Admissible Orderings and Bounds for Gröbner Basis Normal Form Algorithms

T. Dubé   *B. Mishra*   *Chee-Keng Yap*[1]

Courant Institute of Mathematical Sciences
New York University
251 Mercer Street
New York, NY 10012.

July 6, 1995

[1]Supported in part by NSF grants #DCR-84-01898 and #DCR-84-01633.

Abstract

The concepts of admissible orderings and normal form algorithm are basic in Buchberger's Gröbner basis algorithm. We present a constructive and elementary proof of Robbiano's characterization theorem for admissible orderings. Using this characterization, we give a bound on the complexity of the normal form algorithm for arbitrary admissible orderings. Using a simple refinement of the normal form algorithm (ordered reductions), we obtain significantly improved bounds.

1 Introduction

Gröbner basis has become an important algorithmic tool in computational algebraic geometry [Buchberger 1985]. Much of the pioneering work is due to Buchberger. In particular, Buchberger gave an algorithm for constructing a Gröbner basis. We refer to [Mishra and Yap 1986] for a self-contained introduction to the subject.

In Gröbner basis, we are interested in the polynomial ring $R = K[x_1, \ldots, x_n]$ for some field K. The fundamental concept here is the 'reduction' of polynomials. In order to introduce this, we first let $\mathrm{PP} = \mathrm{PP}(x_1, \ldots, x_n)$ be the set of all *power products*

$$\prod_{i=1}^{n} x_i^{e_i}$$

where $e_i \geq 0$ are natural numbers. A total ordering $\underset{\mathrm{A}}{>}$ on the set PP is said to be *admissible* if the following two axioms are satisfied.

1. $x_i \underset{\mathrm{A}}{>} 1 \quad$ for $1 < i < n$
2. $p \underset{\mathrm{A}}{>} q \implies rp \underset{\mathrm{A}}{>} rq \quad$ for all $p, q, r \in \mathrm{PP}$

There are two natural examples of admissible orderings, the lexicographic and the total degree orderings (see next section). Power products are also called *terms*, and admissible orderings are also called term orderings or multiplicative orderings. Relative to such an ordering $\underset{\mathrm{A}}{>}$, we may define the *head monomial*, $\mathrm{Hmono}(f)$, of any polynomial $f \in R$ to be that monomial in f whose power product is the greatest under $\underset{\mathrm{A}}{>}$.

Now we are ready to define 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. Then $m = c \cdot \mathrm{Hmono}(g)$ for some monomial c. 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 $g \in G$. We denote the reflexive transitive closure of $\xrightarrow{G}$ by $\xrightarrow[*]{G}$. 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 a G-normal form of f is not unique in general, and the central idea in Gröbner basis is to enlarge G so that it becomes unique: 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 $f \in R$ is unique, i.e., $|\mathrm{NF}_G(f)| = 1$.

Given a finite set $F \subseteq R$ of polynomials, we define a (trivial) non-deterministic algorithm that, for any input polynomial f, repeatedly apply the reduction step $\xrightarrow{F}$ to f and its reducts until a normal form of f is reached. This simple algorithm will be called the *normal form algorithm*. Let $\mathrm{nf}_F(f)$ denote a final normal form so obtained, if the process halts at all. It can be shown that this process must halt regardless of the choice of reduction – see [Mishra and Yap 1986] for a proof. The normal form algorithm is a basic step in Buchberger's algorithm for constructing Gröbner bases.

In this paper we are interested in a bound on the number of reduction steps in the normal form algorithm. Previously, the only bounds known are for the simple case where $\underset{\mathrm{A}}{>}$ is the total degree ordering. In [Mishra and Yap 1986], a bound for the lexicographic ordering was given. We now extend this bound to the general case. Along the way, we will develop an elementary and constructive proof of a characterization theorem for all admissible orderings. The characterization was first given by [Robbiano 1985] but his proof is highly non-constructive.

2 Admissible Orderings

Example 1: Lexicographic Ordering ($\underset{\mathrm{LEX}}{>}$)

> Let $A = x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}$ and $B = x_1^{b_1} x_2^{b_2} \ldots x_n^{b_n}$. Then $A \underset{\mathrm{LEX}}{>} B$ if $a_i \neq b_i$ for some i, and we have $a_i > b_i$ for the minimum such i. To illustrate this, consider $\mathrm{PP}(x, y, z)$. Then, assuming $x \underset{\mathrm{LEX}}{>} y \underset{\mathrm{LEX}}{>} z$ we have:
>
> $$x \underset{\mathrm{LEX}}{>} y^3 z^2, \quad xy \underset{\mathrm{LEX}}{>} xz, \text{ and } \quad y^2 z \underset{\mathrm{LEX}}{>} yz^2$$

Example 2: Total-Degree Ordering ($\underset{\mathrm{T}}{>}$)

> Let $A = x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}$ and $B = x_1^{b_1} x_2^{b_2} \ldots x_n^{b_n}$. Then $A \underset{\mathrm{T}}{>} B$ if $deg(A) > deg(B)$ where $deg(A) = a_1 + a_2 + \ldots + a_n$.

Considering again the example $\mathrm{PP}(x, y, z)$, we have,

$$y^3 \underset{\mathrm{T}}{>} xy, \quad xyz \underset{\mathrm{T}}{>} y^2, \text{ and } \quad y^2z^2 \underset{\mathrm{T}}{>} xyz$$

Notice however, that total-degree alone does not provide a total ordering since it does not allow comparison of two power products with the same degree. Among the many ways in which total-degree can be extended into a total (admissible) ordering are:

Total-Degree(Lex): We say $A \underset{\mathrm{TL}}{>} B$ if:

$$\begin{array}{ll} \text{either} & deg(A) > deg(B) \\ \text{or} & deg(A) = deg(B) \;\&\; A \underset{\mathrm{LEX}}{>} B \end{array}$$

Total-Degree(Recursive): We say $A \underset{\mathrm{TT}}{>} B$ if:

$$\begin{array}{ll} \text{either} & deg(A) > deg(B) \\ \text{or} & deg(A) = deg(B) \;\&\; x_1^{a_1} x_2^{a_2} \ldots x_{k-1}^{a_{k-1}} \underset{\mathrm{TT}}{>} x_1^{b_1} x_2^{b_2} \ldots x_{k-1}^{b_{k-1}} \end{array}$$

where $k = \max\{i | a_i \neq 0 \text{ or } b_i \neq 0\}$

It is easily verified that both are admissible. To see that these two orderings are in fact different, notice that on $\mathrm{PP}(x, y, z)$ we have

$$\begin{array}{ccc} x \underset{\mathrm{TL}}{>} y \underset{\mathrm{TL}}{>} z & \text{and} & x \underset{\mathrm{TT}}{>} y \underset{\mathrm{TT}}{>} z \\ xyz \underset{\mathrm{TL}}{>} y^3 & \text{but} & y^3 \underset{\mathrm{TT}}{>} xyz \end{array}$$

Remark: Usually, the ordering $\underset{\mathrm{TL}}{>}$ is simply called the 'total-degree ordering'.

Although PP is defined with the natural numbers as exponents, many of our proofs simplify if we extend the exponents to the integers and also to the rational numbers. We write $\mathrm{PP}(\overline{x}; \mathbf{Z})$ and $\mathrm{PP}(\overline{x}; \mathbf{Q})$ to indicate these extensions. We also write $\mathrm{PP}(\overline{x}; \mathbf{N})$ for PP. Admissible orderings for these extensions are defined in the same way:

1. $x_i \underset{\mathrm{A}}{>} 1 \quad$ for $1 < i < n$

2. $p \underset{\mathrm{A}}{>} q \implies rp \underset{\mathrm{A}}{>} rq \quad$ for all $p, q, r \in \mathrm{PP}(\overline{x}; \mathbf{Q})$ $(resp. \mathrm{PP}(\overline{x}; \mathbf{Z}))$

Lemma 1 *Let* $\underset{\mathrm{A}}{>}$ *be an arbitrary admissible ordering on* $\mathrm{PP}(\overline{x};\mathbf{Q})$*,*
For any $M, N \in \mathrm{PP}(\overline{x};\mathbf{Q})$*,* $r \in \mathbf{Q}$*,*

$$\begin{array}{ll} \textit{if } r > 0 \textit{ then} & M \underset{\mathrm{A}}{>} N \iff M^r \underset{\mathrm{A}}{>} N^r \\ \textit{if } r < 0 \textit{ then} & M \underset{\mathrm{A}}{>} N \iff N^r \underset{\mathrm{A}}{>} M^r \end{array}$$

Proof.

($r \in \mathbf{N}$) For $r = 1$, the result is trivial, so assume the result holds for $r - 1$, then $M \underset{\mathrm{A}}{>} N$ implies $M^r \underset{\mathrm{A}}{>} M^{r-1}N \underset{\mathrm{A}}{>} N^r$. Conversely, if $M^r \underset{\mathrm{A}}{>} N^r$, then $M \underset{\mathrm{A}}{>} N$ since $M \underset{\mathrm{A}}{\not>} N$ leads to the contradiction $M^r \underset{\mathrm{A}}{\not>} N^r$.

($r > 0$) Let r be a positive rational of the form $\frac{s}{t}$, then the result follows from $M^{\frac{s}{t}} \underset{\mathrm{A}}{>} N^{\frac{s}{t}} \iff M^s \underset{\mathrm{A}}{>} N^s \iff M \underset{\mathrm{A}}{>} N$ (by two applications of the case $r \in \mathbf{N}$).

($r < 0$) It is easy to check that $M \underset{\mathrm{A}}{>} N \iff N^{-1} \underset{\mathrm{A}}{>} M^{-1}$. Then an application of the case $r > 0$ shows $N^{-1} \underset{\mathrm{A}}{>} M^{-1} \iff N^r \underset{\mathrm{A}}{>} M^r$

Q.E.D.

If $\underset{\mathrm{Q}}{>}$ is an admissible ordering on $\mathrm{PP}(\overline{x};\mathbf{Q})$, then it is clear that $\underset{\mathrm{Q}}{>}$ induces an admissible ordering $\underset{\mathrm{N}}{>}$ on $\mathrm{PP}(\overline{x};\mathbf{N})$, namely $\underset{\mathrm{N}}{>}$ is the restriction of $\underset{\mathrm{Q}}{>}$ to PP. The converse relation is also true. Every admissible order $\underset{\mathrm{N}}{>}$ on $\mathrm{PP}(\overline{x};\mathbf{N})$ induces a relation $\underset{\mathrm{Q}}{>}$ on the rationals defined by:

$$M \underset{\mathrm{Q}}{>} N \iff M^cU \underset{\mathrm{N}}{>} N^cU$$

where $c \in \mathbf{N}$ is chosen such that M^c,$N^c \in \mathrm{PP}(\overline{x};\mathbf{Z})$ and $U \in \mathrm{PP}(\overline{x};\mathbf{Z})$ is chosen such that $M^cU, N^cU \in \mathrm{PP}(\overline{x};\mathbf{N})$. The reader can verify that the induced relation $\underset{\mathrm{Q}}{>}$ is an admissible ordering. It is seen that, for every pair of monomials $M, N \in \mathrm{PP}(\overline{x};\mathbf{N})$,

$$M \underset{\mathrm{Q}}{>} N \iff M \underset{\mathrm{N}}{>} N$$

so the induced admissible orderings on $\mathrm{PP}(\overline{x};\mathbf{Q})$ are simply extensions of the admissible orderings on $\mathrm{PP}(\overline{x};\mathbf{N})$. These are in fact the only admissible orderings on $\mathrm{PP}(\overline{x};\mathbf{Q})$. For any admissible ordering $\underset{\mathrm{A}}{>}$ on $\mathrm{PP}(\overline{x};\mathbf{Q})$, $M \underset{\mathrm{A}}{>} N \iff M^cU \underset{\mathrm{A}}{>} N^cU$, so the ordering is completely specified by the ordering of power products with natural number exponents. This proves:

Lemma 2 *There is a natural bijection between the set of admissible orderings on* $\mathrm{PP}(\overline{x};\mathbf{N})$ *and the set of admissible orderings on* $\mathrm{PP}(\overline{x};\mathbf{Q})$.

A useful characterization of admissible orderings is:

Lemma 3 *If* $\underset{A}{>}$ *and* $\underset{B}{>}$ *are admissible orderings on* $\mathrm{PP}(\overline{x};\mathbf{Q})$, *then* $\underset{A}{>}$ *and* $\underset{B}{>}$ *are identical if and only if the following sets are equal:*

$$\begin{aligned} S_A &= \left\{M\underset{A}{>}1 \;:\; M \in \mathrm{PP}(\overline{x};\mathbf{Q})\right\} \\ S_B &= \left\{M\underset{B}{>}1 \;:\; M \in \mathrm{PP}(\overline{x};\mathbf{Q})\right\} \end{aligned}$$

Proof. If $S_A = S_B$, then $M\underset{A}{>}N \iff MN^{-1} \in S_A \iff MN^{-1} \in S_B \iff M\underset{B}{>}N$. So $\underset{A}{>}$ and $\underset{B}{>}$ are identical.
Otherwise, if $S_A \neq S_B$, then without loss of generality assume that there exists an $N \in S_A - S_B$. Then, $\underset{A}{>}$ and $\underset{B}{>}$are different since $N\underset{A}{>}1$, but $N \underset{B}{\not>}1$.
Q.E.D.

3 Characterizing Admissible Orderings

The main result of this section is a new and constructive proof of Robbiano's theorem [Robbiano 1985]:

Theorem 4 *Any admissible ordering* $\underset{A}{>}$ *on* $\mathrm{PP}(\overline{x};\mathbf{Q})$ *can be characterized by a set of linear 'weight functions'* $W_1, W_2, \ldots, W_n$ *given by*

$$W_k\left(x_1^{\alpha_1}x_2^{\alpha_2}\ldots x_n^{\alpha_n}\right) \;=\; \sum_{i=1}^{n} w_{k,i}\alpha_i \quad \mathit{for}\ 1 \leq k \leq n$$

where the $w_{k,i}$*'s are real, such that if* M *is a power product* $M = x_1^{\alpha_1}x_2^{\alpha_2}\ldots x_n^{\alpha_n}$ *then,*

$$M\underset{A}{>}1 \iff (\exists_k)(W_k(M) > 0 \ \&\ (\forall_{j<k})W_j(M) = 0) \tag{1}$$

Thus,

$$W_k(M) \;=\; -W_k(M^{-1}) \quad \text{and} \quad W_k(MN) \;=\; W_k(M)W_k(N)$$

Note that (1) is a characterization because of lemma 3.

Essentially, we are reduced to a lexicographic ordering on the tuples $(W_1(M), \ldots, W_n(M))$. The existence of the $w_{k,i}$'s will be demonstrated by an explicit construction. We will do the construction in stages. In the k^{th} stage, we will define the function W_k, and also choose a new variable z_k from $\{x_1, \ldots, x_n\}$ which was not chosen in a previous stage.

Stage 1:

Define z_1 to be x_j where for all x_i, $x_j \underset{\mathrm{A}}{\geq} x_i$.

Then choose $w_{1,i}$ to be $\sup \left\{ s \in \mathbf{Q} \middle| \; x_i \underset{\mathrm{A}}{\geq} z_1^s \right\}$.

Set $\left\{ \begin{array}{lcl} \mathbf{X_1} & = & \{x_1, \ldots, x_n\} - \{z_1\} \\ \mathbf{Z_1} & = & \{z_1\} \end{array} \right.$.

Stage k $(k = 2$ to $n)$:

Assume that W_j has been defined for $j = 1, \ldots, k-1$.

Case 1:

There exists $x_i \in \mathbf{X_{k-1}}$ such that for all $N \in \mathrm{PP}(\mathbf{Z_{k-1}}; \mathbf{Q})$

$$(\exists_{j<k}) W_j \, (N x_i) \neq 0 \; .$$

Choose z_k to be any such x_i (for example the least).
For every j, set $w_{k,j} = 0$.

Case 2:

For every $x_i \in \mathbf{X_{k-1}}$, there exists $N \in \mathrm{PP}(\mathbf{Z_{k-1}}; \mathbf{Q})$ such that for all $j < k$, $W_j \, (N x_i) = 0$.
Define $\overline{M}_k \, (M)$, $\gamma_{k,i}$, and $\hat{x}_i$ as follows:
For all $M \in \mathrm{PP}(\overline{x}; \mathbf{Q})$, and $x_i \in \mathbf{X_{k-1}}$, $\overline{M}_k \, (M) = NM$ where $(\forall_{j<k}) W_j \, (NM) = 0$ and $N \in \mathrm{PP}(\mathbf{Z_{k-1}}; \mathbf{Q})$.
We will show later that $\overline{M}_k \, (M)$ is well defined.

$$\gamma_{k,i} \; = \; \left\{ \begin{array}{ll} 1 & \text{if } \overline{M}_k \, (x_i) \underset{\mathrm{A}}{\geq} 1 \\ -1 & \text{otherwise} \end{array} \right.$$

$$\hat{x}_i \; = x_i^{\gamma_{k,i}}$$

Choose z_k to be the $x_j \in \mathbf{X_{k-1}}$ such that for all $x_l \in \mathbf{X_{k-1}}$, $\overline{M}_k \, (\hat{x}_j) \underset{\mathrm{A}}{\geq} \overline{M}_k \, (\hat{x}_l)$,
and let $\hat{z}_k = \hat{x}_j$ where $z_k = x_j$.

Then for all $l = 1, \ldots, n$ choose,

$$w_{k,l} = \begin{cases} 0 & \text{if } x_l \notin \mathbf{X_{k-1}} \\ \gamma_{k,l} \sup \left\{ s \in \mathbf{Q} | \overline{M}_k\left(\hat{x}_l\right) \underset{\mathrm{A}}{\geq} \overline{M}_k\left(\hat{z}_k^s\right) \right\} \end{cases}.$$

(Either case:)

$$\text{Set} \begin{cases} \mathbf{X_k} &= \mathbf{X_{k-1}} - \{z_k\} \\ \mathbf{Z_k} &= \mathbf{Z_{k-1}} \cup \{z_k\} \end{cases}.$$

To verify the correctness of this construction, we must show that the resulting weight functions satisfy (1). To show that (1) holds in the $\Longleftarrow$ direction, we will prove at each stage:
Lemma A_k :

$$W_k\left(M\right) > 0 \ \& \ \forall_{j<k} W_j\left(M\right) = 0 \quad \Longrightarrow \quad M \underset{\mathrm{A}}{>} 1$$

To show that (1) also holds in the $\Longrightarrow$ direction, we will prove at each stage:
Lemma B_k :

$$\text{For any } M \in \mathrm{PP}(\mathbf{Z_k}),\ (\forall_{j \leq k})((W_k\left(M\right) = 0) \Longrightarrow (M = 1))$$

Now, at stage n, this includes all power products $M \in \mathrm{PP}(\overline{x}; \mathbf{Q})$. Let M be any power product with $M \underset{\mathrm{A}}{>} 1$,and so $M^{-1} \underset{\mathrm{A}}{<} 1$. Lemma B_n requires at least one of the $W_i(M^{-1})$ be non-zero, for otherwise M^{-1} would be 1. Let k be the smallest i for which $W_i(M^{-1})$ is non-zero, then

$$W_k(M^{-1}) \neq 0 \ \& \ \forall_{j<k} W_j\left(M^{-1}\right) = 0.$$

If $W_k(M^{-1}) > 0$, then by lemma A_k, $M^{-1} \underset{\mathrm{A}}{>} 1$. But, $M^{-1} \underset{\mathrm{A}}{<} 1$, so $W_k(M^{-1}) < 0$, and therefore $W_k(M) > 0$. Therefore, the two lemmas imply the correctness of the $w_{k,i}$ construction.

Now we are ready to prove lemmas A_k and B_k.

Stage 1:

Lemma 5 *for* $1 < i < n$, $\quad \forall_{q,t \in \mathbf{Q}}\ (qt < w_{1,i} t) \implies (x_i^t \underset{\mathrm{A}}{\geq} z_1^{qt})$

Proof. Otherwise, there exists i, q, and t such that $qt < w_{1,i}t$, and $z_1^{qt} \underset{\mathrm{A}}{>} x_i^t$

Case I: $t > 0$. Then

$$\begin{aligned} z_1^{qt} \underset{A}{>} x_i^t &\implies z_1^q \underset{A}{>} x_i \\ qt < w_{1,i} t &\implies q < w_{1,i} \end{aligned}$$

From the definition of $w_{1,i}$, for each $\epsilon > 0$ it is possible to find an s such that

$$w_{1,i} - s \; < \; \epsilon$$

and,

$$x_i \underset{A}{\geq} z_1^s$$

Choose $\epsilon < w_{1,i} - q$, then $s - q > 0$, which leads to the contradiction

$$\begin{aligned} z_1^q \underset{A}{>} x_i \underset{A}{\geq} z_1^s &\implies z_1^q z_1^{-q} \underset{A}{>} z_1^s z_1^{-q} \\ &\implies 1 \underset{A}{>} z_1^{s-q} \\ &\implies 1 \underset{A}{>} z_1 \end{aligned}$$

Case II: $t = 0$.

This leads to the immediate contradiction $1 \underset{A}{>} 1$.

Case III: $t < 0$.

$$\begin{aligned} z^{qt} \underset{A}{>} x^t &\implies x \underset{A}{>} z^q \\ qt < w_{1,i} t &\implies w_{1,i} < q \end{aligned}$$

But, by definition, $w_{1,i} = \sup \left\{ s | x \underset{A}{>} z^s \right\}$ so, $w_{1,i} \geq q$.

Q.E.D.

Using this result we prove:
Lemma A_1 : $W_1(M) > 0 \implies M \underset{A}{>} 1$
Proof. Let M be any power product $M = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$ such that $W_1(M) > 0$. Since $W_1(M) > 0$ it is possible to find a $c \in \mathbf{Q}$ suct that, $c > 0$ and $W_1(M) > c$. Then, for each i, choose q_i satisfying

$$w_{1,i}\alpha_i - \frac{c}{n} \; < \; q_i \alpha_i \; < \; w_{1,i}\alpha_i$$

Then,

$$M \;=\; \prod_{i=1}^{n} x_i^{\alpha_i} \;\underset{\mathrm{A}}{\geq}\; z_1^{\sum_{i=1}^{n} q_i \alpha_i}$$

but,

$$\sum_{i=1}^{n} q_i \alpha_i \;>\; \sum_{i=1}^{n} (w_{1,i}\alpha_i - \frac{c}{n}) \;=\; W_1(M) - c \;>\; 0$$

leading to the contradiction,

$$M \underset{\mathrm{A}}{\geq} z_1^{W_1(M)-c} \underset{\mathrm{A}}{>} 1$$

Q.E.D.

Lemma B_1 : For any power product $M = z_1^{\beta_1}$, $W_1(M) = 0 \implies M = 1$
Proof. If $z_1 = x_j$ for some j, then it is seen from the definition that $w_{1,j} = 1$. So,

$$W_1(M) \;=\; W_1(x_j^{\beta_1}) \;=\; w_{1,j}\beta_1 \;=\; \beta_1$$

i.e., $M = 1 \iff \beta_1 = 0 \iff W_1(M) = 0$. **Q.E.D.**

Stage k (2 to n):
Assume at stage **k** that Lemmas A_{k-1} and B_{k-1} hold.
Case 1:
There exists $x_i \in \mathbf{X_{k-1}}$ such that for all $N \in \mathrm{PP}(\mathbf{Z_{k-1}}; \mathbf{Q})$

$$(\exists_{j<k}) W_j\,(N x_i) \neq 0$$

In this case, z_k was chosen to be any such x_i, and

$$w_{k,j} \;=\; 0 \;\text{ for all } 1 \leq j \leq n$$

Then lemma A_k $[W_k\,(M) > 0 \;\&\; \forall_{j<k} W_j\,(M) = 0 \implies M \underset{\mathrm{A}}{>} 1]$ holds vacuously since for all M, $W_k\,(M) = 0$.
Lemma B_k:

$$\text{For any } M \in \mathrm{PP}(\mathbf{Z_k}),\; (\forall_{j\leq k})((W_k\,(M) = 0) \Longrightarrow (M = 1))$$

Proof. Let $M = z_1^{\beta_1} z_2^{\beta_2} \ldots z_k^{\beta_k}$ such that $(\forall_{j\leq k}) W_j\,(M) = 0$. If $\beta_k \neq 0$ then let $N = (z_1^{\beta_1} z_2^{\beta_2} \ldots z_{k-1}^{\beta_{k-1}})^{\frac{1}{\beta_k}}$. Then the assumption of this case implies $\exists_{j<k}$, $W_j(N z_k) \neq 0$. But this means that $W_j(M) = \beta_k W_j(N z_k) \neq 0$, contradiction.

So $\beta_k = 0$. But by Lemma $B_k - 1$, we see that $M = z_1^{\beta_1} z_2^{\beta_2} \ldots z_{k-1}^{\beta_{k-1}} = 1$. **Q.E.D.**

Case 2:
For every $x_i \in \mathbf{X_{k-1}}$, there exists $N \in \mathrm{PP}(\mathbf{Z_{k-1}}; \mathbf{Q})$ such that for all $j < k$,

$$W_j\,(N x_i) = 0$$

Recall that in this case we defined:

$$\begin{aligned}
\overline{M}_k\,(M) \;&\equiv\; z_1^{\beta_1} z_2^{\beta_2} \ldots z_{k-1}^{\beta_{k-1}} M \text{ such that } (\forall_{j<k}) W_j \left(\overline{M}_k\,(M)\right) = 0 \\
\gamma_{k,i} \;&=\; \begin{cases} 1 & \text{if } \overline{M}_k\,(x_i) \underset{\mathrm{A}}{\geq} 1 \\ -1 & \text{otherwise} \end{cases} \\
\hat{x}_i \;&=\; x_i^{\gamma_{k,i}} \\
z_k \;&=\; x_j \in \mathbf{X_{k-1}} \quad \text{where } (\forall_{x_i \in \mathbf{X_{k-1}}}) \overline{M}_k\,(\hat{x}_j) \underset{\mathrm{A}}{\geq} \overline{M}_k\,(\hat{x}_i)
\end{aligned}$$

Let $\hat{z}_k = \hat{x}_j$ where $z_k = x_j$
for $1 \leq l \leq n$,

$$w_{k,l} = \begin{cases} 0 & \text{if } x_l \notin \mathbf{X_{k-1}} \\ \gamma_{k,l} \sup \left\{ s \in \mathbf{Q} | \overline{M}_k\,(\hat{x}_l) \underset{\mathrm{A}}{\geq} \overline{M}_k\,(\hat{z}_k^s) \right\} \end{cases}$$

The definition of $\overline{M}_k\,(M)$ in the construction is justified next.

Lemma 6 *For each power product $M = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$, $\overline{M}_k\,(M)$ exists and is unique.*

Proof.

Existence: By the condition of this case, for each variable $x_i \in \mathbf{X_{k-1}}$, there is an $N \in \mathrm{PP}(\mathbf{Z_{k-1}}; \mathbf{Q})$ such that

$$(\forall_{j<k}) W_j\,(N x_i) = 0$$

Let M be any power product, then $M = M'M''$, where $M' \in \mathrm{PP}(\mathbf{X_{k-1}}; \mathbf{Q})$, $M'' \in \mathrm{PP}(\mathbf{Z_{k-1}}; \mathbf{Q})$. Let α_i be the exponent of x_i in M' (and hence in M). Then, we can find $N_i \in \mathrm{PP}(\mathbf{Z_{k-1}}; \mathbf{Q})$ such that

$$(\forall_{j<k}) W_j\,(N_i x_i^{\alpha_i}) = 0$$

The requirements for $\overline{M}_k\,(M)$ are now satisfied by:

$$\overline{M}_k\,(M) \;=\; \prod N_i x_i^{\alpha_i}$$

$\overline{M}_k(M)$ has the correct form since

$$\begin{aligned}\overline{M}_k(M) &= \prod N_i x_i^{\alpha_i} \\ &= ((M'')^{-1} \prod N_i)(M'M'') \\ &= NM\end{aligned}$$

and, for all $j < k$,

$$\begin{aligned}W_j\left(\overline{M}_k(M)\right) &= W_j\left(\prod N_i x_i^{\alpha_i}\right) \\ &= \sum W_j\left(N_i x_i^{\alpha_i}\right) \;=\; 0\end{aligned}$$

Uniqueness: Suppose that for $N_1, N_2 \in \mathrm{PP}(\mathbf{Z_{k-1}};\mathbf{Q})$ both N_1M and N_2M satisfy the requirements for $\overline{M}_k(M)$. Then for $j < k$,

$$W_j\left(N_1N_2^{-1}\right) \;=\; W_j(N_1M) - W_j(N_2M) \;=\; 0$$

so, by lemma B_{k-1}, $N_1 = N_2$.

Q.E.D.

Corollary 1

$$((\forall_{j<k})W_j(M) = 0) \Longrightarrow \overline{M}_k(M) = M$$

Proof. Since $(\forall_{j<k})W_j(M) = 0$, M satisfies the requirements for $\overline{M}_k(M)$ and by the previous corollary, this form is unique.
Q.E.D.

Corollary 2 *For all power products M and N*

$$\overline{M}_k(MN) = \overline{M}_k(M)\overline{M}_k(N)$$

Proof. $\overline{M}_k(M)\overline{M}_k(N)$ is of the form $z_1^{\beta_1} z_2^{\beta_2} \ldots z_{k-1}^{\beta_{k-1}} MN$, and for all $j < k$,

$$W_j\left(\overline{M}_k(M)\overline{M}_k(N)\right) \;=\; W_j\left(\overline{M}_k(M)\right) + W_j\left(\overline{M}_k(N)\right) \;=\; 0$$

By the previous corollary this form is unique.
Q.E.D.

Corollary 3 *For all power products M and $c \in \mathbf{Q}$,*

$$\overline{M}_k(M^c) = (\overline{M}_k(M))^c$$

Proof. $(\overline{M}_k(M))^c$ is of the form $z_1^{\beta_1} z_2^{\beta_2} \ldots z_{k-1}^{\beta_{k-1}} M^c$, and for all $j < k$,

$$W_j\left((\overline{M}_k(M))^c\right) \;=\; cW_j\left(\overline{M}_k(M)\right) \;=\; 0$$

Q.E.D.

Lemma 7 *For x_i $(i = 1, \ldots, n)$, for all $q, t \in \mathbf{Q}$*

$$(qt < \gamma_{k,i} w_{k,i} t) \implies (\overline{M}_k(\hat{x}_i{}^t) \underset{A}{\geq} \overline{M}_k(\hat{z}_k{}^{qt}))$$

Proof. Otherwise, there exist i, q and t such that $qt < w_{k,i} t$, and $\overline{M}_k(\hat{z}_k{}^{qt}) \underset{A}{>} \overline{M}_k(\hat{x}_i{}^t)$

Case I: $x_i \notin \mathbf{X_{k-1}}$.

Then $\overline{M}_k(x_i^t) = 1$ which implies that $qt > 0$. But this leads to a contradiction since $w_{k,i} = 0$ and

$$qt < \gamma_{k,i} w_{k,i} t \implies qt < 0$$

Case II: $x_i \in \mathbf{X_{k-1}}$ & $t > 0$. Then

$$\begin{aligned} \overline{M}_k(\hat{z}_k{}^{qt}) \underset{A}{>} \overline{M}_k(\hat{x}_i{}^t) &\implies \overline{M}_k(\hat{z}_k{}^{q}) \underset{A}{>} \overline{M}_k(\hat{x}_i) \\ qt < \gamma_{k,i} w_{k,i} t &\implies q < \gamma_{k,i} w_{k,i} \end{aligned}$$

From the definition of $w_{k,i}$, for each $\epsilon > 0$ it is possible to find an s such that

$$\gamma_{k,i} w_{k,i} - s \;<\; \epsilon$$

and,

$$\overline{M}_k(\hat{x}_i) \underset{A}{\geq} \overline{M}_k(\hat{z}_k{}^{s})$$

Choosing $\epsilon < \gamma_{k,i} w_{k,i} - q$ gives $s - q > 0$, which leads to the contradiction

$$\begin{aligned} \overline{M}_k(\hat{z}_k{}^{q}) \underset{A}{>} \overline{M}_k(\hat{z}_k{}^{s}) &\implies \overline{M}_k(1) \underset{A}{>} \overline{M}_k(\hat{z}_k{}^{s-q}) \\ &\implies 1 \underset{A}{>} \overline{M}_k(\hat{z}_k) \end{aligned}$$

Case III: $x_i \in \mathbf{X_{k-1}}$ & $t = 0$.
This is vacuously true.

Case IV: $x_i \in \mathbf{X_{k-1}}$ & $t < 0$.

$$\begin{aligned} \overline{M}_k\left(\hat{z}_k{}^{qt}\right) \underset{\mathrm{A}}{>} \overline{M}_k\left(\hat{x}_i{}^{t}\right) &\implies \overline{M}_k\left(\hat{x}_i\right) \underset{\mathrm{A}}{>} \overline{M}_k\left(\hat{z}_k{}^{q}\right) \\ qt < \gamma_{k,i} w_{k,i} t &\implies \gamma_{k,i} w_{k,i} < q \end{aligned}$$

But, by definition, $\gamma_{k,i} w_{k,i} = \sup\left\{ s | \overline{M}_k\left(\hat{x}_i\right) \underset{\mathrm{A}}{>} \overline{M}_k\left(\hat{z}_k{}^{s}\right) \right\}$ so, $\gamma_{k,i} w_{k,i} \geq q$.

Q.E.D.

Now, we may complete our consideration of case 2 with proofs of lemmas A_k, and B_k.
Lemma A_k:

$$W_k\left(M\right) > 0 \;\&\; \forall_{j<k} W_j\left(M\right) = 0 \implies M \underset{\mathrm{A}}{>} 1$$

Proof. Let $M = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$ be any power product such that $W_k\left(M\right) > 0$ and $(\forall_{j<k}) W_j\left(M\right) = 0$. Pick $c \in \mathbf{Q}$ such that $W_k\left(M\right) > c > 0$. For each i, choose a $q_i \in \mathbf{Q}$ such that

$$\gamma_{k,i} \alpha_i w_{k,i} - \frac{c}{n} \;<\; q_i \alpha_i \;\leq\; \gamma_{k,i} \alpha_i w_{k,i}$$

Now, since $(\forall_{j<k}) W_j\left(M\right) = 0$ we can use the corollaries to lemma 6 to get

$$\begin{aligned} M &= \overline{M}_k\left(M\right) \\ &= \prod_{i=1}^{n} \overline{M}_k\left(x_i^{\alpha_i}\right) \;=\; \prod_{i=1}^{n} \overline{M}_k\left(\hat{x}_i^{\gamma_{k,i}\alpha_i}\right) \\ &\underset{\mathrm{A}}{\geq} \prod_{i=1}^{n} \overline{M}_k\left(\hat{z}_k^{\gamma_{k,i} q_i \alpha_i}\right) \quad \text{(by lemma 7)} \\ &\underset{\mathrm{A}}{\geq} \left(\overline{M}_k\left(\hat{z}_k\right)\right)^{\sum_{i=1}^{n} \gamma_{k,i} q_i \alpha_i} \end{aligned}$$

but,

$$\sum_{i=1}^{n} \gamma_{k,i} q_i \alpha_i \;\geq\; \sum_{i=1}^{n} \gamma_{k,i} (\gamma_{k,i} \alpha_i w_{k,i} - \frac{c}{n})$$

$$\begin{aligned} &\geq W_k(M) - \sum_{i=1}^{n} \gamma_{k,i}\frac{c}{n} \\ &\geq W_k(M) - c > 0 \end{aligned}$$

It follows that $M \underset{A}{>} 1$
Q.E.D.

Lemma B_k:

$$\text{For any } M \in \mathrm{PP}(\mathbf{Z_k}),\ (\forall_{j \leq k})((W_k(M) = 0) \Longrightarrow (M = 1))$$

Proof. Let $z_k = x_j \in \mathbf{X_{k-1}}$, so

$$\begin{aligned} w_{k,j} &= \gamma_{k,j} \sup \left\{ s \in \mathbf{Q} | \overline{M}_k(\hat{x}_j) \underset{A}{\geq} \overline{M}_k\left(\hat{x}_j^s\right) \right\} \\ &= \gamma_{k,j} = \pm 1 \end{aligned}$$

Also, for $i = 1, \ldots, n$, if $x_i \notin \mathbf{X_{k-1}}$, then $w_{k,i} = 0$. Thus

$$W_k(M) = w_{k,j}\beta_k = \pm\beta_k$$

Therefore, $W_k(M) = 0 \implies \beta_k = 0$ So $M = z_1^{\beta_1} z_2^{\beta_2} \ldots z_{k-1}^{\beta_{k-1}}$ and inductively by lemma B_{k-1}, $M \equiv 1$.
Q.E.D.

This concludes our proof of theorem 1. We note that our weights $w_{i,j}$ satisfy $|w_{i,j}| \leq 1$. Now, we can construct a modified set of weight functions

$$U_k(x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}) = \sum_{i=1}^{n} u_{k,i}\alpha_i$$

which also satisfy (1), and in addition, have the property that all of the $u_{k,i}$'s are non-negative. This property will be useful in our next section.

The functions U_k can be constructed as follows:

$$U_1 = W_1$$

and for $k = 2$ to n,

$$U_k = W_k + U_{k-1} * \max\left\{\tfrac{-w_{k,i}}{u_{k-1,i}} | w_{k,i} < 0\right\}$$

The resulting functions satisfy (1) since the value of $U_k(M)$ is only of importance if $(\forall j < k) U_j(M) = 0$, and in this case, $U_k(M) = W_k(M)$.

To see that the $u_{k,i}$'s are non-negative, note that the weights in W_1 are non-negative, and for $k > 1$, we have for all j,

$$\begin{aligned} u_{k,j} &= w_{k,j} + u_{k-1,j} \max\left\{\tfrac{-w_{k,i}}{u_{k-1,i}} | w_{k,i} < 0\right\} \\ &\geq w_{k,j} + u_{k-1,j}\left(\frac{-w_{k,j}}{u_{k-1,j}}\right) \geq 0 \ . \end{aligned}$$

To get some intuitions, let us look at the resulting weight functions for the admissible orderings introduced in section 1. For each admissible ordering, let the variables $x_1, \ldots, x_n$ be ordered such that

$$x_1 \underset{A}{>} x_2 \underset{A}{>} \ldots \underset{A}{>} x_n$$

The construction yields the following weight functions:

Example 1 : Lexicographic Ordering

$$\begin{aligned} W_k\,(x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}) &= \alpha_k \qquad (k = 1, \ldots, n) \\ U_k(x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}) &= \alpha_k \qquad (k = 1, \ldots, n) \end{aligned}$$

Example 2 : Total-Degree(Lex) Ordering

$$\begin{aligned} W_1(x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}) &= \alpha_1 + \alpha_2 + \ldots + \alpha_n \\ W_2(x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}) &= -\alpha_2 - \ldots - \alpha_n \\ W_k\,(x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}) &= \alpha_{k-1} \qquad (k = 3, \ldots, n) \end{aligned}$$

$$\begin{aligned} U_1(x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}) &= \alpha_1 + \alpha_2 + \ldots + \alpha_n \\ U_k(x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}) &= \alpha_{k-1} \qquad (k = 2, \ldots, n) \end{aligned}$$

Note: The construction chooses the z_i's in a curious order. x_1 is chosen for z_1, but then x_n is chosen for z_2. The remaining x's are chosen in the order $z_i = x_{i-1}$.

Example 3 : Total-Degree(Recursive) Ordering

$$\begin{aligned} W_1(x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}) &= \alpha_1 + \alpha_2 + \ldots + \alpha_n \\ W_k\,(x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}) &= -\alpha_{n-k+2} \qquad (k = 2, \ldots, n) \end{aligned}$$

$$U_k(x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}) = \alpha_1 + \alpha_2 + \ldots + \alpha_{n-k+1} \qquad (k = 1, \ldots, n)$$

4 Bounds on Normal Form Algorithms

We now quantify the termination process of the normal form algorithm. Here we allow $\underset{A}{>}$ to be any admissible ordering on[2] $\mathrm{PP}(\overline{x}) = \mathrm{PP}(\overline{x}; \mathbf{N})$. We also fix a set of non-negative weight functions $U_1, \ldots, U_n$, which characterize $\underset{A}{>}$ as described in the previous section. Let $F \subseteq R$ be a finite set and $g \in R$. Let

$$g = g_0 \xrightarrow{F} g_1 \xrightarrow{F} \cdots \xrightarrow{F} g_k = \mathrm{nf}_F(g). \tag{2}$$

Our goal is to bound the maximum value of k in the reduction sequence (2). The bound on the reduction sequence depends on three factors:

1. *The set of polynomials F.*
   Let ℓ = maximum length of any f_i in F. By the *length* of a polynomial we mean the number of monomials in it.

2. *The admissible ordering $\underset{A}{>}$ and the choice of the non-negative weight functions U_k.* Relative to the set F, the influence of $\underset{A}{>}$ on the reduction sequence bound can be quantified as follows. For any polynomial f written as a sum of monomials $f = f_1 + f_2 + \ldots + f_\ell$ where the monomials are ordered $f_1 \underset{A}{>} f_2 \underset{A}{>} \ldots \underset{A}{>} f_\ell$, define

$$\begin{aligned}
\Delta_k(f) &= \{U_k(f_{j-1}) - U_k(f_j) | j = 2, \ldots, \ell, \text{and } U_k(f_{j-1}) > U_k(f_j)\} \\
r_1 &= \max\{u | u \in \Delta_k(f), f \in F, k = 1, \ldots, n\} \\
r_2 &= \min\{u | u \in \Delta_k(f), f \in F, k = 1, \ldots, n\}
\end{aligned}$$

   Note: The sets $\Delta_k(f)$ are empty for all k only if $\ell = 1$, in which case the definitions of r_1, r_2, and the following function $W_F(M)$ are not used.

3. *The input polynomial g.*
   Let L be the length of g, and write g as a sum of monomials $g = g_1 + g_2 + \ldots + g_L$. The bound on the reduction sequence is dependent upon L and the values of $U_k(g_i)$ $(i = 1, \ldots, L)$.

If $\ell > 1$, we define a weighting function $W_F : \mathrm{PP} \to \mathbf{N}$ on monomials as follows:

$$W_F(M) = \frac{1}{r_2} \sum_{i=1}^{n} (\frac{r_1}{r_2} + 1)^{n-i} U_i(M)$$

[2]The notion of a reduction is not defined except where the exponents are natural numbers.

Lemma 8 *Let $f \in F$. 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, $W_F(f_{j-1}) \geq 1 + W_F(f_j)$ for $j = 2, \ldots, k$..*

Proof. Since $f_{j-1} \underset{A}{>} f_j$ there exists a k_0 such that

$$U_{k_0}(f_{j-1}) > U_{k_0}(f_j) \ \& \ (\forall_{i<k_0}) U_i(f_{j-1}) = U_i(f_j) \ .$$

So, we get

$$\begin{aligned}
W_F(f_{j-1}) - W_F(f_j) &= \frac{1}{r_2}\sum_{i=1}^{n}(\frac{r_1}{r_2}+1)^{n-i}(U_i(f_{j-1}) - U_i(f_j)) \\
&= \frac{1}{r_2}(\frac{r_1}{r_2}+1)^{n-k_0}(U_{k_0}(f_{j-1}) - U_{k_0}(f_j)) + \\
&\quad \frac{1}{r_2}\sum_{i=k_0+1}^{n}(\frac{r_1}{r_2}+1)^{n-i}(U_i(f_{j-1}) - U_i(f_j)) \\
&\geq \frac{1}{r_2}(\frac{r_1}{r_2}+1)^{n-k_0}(r_2) - \frac{1}{r_2}\sum_{i=k_0+1}^{n}(\frac{r_1}{r_2}+1)^{n-i}(r_1) \\
&\geq 1
\end{aligned}$$

Q.E.D.

Immediately by induction we have:

Corollary 4 *Let $f \in F$ be written as a sum of monomials $f = f_1 + f_2 + \cdots + f_k$ as before. Then, $W_F(f_1) \geq k - 1$*

Now we define a weight function on polynomials. Recall that the length of each polynomial in F is at most ℓ. For any polynomial we define its weight to be

$$\bar{W}_F(g) = \begin{cases} L & \ell = 1 \\ L + \sum_{i=1}^{L} W_F(g_i) & \ell = 2 \\ \sum_{i=1}^{L} 2^{W_F(g_i)} & \ell \geq 3 \end{cases}$$

Lemma 9 *If $g \xrightarrow{F} h$ then $\bar{W}_F(g) \geq 1 + \bar{W}_F(h)$.*

Proof. Suppose $h = g - Mf$ for some $f \in F$ and monomial M. Let $f = f_1 + f_2 + \cdots + f_k$ with the monomials ordered as before. The reduction removes the monomial Mf_1 from g, and 'replaces' it with $Mf_2 + Mf_3 + \ldots + Mf_k$. If $\ell = 1$, then each reduction removes a monomial without adding any new ones, so the length of h is one less than the length of g.

If $\ell = 2$, and $k = 1$, once again the reduction results only in the removal of a monomial, so the length is reduced and the lemma satisfied. So, assuming that $\ell = 2$ and $k = 2$, then from lemma 8 we have

$$\begin{aligned} \bar{W}_F(g) - \bar{W}_F(h) &= W_F(Mf_1) - W_F(Mf_2) \\ &= W_F(f_1) - W_F(f_2) \ \geq \ 1 \end{aligned}$$

Now, consider $\ell \geq 3$. If $k = 1$, the removal of a monomial reduces the weight by at least 1, so assume $k \geq 2$, then

$$\begin{aligned} \bar{W}_F(g) - \bar{W}_F(h) &= 2^{W_F(Mf_1)} - \sum_{i=2}^{k} 2^{W_F(Mf_i)} \\ &\geq 2^{W_F(Mf_1)} - \sum_{i=2}^{k} 2^{W_F(Mf_1)-i+1} \\ &\qquad \text{(repeated application of lemma 8).} \\ &= 2^{W_F(Mf_1)} - 2^{W_F(Mf_1)} + 2^{W_F(Mf_1)-k+1} \\ &\geq 2^{W_F(Mf_1)-k+1} \ \geq \ 1 \ \text{ by Corollary 4} \end{aligned}$$

Q.E.D.

Therfore, by induction, the length of a normal form reduction sequence is bounded by $\bar{W}_F(g)$. Let $\overline{U}(M) = \max\{U_k(M)\}$. Then

$$\begin{aligned} W_F(M) &\leq \frac{1}{r_2}\sum_{i=1}^{n}(\frac{r_1}{r_2}+1)^{n-i}\overline{U}(M) \\ &\leq \frac{1}{r_1}(\frac{r_1}{r_2}+1)^{n}\overline{U}(M) \end{aligned}$$

Now, collecting the constant factor, let $R_F = \frac{1}{r_1}(\frac{r_1}{r_2}+1)^n$, then

$$W_F(M) \ \leq \ R_F\overline{U}(M) \tag{3}$$

We immediately conclude:

Theorem 10 *For any admissible ordering $\underset{A}{>}$, the length of any sequence of reductions beginning from an input polynomial g is at most*

$$\bar{W}_F(g) \leq \begin{cases} L & \ell = 1 \\ (1 + R_F\overline{U})L & \ell = 2 \\ 2^{R_F\overline{U}}L & \ell \geq 3 \end{cases}$$

where

L is the length of g.

ℓ is the maximum length of a polynomial in F.

R_F is a constant which depends on the admissible ordering $\underset{\mathrm{A}}{>}$ and F.

$\overline{U}$ is the maximum of the weights $U_k(g_i)$ where g_i is a monomial of g.

Remark: We normally prefer to get bounds in terms of the total degree $\deg(g)$ of g, but assuming $\underset{\mathrm{A}}{>}$ is fixed,

$$\overline{U} = O(\deg(g)).$$

5 Lower Bound on Normal Form Reduction

In this section, we show that the upper bound for the normal form algorithm is tight by demonstrating an admissible ordering and a set F which nearly achieves the upper bound. The admissible ordering we will consider is the lexicographic ordering $\underset{\mathrm{LEX}}{>}$. Let the variables be ordered such that

$$x_1 \underset{\mathrm{LEX}}{>} x_2 \underset{\mathrm{LEX}}{>} \dots \underset{\mathrm{LEX}}{>} x_n$$

The set F we consider contains the following polynomials, where d and ℓ are arbitrary numbers with $d \geq \ell - 2 > 0$.

$$\begin{aligned}
f_1 &= x_1 - (x_2^d x_3^d \dots x_{n-1}^d)(x_n^d + x_n^{d-1} + \dots + x_n^{d-\ell+2}) \\
f_2 &= x_2 - (x_3^d x_4^d \dots x_{n-1}^d)(x_n^d + x_n^{d-1} + \dots + x_n^{d-\ell+2}) \\
&\vdots \\
f_{n-1} &= x_{n-1} - x_n^d - x_n^{d-1} - \dots - x_n^{d-\ell+2} \\
f_n &= x_n^\ell - x_n^{\ell-1} - \dots - x_n \\
f_{n+1} &= x_n^{\ell-1} - x_n^{\ell-2} - \dots - x_n \\
&\vdots \\
f_{n+\ell-2} &= x_n^2 - x_n \\
f_{n+\ell-1} &= x_n - 1
\end{aligned}$$

Let g, the input polynomial being reduced, be:

$$g = x_1^D x_n^L + x_1^D x_n^{L-1} + \dots + x_1^D x_n$$

where $D > L$. And, let

$$g \xrightarrow{F} g_1 \xrightarrow{F} g_2 \xrightarrow{F} \ldots \xrightarrow{F} g_m \ ,$$

be a normal form reduction sequence for g.

Before considering an actual reduction sequence, and the number of steps involved, let us compute the bound on the length m of the reduction sequence according to the previous theorem.

For lexicographic order, $U_i(x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}) = \alpha_i$, so

$$\begin{aligned} r_1 &= d \\ r_2 &= 1 \\ \overline{U} &= \max\{U_i(g_j) | g_j \text{ a monomial of } g\} \ = \ D \end{aligned}$$

According to theorem 10, the length of the reduction sequence is bounded by

$$m \ \leq \ 2^{\frac{1}{d}(d+1)^n D} L$$

Consider the reduction sequence which results when the reductions are made in the following order. At each step $g_i \xrightarrow{F} g_{i+1}$, choose M_i the least monomial of g_i (relative to $\underset{\text{LEX}}{>}$), and perform the reduction $g_{i+1} = g_i - cf_j$, where $\text{Hmono}(cf_j) \ = \ M_i$ and $j = \min\{k | f_k \text{ divides } M_i\}$. For any polynomial h, let the number of reductions which are made using this strategy be denoted as $s(h)$. This order of reduction avoids any cancellation of terms, so that for any polynomial h which may result during the normal form reduction sequence, if $h = h_1 + h_2 + \ldots + h_k$, then

$$s(h) \ = \ s(h_1) + s(h_2) + \ldots + s(h_k)$$

Claim: For any monomial $M = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$,

$$s(M) \ \geq \ 2^{\frac{\ell-2}{\ell-1}((\alpha_1(d+1)^{n-1} + \alpha_2(d+1)^{n-2} + \ldots + \alpha_n - 1)}$$

Proof. The claim holds for $M = x_n$, since $s(x_n) = 1$. Now, assume that the claim is valid for all N such that $M \underset{\text{LEX}}{>} N$. Then,

Case 1: $M = x_n^{\alpha_n}$, $\alpha_n < \ell$, then M will be reduced by

$$M \xrightarrow{f_{n+\ell-\alpha_n}} x_n^{\alpha_n - 1} + x_n^{\alpha_n - 2} + \ldots + x_n$$

so,

$$\begin{aligned} s(M) &= 1 + s(x_n^{\alpha_n-1}) + s(x_n^{\alpha_n-2}) + \ldots + s(x_n) \\ &\geq 1 + 2^{\frac{\ell-2}{\ell-1}(\alpha_n-2)} + \ldots + 2^{\frac{\ell-2}{\ell-1}(0)} \\ &= 1 + (2^{\frac{\ell-2}{\ell-1}(\alpha_n-1)} - 1)/(2^{\frac{\ell-2}{\ell-1}} - 1) \\ &\geq 2^{\frac{\ell-2}{\ell-1}(\alpha_n-1)} \end{aligned}$$

Case 2: $M = x_n^{\alpha_n}$, $\alpha_n \geq \ell$, then M will be reduced by

$$M \xrightarrow{f_n} x_n^{\alpha_n-1} + x_n^{\alpha_n-2} + \ldots + x_n^{\alpha_n-\ell+1}$$

so,

$$\begin{aligned} s(M) &= 1 + s(x_n^{\alpha_n-1}) + s(x_n^{\alpha_n-2}) + \ldots + s(x_n^{\alpha_n-\ell+1}) \\ &\geq 2^{\frac{\ell-2}{\ell-1}(\alpha_n-2)} + \ldots + 2^{\frac{\ell-2}{\ell-1}(\alpha_n-\ell)} \\ &= (2^{\frac{\ell-2}{\ell-1}(\alpha_n-1)} - 2^{\frac{\ell-2}{\ell-1}(\alpha_n-\ell)})/(2^{\frac{\ell-2}{\ell-1}} - 1) \\ &= 2^{\frac{\ell-2}{\ell-1}(\alpha_n-1)}(1 - 2^{\frac{\ell-2}{\ell-1}(-\ell+1)})/(2^{\frac{\ell-2}{\ell-1}} - 1) \\ &\geq 2^{\frac{\ell-2}{\ell-1}(\alpha_n-1)} \qquad \text{(see justification below)} \end{aligned}$$

Case 3: $M = x_i^{\alpha_i} \ldots x_n^{\alpha_n}$, $i < n$ and $\alpha_i \geq 1$, M will be reduced by

$$M \xrightarrow{f_i} (x_i^{\alpha_i-1} x_{i+1}^{\alpha_{i+1}+d} \ldots x_{n-1}^{\alpha_{n-1}+d})(x_n^{\alpha_n+d} + \ldots + x_n^{\alpha_n+d-\ell+2})$$

so,

$$\begin{aligned} s(M) &= s(x_i^{\alpha_i-1} x_{i+1}^{\alpha_{i+1}+d} \ldots x_{n-1}^{\alpha_{n-1}+d} x_n^{\alpha_n+d}) + \ldots + s(x_i^{\alpha_i-1} x_{i+1}^{\alpha_{i+1}+d} \ldots x_{n-1}^{\alpha_{n-1}+d} x_n^{\alpha_n+d-\ell+2}) \\ &\geq 2^{\frac{\ell-2}{\ell-1}((\alpha_i-1)(d+1)^{n-i}+(\alpha_{i+1}+d)(d+1)^{n-i-1}+\ldots+(\alpha_{n-1}+d)(d+1)+\alpha_n+d-1)} + \ldots + \\ &\quad 2^{\frac{\ell-2}{\ell-1}((\alpha_i-1)(d+1)^{n-i}+(\alpha_{i+1}+d)(d+1)^{n-i-1}+\ldots+(\alpha_{n-1}+d)(d+1)+\alpha_n+d-\ell+1)} \\ &= (2^{\frac{\ell-2}{\ell-1}((\alpha_i-1)(d+1)^{n-i}+(\alpha_{i+1}+d)(d+1)^{n-i-1}+\ldots+(\alpha_{n-1}+d)(d+1)+\alpha_n+d)} - \\ &\quad 2^{\frac{\ell-2}{\ell-1}((\alpha_i-1)(d+1)^{n-i}+(\alpha_{i+1}+d)(d+1)^{n-i-1}+\ldots+(\alpha_{n-1}+d)(d+1)+\alpha_n+d-\ell+1)})/(2^{\frac{\ell-2}{\ell-1}} - 1) \\ &= 2^{\frac{\ell-2}{\ell-1}((\alpha_i-1)(d+1)^{n-i}+(\alpha_{i+1}+d)(d+1)^{n-i-1}+\ldots+(\alpha_{n-1}+d)(d+1)+\alpha_n+d)}(1 - 2^{\frac{\ell-2}{\ell-1}(-\ell+1)})/(2^{\frac{\ell-2}{\ell-1}} - 1 \\ &\geq 2^{\frac{\ell-2}{\ell-1}((\alpha_i-1)(d+1)^{n-i}+(\alpha_{i+1}+d)(d+1)^{n-i-1}+\ldots+(\alpha_{n-1}+d)(d+1)+\alpha_n+d)} \\ &\geq 2^{\frac{\ell-2}{\ell-1}((\alpha_i)(d+1)^{n-i}+(\alpha_{i+1})(d+1)^{n-i-1}+\ldots+(\alpha_{n-1})(d+1)+\alpha_n-1)} \end{aligned}$$

In cases 2 and 3 we use the fact that for $\ell \geq 3$,

$$1 - 2^{-(\ell-2)} \;>\; 2^{\frac{\ell-2}{\ell-1}} - 1$$

Q.E.D.

Hence, the number of reductions for our input polynomial g is greater than $s(g)$,

$$\begin{aligned} s(g) &= s(x_1^D x_n^L) + s(x_1^D x_n^{L-1}) + \ldots s(x_1^D x_n) \\ &\geq L\ s(x_1^D x_n) \\ &\geq 2^{\frac{\ell-2}{\ell-1}(d+1)^{n-1}D} L \end{aligned}$$

6 Ordered Reductions

In the previous sections, we considered normal form reduction sequences. At each reduction step $g \xrightarrow{F} h$, $h = g - cf$, where f could be any polynomial in F such that the head monomial of cf was equal to g_i, where g_i is any monomial of g.

We next give a better bound for $\ell \geq 3$ under the assumption that the normal form algorithm always chooses to eliminate the $\underset{\mathrm{A}}{>}$-largest monomial that could be eliminated. More precisely, suppose that in the reduction step $g_{i-1} \xrightarrow{F} g_i$ in (2) the monomial M_i is eliminated. We say that the reduction sequence (2) is *ordered* if

$$M_1 \underset{\mathrm{A}}{>} M_2 \underset{\mathrm{A}}{>} \ldots \underset{\mathrm{A}}{>} M_k \tag{4}$$

In the sequence (2), assume M_i is eliminated by application of $f_i \in F$. Thus

$$g_i = g_{i-1} - c_i f_i$$

where the monomial M_i of g_{i-1} is equal to the head monomial of $c_i f_i$. Once again, we will use the monomial weighting function $W_F(M)$.

Lemma 11 *Let g and h be any polynomials such that $g \xrightarrow{F} h$, and let $g = g_1 + \ldots + g_s$ and $h = h_1 + \ldots + h_t$, then*

$$\max\{W_F(h_j) | j = 1, \ldots, t\} \leq \max\{W_F(g_i) | i = 1, \ldots, s\}$$

Proof. Each monomial h_j is either a monomial of g, or it is a monomial of cf where $f \in F$, and $\text{Hmono}(cf) = g_i$ for some g_i, in which case

$$W_F(h_j) \;<\; W_F(\text{Hmono}(cf)) \;\leq\; \max\{W_F(g_i) | i = 1, \ldots, s\}$$

Q.E.D.

Now, let

$$\begin{aligned} V(g) &= \max\{W_F(g_i) | i \leq \text{length of } g\} \\ &\leq \frac{1}{r_2}(\frac{r_1}{r_2} + 1)^n \overline{U} - 1 \end{aligned}$$

Immediately by induction we have:

Corollary 5 *Let $M_1, \ldots, M_k$ be the sequence of monomials eliminated during normal form reduction of g. Then for each M_j, $W_F(M_j) \leq V(g)$.*

By linearity of the weight functions, $W_F(x_i^\alpha) = \alpha W_F(x_i)$. Therefore, for each x_i, the exponent of x_i in M_j is bounded by $V(g)/W_F(x_i)$. But, $W_F(x_i)$ is just another constant which quantifies the admissible ordering relative to F, so let $\mu_i = W_F(x_i)$. The number of monomials whose exponent in each variable x_i is $\leq V(g)/\mu_i$, is

$$\begin{aligned} \prod_{i=1}^{n} \frac{V(g)+1}{\mu_i} &= (V(g)+1)^n \prod_{i=1}^{n} \frac{1}{\mu_i} \\ &\leq \frac{1}{r_2^n}(\frac{r_1}{r_2} + 1)^{n^2} \overline{U}^n \prod_{i=1}^{n} \frac{1}{\mu_i} \;. \end{aligned}$$

Collecting the constant which depends on F, let

$$C_F \;=\; \frac{1}{r_2^n}(\frac{r_1}{r_2} + 1)^{n^2} \prod_{i=1}^{n} \frac{1}{\mu_i} \;.$$

Now, since the M_j's are ordered, they are all distinct. We conclude:

Theorem 12 *For any admissible ordering $\underset{\text{A}}{>}$, the length of any sequence of ordered reductions beginning from an input polynomial g is at most $C_F \overline{U}^n$ where*

n is the number of variables

C_F is a constant which quantifies the admissible ordering $\underset{A}{>}$ with respect to F

$\overline{U}$ is the maximum of the weights $U_k(g_i)$ where g_i is a monomial of g.

We apply this result to the admissible orderings which have appeared in the previous examples. We will use the following additional notation:

d is the maximum degree of any monomial of f, $f \in F$.

D is the maximum degree of any monomial of g.

$e_i(M)$ is the exponent of variable x_i in M.

Lexicographic Order : Recall $U_k(x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}) = \alpha_k$. So,

$$\begin{aligned}
\Delta_k(f) &= \{e_k(f_{j-1}) - e_k(f_j) | e_k(f_{j-1}) > e_k(f_j)\} \\
r_1 &= \max\{u | u \in \Delta_k(f), f \in F\} \ \leq \ d
\end{aligned}$$

and since all elements of the Δ_k sets are positive integers, $r_2 \geq 1$.

$$\begin{aligned}
\mu_i &= W_F(x_i) \ = \ \frac{1}{r_2} \sum_{j=1}^{n} (\frac{r_1}{r_2} + 1)^{n-j} U_j(x_i) \\
&= \frac{1}{r_2} (\frac{r_1}{r_2} + 1)^{n-i} \\
C_F &= \frac{1}{r_2^n} (\frac{r_1}{r_2} + 1)^{n^2} \prod_{i=1}^{n} \frac{1}{\mu_i} \\
&= (\frac{r_1}{r_2} + 1)^{\frac{n^2+n}{2}} \ \leq \ (d+1)^{\frac{n^2+n}{2}} \\
\overline{U} &= \max\{U_k(g_i)\} \ \leq \ D
\end{aligned}$$

The length of an ordered reduction sequence is therfore bounded by $(d+1)^{\frac{n^2+n}{2}} D^n$.

Total-Degree Order (Lex or Recursive): In either case, $U_1(M) = deg(M)$, and $U_k(M) \leq deg(M)$ for all $k > 1$. So,

$$\begin{aligned}
r_1 &\leq d \\
r_2 &\geq 1 \\
U &\leq D
\end{aligned}$$

For each i, $u_{1,i} = 1$, so

$$\mu_i \;\geq\; \frac{1}{r_2}(\frac{r_1}{r_2}+1)^{n-1}$$

and so,

$$C_F \;\leq\; (\frac{r_1}{r_2}+1)^n \;\leq\; (d+1)^n\ .$$

The length of an ordered reduction sequence is therefore bounded by $(d+1)^n D^n$.

Note: A tighter bound of $(D+1)^n$ is also known for this case [Mishra and Yap 1986].

Final Remarks: If we omit the first condition $(x_i \underset{A}{>} 1)$ in the definition of an admissible ordering, the resulting ordering is called *semi-admissible*. Normal form reduction can also be defined relative to a semi-admissible ordering. However, to insure that the algorithm terminates, we must be more careful in our definition of divisibility. For semi-admissible orderings, we say f divides g if $cf = g$ and $c \underset{A}{>} 1$. The analysis for semi-admissible orderings can be reduced to that for admissible orderings by replacing each variable x_i, where $1 \underset{A}{>} x_i$, with x_i^{-1}.

References

[Buchberger 1985] Bruno Buchberger, *Gröbner basis: An algorithmic method in polynomial ideal theory*, in chapter 6 of **Multidimensional Systems Theory**, (editor, N. K. Bose), D.Reidel Publishing Company, 184-229.

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

[Mishra and Yap 1986] B. Mishra and C.Yap, *Notes on Gröbner Basis*, **NYU-Courant Robotics Lab Report No 87**, Nov 1986.

[Robbiano 1985] L. Robbiano, *Term Orderings on the Polynomial Ring*, **EUROCAL '85**, Lecture Notes in Computer Science N. 204, 513-517.

[Robbiano 1986] L. Robbiano, *On the Theory of Graded Structures*, **J. Symbolic Computation 2**, 1986, 139-170.