we do not know whether any two successive cones are adjacent. We also tried to run the sequence of FGLM transformations using at each step other weight vectors. Approaching the target weight vector slowlier gives rise to more but shorter steps and on the vice-versa approaching the target vector faster gives rise to less but longer steps. In our experiments, we did not find that another choice of intermediate weight vectors performed better as the $\omega_i = (2^{i^{(n-1)}}, 2^{i^{(n-2)}}, \ldots, 1)$, hence the ω_i seem to be a good choice.

One more remark is that for system a26 there was no big improvement when using a sequence of FGLM conversions instead of the original FGLM algorithm. This is due to the fact that in this example most of the computation time is required by the search for dependency relations. In the previous table one sees that the coefficients of the polynomials in the final Gröbner basis had up to 441 digits, and this made the matrix computations costlier, whereas the normal form computations did not amount to a big part of the runtime.

Summarizing now our results we have the following timings, where the second and third columns contain respectively the total runtime of the Gröbner walk and of the FGLM sequence algorithm, the fourth column contains the ratio FGLM seq. over GW.

	GW	FGLM seq.	ratio
a5	2.07	3.09	1
a12	3.47	21.08	6
a18	.44	2.52	6
a19	.37	2.17	6
a26	4.30	23.47	5
a27	26.99	183.31	7
a28	12.98	164.82	13

From this table we see that with a fair comparison the ratio FGLM/GW has improved and is at most 13.

Finally, a fair comparison for some more zero-dimensional polynomial systems. These examples come from [6] and are listed in Appendix A.

		GW		FGLM seq.		ratio
Ex1	$n = 3$		10.41		49.41	5
	$d = 4$	$weight$	.44	$normalf$	6.43	
	$D = 45$	GB	1.26	$nextterm$	.08	
	$C = 106$	$lift$	8.62	$dependency$	42.80	
		$steps$	36	$steps$	5	
Ex2	$n = 3$		11.09		263.42	24
	$d = 4$	$weight$	.10	$normalf$	11.57	
	$D = 46$	GB	2.23	$nextterm$	.65	
	$C = 261$	$lift$	6.85	$dependency$	121.52	
		$steps$	47	$steps$	6	
Ex3	$n = 3$		17.19		193.54	11
	$d = 4$	$weight$	2.70	$normalf$	11.45	
	$D = 53$	GB	3.37	$nextterm$	.66	
	$C = 183$	$lift$	9.04	$dependency$	91.55	
		$steps$	57	$steps$	5	
s6	$n = 6$		27.62		20.85	1
	$d = 2$	$weight$	1.32	$normalf$	3.77	
	$D = 64$	GB	19.16	$nextterm$	3.08	
	$C = 14$	$lift$	6.02	$dependency$	12.60	
		$steps$	41	$steps$	3	
s7	$n = 7$		300.60		389.34	1
	$d = 2$	$weight$	15.04	$normalf$	39.52	
	$D = 127$	GB	191.04	$nextterm$	51.30	
	$C = 122$	$lift$	89.56	$dependency$	293.50	
		$steps$	144	$steps$	7	

The ratio here is at most 24, and in two cases it goes down to 1.

In the implementation of the FGLM sequence one often has to deal with weight vectors whose entries are big integers. By using the `relint` function of the convex package, one can always find a weight vector with smaller entries that lies in the cone of the intermediate basis, and refine this vector to a term ordering that lies within the cone of the basis. Since this vector is computed after having converted the basis, we do not require that it has positive entries. Using smaller weight vectors for normal forms computations with respect to the old basis also seems to speed up this part of the algorithm, but we haven't investigated that in detail yet.

In a future implementation of the FGLM sequence it might be helpful to keep track at each step the polynomials in the previous bases in order to

skip some dependency computations. It is often the case, in fact, that two reduced Gröbner bases of the same ideal have one or more polynomials in common.

5.2 Positive dimensional ideals

For positive dimensional ideals we compared the runtimes of the Gröbner walk with the runtime of a sequence of FGLM conversions to sequential orderings as in the previous section. Each FGLM conversion was carried out with the algorithm described in Section 4.3. In the following table we list a few examples where we compared the two algorithms . For each system, we listed

- n, the number of variables
- d, the maximum total degree of the generators
- k, the dimension of the ideal
- C, the number of digits of the longest coefficients in the final basis

The third and fourth columns contain the timings obtained when running `GWalk` and a sequence of FGLM conversions to sequential orderings, as in the previous section.

	Info	GW		FGLM		ratio
b1	$n = 3$		.03		18.66	622
	$d = 3$	$weight$	0	$normalf$	1.22	
	$k = 1$	GB	0	$nextterm$	.43	
	$C =$	$lift$	.01	$dependency$	14.747	
		$steps$	1	$steps$	1	
b2	$n = 4$		.21		3.99	19
	$d = 3$	$weight$	.08	$normalf$	.45	
	$k = 1$	GB	.04	$nextterm$	.08	
	$C = 2$	$lift$	.05	$dependency$	2.05	
		$steps$	5	$steps$	1	
b3	$n = 4$		3.07		> 6000	> 1954
	$d = 31$	$weight$	.40	$normalf$		
	$k = 1$	GB	.83	$nextterm$		
	$C = 3$	$lift$	1.54	$dependency$		
		$steps$	26			

It soon became clear to us that for positive dimensional ideals the Gröbner walk algorithm performs way better than the FGLM sequence. This extremely bad behaviour of the FGLM sequence can be easily explained by the fact that dependency relations have to be sought among very large families of terms, and these families get bigger whenever we increase the coordinates of the weight vector ω.

In the first two examples the sequence of FGLM conversions required just one step. Even in this case the Gröbner walk algorithm was much faster. In the third example we stopped the FGLM sequence after 6000 seconds while it was still completing the first step. By looking at the final Gröbner basis with respect to the pure lexicographic ordering $\prec_{plex}$ and the variables ordered by $x > y > z > t$, one can see that the smallest i such that the weight vector

$$\omega_i = (2^{i^3}, 2^{i^2}, 2^i, 1)$$

is contained in the cone of $\prec_{plex}$ is 3. Therefore the sequence of FGLM conversions would have required 3 steps.

Let `diff_vectors` be a Maple procedure that computes the set of difference vectors of a set of polynomials given its initial terms. Then the following Maple session shows how to check if the vectors $(64, 16, 4, 1)$ and $(512, 64, 8, 1)$ belong to the cone `M1` generated by the difference vectors, that is the cone of $\prec_{plex}$, by using the function `iscontained` from the `Convex` package.

```
> with(Ore_algebra): with(Groebner):

with(casa): with(convex):

> A:=poly_algebra(x,y,z,t):

> F:=[x^8-z, x^10-t, x^31-x^6-x-y];

                    8       10       31    6
          F := [x  - z, x   - t, x   - x  - x - y]

> Told:=termorder(A,tdeg(x,y,z,t)):

> Tnew:=termorder(A,plex(x,y,z,t)):

> Gold:=gbasis(F,Told):
```

```
> Gnew:=GWalk(Gold,[x,y,z,t]):

> LT:=map(leadterm,Gnew,Tnew):

                          [x, y, z, t]

> dv:=diff_vectors([x,y,z,t],Gnew,LT):

> M1:=intersection(op(dv));

                 M1 := cone(4, 4, 0, 4, 4)

> a:=4: iscontained([a^3,a^2,a,1],M1);

                              false

> a:=8: iscontained([a^3,a^2,a,1],M1);

                              true
```

Bibliography

[1] SymbolicData Benchmark problems. Available at http://www.symbolicdata.org.

[2] W. Adams and P. Loustaunau. *An introduction to Gröbner Bases*. Graduate studies in mathematics. American Mathematical Society, 1994.

[3] K. Aigner. Maple V procedure for the computation of Gröbner bases by the Gröbner walk. RISC Linz Report Series 97-14, Research Institute for Symbolic Computation, 4040 Linz, Austria, Europe, 1997.

[4] B. Amrhein and O. Gloor. The Fractal Walk. In B. Buchberger and F. Winkler, editors, *Gröbner Bases and Applications*, pages 305–322. London Mathematical Society, 1998.

[5] B. Amrhein, O. Gloor, and W. Küchlin. Walking faster. In *Design and Implementation of Symbolic Computation Systems*, pages 150–161, 1996.

[6] B. Amrhein, O. Gloor, and W. Küchlin. On the Walk. *Theoretical Computer Science*, 187(1–2):179–202, 1997.

[7] E. Babson, S. Onn, and R. Thomas. The Hilbert Zonotope and a Polynomial Time Algorithm for Universal Gröbner Bases. *Advances in Applied Mathematics*, 30(3):529–544, April 2003.

[8] E. Becker, T. Mora, M.G. Marinari, and C. Traverso. The shape of the Shape Lemma. In *ISSAC '94: Proceedings of the 1994 International Symposium on Symbolic and Algebraic Computation: July 20–22, 1994, Oxford, England, United Kingdom*, pages 129–133. ACM press, 1994.

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

[10] A. Brondsted. *An introduction to convex polytopes*. Springer, 1982.

[11] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassringes nach einem nulldimensionalen Polynomideal*. PhD thesis, University of Innsbruck, 1965.

[12] B. Buchberger. Gröbner bases: an algorithmic method in polynomial ideal theory. In *Recent trends in multidimensional system theory*, pages 184–232. Springer, 1985.

[13] B. Buchberger. Introduction to Gröbner bases. In B. Buchberger and F. Winkler, editors, *Gröbner Bases and Applications*, pages 3–31. London Mathematical Society, 1998.

[14] S. Collart, M. Kalkbrener, and D. Mall. Converting bases with the Gröbner walk. *Journal of Symbolic Computation*, 24(3–4):465–470, 1997.

[15] S. Collart and D. Mall. Toric degenerations of polynomial ideals and complex duality. In *Proceedings of the Rhine Workshop on Computer Algebra*, pages 147–154, 1994.

[16] S. Collart and D. Mall. The ideal structure of Gröbner base computations. In *Integrating Symbolic Mathematical Computation and Artificial Intelligence*, volume 958 of *LNCS*, pages 156–166. Springer, 1995.

[17] S. Collart and D. Mall. A combinatorial result on Gröbner fans with an application to universal gröbner bases. *Applicable Algebra in Engineering, Communication and Computing*, 7(5):365–375, 1996.

[18] S. Collart and D. Mall. Toric degenerations of polynomial ideals and geometric localization of fans. *Journal of Symbolic Computation*, 24(3–4):443–464, 1997.

[19] P. Conti and C. Traverso. Buchberger algorithm and integer programming. In *AAECC 9*, volume 539 of *LNCS*. Springer, 1991.

[20] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms*. Springer, 1996.

[21] D. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry*. Springer, 1997.

[22] B. A. Davey and H. A. Priestley. *Introduction to lattices and order*. Cambridge University Press, 1990.

[23] T. D. Dubé. The structure of polynomial ideals and Gröbner bases. *SIAM Journal of Computing*, 19:750–773, 1990.

[24] J. Erdös. On the structure of ordered real vector spaces. *Publ. math. Debrecen*, 1956.

[25] G. Ewald. *Combinatorial Convexity and Algebraic Geometry*. Springer, 1996.

[26] 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.

[27] Matthias Franz. convex - a Maple package for convex geometry, Version 0.93. Available at http://www.mathe.uni-konstanz.de/ franz/convex, 2001.

[28] R. Fröberg. *An Introduction to Gröbner bases*. John Wiley & Sons, 1997.

[29] A. M. W. Glass. *Partially ordered groups*. Series in Algebra. World Scientific, 1999.

[30] H. Hahn. Über die nichtarchimedischen Grössensysteme. *Sitzungsbericht der Akad. Wiss. Wien*, 1907.

[31] R. Hemmecke and F. Winkler. CASA user manual (version casa 2.5). RISC Linz Report Series 00-30, Research Institute for Symbolic Computation, 4040 Linz, Austria, Europe, September 2000.

[32] Ralf Hemmecke, Erik Hillgarter, and Franz Winkler. The CASA system. In J. Grabmeier, E. Kaltofen, and V. Weispfenning, editors, *Handbook of Computer Algebra: Foundation, Applications, Systems*. Springer, Heidelberg, 2000.

[33] S. Hosten and R. Thomas. Gröbner bases and integer programming. In B. Buchberger and F. Winkler, editors, *Gröbner Bases and Applications*, pages 144–158. London Mathematical Society, 1998.

[34] D. T. Huyn. A superexponential lower bound for Gröbner bases and Church-Rosser Thue systems. *Inf. Control*, 68:196–206, 1986.

[35] M. Kalkbrener. On the complexity of Gröbner bases conversion. *Journal of Symbolic Computation*, 28(1–2):265–273, 1999.

[36] K. Kalorkoti. Counting and Gröbner bases. *Journal of Symbolic Computation*, 31:307–313, 2001.

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

[38] M. Kreuzer and L. Robbiano. *Computational commutative algebra*. Springer, 2000.

[39] S. Licciardi and T. Mora. Implicitization of hypersurfaces and curves by the Primbasissatz and basis conversion. In *Design and Implementation of Symbolic Computation Systems*, pages 150–161, 1996.

[40] D. G. Luenberger. *Linear and nonlinear programming*. Addison-Wesley, 1984.

[41] H. Minkowski. *Geometrie der Zahlen*. Leipzig, 1896.

[42] B. Mishra. *Algorithmic Algebra*. Springer, 1993.

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

[44] L. Robbiano. Term orderings on the polynomial ring. In *EUROCAL 85*, Lecture Notes in Computer Science. Springer, 1985.

[45] L. Robbiano. On the Theory of Graded Structures. *Journal of Symbolic Computation*, 2(2):139–170, 1986.

[46] G. Roda. On the classification of term ordering types. *WSEAS Transactions on Mathematics*, 2(30):116–121, 2003.

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

[48] B. Sturmfels. *Gröbner bases and convex polytopes*. University lecture series. American Mathematical Society, 1995.

[49] Quoc-Nam Tran. A fast algorithm for Gröbner basis conversion and its applications. *Journal of Symbolic Computation*, 30(4):451–467, October 2000.

[50] V. Weispfenning. Admissible orders and linear forms. *ACM SIGSAM Bulletin*, 21:16–18, 1987.

[51] F. Winkler. *Polynomial algorithms in computer algebra*. Springer, 1996.

[52] G. Ziegler. *Lectures on Polytopes*. Springer, 1995.

Index

Appendix A

Benchmarks

Zero-dimensional systems

The following table contains examples of zero-dimensional polynomial systems from the SymbolicData library ([1]).

a1	$[x, y, z]$ $y^4 + xy^2z + x^2 - 2xy + y^2 + z^2$ $xy^4 + yz^4 - 2x^2y - 3$ $-x^3y^2 + xyz^3 + y^4 + xy^2z - 2xy$
a2	$[x, y, z]$ $2y + 2z + x - 1$ $2yz + 2yx - y$ $2y^2 + 2z^2 + x^2 - x$
a3	$[u_0, u_1, u_2, u_3, u_4]$ $u_0 + 2u_1 + 2u_2 + 2u_3 + 2u_4 - 1$ $2u_1u_2 + 2u_0u_3 + 2u_1u_4 - u_3$ $u_1^2 + 2u_0u_2 + 2u_1u_3 + 2u_2u_4 - u_2$ $2u_0u_1 + 2u_1u_2 + 2u_2u_3 + 2u_3u_4 - u_1$ $u_0^2 + 2u_1^2 + 2u_2^2 + 2u_3^2 + 2u_4^2 - u_0$
a4	$[x_1, x_2]$ $x_1^2 + x_2^2 - 10$ $x_1^2 + x_1x_2 + 2x_2^2 - 16$
a5	$[a, b, c]$ $a^2bc + ab^2c + abc^2 + abc + ab + ac + bc$ $a^2b^2c + ab^2c^2 + a^2bc + abc + bc + a + c$ $a^2b^2c^2 + a^2b^2c + ab^2c + abc + ac + c + 1$

a6	$[x, y]$ $y^2 + 2x - 7y + 5$ $x^2 + 6x + 3y - 4$
a7	$[x, y, z]$ $y^2 + 2x - 7y + 2z + 5$ $x^2 + 6x + 3y + 6z - 4$ $x^2 + y^2 + z^2 - 1$
a8	$[x_1, x_2, x_3]$ $-5x_1^2 + 2x_1x_2 - 2x_2^2 + 8x_1x_3 - 10x_2x_3 - 13x_3^2 + x_1 - x_2$ $-2x_1^2 - 2x_2^2 - 4x_1x_3 - 4x_2x_3 - 4x_3^2 + x_1 + x_2$ $6x_1^2 - 4x_1x_2 + 3x_2^2 - 8x_1x_3 + 10x_2x_3 + 13x_3^2 - 1$
a9	$[x, y, z]$ $2x^2 + 3y^2 + 7xz + 9yz + 5z^2 + 4x$ $3x^4 + 6y^3 + xyz + 3xz^2 + 2yz^2 + 4z^2 + 5$ $3y^4z + 7x^3 + 10z^3 + 8xy + 12y^2 + 18xz + 12$
a10	$[x, y]$ $x^4 + y^4 - 1$ $x^5y^2 + x^2y^5 - 4x^3y^3 - 1$
a11	$[x, y, z]$ $2x^2 + 4xy + 3y^2 + 7xz + 9yz + 5z^2 + 2$ $3x^2 + xy + 6y^2 + 3xz + 2yz + 4z^2 + 5$ $7x^2 + 8xy + 12y^2 + 18xz + 3yz + 10z^2 + 12$
a12	$[x, y, z]$ $7xy + 3yz + x + 4y + 2z + 10$ $x^3 + x^2y + 2y^3 + 3xyz + 6y^2z + 5xy + yz + 3x + 1$ $3x^4 + 2x^2y^2 + 4x^2z^2 + 5z^4 + 3x^2y + xyz + 6y^2z + xz^2$
a13	$[x_1, x_2, x_3]$ $-4x_1 + x_2 + x_3 - 3$ $5x_1^2 + 3x_2^2 + 4x_3^2 + 2x_1 - 1$ $5x_3^3 + 16x_1^2 + 3x_2^2 - 1$
a14	$[x_1, x_2, x_3, x_4]$ $-4x_1 + x_2 + x_3 + x_4$ $-4x_1^2 + x_2^2 + x_3^2 + x_4^2 + 4x_1 + x_2 + x_3 + x_4 - 3$ $5x_1^3 + 4x_3^2x_4 + 3x_2^2 + 2x_1x_4 + 4x_1 + x_2 + x_3 + 2x_4 - 1$ $5x_3^4 + x_4^3 + 16x_1^2 + 3x_2^2 - 4x_4 - 1$
a15	$[x, y, z]$ $4x + 5y + 6$ $2x^2z + 4y^2z + 4yz^2 + 3xy + 25y^2 + 7xz + 2y - 3z$ $x^2y + 3xyz + xz^2 + 15x^2 + xy + 9yz + 7$

a16	$[x, y]$ $xy^2 + x + y + 1$ $7x^2y^2 + x^2y + x + y$
a17	$[t_1, t_2, t_3]$ $4t_2^2t_3^2 + 2t_2^2 + 5t_2t_3 + 3t_3^2 + 1$ $4t_1^2t_3^2 + 3t_1^2 + 5t_1t_3 + 2t_3^2 + 1$ $4t_1^2t_2^2 + 2t_1^2 + 5t_1t_2 + 3t_2^2 + 1$
a18	$[x, y, z, w]$ $-3w^2 + x + 3y + 2z + 13$ $-11z^2 + x + 3z + 7w - 9$ $4y^2 + 4x + 3z + 2w + 4$ $5x^2 + 6x + 3y + 6z + 2w + 3$
a19	$[x, y, z, w]$ $-3w^2 + x + 3y + 2z + 13$ $-11z^2 + x + 3z + 7w - 9$ $4y^2 + 4x + 3z + 2w + 4$ $5x^2 + 6x + 3y + 6z + 2w + 3$
a20	$[w, x, y, z]$ $-2w^2 + 9wx + 8x^2 + 9wy + 9xy + 6y^2 - 7wz -$ $\quad -3xz - 7yz - 6z^2 - 4w + 8x + 4y + 8z + 2$ $3w^2 - 5wx + 4x^2 - 3wy + 2xy + 9y^2 - 6wz -$ $\quad -2xz + 6yz + 7z^2 + 9w + 7x + 5y + 7z + 5$ $7w^2 + 5wx + 2x^2 + 3wy + 9xy - 4y^2 - 5wz -$ $\quad -7xz - 5yz - 4z^2 - 5w + 4x + 6y - 9z + 2$ $8w^2 + 5wx + 5x^2 - 4wy + 2xy + 7y^2 + 2wz -$ $\quad -7xz - 8yz + 7z^2 + 3w - 7x - 7y - 8z + 8$
a21	$[x, y, z, t]$ $2yzt + xt^2 - x - 2z$ $y^2z + 2xyt - 2x - z$ $-xz^3 + 4yz^2t + 4xzt^2 + 2yt^3 + 4xz + 4z^2 - 10yt - 10t^2 + 2$ $-x^3z + 4xy^2z + 4x^2yt + 2y^3t + 4x^2 - 10y^2 + 4xz - 10yt + 2$
a22	$[x, y]$ $3x^2y^9 + y^9 + 5x^4$ $9x^3y^8 + 11y^{10} + 9xy^8$
a23	$[x, y, z]$ $x^2yz + xy^2z + xyz^2 + xyz + xy + xz + yz$ $x^2y^2z + xy^2z^2 + x^2yz + xyz + yz + x + z$ $x^2y^2z^2 + x^2y^2z + xy^2z + xyz + xz + z + 1$

a24	$[y, z, x, t]$ $2yzt + xt^2 - 2z - x$ $y^2z + 2yxt - z - 2x$ $-z^3x + 4yz^2t + 4zxt^2 + 2yt^3 + 4z^2 + 4zx - 10yt - 10t^2 + 2$ $4y^2zx - zx^3 + 2y^3t + 4yx^2t - 10y^2 + 4zx + 4x^2 - 10yt + 2$
a25	$[t, x, y, z]$ $t^2z + x^2z + y^2z + z - 1$ $t^2y + x^2y + yz^2 + y - 1$ $tx^2 + ty^2 + tz^2 + t - 1$ $t^2x + xy^2 + xz^2 + x - 1$
a26	$[w, x, y, z]$ $-2w^2 + 9wx + 8x^2 + 9wy + 9xy + 6y^2 - 7wz-$ $\quad -3xz - 7yz - 6z^2 - 4w + 8x + 4y + 8z + 2$ $3w^2 - 5wx + 4x^2 - 3wy + 2xy + 9y^2 - 6wz-$ $\quad -2xz + 6yz + 7z^2 + 9w + 7x + 5y + 7z + 5$ $7w^2 + 5wx + 2x^2 + 3wy + 9xy - 4y^2 - 5wz-$ $\quad -7xz - 5yz - 4z^2 - 5w + 4x + 6y - 9z + 2$ $8w^2 + 5wx + 5x^2 - 4wy + 2xy + 7y^2 + 2wz-$ $\quad -7xz - 8yz + 7z^2 + 3w - 7x - 7y - 8z + 8$
a27	$[x, y, z]$ $xy^3 + y^4 - 2xz^3 + yz^2 - z^3$ $x^3y + 2xy^2z + 2x^2y$ $2x^3y + yz^3 - 3x^2y + 2$
a28	$[z, y, x]$ $y^4 + zy^2x + z^2 + y^2 - 2yx + x^2$ $z^3yx - y^2x^3 + y^4 + zy^2x - 2yx$ $z^4y + y^4x - 2yx^2 - 3$

The following table contains examples from the article [6] by Amrhein, Gloor, and Küchlin.

Ex1	$[z, y, x]$ $xy^3 + y^4 + yz^2 - z^3 - 2xz^3$ $2x^2y + x^3y + 2xy^2z$ $2 - 3x^2y + 2x^3y + yz^3$
Ex2	$[z, y, x]$ $x + 3xy^3 + y^4 + yz^2$ $-x^2z + 2y^3z + z^2 + 2yz^2 + 3xyz^2$ $3x^3 + xy^2 + yz^2 - 2xz^3$

Ex3	$[z, y, x]$ $x^2 + y^4 + x^3z + yz - 2xz^3$ $x^2y^2 + y^3z + z^3 + 3yz^3$ $y^4 - x^2z + 2y^2z - 2xyz^2$
s6	$[x_1, x_2, x_3, x_4, x_5, x_6]$ $2x_6x_2 + 2x_5x_3 + x_4^2 + x_1^2 + x_1$ $2x_6x_3 + 2x_5x_4 + 2x_2x_1 + x_2$ $2x_6x_4 + x_5^2 + 2x_3x_1 + x_3 + x_2^2$ $2x_6x_5 + 2x_4x_1 + x_4 + 2x_3x_2$ $x_6^2 + 2x_5x_1 + x_5 + 2x_4x_2 + x_3^2$ $2x_6x_1 + x_6 + 2x_5x_2 + 2x_4x_3$
s7	$[x_1, x_2, x_3, x_4, x_5, x_6, x_7]$ $2x_7x_2 + 2x_6x_3 + 2x_5x_4 + x_1^2 + x_1$ $2x_7x_3 + 2x_6x_4 + x_5^2 + 2x_2x_1 + x_2$ $2x_7x_4 + 2x_6x_5 + 2x_3x_1 + x_3 + x_2^2$ $2x_7x_5 + x_6^2 + 2x_4x_1 + x_4 + 2x_3x_2$ $2x_7x_6 + 2x_5x_1 + x_5 + 2x_4x_2 + x_3^2$ $x_7^2 + 2x_6x_1 + x_6 + 2x_5x_2 + 2x_4x_3$ $2x_7x_1 + x_7 + 2x_6x_2 + 2x_5x_3 + x_4^2$

Positive dimensional systems

b1	Neff-89 $[z, y, x]$ $2zy + 2y^2zx + x^2 - 3z - y - 2x$ $z^2 - 8zy - 4y^2 + 4zx + 3x^2 - 4x + 1$
b2	Wang-92c $[d, c, b, a]$ $-3dc + b^2 - 2a + 2$ $-3da^2 - 4cb + 2b^2 - 6ca + 3ba$ $-3dc^2 + cb^2 - da + b$
b4	TD-89 $[x, y, z, t]$ $x^8 - z$ $x^{10} - t$ $x^{31} - x^6 - x - y$

Curriculum vitae

Geboren 1966 in Trento (Italien), Kindheit und Jugend in Catania, Cosenza und Udine.
Studium der Mathematik in Bologna 1985-1992.
Dr.-Studium am RISC Institut in Linz 1992-1996.
Verschiedene Jobs als Programmiererin in Linz, Salzburg und Wien 1996-2003.
Wissenschaftliche Arbeiten:

- *Aspetti algoritmici in algebra commutativa*, Diplomarbeit, Universität Bologna, 1992
- *On the transformation of Gröbner bases*, Präsentation im CoCoA IV Workshop, 1995
- *Linear algebra methods for the transformation of Gröbner bases*, Tech. Rep. RISC No. 95-54, 1995
- *On the classification of term orderings types*, WSEAS Transactions on Mathematics, 2(30), 2003