

Math 465 Lecture Notes

Brendan Hassett

January 18, 2002

3 Lecture 3: Gröbner bases and the division algorithm

Algorithm 3.1 (Naive division algorithm) Fix a monomial order $>$ on $k[x_1, \dots, x_n]$ and polynomials $f_1, \dots, f_r \in k[x_1, \dots, x_n]$.

Given $g \in k[x_1, \dots, x_n]$, we want to determine whether $g \in \langle f_1, \dots, f_r \rangle$:

Step 0:

i) Put $g_0 = g$ and look for some f_j with $\text{LM}(f_j) | \text{LM}(g_0)$.

ii) Cancel leading terms by putting

$$g_1 = g_0 - f_j \text{LT}(g_0) / \text{LT}(f_j).$$

General Step:

i) Given g_i , look for some f_j with $\text{LM}(f_j) | \text{LM}(g_i)$.

ii) Cancel leading terms by putting

$$g_{i+1} = g_i - f_j \text{LT}(g_i) / \text{LT}(f_j).$$

Unfortunately, we have seen that this sometimes breaks down: even when $g \in \langle f_1, \dots, f_r \rangle$, it may happen that $\text{LM}(g)$ is not divisible by any $\text{LM}(f_j)$. To understand better when this break down occurs, we make the following definitions:

Definition 3.2 (Ideal of Leading Terms) Fix a monomial order $>$ and let $I \subset k[x_1, \dots, x_n]$ be an ideal. The *ideal of leading terms* is defined

$$\text{LT}(I) := \{ \text{sums of leading terms } \text{LT}(g) : g \in I \}.$$

This is actually an ideal! Given any monomial x^α we have

$$\text{LT}(gx^\alpha) = x^\alpha \text{LT}(g),$$

thus if $g \in I$ and $\text{LT}(g) \in \text{LT}(I)$ then $x^\alpha \text{LT}(g) \in \text{LT}(I)$.

Definition 3.3 (Monomial Ideal) A monomial ideal $J \subset k[x_1, \dots, x_n]$ is an ideal generated by a collection of monomials $\{x^\alpha\}_{\alpha \in A}$.

Of course, the main example is the ideal of leading terms of an arbitrary ideal $I \subset k[x_1, \dots, x_n]$.

If I had explicitly stated the following lemma in lecture, some confusion might have been avoided:

Lemma 3.4 (Clarifying Lemma) Let $I = \langle x^\alpha \rangle_{\alpha \in A}$ be a monomial ideal. Then every monomial in I is a multiple of some x^α .

proof: Let x^β be a monomial in I . Then we can write

$$x^\beta = \sum_i x^{\alpha(i)} w_i$$

where the w_i are polynomials. In particular, x^β appears in the right-hand side, is a monomial of $x^{\alpha(i)} w_i$ for some i , and thus is divisible by $x^{\alpha(i)}$. \square

Definition 3.5 (Gröbner basis) Fix a monomial order $>$ and let $I \subset k[x_1, \dots, x_n]$ be an ideal. A Gröbner basis for I is a collection of polynomials

$$\{f_1, \dots, f_r\} \subset I$$

such that $\text{LT}(f_1), \dots, \text{LT}(f_r)$ generate $\text{LT}(I)$.

Nothing in the definition says that a Gröbner basis actually generates I ! We prove this *a posteriori*.

Remark 3.6 Every generator for a principal ideal is a Gröbner basis.

Algorithm 3.7 (Division Algorithm) Fix a monomial order $>$ on $k[x_1, \dots, x_n]$, $I \subset k[x_1, \dots, x_n]$ an ideal, and $f_1, \dots, f_r \in k[x_1, \dots, x_n]$ a Gröbner basis for I .

Given $g \in k[x_1, \dots, x_n]$, we want to determine whether $g \in I$:

Step 0:

- i) Put $g_0 = g$ and look for some f_j with $\text{LM}(f_j) | \text{LM}(g_0)$.*
- ii) Cancel leading terms by putting*

$$g_1 = g_0 - f_j \text{LT}(g_0) / \text{LT}(f_j).$$

General Step:

- i) Given g_i , look for some f_j with $\text{LM}(f_j) | \text{LM}(g_i)$.*
- ii) Cancel leading terms by putting*

$$g_{i+1} = g_i - f_j \text{LT}(g_i) / \text{LT}(f_j).$$

Proposition 3.8 *Retain the notation of the Division Algorithm.*

- 1. The algorithm terminates in a finite number of steps, with either $g_i = 0$ or $\text{LT}(g_i)$ not divisible by any of the leading terms $\text{LT}(f_j)$.*
- 2. In the first case, the algorithm returns a representation*

$$g = h_1 f_1 + \dots + h_r f_r \quad h_j \in k[x_1, \dots, x_n],$$

and $g \in I$. In the second case, we may conclude that $g \notin I$.

The proposition immediately implies the following:

Corollary 3.9 Fix a monomial order $>$. Let $I \subset k[x_1, \dots, x_n]$ be an ideal and f_1, \dots, f_r a Gröbner basis for I . Then $I = \langle f_1, \dots, f_r \rangle$.

proof: We first remark that, iterating (ii), we may write

$$g = \sum_{l=0}^{l-1} c_l x^{\alpha(l)} f_{j_l} + g_i, \tag{1}$$

where $c_l \alpha(l) = \text{LT}(g_l) / \text{LT}(f_{j_l})$. In particular,

$$g - g_i \in \langle f_1, \dots, f_r \rangle \subset I.$$

We now use the definition of a Gröbner basis: if, for some i , the leading term $\text{LT}(g_i)$ is not divisible by $\text{LT}(f_j)$ for any j , then

$$\text{LT}(g_i) \notin \langle \text{LT}(f_1), \dots, \text{LT}(f_r) \rangle$$

by Lemma 3.4. It follows that $g_i \notin I$ and thus $g \notin I$ by the expression above. Otherwise, we get a sequence of g_i with

$$\text{LT}(g_0) > \text{LT}(g_1) > \text{LT}(g_2) > \dots$$

However, one of the defining properties of a monomial order is that any such descending sequence terminates after a finite number of steps, after which $g_i = 0$. Then Equation 1 gives an expression of g as an element of $\langle f_1, \dots, f_r \rangle$.
 \square