Notes on Gröbner Basis

Bud Mishra and Chee Yap
Courant Institute of Mathematical Sciences
New York University
New York, N.Y.10012

June 1, 1987

Abstract

We present a self-contained exposition of the theory of Gröbner basis and its applications.

1 Introduction

These notes attempt to present in a self-contained manner the basic facts about the theory of Gröbner basis and related algorithms. Except for an excellent survey on the subject by Buchberger [Buchberger 1985] the literature on the subject is somewhat scattered. Since our interest is in complexity of algorithms, we attempt to give quantitative forms of theorems whenever possible. Much of the material in these notes is ultimately owed to Buchberger even if not explicitly mentioned.

A Gröbner basis is a special basis for a multivariate polynomial ideal over a field with certain attractive computational properties. It turns out that many important computational problems involving ideals can be easily solved once we have a Gröbner basis for the ideals. Buchberger defined the concept in his PhD thesis in 1965, naming it for his teacher, W. Gröbner. Buchberger also gave an algorithm (the 'basic algorithm' in section 3) to construct them. The closely related concept of *standard bases* was defined by Hironaka [Hironaka 1964] – see the appendix for the connection.

More generally, this area falls under that of computational algebraic geometry. Hilbert is often cited as launching the mainstream modern mathematical trend which favors non-constructive results. In particular Hilbert solved the outstanding problem in the theory of invariants via his celebrated Basis Theorem: that every polynomial ideal has a finite basis. In a sense, he invented his solution of Basis Theorem because his solution was not in the spirit of what the geometers of his day (Gordan was the principal representative) were trying to do. The geometers were trying to give constructive or algorithmic solutions. Hilbert turned it into an existence question, although he was later able to return to the original problem to give a satisfactory construction. As for the trend towards non-constructive abstractions, the subject of algebraic geometry itself is the best illustration of the phenomenon (see the historical survey of the whole subject till present day in [Dieudonné 1985]). Meanwhile, the constructive spirit in algebraic geometry has survived, though not thrived. A key paper in this regards is that of Hermann [Hermann 1926]. Another more modern attempt to return to the classical questions is Seidenberg [Seidenberg 1974]. Since then a number of papers have begun to revitalize this area, and among the reasons for this is the promise of practical computational algebra systems.

We would like to make two remarks here: a prominent algebraic geometer advocating the constructive viewpoint is Abhyankar (see his delightful historical exposé in [Abhyankar 1976]). As computer scientists, we take Professor

Abhyankar's viewpoint to the extreme[1]: we regard the existence of a construction only as a first step towards a precise classification of the inherent computational complexity of a computational algebraic problem. Studies motivated by this extreme requirement might be termed *algorithmic algebraic geometry.* It is our belief that this standpoint can transform a large area of classical algebraic geometry to a new level of beauty and understanding. Already this algorithmic standpoint has revived the study of elementary Euclidean geometry. The other remark is the following: the study of algorithmic algebraic geometry implies *quantitative algebraic geometry* in which a variety of bounds are sought. To illustrate this point, Hilbert's basis theorem tells us that all ascending chains of polynomial ideals are finite. We seek to bound the length of such chains. (It appears that we cannot bound the length as a function of the initial ideal alone [Seidenberg 1971]). Or again, Hillbert's Nullstellensatz says that if f vanishes at all the zeroes of an ideal $I \subseteq k[x_1, \ldots, x_n]$ where k is algebraically closed then $f^d \in I$ for some d. In fact it had been noted that d depends only on I, not on f. We again ask for good bounds on d as a function of the size of I.

2 Basic Terminology

Let us fix a polynomial ring $R = K[x_1, \ldots, x_n]$, $n \geq 1$, and K is any field. Given elements $a, b \in R$ we say that a *divides* b, equivalently b is a *multiple* of a, if $b = ac$ for some $c \in R$. If $a_1, \ldots, a_n$ are elements in R and $F \subseteq R$ then the ideals generated by $\{a_1, \ldots, a_n\}$ and F (respectively) are denoted by $(a_1, \ldots, a_n)$ and (F).

A *power product* is an element of R of the form

$$p = x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}, \ e_i \geq 0.$$

Sometimes power products are also called *terms.* The *total degree* of p is $deg(p) = \sum_{i=1}^{n} e_i$. The degree of p in any variable x_i is $deg_{x_i}(p) = e_i$. The *least common multiple (LCM)* of two power products $p = x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ and $q = x_1^{d_1} x_2^{d_2} \cdots x_n^{d_n}$ is given by $x_1^{\max(d_1, e_1)} \cdots x_n^{\max(d_n, e_n)}$. A *monomial* is a term of the form ap where $a \in K$ and p is a power product. The *length* of a polynomial is the number of monomials that occurs in it. The *LCM* of two monomials am and $a'm'$, where $a, a' \in K$ and m, m' are power products, is

[1] Alternatively, as computer scientists, we have more precise notions of constructiveness and a rich vocabulary to make finer distinctions.

defined as follows:

$$LCM(am, am') = aa' \cdot LCM(m, m').$$

We remark that if K is an Euclidean domain then a better definition of the LCM would be $LCM(a, a') \cdot LCM(m, m')$.

Let $\mathrm{PP} = \mathrm{PP}(x_1, \ldots, x_n)$ be the set of all power products involving $x_1, \ldots, x_n$. A total ordering $\underset{A}{\leq}$ on the set of power products is said to be *admissible* if for all power products p, q, (i) $1 \underset{A}{\leq} p$ and (ii)

$$(\forall a \in \mathrm{PP})\ p \underset{A}{\leq} q \ \Rightarrow\ ap \underset{A}{\leq} aq$$

The main examples of admissible orderings are *(pure) lexicographical ordering* (i.e. $p \underset{A}{>} q$ if $d_i > e_i$ at the smallest index i where the exponents d_i, e_i of x_i in p, q differ) and the *total degree ordering* (i.e. $p \underset{A}{>} q$ if either $deg(p) > deg(q)$ or, in case $deg(p) = deg(q)$, then p is lexicographically greater than q.) Note that both the lexicographical and total degree ordering are completely specified by a total ordering on the variables, say, $x_1 \underset{A}{\leq} \cdots \underset{A}{\leq} x_n$.

Remark 2.1 Admissible orderings are sometimes called *term orderings* in the literature. Any ordering that satisfies (ii) (but not necessarily (i)) may be called *semi-admissible*. For instance, the *reverse* of any admissible ordering is semi-admissible. One crude classification of semi-admissible orderings is given by the total order imposed on the set $\{1, x_1, x_2, \ldots, x_n\}$; a more intrinsic classification is by their order-type (e.g. the order-types of total degree ordering and pure lexicographical ordering are ω and ω^n, respectively).

Henceforth, fix $\underset{A}{\leq}$ to be any admissible ordering. We also write $f \underset{A}{>} g$ if $f \neq g$ and $g \underset{A}{\leq} f$. Let $f \in R$ be a polynomial. The *head monomial* Hmono(f) of f is the monomial in f whose power product is largest relative to $\underset{A}{\leq}$. (If $f = 0$ we define Hmono$(f) = 0$.) For instance, relative to the total degree ordering, the head term of $f = 4xy + y - 5$ is $H(f) = 4xy$. We may define the *head term* Hterm(f) to be the power product in Hmono(f); the definition of *head coefficient* Hcoef(f) of f is then clear. Thus Hmono$(f) =$ Hcoef$(f) \cdot$ Hterm(f). Ocassionally, it is useful to have the notation Tail(f) for $f -$ Hmono(f).

For any set S of polynomials, let the *head ideal* of S, denoted Head(S), be the ideal $(\{Hmono(f) : f \in S\})$ generated by the head monomials in S. This definition will be important for one characterization of Gröbner bases.

A basic concept in Gröbner basis is the idea of *reduction*. Given two polynomials $f, g \in R$, we say f is *reducible* by g if $\mathrm{Hmono}(g)$ divides some monomial m in f. Say $m = c \cdot \mathrm{Hmono}(g)$. Then we say the polynomial $h = f - c \cdot g$ is the *reduct* of f by g and denote the relationship by

$$f \xrightarrow{g} h.$$

We say that the monomial m (or the corresponding power product p) is *eliminated by application of* g in this case. If G is a set of polynomials, we write $f \xrightarrow{G} h$ if $f \xrightarrow{g} h$ holds for some $g \in G$. If there is a finite sequence $h_1, h_2, \ldots, h_n$ $(n \geq 1)$ such that $h_1 = f, h_n = h$ and $h_i \xrightarrow{G} h_{i+1}$ for $i = 1, \ldots, n-1$, then we write

$$f \xrightarrow[*]{G} h.$$

If f is not reducible by any $g \in G$, we indicate this by writing $f \xrightarrow{G} f$. We say h is a *G-normal form* of f if $f \xrightarrow[*]{G} h \xrightarrow{G} h$, and we write $\mathrm{NF}_G(f)$ for the set of all G-normal forms of f. It is important to realize that the G-normal form of f is not unique in general, and the central idea in Gröbner basis is to enlarge ('complete') G so that it becomes unique. Finally, we are ready for the main definition: A finite set $G \subseteq R$ is said to be a *Gröbner basis* (for the ideal generated by G) if the G-normal form of every polynomial f is unique, i.e., $|\mathrm{NF}_G(f)| = 1$.

Remark 2.2 Computationally, it may be more efficient (asymptotically) to use the reflexive transitive closure of $\xrightarrow{g}$. If $\overset{g}{\Rightarrow}$ denotes this closure, then $f \overset{g}{\Rightarrow} h$ implies that no monomial in h is a multiple of $\mathrm{Hmono}(g)$.

It turns out that the concept of a Gröbner basis is intimately related to that of the *S-polynomial* $S(f, g)$ of two polynomials $f, g \in R$. This is defined by

$$S(f, g) = \frac{m}{\mathrm{Hmono}(f)} f - \frac{m}{\mathrm{Hmono}(g)} g$$

where $m = LCM(\mathrm{Hmono}(f), \mathrm{Hmono}(g))$. For example, assuming a total degree ordering,

$$S(2x^2y + xy + y^2 - 3, 5y^2 - y + x) = 5y(xy + y^2 - 3) - 2x^2(-y + x).$$

Example 2.3 Admissible orderings can be quite complex. The following example is due to T. Dubé: it shows an ordering on $\mathrm{PP}(x, y, z)$ with the property that the restriction of the ordering to $\mathrm{PP}(x, y)$ is a total degree ordering with $y \underset{A}{>} x$, $x \underset{A}{>} z^i$ and $y \underset{A}{>} z^i$ for all i and yet $xz \underset{A}{>} y$. The rule is this. Suppose $m = x^a y^b z^c$ and $m' = x^{a'} y^{b'} z^{c'}$. Then $m \underset{A}{>} m'$ iff one of the following sequence of tests yields an affirmative answer when applied in the indicated order: (1) $a + b > a' + b'$, (2) $c > c'$, (3) $a < a'$. One should check that this is an admissible ordering and has the claimed properties.

3 Normal Form Algorithm

Henceforth we fix some admissible ordering $\underset{A}{\leq}$ on monomials. For any finite set $F \subseteq R$, we define a "non-deterministic" algorithm which for any input polynomial f, computes an element in $\mathrm{NF}_F(f)$. The algorithm is trivial: apply any reduction $\xrightarrow{g}$, $g \in F$, to transform the input polynomial f. Now as long as the (transformed input) polynomial is not in $\mathrm{NF}_F(f)$, repeat the reduction. We write $\mathrm{nf}_F(f)$ for the polynomial produced by this algorithm. All reductions in this section are relative to a fixed but arbitrary set F.

Before proving the termination of this algorithm we prove Dickson's lemma [Dickson 1913] and two general results on well-ordering.

Lemma 3.1 (Dickson) *Every set $X \subseteq \mathrm{PP}$ of monomials contains a finite subset $F \subseteq X$ such that each $m \in X$ is a multiple of some monomial in F.*

PROOF.

We use induction on the number n of variables. If $n = 1$ then we let F consist of the unique polynomial in X of minimum degree. So we may assume $n > 1$. Pick any $f_0 \in X$ and say

$$f_0 = x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}.$$

Then every $m \in X$ that is not divisible by f_0 belongs to one of $\sum_{i=1}^{n} e_i$ different sets: let $i = 1, \ldots, n$ and $v = 0, 1, \ldots, e_i - 1$. Then the set $X_{i,v}$ consists of those monomials $m \in X$ such that $deg_{x_i}(m) = v$. Let $X'_{i,v}$ denote the set of monomials obtained by omitting the factor x_i^v from monomials in $X_{i,v}$. By inductive hypothesis, there exists finite subsets $F'_{i,v} \subseteq X'_{i,v}$ such that each monomial in $X'_{i,v}$ is a multiple of some monomial in $F'_{i,v}$. We obtain $F_{i,v}$ as $\{m \cdot x_i^v \ : \ m \in F'_{i,v}\}$. It is then clear that every monomial in X is a multiple of some monomial in the finite set

$$\{f_0\} \cup \bigcup_{i,v} F_{i,v}.$$

□

Lemma 3.2 *Every admissible ordering $\underset{A}{\leq}$ on* PP *is a well-ordering.*

PROOF.

This is an easy consequence of the Dickson's lemma. Suppose we have an infinite descending sequence of monomials

$$m_1 \underset{A}{>} m_2 \underset{A}{>} \cdots \underset{A}{>} m_i \underset{A}{>} \cdots.$$

Let $X = \{m_1, m_2, \ldots, m_i, \ldots\}$ and let $F \subseteq X$ be a finite subset such that every $m \in X$ is a multiple of some monomial in F. Let m' be the monomial that is smallest in F under the ordering $\underset{A}{\leq}$. Since every $m \in X$ is greater than some monomial in F, we have $m' \underset{A}{\leq} m$. Thus m' terminates the descending sequence, contradicting our assumption that the sequence is infinite. $\square$

For the next result, we need a definition. Let X be any set with a total ordering $\leq'$ and let $S(X)$ be the set of all finite decreasing sequences of elements of X:

$$S(X) = \{(x_1, x_2, \ldots, x_n) \ : \ x_i \in X, x_1 >' x_2 >' \cdots >' x_n\}$$

Let $S(X)$ have the following induced total-ordering:

$$(x_1, x_2, \ldots, x_n) \leq' (y_1, y_2, \ldots, y_m)$$

if either for some $i < \min(n, m)$, $x_1 = y_1, \ldots, x_i = y_i$ and $x_{i+1} <' y_{i+1}$, or else the sequence $(x_1, \ldots, x_n)$ is a prefix of the sequence $(y_1, \ldots, y_m)$ (thus $n < m$).

Lemma 3.3 *If X is well-ordered by $\leq'$ then $S(X)$ is well-ordered under the induced ordering.*

PROOF.

For the sake of contradiction, suppose $\sigma_1 >' \sigma_2 >' \cdots$ is an infinite descending chain in $S(X)$. Let $\sigma_i = (x_{i,1}, x_{i,2}, \ldots, x_{i,n(i)})$. There are two cases.

(i) The $n(i)$'s are bounded, say $k = \max\{n(i) \ : \ i = 1, 2, \cdots\}$. We use induction on k. We get an immediate contradiction for $k = 1$, so assume $k > 1$. If there are infinitely many i's such that $n(i) = 1$ then we get a contradiction from the subsequence consisting of such σ_i's. Hence we may assume that the $n(i)$'s are all greater than 1. Now there is an i_0 such that for all $i \geq i_0$, $x_{i,1} = x_{i+1,1}$. Let $\sigma'_i = (x_{i,2}, x_{i,3}, \ldots, x_{i,n(i)})$ be obtained from σ_i by omitting the leading item in the sequence. Then the sequence $\sigma'_{i_0}, \sigma'_{i_0+1}, \cdots$

constitute a strictly decreasing decreasing infinite chain with each σ_i' of length $< k$. This contradicts the inductive hypothesis.
(ii) The $n(i)$'s are unbounded. By taking a subsequence if necessary, we may assume that $n(i)$ is strictly increasing in i. Define $m(1)$ to be the largest index such that $x_{m(1),1} = x_{j,1}$ for all $j \geq m(1)$. For each $i > 1$ define $m(i)$ to be the largest index greater than $m(i-1)$ such that $x_{m(i),i} = x_{j,i}$ for all $j \geq m(i)$. Note that the sequence

$$x_{m(1),1}, x_{m(2),2}, x_{m(3),3}, \cdots$$

is strictly decreasing. This contradicts the well-foundedness of X. □

Theorem 3.4 *The normal-form algorithm terminates.*
PROOF.
We map a polynomial g to the sequence of monomials $\bar{g} = (m_1, \ldots, m_k)$ where m_i are the monomials occurring in g and $m_1 \underset{A}{>} m_2 \underset{A}{>} \cdots \underset{A}{>} m_k$. By the last two lemmas, the set of $\bar{g}$'s are well-ordered under the induced ordering $\underset{A}{\leq}$. It is seen that if $g \xrightarrow{F} h$ then $\bar{g} \underset{A}{>} \bar{h}$. The termination of the algorithm is equivalent to the well-foundedness of the induced ordering. □

4 Bounds on Normal Form Algorithms

We now quantify the termination process of the normal algorithm. More precisely, let $F \subseteq R$ be a finite set and $g \in R$. Let

$$g = g_0 \xrightarrow{F} g_1 \xrightarrow{F} \cdots \xrightarrow{F} g_k = \mathrm{nf}_F(g). \tag{1}$$

Our goal is to bound the maximum value of k in the reduction sequence (1). It is not surprising that the bounds will depend on (a) the strategy for choosing reduction steps and (b) the choice of admissible ordering. Note that the strategy in (a) includes the one of 'no strategy' (as implied in the description of the normal form algorithm in the last section). We will consider two important admissible orderings: total degree ordering and lexicographical ordering. The following notations will be used

F = a finite subset of R
g = input polynomial
n = the number of variables, $R = K[x_1, \ldots, x_n]$
d = the maximum degree in any variable x_i of polynomials in F

$\ell =$ the maximum length of any polynomial in F
$D =$ the maximum degree in any variable x_i of g
$m =$ the number of polynomials in F.

First we consider the easier case of total degree ordering.

Lemma 4.1 *If the total degree ordering is used, the number of reductions steps to derive* $\mathrm{nf}_F(g)$ *starting from* g *is bounded by* $2^{(D+1)^n}$.

PROOF.
Consider the polynomials g_i, $(i = 0, 1, \cdots)$ in the above reduction sequence (1). The number of power products where the maximum degree in any variable is D is $(D+1)^n$. Thus the number of distinct polynomials with such power products (modulo the map $g \mapsto \bar{g}$) is $2^{(D+1)^n}$. Since all the g_i are distinct, the desired bound in the lemma follows. $\square$

We next give a better bound under the assumption that the normal form algorithm always chooses to eliminate the $\underset{A}{\leq}$-largest monomial that could be eliminated. More precisely, suppose that in the reduction step $g_{i-1} \xrightarrow{F} g_i$ in (1) the monomial m_i is eliminated. We say that the reduction sequence (1) is *ordered* if

$$m_1 \underset{A}{>} m_2 \underset{A}{>} \cdots \underset{A}{>} m_k.$$

In the sequence (1), assume m_i is eliminated by application of $f_i \in F$. Thus

$$g_i = g_{i-1} - \alpha_i f_i$$

for some monomial α_i.

Lemma 4.2 *Under the total ordering, the length of an ordered reduction sequence is at most* $(D+1)^n$.

The proof is immediate. However we note that there may be members of $\mathrm{NF}_F(g)$ not reachable by ordered reduction sequences and furthermore, the shortest reduction sequence from g to some f by an ordered reduction sequence may actually be longer than allowing arbitrary reduction sequences.

Now we consider the case where $\underset{A}{\leq}$ is the lexicographical ordering. We had noted before that every admissible ordering can be crudely classified by considering the order on the n variables. We will assume in the rest of this paper that

$$x_n \underset{A}{>} x_{n-1} \underset{A}{>} \cdots \underset{A}{>} x_1.$$

We define a weighting function $W_F : \mathrm{PP} \to \mathbf{N}$ ($\mathbf{N}$ is the set of natural numbers) as follows:

$$W_F(x_1^{e_1} \cdots x_n^{e_n}) = e_1(d+1)^0 + e_2(d+1)^1 + \cdots + e_n(d+1)^{n-1}$$

If f is any polynomial, we extend the weight function to let $W_F(f)$ denote the weight function applied to the head term in f.

Note. Unlike the case of total ordering, our bounds for lexicographical ordering will depend on the set F. This is reflected in the appearance of the subscript F in the weighting function W_F (and also $\bar{W}_F$ to be introduced below). □

Lemma 4.3 *Let $f \in F$ and let m be any monomial. Write f as a sum of monomials, $f = f_1 + f_2 + \cdots + f_k$ where $f_1 \underset{A}{>} f_2 \underset{A}{>} \cdots \underset{A}{>} f_k$. Then for any monomial m, we have that $W_F(mf_{j-1}) > W_F(mf_j)$ for $j = 2, \ldots, k$..*

PROOF.
Let $f_{j-1} = x_1^{d_1} \cdots x_n^{d_n}$ and $f_j = x_1^{e_1} \cdots x_n^{e_n}$. Then $f_{j-1} \underset{A}{>} f_j$ iff there is some $i = 1, \ldots, n$ such that $d_n = e_n, d_{n-1} = e_{n-1}, \ldots, d_{i+1} = e_{i+1}$ and $d_i > e_i$. We get

$$\begin{aligned} W_F(mf_{j-1}) - W_F(mf_j) &= W_F(f_{j-1}) - W_F(f_j) \\ &\geq (d+1)^{i-1} - [(e_{i-1} - d_{i-1})(d+1)^{i-2} + \\ &\quad (e_{i-2} - d_{i-2})(d+1)^{i-3} + \cdots + (e_1 - d_1)(d+1)^0]. \end{aligned}$$

We note that $e_j - d_j$ is at most d (the maximum degree of any polynomial in F; hence the summation in the square brackets above is at most

$$d(d+1)^{i-2} + \cdots + d(d+1)^0 = (d+1)^{i-1} - 1.$$

Thus $W_F(mf_{j-1}) > W_F(mf_j)$. □

Now we define a weight function on polynomials. Recall that the length of each polynomial in F is at most ℓ. For any polynomial h where $h = h_1 + h_2 + \cdots + h_k$, $h_1 \underset{A}{>} h_2 \underset{A}{>} \cdots \underset{A}{>} h_k$, we define its weight to be

$$\bar{W}_F(h) = \sum_{i=1}^{k} (\ell)^{W_F(h_i)}.$$

Note that if the length of h is L and the maximum degree of any variable is D then $W_F(h_i) \leq (d+1)^n(D/d)$ and

$$\bar{W}_F(h) \leq \ell^{(d+1)^n(D/d)} L.$$

Lemma 4.4 *If* $f \xrightarrow{F} g$ *then* $\bar{W}_F(f) > \bar{W}_F(g)$.

PROOF.

Suppose $g = f - mh$ for some $h \in F$ and monomial m. Let the monomials of h be ordered as $h_1 \underset{A}{>} h_2 \underset{A}{>} \cdots$. Consider how the weight of g differ from that of f. The decrease in the weight of g over f due to the elimination of mh_1 is at least $\ell^{W_F(mh_1)}$. Clearly, all the new (i.e. not in f) monomials in g is of the form mh_i for some $i > 1$. Since there are at most $\ell - 1$ new monomials in g, the increase in the weight of g over f due to their presence is at most $(\ell-1)\ell^{W_F(mh_2)}$. Hence

$$\begin{aligned} \bar{W}_F(f) - \bar{W}_F(g) &\geq \ell^{W_F(mh_1)} - (\ell-1)\ell^{W_F(mh_2)} \\ &= \ell^{W_F(mh_1)} - \ell^{1+W_F(mh_2)} + \ell^{W_F(mh_2)}. \end{aligned}$$

By the previous lemma, $W_F(mh_1) > W_F(mh_2)$. Hence $\bar{W}_F(f) - \bar{W}_F(g) \geq \ell^{W_F(mh_2)} > 0$. $\square$

We immediately conclude:

Theorem 4.5 *Assuming the lexicographical ordering, the length of any sequence of reductions beginning from an input polynomial* g *is at most*

$$\bar{W}_F(g) \leq \ell^{(d+1)^n(D/d)} L$$

where L *is the length of* g, ℓ *is the maximum length of a polynomial in* F *and* D *is the maximum degree of* g *in any variable.*

In a subsequent paper [Dubé, Mishra and Yap 1986], we will extend the preceding analysis of normal form algorithms to arbitrary admissible orderings.

5 Characterizations of Gröbner Basis

Recall that a finite set $G \subseteq R$ is a Gröbner basis (for the ideal $I = (G)$) if the G-normal form of every polynomial is unique. We now present several alternative characterizations of Gröbner basis, in an effort to increase our understanding of the above definition.

We first note two general results on partial ordering relations. Let X be any set and $\longrightarrow$ be a binary relation on X and $\underset{*}{\longrightarrow}$ be its reflexive transitive closure. Let $g, g', h \in X$. We call h a *common successor* of g and g' if $g \underset{*}{\longrightarrow} h$ and $g' \underset{*}{\longrightarrow} h$. We say the relation $\longrightarrow$ is *Church-Rosser* if for all elements $f, g, g' \in X$ we have:

> $f \underset{*}{\longrightarrow} g$ and $f \underset{*}{\longrightarrow} g'$ implies that g and g' have a common successor.

The relation $\longrightarrow$ is *locally Church-Rosser* if for all elements $f, g, g' \in X$ we have:

> $f \longrightarrow g$ and $f \longrightarrow g'$ implies that g and g' have a common successor.

(Note: "Confluent" is an alternative terminology for "Church-Rosser".) The relation $\longrightarrow$ is *Noetherian* if there is no infinite sequence of the form $f_1 \longrightarrow f_2 \longrightarrow \cdots$. Note that if $\longrightarrow$ is Noetherian then $f \longrightarrow f$ must not hold for any $f \in X$. An element $f \in X$ such that $f \underset{*}{\longrightarrow} g$ implies that $f = g$ is said to be in *normal form.* Thus normal form elements are "minimal" elements (assuming the reduct of an element is smaller than the original). We say g is a normal form of f if $f \underset{*}{\longrightarrow} g$; the set of all normal forms of f is denoted $\mathrm{NF}(f)$.

Following are two general results about Noetherian relations. The first proof uses a very powerful principle called the *Principle of Noetherian Induction*:

> For a Noetherian relation $\longrightarrow$, to establish the validity of a predicate $P(x)$ for all $x \in X$, it is sufficient to show: if $P(y)$ holds for all y such that $x \underset{*}{\longrightarrow} y$ and $x \neq y$ then $P(x)$ holds.

Let us demonstrate the validity of this principle. Suppose that it is shown that $P(x)$ holds whenever $P(y)$ holds for all $y \neq x$ where $x \underset{*}{\longrightarrow} y$. For the sake of contradiction, suppose $P(x_0)$ fails. Then for some $x_1 \neq x_0$, $x_0 \underset{*}{\longrightarrow} x_1$ and $P(x_1)$ fails. Continuing in this fashion, we obtain an infinite descending sequence $x_0, x_1, x_2, \ldots$, which contradicts the Noetherian property.

Lemma 5.1 *Let $\longrightarrow$ be a Noetherian relation. Then it is Church-Rosser if and only if it is locally Church-Rosser.*

PROOF.

One direction is immediate. In the other direction, assume that the relation is locally Church-Rosser. Let $f \underset{*}{\longrightarrow} g$ and $f \underset{*}{\longrightarrow} h$. If $f = g$ or $f = h$ then the result is immediate. Otherwise, let $f \longrightarrow g' \underset{*}{\longrightarrow} g$ and $f \longrightarrow h' \underset{*}{\longrightarrow} h$. Since the relation is locally Church-Rosser, g' and h' have a common successor f'. By the principle of Noetherian induction (as applied to g'), g and f' have a common successor g''; similarly, h and f' have a common successor h''. By a third application of the principle to f', we get that g'' and h'' have a common successor f''. Clearly f'' is a common successor of g and h. $\square$

Lemma 5.2 *Let $\longrightarrow$ be a Noetherian relation on X. Then $\longrightarrow$ is Church-Rosser if and only if every element $f \in X$ has a unique normal form, $|\mathrm{NF}(f)| = 1$.*

PROOF.

($\Rightarrow$)
By our assumption that the relation is Noetherian, $\mathrm{NF}(f)$ is non-empty for any f. If $g, g' \in \mathrm{NF}(f)$, then the Church-Rosser property implies that g and g' have a common successor h. But g is in normal form implies $g = h$ and similarly $g' = h$.
($\Leftarrow$)
Suppose $f \underset{*}{\longrightarrow} g$ and $f \underset{*}{\longrightarrow} g'$. Then $\mathrm{NF}(g) \subseteq \mathrm{NF}(f)$. Since $\mathrm{NF}(g)$ is non-empty (Noetherian assumption) and $|\mathrm{NF}(f)| = 1$, we conclude that $\mathrm{NF}(g) = \mathrm{NF}(f)$. Thus f and g have a unique common normal form, say h. Similarly for f and g'. Thus h serves as the common successor of g and g'. $\square$

We now return to our original reduction relation $\xrightarrow{F}$ (for some fixed finite set F of polynomials). An immediate corollary of the last lemma gives us the first equivalent formulation of a Gröbner basis.

Corollary 5.3 *G is a Gröbner basis if and only if the relation $\xrightarrow[*]{G}$ is Church-Rosser.*

The following is a useful tool.

Lemma 5.4 *If $f - g \xrightarrow[*]{F} 0$ then f and g have a common successor.*

PROOF.
We use induction on the number of steps to get from $f - g$ to 0. If the number of steps is zero then the result is immediate. Otherwise, suppose

$$(f - g) \xrightarrow{F} h \xrightarrow[*]{F} 0.$$

It is sufficient to show that $h = f' - g'$ for some f' and g' such that $f \xrightarrow{F} f'$ and $g \xrightarrow{F} g'$. For then, the induction hypothesis shows that f' and g' have a common successor which is also the common successor of f and g. Note that

$h = (f - g) - \alpha t f_0$ for some $f_0 \in F$, $\alpha \in K$ and some term $t \in \mathrm{PP}$. Let $t_0 = \mathrm{Hterm}(tf_0)$ be the eliminated term. It is clear that t_0 occurs in f and g with some (possibly zero) coefficients α_1 and α_2 (respectively) such that $\alpha = \alpha_1 - \alpha_2$. Thus

$$h = (f - g) - (\alpha_1 - \alpha_2)tf_0 = (f - \alpha_1 t f_0) - (g - \alpha_2 t f_0)$$

and we may choose $f' = \alpha_1 t f_0$, $g' = \alpha_2 t f_0$. □

Let $\xleftrightarrow{F}$ be the relation obtained as the union of $\xrightarrow{F}$ and its reverse:

$f \xleftrightarrow{F} g$ if and only if either $f \xrightarrow{F} g$ or $g \xrightarrow{F} f$ holds.

Let $\xleftrightarrow[*]{F}$ denote the reflexive transitive closure of $\xleftrightarrow{F}$.

The following is from [Bachmair and Buchberger 1980]

Lemma 5.5 *$f - g \in (F)$ if and only if $f \xleftrightarrow[*]{F} g$.*

PROOF.

($\Leftarrow$)

This is easily shown by induction on the number of steps between f and g. Let

$$f = g_0 \xleftrightarrow{F} g_1 \xleftrightarrow{F} \cdots \xleftrightarrow{F} g_k = g$$

for some $k \geq 0$. The result is trivial for $k = 0$. Otherwise, by induction, $g_1 - g_k \in (F)$ and it is seen directly from the definition that $g_0 - g_1 \in (F)$. Thus $g_0 - g_k \in (F)$.

($\Rightarrow$)

If $f - g \in (F)$ then we can express $f - g$ as $\sum_{i=1}^{m} \alpha_i f_i$ where each α_i is a non-zero monomial and the f_i are members of F. The f_i's are not necessarily distinct here. If $m = 0$ the result is trivial. If $m \geq 1$ then we can write $g' = g + \alpha_m f_m$ and $f - g' = \sum_{i=1}^{m-1} \alpha_i f_i$. By induction hypothesis, $f \xleftrightarrow[*]{F} g'$. We also have that $g' - g = \alpha_m f_m \xrightarrow{F} 0$. By the previous lemma, we conclude that g and g' have a common successor h. This implies $g' \xleftrightarrow[*]{F} h \xleftrightarrow[*]{F} g$. This shows $f \xleftrightarrow[*]{F} g' \xleftrightarrow[*]{F} g$. □

Lemma 5.6 *If $f \xleftrightarrow[*]{F} g$ then f and g have a common successor.*

PROOF.

We use induction on the number of steps to get from f to g. The result is trivial for 0 or 1 step. Suppose $f \overset{F}{\longleftrightarrow} f' \underset{*}{\overset{F}{\longleftrightarrow}} g$. By induction hypothesis, f' and g have a common successor h. If in fact $f \xrightarrow{F} f'$ then f and g have the common successor h. Otherwise, suppose $f' \xrightarrow{F} f$. But, since f and h are both successors of f', an application of the Church-Rosser property for $\underset{*}{\xrightarrow{F}}$ implies that f and h have a common successor. Then $g \underset{*}{\xrightarrow{F}} h$ implies that f and g have the same common successor. $\square$

Remark 5.1 The preceding result holds for any relation $\underset{*}{\longrightarrow}$ that is Noetherian and Church-Rosser.

Theorem 5.7 (Buchberger) *G is a Gröbner basis if and only if for all $f \in (G)$, $0 \in \mathrm{NF}_G(f)$.*
PROOF.

$(\Leftarrow)$
Let h be any polynomial. We want to show that $|\mathrm{NF}_G(h)| = 1$. Let $g, g' \in \mathrm{NF}_G(h)$. Then $h-g \in (G)$ and $h-g' \in (G)$. Hence $g-g' = (h-g')-(h-g) \in (G)$. It follows that $g - g' \underset{*}{\xrightarrow{G}} 0$. But $g - g'$ is in normal form (since g and g' are). It follows that $g - g' = 0$ or $g = g'$, as desired.
$(\Rightarrow)$
Suppose $f \in (G)$. Since $0 \in (G)$, we have $f - 0 \in (G)$. Then lemma 5.5 implies $f \underset{*}{\overset{G}{\longleftrightarrow}} 0$. The preceding lemma next implies that f and 0 have a common successor h. Since 0 is in normal form, $h = 0$. This proves that $0 \in \mathrm{NF}_G(f)$. $\square$

Theorem 5.8 (Buchberger) *G is a Gröbner basis if and only if for all $f, g \in G$, $0 \in \mathrm{NF}_G(S(f,g))$.*
PROOF.

$(\Rightarrow)$
This is immediate since $S(f,g) \in (G)$ if $f, g \in G$.
$(\Leftarrow)$
By preceding results, it is enough to show that $\xrightarrow{G}$ is locally Church-Rosser. So let $f \xrightarrow{G} g$ and $f \xrightarrow{G} h$ and we are required to show that g and h have a common successor. So

$$g = f - \alpha_1 f_1 \text{ and } h = f - \alpha_2 f_2$$

where α_1, α_2 are monomials and $f_1, f_2 \in G$. Let the eliminated monomials be $m_1 = \text{Hmono}(\alpha_1 f_1)$ and $m_2 = \text{Hmono}(\alpha_2 f_2)$. There are two cases:

Case $m_1 \underset{A}{>} m_2$. (By symmetry, this covers the case $m_2 \underset{A}{>} m_1$ as well.) Then we see that m_1 still occurs in h. Therefore we have $h \xrightarrow{G} h'$ where

$$h' = h - \alpha_1 f_1 = f - (\alpha_1 f_1 + \alpha_2 f_2).$$

Now observe that $g - h' = \alpha_2 f_2 \xrightarrow{G} 0$. By lemma 5.4 we conclude that g and h' have a common successor. Then g and h have the same common successor.

Case $m_1 = m_2$. Here is where the S-polynomials come in. By definition,

$$S(f_1, f_2) = \beta_1 f_1 - \beta_2 f_2$$

where

$$\text{Hmono}(\beta_1 f_1) = m = \text{Hmono}(\beta_2 f_2) \tag{2}$$

for some monomial m whose corresponding power product is $LCM(\text{Hterm}(f_1), \text{Hterm}(f_2))$. Since both $\text{Hterm}(f_1)$ and $\text{Hterm}(f_2)$ divide m_1 $(= m_2)$, we conclude that m divides m_1. Therefore let us express m_1 as

$$m_1 = mm'$$

for some monomial m'. Since $\text{Hmono}(\alpha_i f_i) = mm'$ and $\text{Hmono}(f_i)$ divides m, we have that m' divides α_i. Again, we may factor α_i as

$$\alpha_i = m'\gamma_i$$

for some monomial γ_i $(i = 1, 2)$. It is now seen that

$$\begin{aligned} g - h &= \alpha_2 f_2 - \alpha_1 f_1 \\ &= m'\gamma_2 f_2 - m'\gamma_1 f_1 \\ &= \frac{m_1}{m}(\gamma_2 f_2 - \gamma_1 f_1) \end{aligned}$$

Since $\text{Hmono}(\alpha_i f_i) = m_1$, it follows from the last equation that $\text{Hmono}(\frac{\gamma_i f_i}{m}) = 1$ or $m = \text{Hmono}(\gamma_i f_i)$. Comparing this with (2), we conclude that $\gamma_i = \beta_i$. In otherwords,

$$g - h = m' \cdot S(f_1, f_2).$$

Since we assume $S(f_1, f_2) \xrightarrow[*]{G} 0$, lemma 5.4 implies g and h have a common successor. This concludes our proof of this case.

Note that the above two cases are exhaustive: in particular, it is not possible that $\text{Hterm}(m_1) = \text{Hterm}(m_2)$ and $\text{Hcoef}(m_1) \neq \text{Hcoef}(m_2)$. $\square$

Remark 5.2 Compared to the definition of a Gröbner basis, theorems 15 and 16 are successively better characterizations of a Gröbner basis. More precisely, in the original definition we insist that every polynomial must have a unique normal form, theorem 15 has a similar requirement but only for polynomials in the ideal, and theorem 16 has the same test restricted to only a finite set of polynomials. Thus, theorem 16 is an effective criterion to test if a given F is indeed a Gröbner basis: given F, for each pair $f, g \in F$, we compute $\mathrm{nf}_F(S(f,g))$ and see if it is equal to zero. If this is zero for all f, g then we know F is a Gröbner basis. Conversely, if any $\mathrm{nf}_F(S(f,g)) \neq 0$ then either $|\mathrm{NF}_F(S(f,g))| > 0$ or $0 \notin \mathrm{NF}_F(S(f,g))$. In either case F is not a Gröbner basis. Of course, this still does not tell us how to construct a Gröbner basis for the ideal generated by a given F. The next section will do this.

To conclude this section, we now give characterizations of Gröbner basis based on looking at headterms.

Theorem 5.9 *$G = \{g_1, \ldots, g_r\}$ is a Gröbner basis if and only if every polynomial $f \in (G)$ can be expressed in the form*

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

where $\mathrm{Hterm}(\alpha_i g_i) \underset{A}{\leq} \mathrm{Hterm}(f)$ *for all i.*

PROOF.

$(\Rightarrow)$
Let $f \in (G)$ and let

$$f = f_0 \xrightarrow{h_1} f_1 \xrightarrow{h_2} f_2 \xrightarrow{h_3} \ldots \xrightarrow{h_k} f_k = 0$$

be a reduction sequence witnessing the fact that $f \underset{*}{\xrightarrow{G}} 0$. So for $j = 1, \ldots, k$, $h_j \in G$ and $f_j = f_{j-1} - m_j h_j$ for some monomial m_j. We say that m_j is *associated* with h_j. Then we see that $f = \sum_{i=1}^{r} \alpha_i g_i$ where $g_i \in G$ and the α_i are obtained by summing all the monomials associated with g_i. Now $\mathrm{Hterm}(m_j h_j) \underset{A}{\leq} \mathrm{Hterm}(f_{j-1})$ and $\mathrm{Hterm}(f_j) \underset{A}{\leq} \mathrm{Hterm}(f_{j-1})$ for all j and hence $\mathrm{Hterm}(m_j h_j) \underset{A}{\leq} \mathrm{Hterm}(f_0)$. We conclude that $\mathrm{Hterm}(\alpha_i g_i) \underset{A}{\leq} \mathrm{Hterm}(f_0)$, as we wanted to show.

($\Leftarrow$)
Let $f_0 \in (G)$. By assumption,

$$f_0 = \sum_{i=1}^{r} \alpha_i g_i$$

where $\mathrm{Hterm}(\alpha_i g_i) \underset{A}{\leq} \mathrm{Hterm}(f_0)$. This implies that there is some set of indices $J \subseteq \{1, \ldots, r\}$ such that $\mathrm{Hmono}(f_0) = \sum_{j \in J} \mathrm{Hmono}(\alpha_j g_j)$. Choose any $j \in J$ and it is not hard to see that the head monomial of f_0 can be eliminated by applying g_j. Let f_1 be the result of this elimination. Since $f_1 \in (G)$, we may apply the same argument to eliminate the head monomial of f_1 to obtain f_2. Repeating this, we get the sequence $f_0 \xrightarrow{G} f_1 \xrightarrow{G} f_2 \xrightarrow{G} \cdots$. This sequence must be finite and it is easy to see that the last term is 0. This shows that G is a Gröbner basis. $\square$

Theorem 5.10 *Let $G = \{g_1, \ldots, g_r\}$ be a basis for ideal I. Every polynomial $f \in (G)$ can be expressed in the form*

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

where $\mathrm{Hterm}(f) \geq \mathrm{Hterm}(\alpha_i g_i)$ *for all i if and only if* $\mathrm{Head}(G) = \mathrm{Head}(I)$.
PROOF.

($\Rightarrow$)
Suppose $f \in (I')$, we have to express it as an element of (G'). We can write f in the form $f = \sum_{j=1}^{k} \mathrm{Hmono}(f_j)$ for some k and $f_j \in (G)$. But each f_j can be expressed as $f_j = \sum_{i=1}^{r} \alpha_{j,i} g_i$ where $\mathrm{Hterm}(f_j) \geq \mathrm{Hterm}(\alpha_{j,i} g_i$ for all i. Then we see that

$$f = \sum_{j=1}^{k} \mathrm{Hmono}(\sum_{i=1}^{r} \alpha_{j,i} g_i)$$

This implies that f can be generated from $G' = \{\mathrm{Hmono}(g_i) : i = 1, \ldots, r\}$.
($\Leftarrow$)
Given $f \in (G)$, by assumption, $\mathrm{Hmono}(f)$ can be expressed as $\sum_{i=1}^{r} m_i \mathrm{Hmono}(g_i)$ for suitable monomials m_i. In fact we see that all but one of the m_i's may be assumed to be zero. Let $f_0 = f$ and $f_1 = f_0 - \sum_{i=1}^{r} m_i g_i$. Observe that $\mathrm{Hterm}(f_0) \underset{A}{>} \mathrm{Hterm}(f_1)$. Since $f_1 \in (G)$, we can repeat this argument to obtain f_2 with $\mathrm{Hterm}(f_1) \underset{A}{>} \mathrm{Hterm}(f_2)$. This process must halt

after k repetitions; the last polynomial f_k is seen to be 0. It follows that f_0 can be expressed as a sum of the form $\sum_{i=1}^{r} \alpha_i g_i$ where $\mathrm{Hterm}(\alpha_i g_i) \underset{A}{\leq} \mathrm{Hterm}(f_0)$.
□

Remark 5.3 Combining the last two theorems, we see that G is a Gröbner basis for I if and only if $\{\mathrm{Hmono}(f) \; : \; f \in G\}$ is a basis for $\mathrm{Head}(I)$. This is often taken as the definition of Gröbner basis (and is borrowed from the definition of standard basis). An attraction of this definition is that it does not require the concept of reduction.

6 The Basic Algorithm of Buchberger

Now we are ready to present the basic form of the Gröbner basis algorithm of Buchberger. The algorithm is deceptively simple – its complexity analysis is not. Like the normal form algorithm, it is non-deterministic. In fact, it calls the normal form algorithm at a crucial point.

```
Input: F a finite set of polynomials.
Output: G a Gröbner basis for F.

G := F
B := {{f, g} : f, g ∈ G, f ≠ g}
while B ≠ ∅ do begin
        Choose {f, g} to be any pair in B
        B := B − {{f, g}}
        h := S(f, g)
        h' := nf_G(h)
        if h' ≠ 0 then begin
           B := B ∪ {{f', h'} : f' ∈ G}
           G := G ∪ {h'}
        end {if}
end {while}
```

Lemma 6.1 *The basic algorithm terminates.*

PROOF.

Since we have already shown that the normal form algorithm terminates, it suffices to show that the number of iterations of the while-loop is finite. Let h_i be the polynomial assigned to the program variable h' in the ith iteration of the loop. For the sake of contradiction, assume that there are infinitely many iterations. It is seen that in each iteration in which h' is zero the size of the set B decreases. Since B is always finite in size, there cannot be an infinite succession of iterations in which $h' = 0$. Hence there are infinitely many non-zero values of h_i.

Now let H be the infinite set consisting of all the non-zero h_i's. By Dixon's lemma, there is a finite set of indices I such that each $g \in H$ is a multiple of h_i for some $i \in I$. Let i_0 be the largest index in I. Then for all $j > i_0$, if $h_j \neq 0$ then h_j is a multiple of h_i for some $i \in I$. However, during the jth interation, the polynomial h_i is in the set G. Hence h_j is not a G-normal form, contradiction. □

Theorem 6.2 *The Basic Algorithm is correct.*

PROOF.

Since the algorithm terminates, we only have to show that at termination the set G is a Gröbner basis. By a characterization in the previous section, we must show that for all $f, g \in G$, $S(f,g) \xrightarrow[*]{G} 0$. The loop invariant that we may observe is this: for all $f, g \in G$, if $\{f, g\} \notin B$ then $S(f,g) \xrightarrow[*]{G} 0$. This invariant holds at the beginning of the iterations. Each iteration preserves the invariant. Since the set B is empty on termination, the set G is indeed a Gröbner basis. □

Unfortunately, there are no upper bounds on the running time of the algorithm except for some special cases. Unless otherwise noted, complexity of this algorithm will be just the worst case number of iterations of the while-loop. For instance, upper bounds are known for the two and three variable cases and assuming a total degree ordering of terms; the bounds in these cases are a polynomial and a single exponential, respectively. Other bounds are known in terms of more technical quantities such as the 'regularity' of ideal. As for lower bounds, there is a double exponential lower bound essentially due to Mayr and Meyer.[2]

[2]Since these notes were written, we had been able to provide an upper bound on the running time of the Basic Algorithm for any number of variables. In [Dube, Mishra and Yap 1986], we show that for each n, if the number of variables is n then the running time of the Basic Algorithm lies in the nth level of the Wainer hierarchy of primitive recursive functions. No particular admissible ordering is assumed. (This bound is better than one's initial guess, namely, an Ackerman-type bound.) From the work of Möller and Mora, and also Guisti, it is also known that the minimum degree Gröbner basis is at most double-exponential in the maximum degree of a set of input polynomials. The proof involves several auxilliary concepts and results. We will give an self-contained exposition of this proof in a future installation of these notes. In any case, armed with this degree bound, it

7 Uniqueness of Reduced Gröbner Bases

In this section we show that a Gröbner basis that is "reduced" in a certain sense is unique for an ideal. We give a method to obtain such bases.

We call a basis F *minimal* if for all $f \in F$, $(F) \neq (F - \{f\})$. A basis F is *self-reduced* if for all $f \in F$, f is a $(F - \{f\})$-normal form.

We call a Gröbner basis G *reduced* if

1. for all $g \in G$, $\mathrm{Hcoef}(g) = 1$
2. G is self-reduced

Note that if F is a minimal basis and $(F) \neq (0)$ then $0 \notin F$.

Let us first relate the concepts of minimality and self-reduction:

Lemma 7.1 *If G is a reduced Gröbner basis then G is minimal.* PROOF.

□

Lemma 7.2 *If $g, g' \in G$ are distinct polynomials in a minimal Gröbner basis G then* $\mathrm{Hterm}(g)$ *does not divide* $\mathrm{Hterm}(g')$*. In particular, no two polynomials in G have the same headterm.*

PROOF.

Note that $(G) \neq (0)$ so g, g' are distinct from 0. Let $\mathrm{Hterm}(g)$ divide $\mathrm{Hterm}(g')$ and $G' = G - \{g'\}$. Since G is minimal, $(G') \neq (G)$. So $g' \notin (G')$ and if $h \in \mathrm{NF}_{G'}(g')$ then $h \neq 0$. But since G is a Gröbner basis, $h \xrightarrow[*]{G} 0$. In particular, h is reducible by some polynomial $f \in G$. If $f = g'$ then since $\mathrm{Hterm}(g)$ divides $\mathrm{Hterm}(g')$, h is also reducible by g. Since $g \in G'$, this contradicts the assumption that h is a G'-normal form. On the other hand, if $f \neq g'$ then $f \in G$ and we arrive at the same contradiction. □

Lemma 7.3 *If G, G' are minimal Gröbner basis for the same ideal, $(G) = (G')$, then the set of headterms in G is equal to the set of headterms in G'.*

PROOF.

Suppose for some $g \in G$, $\mathrm{Hterm}(g)$ does not occur among the headterms of polynomials in G'. Since $g \xrightarrow[*]{G'} 0$ and $g \neq 0$, there is some $g' \in G'$ such that $\mathrm{Hterm}(g')$ properly divides $\mathrm{Hterm}(g)$. Again, since $g' \xrightarrow[*]{G} 0$, there is some

is not hard to modify the Basic Algorithm to give an algorithm with an elementary time bound.

$g'' \in G$ such that $\mathrm{Hterm}(g'')$ divides (not necessarily properly) $\mathrm{Hterm}(g)$. This means that $\mathrm{Hterm}(g'')$ properly divides $\mathrm{Hterm}(g)$, contradicting the preceding lemma. □

Corollary 7.4 *If G, G' are two minimal Gröbner bases for the same ideal then $|G| = |G'|$.*

Of course the size of the minimal Gröbner bases for any ideal may still depend on the choice of admissible orderings.

Theorem 7.5 *The reduced Gröbner basis of an ideal is unique (relative to the choice of an admissible ordering).*

PROOF.

Let G, G' be two reduced minimal Gröbner bases for the same ideal. We obtain a contradiction by supposing that there is some polynomial g in $G - G'$. By the previous lemma, there is some other polynomial g' in $G' - G$ such that $\mathrm{Hmono}(g) = \mathrm{Hmono}(g')$ (recall that $\mathrm{Hcoef}(g) = 1 = \mathrm{Hcoef}(g')$). Let $h = g - g'$. Then $h \neq 0$ and $h \xrightarrow[*]{G} 0$ since G is a Gröbner basis. So some term t occuring in h can be eliminated by application of some $f \in G$. Now t must occur in g or g'. If t occurs in g then g is reducible by f, contradicting the assumption that G is reduced. If t occurs in g' then let $f' \in G'$ such that $\mathrm{Hterm}(f') = \mathrm{Hterm}(f)$. Again g' is reducible by f', contradicting the assumption that G' is reduced. □

First we present a method to compute the reduced Gröbner basis corresponding to any input set F of polynomials:

```
Function SelfReduce(F)
Input: F a finite set of polynomials.
Output: R a reduced basis for (F).

R := ∅
while F ≠ ∅ do begin
      Choose f from F and set F := F − {f}
      f := nf_R(f)
      if f ≠ 0 then begin
         TEMP := {{g ∈ R : g is reducible by f}
         R := (R − TEMP) ∪ {f}
         F := F ∪ TEMP
      end {if}
end {while}
return(R)
```

Lemma 7.6 *The routine SelfReduce terminates.*

PROOF.

We will trace the history of transformations for a single polynomial f from the original input set F. In each iteration of the while-loop, there is a selected polynomial f, and in a natural way, this polynomial can be associated with a polynomial in the original input set F. Observe that except possibly for the first time that the polynomial f is selected, all subsequent selection of (versions of) f will result in a further transformation, i.e., in the loop, $f \neq \mathrm{nf}_R(f)$. If $f = f_0, f_1, f_2, \ldots,$ constitute the successive transformed versions of f then the same argument used in the termination proof for the Normal Form algorithm implies that this sequence of f_i's is finite. Since this is true for every f in the original F, there can only be a finite number of iterations. □

Lemma 7.7 *The routine SelfReduce is correct.*

PROOF.

Two loop-invariants can be easily checked to hold: (i) the set R is self-reduced and (ii) the ideal $(F \cup R)$ does not vary. The final result then has the desired property. □

We are finally ready to present the algorithm for computing reduced Gröbner bases. This is done by simple modifications to the Basic Algorithm.

```
Input: F a finite set of polynomials.
Output: G a Gröbner basis for F.

G := SelfReduce(F)
B := {{f, g} : f, g ∈ G, f ≠ g}
while B ≠ ∅ do begin
        Choose {f, g} to be any pair in B
        B := B − {{f, g}}
        h := S(f, g)
        h' := nf_G(h)
        if h' ≠ 0 then begin
           B := B ∪ {{f', h'} : f' ∈ G}
           G := SelfReduce(G ∪ {h'})
        end {if}
end {while}
```

We leave the correctness proof for this procedure to the reader. Note that the application of SelfReduce($G \cup \{h'\}$) within the while-loop can be made more efficient if we exploit the fact that G is already self-reduced. We also leave this improvement of the procedure SelfReduce to the reader.

8 Applications

In this section, we discuss applications of the Gröbner basis algorithm to decide several fundamental problems in Ideal Theory. The wide range of applicability of the Gröbner basis algorithm is a clear testimony to the power of this concept.

8.1 Ideal Theoretic Problems

Let $R = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K, and $(F) \subseteq R$ be an ideal defined by a finite set of generators F. In what follows, G will always stand for the Gröbner basis of (F).

We define, in the usual way, an equivalence relation for any ideal $I \subseteq R$, $\equiv \bmod I$, (*congruence modulo the ideal* I) over R as follows: for all $f, g \in R$,

$$f \equiv g \bmod I \text{ iff } f - g \in I.$$

Let $F \subseteq R$, and G the Gröbner basis of (F). It is easy to see that if $f \xrightarrow{G} g$ then $f \equiv g \bmod (G)$. By transitivity, if $f \xrightarrow[*]{G} g$ then $f \equiv g \bmod (G)$ In particular, $f \equiv \mathrm{nf}_G(f) \bmod (G)$.

Next, if $\mathrm{nf}_G(f) = \mathrm{nf}_G(g)$ then, by the above argument, we conclude that $f \equiv g \bmod (G)$. Conversely, if $f \equiv g \bmod (F)$ then, by Lemmas 5.5 and 5.6, we see that f and g have a common successor h with respect $\xrightarrow[*]{G}$. Since G is Gröbner, a corollary of Lemma 5.2 implies that $\mathrm{nf}_G(f) = \mathrm{nf}_G(h) = \mathrm{nf}_G(g)$. Thus

$$f \equiv g \bmod (F) \Leftrightarrow \mathrm{nf}_G(f) = \mathrm{nf}_G(g).$$

Let T be an arbitrary set with an equivalence relation $\sim$ defined on it. For instance, for our application, we may choose T to be $R = K[x_1, \ldots, x_n]$ and $\sim$ to be the equivalence relation, $\equiv \bmod(F)$. We will also assume that T is a decidable set, i.e. there exists a decision procedure for the membership problem for T. This will be true of all the polynomial rings of interest to us.

Following Buchberger, we define a *canonical simplifier* for $\sim$ on T to be an algorithm C with input and output in T such that for all $f, g \in T$

- $f \sim C(f)$ and

- $f \sim g \Rightarrow C(f) = C(g)$.

Notice that the function C gives a unique representative in each equivalence class of $T/\sim$. $C(f)$ is called a *canonical form* of f.

Problem 8.1 [CANONICAL SIMPLIFIER]

- INPUT: *$F \subseteq R$.*
- OUTPUT: *A canonical simplifier algorithm C for $\equiv \bmod(F)$ on $K[x_1, \ldots, x_n]$.*

First, compute G the Gröbner basis of F. For any f let $C(f) = \mathrm{nf}_G(f)$. The correctness of this method follows directly from the discussion above.

Problem 8.2 [IDEAL CONGRUENCE]

- INPUT: *$F \subseteq R$, and $f, g \in R$.*
- DECIDE: *$f \equiv g \bmod (F)$?*

As before, compute G the Gröbner basis of (F). Determine $\mathrm{nf}_G(f)$ and $\mathrm{nf}_G(g)$. Output true if $\mathrm{nf}_G(f) = \mathrm{nf}_G(g)$; otherwise, false. The correctness of this method is follows from the preliminary observations made above.

Problem 8.3 [IDEAL MEMBERSHIP]

- INPUT: *$F \subseteq R$, and $f \in R$.*
- DECIDE: *$f \in (F)$?*

We note that van der Waerden calls this 'the central problem of ideal theory.'

Compute G the Gröbner basis of F, and the normal form of f, $\mathrm{nf}_G(f)$, with respect to $\xrightarrow[*]{G}$. Output true if $\mathrm{nf}_G(f) = 0$; otherwise, false. To see the correctness of the algorithm,

$$\begin{aligned} f \in (F) \quad &\text{iff} \quad f \in (G) \\ &\text{iff} \quad \mathrm{nf}_G(f) = 0 \quad \text{(from Theorem 5.7)} \end{aligned}$$

Problem 8.4 [SUBIDEALS]

- INPUT: $F_1, F_2 \subseteq R$.
- DECIDE: $(F_1) \subseteq (F_2)$ *(Is* (F_1) *a subideal of* (F_2)*)?*

Compute G_2 the Gröbner basis of (F_2). Output true if for all $f \in F_1$, $\mathrm{nf}_{G_2}(f) = 0$; otherwise, false. It is easily seen that

$$(F_1) \subseteq (F_2) \Leftrightarrow \forall_{f \in F_1} f \in (F_2).$$

Problem 8.5 [IDEAL EQUALITY]

- INPUT: $F_1, F_2 \subseteq R$.
- DECIDE: $(F_1) = (F_2)$?

This problem clearly reduces to the previous problem.

Alternatively, compute G_1' and G_2' the *reduced* Gröbner bases for (F_1) and (F_2), respectively. Output true if $G_1' = G_2'$; otherwise, false. By Theorem 7.5, $(F_1) = (F_2)$ if and only if $G_1' = G_2'$, and the correctness follows.

8.2 Residue Class Ring Modulo an Ideal

Let $R = K[x_1, \ldots, x_n]$ be a polynomial ring over the field K and I an ideal of R. Then the equivalence relation $\equiv \bmod I$ partitions the ring R into equivalence classes such that $f, g \in R$ belongs to the same class, if $f \equiv g \bmod I$. The equivalance classes of R are called its *residue classes* modulo I. We use the notation R/I to represent the set of residue classes of R with respect to I. Let $\bar{f}$ denote the set $\{g \mid f \equiv g \bmod I\}$. It is easy to see that the map $f \mapsto \bar{f}$ is the *natural ring homomorphism* of R onto R/I. We sometimes write $f + I$ for $\bar{f}$. R/I is called the *residue class ring modulo* I.

Lemma 8.1 *R/I is a vector space over K.*

Lemma 8.2 *Let G be a Gröbner basis, and let*

$$\begin{aligned} B \;=\; & \{\bar{p} \mid p \in \mathrm{PP}(x_1, \ldots, x_n) \text{ such that } p \text{ is not a multiple} \\ & \quad \text{of the Hterm of any of the polynomials in } G\}. \end{aligned} \tag{3}$$

Then B is a linearly independent (vector space) basis of $R/(G)$ over K.

PROOF.
Let $\bar{f} = f + (G)$ be an element of $R/(G)$ and let

$$\begin{aligned} \mathrm{nf}_G(f) &= c_1 \cdot p_1 + \cdots + c_l \cdot p_l, \\ & \qquad \text{where } c_i \in K \text{ and } p_i \in \mathrm{PP}(x_1, \ldots, x_n). \end{aligned}$$

Hence, for all $1 \leq i \leq l$, p_i is not a multiple of the Hterm of any polynomial in G, and $\bar{p_i} \in B$. Since we can write $\bar{f}$ as

$$\bar{f} = c_1 \cdot \bar{p_1} + \cdots + c_l \cdot \bar{p_l},$$

B spans the vector space $R/(G)$.

Furthermore, the elements of B are linearly independent. Assume to the contrary, that is, for some $\bar{p_1}$, ..., $\bar{p_m} \in B$, we can obtain c_1, ..., c_m, not all 0, such that

$$c_1 \cdot \bar{p_1} + \cdots + c_m \cdot \bar{p_m} = \bar{0}.$$

In other words,

$$f = c_1 \cdot p_1 + \cdots + c_m \cdot p_m \in (G).$$

Hence $\mathrm{nf}_G(f) = f = 0$, i.e., $c_1 = \cdots = c_m = 0$, thus resulting in a contradiction. □

Problem 8.6 [FINITE DIMENSIONALITY OF A RESIDUE CLASS RING]

- INPUT: *$F \subseteq R$.*
- DECIDE: *Is $R/(F)$ finite-dimensional?*

Compute G the Gröbner basis of (F). Output true if for all i $(1 \leq i \leq n)$, a power product of the form $x_i^{j_i}$ $(j_i \geq 0)$ occurs among the Hterm's of the polynomials in G; otherwise, false. To see this, if for some i, none of the power products of Hterms in G has the required form then we get an infinity of basis elements. The converse is similar.

Problem 8.7 [BASIS OF A RESIDUE CLASS RING]

- INPUT: *$F \subseteq R$.*
- OUTPUT: *If $R/(F)$ is a finite dimensional vector space then output*

  1. A basis B of the vector space $R/(F)$.

2. *The 'multiplication table' for $R/(F)$; the $(\bar{p_i}, \bar{p_j})$th entry of the table gives a linear representation of $\bar{p_i} \cdot \bar{p_j}$ in terms of the basis elements in B.*

Compute G the Gröbner basis of (F). Let the set B be as in the Equation 3. This is easily computed.

For each $\bar{p_i}$, $\bar{p_j} \in B$, compute the normal form of $p_i \cdot p_j$:

$$\mathrm{nf}_G(p_i \cdot p_j) = c_1 \cdot p_1 + \cdots + c_m \cdot p_m.$$

Then $(\bar{p_i}, \bar{p_j})$th entry of the multiplication table is

$$c_1 \cdot \bar{p_1} + \cdots + c_m \cdot \bar{p_m}.$$

The correctness of the procedure follows immediately from the Lemma 8.2.

8.3 Solving Systems of Polynomial Equations

Gröbner bases can be advantageously used to settle several important questions about solvability, number of zeroes and finally, finding the zeroes of a system of polynomials F. We first show a result that is essentially equivalent to Hilbert's Nullstellensatz.

Lemma 8.3 *Every maximal ideal M, distinct from the unit ideal R has a zero in an algebraic extension of K.*

PROOF.

To every polynomial $f(x_1, x_2, \ldots, x_n)$ assign an element of the residue class ring R/M, given by the natural ring homomorphism. Since $M \neq R$, every element a of K will correspond to the distinct element $\bar{a} = a + M$. (Otherwise, if $a \neq b$ and $\bar{a} = \bar{b}$ then $a - b \in M$ so $1 = (a-b)(a-b)^{-1} \in M$ and then $M = R$.) Since M is a maximal ideal, R/M is an algebraic (field) extension of K.

Let $\bar{x_1}, \bar{x_2}, \ldots, \bar{x_n}$ be the images of $x_1, x_2, \ldots, x_n$ under the natural ring homomorphism from R into R/M.

Since, the ring operations in R/M are naturally induced from the same operations in R, and $a \in K$ maps into itself, we see that, for every $f \in M$, $f(\bar{x_1}, \bar{x_2}, \ldots, \bar{x_n}) = 0$ in R/M. Hence, M has a zero in an extension field of K. $\square$

Theorem 8.4 *F is solvable if and only if $1 \notin (F)$.*

PROOF.
If $1 \in (F)$ then it is easily seen that F is unsolvable. We prove the converse by contradiction. Among all the ideals I such that $1 \notin I$, but I is unsolvable, there is a maximal ideal M (follows from the maximum principle). Since $1 \notin M$, M is distinct from the unit ideal. Since M is maximal, from the previous Lemma (8.3), we conclude that M has a zero in some extension field of K, thus deriving a contradiction. $\square$

Problem 8.8 [SOLVABILITY]

- INPUT: $F \subseteq R$.
- DECIDE: *Does F have a solution in an algebraic extension of K?*

Compute G the reduced Gröbner basis of (F). Output true if $1 \notin G$; otherwise, false. From Theorem 8.4, it follows that F is unsolvable if and only if $1 \in (G)$. But $1 \in (G)$ if and only if $\mathrm{nf}_G(1) = 0$, that is, if and only if $1 \in G$.

We state the following useful theorem without proof:

Theorem 8.5 *F has finitely many zeroes (in every algebraic extension of K) if and only if the vector space $R/(F)$ has a finite vector space dimension.*

Problem 8.9 [NUMBER OF ZEROES]

- INPUT: $F \subseteq R$.
- DECIDE: *Does F have a finitely many solutions?*

Output true if $R/(F)$ is a finite-dimensional vector space (this can be found out using the solution to Problem 8.6); otherwise false. The correctness of this method follows from the Theorem 8.5.

Next we discuss the problem of finding all the zeroes of a systems of polynomials F, over some algebraic extension of K. We assume an 'oracle' that provides all the zeroes of a univariate polynomial p. One interesting special case is when K is the field of reals and we want to determine all the real solutions of F. In general we cannot represent the roots using finite precision numbers. However, there are techniques to represent algebraic numbers so that we can answer any question about the roots without error. This is not really a deficiency of Buchberger's algorithm but an intrinsic limitation of algorithmic solvability of polynomial equations.

For the method below, we assume that the Gröbner basis is computed using a lexicographic admissible ordering on the power products; the method can be modified to deal with other admissible orderings. For simplicity, we omit discussions of the other methods. The method discussed below is adapted from Buchberger's survey paper.

The following useful lemma shows that the 'i^{th} *elimination ideal*' of a Gröbner basis G is generated by just those polynomials in G that depends on the variables $x_1, \ldots, x_i$.

Lemma 8.6 *Let G be Gröbner basis with respect to the purely lexicographic ordering of power products. Without loss of generality let us assume that $x_1 <_{\text{lex}} x_2 <_{\text{lex}} \cdots <_{\text{lex}} x_n$. Then for $1 \le i \le n$*

$$(G) \cap K[x_1, \ldots, x_i] = (G \cap K[x_1, \ldots, x_i]).$$

PROOF.
Let $f \in (G) \cap K[x_1, \ldots, x_i]$. Then $f \xrightarrow[*]{G} 0$, i.e.

$$f = f_0 \xrightarrow{g'_0} f_1 \xrightarrow{g'_1} \cdots \xrightarrow{g'_{m-1}} f_m \xrightarrow{g'_m} f_{m+1} = 0,$$

where g'_j's are in G. We claim that, for all j $(0 \le j \le m+1)$, f can be written as

$$f = f_j + \alpha_1 \cdot g_1 + \cdots + \alpha_l \cdot g_l,$$

where $f_j \in (G) \cap K[x_1, \ldots, x_i]$, g_k's are in $G \cap K[x_1, \ldots, x_i]$ and α_k's are in $K[x_1, \ldots, x_i]$.

Clearly $f = f_0$ satisfies the claim. Consider the j^{th} $(j \geq 0)$ reduction: $f_j \xrightarrow{g'_j} f_{j+1}$. Since, by the inductive hypothesis, $f_j \in (G) \cap K[x_1, \ldots, x_i]$, the Hmono of g'_j must involve only the first i variables. Furthermore, since the admissible ordering chosen is lexicographic, every monomial of g'_j involves the same set of variables. Hence, $f_{j+1} = f_j - m_j \cdot g'_j$, and m_j is a monomial in the first i variables, thus the claim follows immediately.

In particular, we can write f as

$$f = \alpha_1 \cdot g_1 + \cdots + \alpha_l \cdot g_l,$$

where g_k's are in $G \cap K[x_1, \ldots, x_i]$ and α_k's are in $K[x_1, \ldots, x_i]$. Hence $f \in (G \cap K[x_1, \ldots, x_i])$, where the ideal is formed in $K[x_1, \ldots, x_i]$.

This shows that

$$(G) \cap K[x_1, \ldots, x_i] \subseteq (G \cap K[x_1, \ldots, x_i]).$$

The converse is trivial:

$$(G) \cap K[x_1, \ldots, x_i] \supseteq (G \cap K[x_1, \ldots, x_i]).$$

□

Problem 8.10 [FINDING ALL THE ZEROES OF F]

- INPUT: *$F \subseteq R$. F is solvable, with finitely many solutions.*
- OUTPUT: *All the solutions of the system F.*

Compute G the Gröbner basis of (F) with respect to the purely lexicographic ordering of the monomials. Let G_i $(1 \leq i \leq n)$ be defined as follows:

$$\begin{aligned} G_1 &= G \cap K[x_1] \\ G_i &= G \cap K[x_1, \ldots, x_i] - K[x_1, \ldots, x_{i-1}], \quad 2 \leq i \leq n \end{aligned}$$

By the previous lemma $(G) \cap K[x_1, \ldots, x_i] = (\cup_{j=1}^{i} G_j)$. Furthermore G contains exactly one polynomial p of $K[x_1]$.

The successive elimination can be carried out by the following algorithm:

```
p := the polynomial in G_1
X_1 := {(a) | p(a) = 0}
for i := 1 to n − 1 do begin
    X_{i+1} := ∅
    forall (a_1, ..., a_i) ∈ X_i do begin
        H := {g(a_1, ..., a_i, x_{i+1}) | g ∈ G_{i+1}}
        p := the greatest common divisor of the polynomials in H
        if p ≠ 1 then begin
          X_{i+1} := X_{i+1} ∪ {(a_1, ..., a_i, a) | p(a) = 0}
        end {if}
    end {forall}
end {for}
return X_n
```

8.4 Other Applications

There are several other applications of Gröbner basis found in the literature, and the list of new applications are growing at a rather fast rate. A large number of applications are aimed towards developing a 'computational commutative algebra,' and include problems such as computing the intersection of a set of ideals, the quotient of an ideal with respect to another, the saturation of an ideal with respect to a multiplicatively closed subset of the ring, the radical of an ideal, testing if an ideal is principal, testing if an ideal is prime, Lasker-Noether decomposition of an ideal, etc. Yet another large group of applications involve computing the free-resolutions of an ideal, syzygies, Hilbert functions and polynomials etc. The latter problems have interesting applications in algebraic geometry. All these applications are outside the limited scope of the current paper, and will be discussed in a sequel. The survey paper of Buchberger [Buchberger 1985] contains an extensive list of applications, and pointers to the relevant literature.

References

[Abhyankar 1976] Shreeram S. Abhyankar, *Historical ramblings in algebraic geometry and related algebra*, **Amer. Math. Monthly 83**, 409–448.

[Bachmair and Buchberger 1980] L. Bachmair and B. Buchberger, *A simplified proof of the characterization theorem for Gröbner*, **SIGSAM bulletin**, 29-34.

[Bayer 1982] D. Bayer, *The division algorithm and the Hilbert scheme*, **PhD Thesis**, Harvard University.

[Buchberger 1965] B. Buchberger, *An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal*, (German) **PhD Thesis**, Univ. of Innsbruck, Austria.

[Buchberger 1985] B. Buchberger, *Gröbner: An algorithmic method in polynomial ideal theory*, in chapter 6 of **Multidimensional systems theory** (ed. N. K. Bose), D. Reidel Publishing Company.

[Buchberger 1983] B. Buchberger, *A note on the complexity of constructing Gröbner*, **Proc. European Computer Algebra conf., EUROCAL '83**, London, Lecture notes in Computer Science 162, 137–145.

[Buchberger 1985] B. Buchberger, *The parallel L-machine for symbolic computation*, **EUROCAL '85**, Lecture Notes in Computer Science, No. 204, 541–542. (see also 1985 Conf. on Applied Algebra and Error Correcting Codes, Lecture Notes in Comp. Sci.).

[Dieudonné 1985] Jean Dieudonné, *History of algebraic geometry*, (trans. from French, Judith D. Sally), **Wadsworth Advanced Books & Software**, Monterey, California.

[Dickson 1913] L. E. Dickson, *Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors*, **Am. J. of Math. 35**, 413-426.

[Dubé, Mishra and Yap 1986] T. Dubé, B. Mishra and C. Yap, *Admissible orderings and bounds on Gröbner normal form algorithm* **NYU Computer Science Tech. Rep.**.

[Dubé, Mishra and Yap 1986a] T. Dubé, B. Mishra and C. Yap, *Complexity of Buchberger's Algorithm for Grobner Bases* **Extended Abstract**.

[Hermann 1926] G. Hermann, *Die frage der endlich vielen schritte in der theorie der polynomideale*, **Math. Ann. 95**, 736-788.

[Hironaka 1964] H. Hironaka, *Resolution of singularities of an algebraic variety over a field of characteristic 0*, **Ann. of Math. 79**, 109-326.

[Mayr and Meyer 1982] E. W. Mayr and A. R. Meyer, *The complexity of the word problems for commutative semigroups and polynomial ideals* **Advances in Mathematics 46**, 305-329.

[Möller and Mora 1984] H. Michael Möller and Ferdinando Mora, *Upper and lower bounds for the degreee of Groebner bases*, **EUROSAM '84**, Lecture Notes in Computer Science, No. 174, 172–183.

[Richman 1974] F. Richman, *Constructive aspects of Noetherian Rings*, **Proc. AMS 44**, 436–441.

[Robbiano 1985] L. Robbiano, *Term orderings on the polynomial ring*, **EUROCAL '85**, Lecture Notes in Computer Science, No. 204, 513–517.

[Robbiano 1986] L. Robbiano, *On the theory of graded structures*, **J. Symbolic Computation 2**, 139–170.

[Seidenberg 1971] A. Seidenberg, *On the length of a Hilbert ascending chain*, **Proc. AMS 29**, 443–450.

[Seidenberg 1972] A. Seidenberg, *Constructive proof of Hilbert's theorem on ascending chain*, **Trans. AMS 174**, 305–312.

[Seidenberg 1974] A. Seidenberg, *Constructions in algebra*, **Trans. AMS 197**, 273–313.

[Winkler 1984] F. Winkler, *On the complexity of the Gröbner algorithm over* $K[x, y, z]$, **Eurosam '84**, Lecture Notes in Computer Science 174, 184–193.

[Yap 1985] C. K. Yap, *Lecture Notes on Symbolic Algebraic Computation*, Class Notes, Courant Institute-NYU, Fall 1985.