

Lecture 13 Groebner Bases — March 6

Lecturer: Richard Karp

Scribe: Aria Haghighi

Groebner Bases

Introduction

The problem we are going to explore today is how to decide if a polynomial is in the ideal generated by a finite number of given polynomials. Formally, suppose we are given $f_1, \dots, f_s \in K[x_1, \dots, x_n]$, where $K[x_1, \dots, x_n]$ is the set of polynomials over (x_1, \dots, x_n) with integer coefficients. We will briefly recall the definition of an ideal:

Definition A set of polynomials I is an ideal if

- $0 \in I$
- $f \in I, g \in I \Rightarrow f + g \in I$
- $f \in I \Rightarrow hf \in I$, for all polynomials h

Let $\langle f_1, \dots, f_s \rangle$ be the ideal generated by $\{f_1, \dots, f_s\}$.¹ We are interested in deciding if a given polynomial f is in $\langle f_1, \dots, f_s \rangle$.

Recall that if we are dealing with polynomials in a single variable x , we can use the Euclidean algorithm for such polynomials to decide membership in $\langle f_1, \dots, f_s \rangle$. If $g = \gcd(f_1, \dots, f_s)$, then we have $\langle f_1, \dots, f_s \rangle = \langle g \rangle$, and $f \in \langle g \rangle$ if and only if the remainder of dividing f by g is 0. Can this same idea be carried over to polynomials in several variables?

Unfortunately the answer is no. We first define an ordering (\succ) on terms in a polynomial. We say that:

$$x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} \succ x_1^{\beta_1} x_2^{\beta_2} \dots x_n^{\beta_n}$$

if and only if there is some $\alpha_i > \beta_i$ and for each $j < i$, $\alpha_j = \beta_j$. We denote the maximal term in a polynomial f by $LT(f)$, the *leading term* of f . Given polynomials f_1, \dots, f_s and f , the generalized Euclidean division algorithm will give us polynomials h_1, \dots, h_s and r such that

$$f = \sum_{i=1}^s h_i f_i + r$$

where no term in r is divisible by $LT(f_1), \dots, LT(f_s)$. The properties of this algorithm are:

1. r is *not* uniquely defined

¹Formally the intersection of all the ideals of $K[x_1, \dots, x_n]$ containing $\{f_1, \dots, f_s\}$

2. $r = 0 \Rightarrow f \in \langle f_1, \dots, f_s \rangle$
3. $r \neq 0$ does not imply $f \notin \langle f_1, \dots, f_s \rangle$

In order to remedy this problem we will define a basis with the property that the remainder upon division is uniquely defined and the remainder is zero if and only if the polynomial is in the ideal generated by the basis.

13.1 Groebner Basis

Definition A set of polynomials g_1, \dots, g_t is a *Groebner basis* if for any polynomial f we can write $f = \sum_i h_i g_i + r$ for polynomials h_1, \dots, h_t such that:

1. $r = 0$ if and only if $r \in \langle g_1, \dots, g_t \rangle$
2. r is uniquely defined

Our tactic will be to convert our basis f_1, \dots, f_t into a Groebner basis g_1, \dots, g_s such that $\langle f_1, \dots, f_t \rangle = \langle g_1, \dots, g_s \rangle$. In order to develop properties of Groebner bases, we will take a small digression into monomial ideals.

13.1.1 Monomial Ideals

Definition An ideal I is a *monomial ideal* if it has a basis consisting of a (possibly infinite) set of monomials, $I = \langle x^\alpha \mid \alpha \in A \rangle$, where x^α is shorthand for $x_1^{\alpha_1}, \dots, x_n^{\alpha_n}$.

We prove the following lemma:

Lemma 13.1. *Let I be a monomial ideal. Then a monomial x^β is in I if and only if x^β is divisible by x^α for some $\alpha \in A$.*

Proof: Clearly if $x^\beta = hx^\alpha$ for some polynomial h , then $x^\beta \in I$. Now for the other direction, suppose $x^\beta \in I$, then we have $x^\beta = \sum_\alpha h_\alpha x^\alpha$. Note that each term of this sum can be written as $c_\delta x^\delta$ where c_δ where some generator x^α divides x^δ .

We can associate each monomial $x^\beta \in I$, with a point β in \mathbb{Z}_+^n , the positive quadrant in the integer lattice of n dimensions. This set of points, S , corresponding to each monomial in I is *upward-closed*, i.e if $\delta \succ \beta$ ² then β is in the set, then so is δ .

Therefore, the monomial ideal I is generated by the monomials corresponding to the minimal points in the upward-closed set S . It is easy to prove by induction on n , that every upward-closed set in \mathbb{Z}_+^n has a finite set of minimal elements. This set of minimal points corresponds to a finite set of monomials which generates the entire ideal I . If we set A to be this set of monomials, we have the desired implication. \square

²There is some i such that $\delta_i > \beta_i$ and for $j < i$, $\delta_j = \beta_j$

13.2 Hilbert Basis Theorem

Let I be a non-zero ideal over polynomials in variables x_1, \dots, x_n . Consider the set of polynomials $LT(I) = \{LT(f) | f \in I\}$. Note that $\langle LT(f_1), \dots, LT(f_s) \rangle$ may be properly contained in $LT(I)$.

Example Let $f_1 = x^3 - 2xy$ and $f_2 = x^2y - 2y^2 + x$. Then we have $yf_1 - xf_2 = -x^2 - 2xy^2$. So that $-x^2 \in LT(I)$, but it does not lie in $\langle LT(f_1), LT(f_2) \rangle = \langle x^3, x^2y \rangle$, since $(2, 0)$ does not lie in the upward-closed set with minimal elements $(3, 0), (2, 1)$.

Theorem 13.2. *Suppose $I \subset K(x_1, \dots, x_n)$ be an ideal, then $\langle LT(I) \rangle$ is a monomial ideal, and furthermore there are $g_1, \dots, g_t \in I$ such that $\langle LT(I) \rangle$ is generated by $LT(g_1), \dots, LT(g_t)$.*

Proof: Since $\langle LT(I) \rangle$ is a monomial ideal it is finitely generated by elements $LT(g_1), \dots, LT(g_t)$ in $\langle LT(I) \rangle$, and each of these terms is a leading term of some polynomial in I . \square

We now prove the Hilbert basis theorem:

Theorem 13.3. *Every ideal has a finite basis set g_1, \dots, g_t such that $\langle LT(g_1), \dots, LT(g_t) \rangle = LT(I)$.*

Proof: Let $g_1, \dots, g_t \in I$ such that $\langle LT(g_1), \dots, LT(g_t) \rangle = LT(I)$ guaranteed to exist by the last theorem. Clearly, we have $\langle g_1, \dots, g_t \rangle \subseteq I$, since each $g_i \in I$. Let f be an element of I , by the division algorithm

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

where no term of r is divisible by $LT(g_i)$ for each g_i . This implies that $LT(r) \notin \langle LT(g_1), \dots, LT(g_t) \rangle$. But $r \in I$, since $r = f - \sum_{i=1}^t h_i g_i$. But if $r \neq 0$, $LT(r) \in \langle LT(g_1), \dots, LT(g_t) \rangle$ and therefore is divisible by $LT(g_i)$ for some i (since it is a monomial ideal, every term in every member of the ideal is divisible by one of the generators). We conclude that $r = 0$.

This proves that g_1, \dots, g_t is a basis for the ideal I . \square

We define a Groebner basis for an ideal I , to be a basis g_1, \dots, g_t such that $LT(I) = \langle LT(g_1), \dots, LT(g_t) \rangle$. Our last theorem showed that every polynomial ideal has a Groebner basis.

13.3 Constructing a Groebner basis

Let f be a polynomial with leading term $c_\alpha x^\alpha$. Then we define $\text{multideg}(f) = \alpha$.

Example Let $f = 3x^3y^2 - 2xyz^10$, then $\text{multideg}(f) = (3, 2, 0)$

Suppose $f, g \in K(x_1, \dots, x_n)$ be non-zero polynomials. We make two definitions:

- If $\text{multideg}(f) = \alpha$ and $\text{multideg}(g) = \beta$, then we let δ be the component-wise maximum of α and β . We call x^δ the *least common multiple* of f and g .
- The S -polynomial of f and g is the combination:

$$S(f, g) = \frac{x^\delta}{LT(f)}f - \frac{x^\delta}{LT(g)}g$$

Example Let $f = x^3y^2 - x^2y^3 + x$ and $g = 3x^4y + y^2$. Then we have $\alpha = (3, 2), \beta = (4, 1)$ and $\delta = (4, 2)$. The S -polynomial is

$$\begin{aligned} S(f, g) &= \frac{x^4y^2}{x^3x^2}(x^3y^2 - x^2y^3 + x) - \frac{x^4y^2}{3x^4y}(3x^4y + y^2) \\ &= -x^3y^3 + x^2 - \frac{y^3}{3} \end{aligned}$$

This construction is designed to cancel the leading terms of f and g . We now state the following property of Groebner basis whose proof we omit.

Theorem 13.4. *Let I be a polynomial ideal, and let $G = \{g_1, \dots, g_s\}$ be a basis for I . Then G is a Groebner basis if and only if, for all i and j , the remainder on division by $S(g_i, g_j)$ by G is zero.*

13.4 Buchberger's Algorithm

We use the theorem from the previous section to iteratively change a given basis into a Groebner basis. First we define $\overline{S(p, q)}^G$ to be the remainder polynomial when we divide $S(p, q)$ by the basis G .

Algorithm 1. *Buchberger's Algorithm*

1. $G = \{f_1, \dots, f_s\}$
2. do
3. $G' = G$
3. for each $p, q \in G'$
4. $S = \overline{S(p, q)}^G$
5. if $S \neq 0$
6. $G = G \cup \{S\}$
7. while $G = G'$

We leave determining that the algorithm terminates to the reader.