6.966 Algebra and Computation October 21, 1998

Lecture 13

Lecturer: Madhu Sudan *Scribe: Amit Sahai*

1 Introduction

In the last lecture, we discussed a division algorithm for polynomials in many variables. The algorithm, while efficient, had several drawbacks, the primary one being a lack of uniqueness of the remainder when dividing a polynomial f by several polynomials $p_1, \ldots, p_n$. We decided that what we really wanted was a way to "divide" f by the *ideal* $\mathcal{J}$ generated by $p_1, \ldots p_n$ – *i.e.* find the residue of f in the ring modulo $\mathcal{J}$. The tool we introduced for accomplishing this task is the Groebner basis of an ideal. We claimed (and will show in this lecture) that if we divide f by a Groebner basis for the ideal $\mathcal{J}$, then the remainder will have the uniqueness properties we desire.

The main result of this lecture is that every ideal in a polynomial ring over a field in finitely many variables has a finite Groebner basis. A useful reference for this material is the book "Ideals, Varieties and Algorithms" by Cox, Little and O'Shea. We begin by reviewing some definitions we will need from the last lecture:

2 Defintions

For $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$ we write x^α to denote the monomial $x_1^{\alpha_1} \ldots x_n^{\alpha_n}$.

Definition 1 *A relation $\succeq$ on the set of monomials in $K[x_1, \ldots, x_n]$ is an* admissible monomial ordering *if it satisfies the following properties:*

1. *$\succeq$ is a total ordering, i.e. for any $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, either $\alpha \succ \beta, \alpha = \beta$, or $\alpha \prec \beta$.*
2. *for all $\alpha, \beta, \gamma \in \mathbb{Z}^n_{\geq 0}$, if $x^\alpha \succeq x^\beta$ then $x^{\alpha+\gamma} \succeq x^{\beta+\gamma}$.*
3. *for all $\alpha \in \mathbb{Z}^n_{\geq 0}$, it holds that $x^\alpha \succeq 1$.*

Let $\succeq$ be an admissible monomial ordering over the variables $x_1, \ldots, x_n$ and let $f \in K[x_1, \ldots, x_n]$.

- The *leading monomial* of f, written $LM(f)$, is the monomial which is ranked highest under $\succeq$ of all monomials which have nonzero coefficients in f.
- The *leading coefficient* of f, written $LC(f)$, is the coefficient of $LM(f)$ in f.
- The *leading term* of f, written $LT(f)$, is $LC(f) \cdot LM(f)$. Note that if f is a nonconstant polynomial, then $LM(f) \succ LM(f - LT(f))$.
- The *degree* of f, written $\deg(f)$, is α such that $x^\alpha = LM(f)$.

Note that since we work in a field, we will often abuse notation by speaking of $LT(f)$ as if it were a monomial. This should not cause concern since any ideal that contains $LT(f)$ must also contain $LM(f)$, and vice versa.

Remainder Property. We first recall the fundamental property of our division algorithm `Divide` is that after dividing a polynomial f by a sequence of polynomials $p_1, \ldots, p_n$, *no term in the remainder r is divisible by any of $LT(p_1), \ldots, LT(p_n)$.* Unfortunately, this property does not suffice to guarantee uniqueness, and indeed can fail dramatically to do "what we want." (*e.g.* consider dividing $y-z$ by $p_1 = x-y$ and $p_2 = x-z$, under the lexicographic ordering where $x > y > z$. Here, $y-z$ is still a remainder satisfying the Remainder Property even though $y-z = p_2 - p_1$.) Intuitively what we wanted was to find a remainder that satisfies the Remainder Property not only for the given polynomials but for all polynomials in the ideal generated by them. This motivates the definition of the notion of a Groebner basis:

Definition 2 *Under a fixed monomial ordering $\succeq$, a finite subset $\{g_1, \ldots, g_t\}$ of an ideal $\mathcal{J}$ forms a* Groebner basis *for $\mathcal{J}$ if*

1. $\mathcal{I}(g_1, \ldots, g_t) = \mathcal{J}$ *and*
2. $\mathcal{I}(LT(g_1), \ldots, LT(g_t)) = \mathcal{I}(LT(\mathcal{J}))$, *where* $LT(\mathcal{J}) = \{LT(h) : h \in \mathcal{J}\}$.

3 Existence of finite Groebner bases

In this section, we prove that every ideal in a polynomial ring over finitely many variables has a finite Groebner basis. Suppose $\mathcal{J}$ is an ideal in $K[x_1, \ldots, x_n]$. We will build our Groebner basis by first finding a set of polynomials satisfying the second Groebner basis condition, and then conclude that this set must also be a basis for $\mathcal{J}$.

Consider the ideal $\mathcal{L} = \mathcal{I}(LT(\mathcal{J}))$. By Dickson's Lemma, which we proved last time, we know that every monomial ideal – one that can be generated by a set of monomials – has a finite basis of monomials. So in particular this means that $\mathcal{L}$ has a finite basis of monomials $\{m_1, \ldots, m_t\}$. In the last lecture, we showed:

Claim 3 *Let h be a monomial and M be a set of monomials in $K[x_1, \ldots, x_n]$. Then $h \in \mathcal{I}(M)$ iff m divides h for some $m \in M$.*

Thus, since $\mathcal{L}$ is generated by the leading terms of polynomials in $\mathcal{J}$, for each m_i there must exist some $g_i \in \mathcal{J}$ such that m_i is divisible by $LT(g_i)$. Hence, we have immediately that

$$\mathcal{I}(LT(g_1), \ldots, LT(g_t)) = \mathcal{I}(m_1, \ldots, m_t) = \mathcal{L} = \mathcal{I}(LT(\mathcal{J})).$$

All that remains in showing that $\{g_1, \ldots, g_t\}$ is a Groebner basis for $\mathcal{J}$ is to show that it does actually generate all of $\mathcal{J}$. Suppose $f \in \mathcal{J}$. Consider what happens when we use our Division Algorithm to divide f by $g_1, \ldots, g_t$. Suppose the algorithm outputs remainder r and quotients $q_1, \ldots, q_t$. If the remainder that is output is 0, then this implies $f \in \mathcal{I}(g_1, \ldots, g_t)$. We claim that this must be the case:

Lemma 4 *Let $\mathcal{J} \subset K[x_1, \ldots, x_n]$ be any polynomial ideal. Let $g_1, \ldots, g_t \in \mathcal{J}$ be any set of polynomials satisfying $\mathcal{I}(LT(g_1), \ldots, LT(g_t)) = \mathcal{I}(LT(\mathcal{J}))$. Let* `Divide` *be any division algorithm satisfying the Remainder Propery. Then for any $f \in \mathcal{J}$, the remainder output by* `Divide`$(f;\ g_1, \ldots, g_t)$ *is* 0.

Proof Suppose that the remainder $r \neq 0$. Since $r = f - q_1 g_1 - \cdots - q_t g_t$ for the quotients q_i output by the division algorithm, it must be that $r \in \mathcal{J}$. Hence $LT(r) \in \mathcal{I}(LT(\mathcal{J})) = \mathcal{I}(LT(g_1), \ldots, LT(g_n))$. Since $\mathcal{I}(LT(\mathcal{J}))$ is a monomial ideal, Claim 3 implies that $LT(r)$ must be divisible by $LT(g_i)$ for some i. But the Remainder Property of the Division Algorithm states that $LT(r)$ cannot be divisible by any of $LT(g_1), \ldots, LT(g_t)$, a contradiction. ■

Thus we have that all $f \in \mathcal{J}$ are also in $\mathcal{I}(g_1, \ldots, g_t)$. Hence $\mathcal{I}(g_1, \ldots, g_t) = \mathcal{J}$, and we have shown that every polynomial ideal over a field with finitely many variables has a finite Groebner basis. Note that in particular, this shows that every such ideal has a finite basis, which is the Hilbet Basis Theorem.

4 Division using Groebner bases

We first show that Groebner bases allow for a robust notion of division by polynomial ideals. Lemma 4 already shows that any polynomial in an ideal will yield a remainder of 0 when divided by any Groebner basis for the ideal. Using this basic fact, we can show that division by Groebner bases allows for a strong notion of uniqueness of remainder.

Lemma 5 *For any polynomial ideal $\mathcal{J} \subset K[x_1, \ldots, x_n]$ and any $f \in K[x_1, \ldots, x_n]$, the remainder r produced by* `Divide`$(f; g_1, \ldots, g_t)$ *will be unique for any Groebner basis $g_1, \ldots, g_t$ of $\mathcal{J}$ and any division algorithm* `Divide` *satisfying the Remainder Property.*

Proof Suppose that r_1 and r_2 were two remainders produced by possibly different division algorithms using Groebner bases $g_1, \ldots, g_s$ and $h_1, \ldots, h_t$, respectively. By the Remainder Property, we know that no term of r_1 is divisible by $LT(g_i)$ for any i, and no term of r_2 is divisible by $LT(h_j)$ for any j. Since the leading terms of any Groebner basis for $\mathcal{J}$ generate $\mathcal{I}(LT(\mathcal{J}))$, by Claim 3, we have that no terms of r_1 or r_2 are in $\mathcal{I}(LT(\mathcal{J}))$. Now, for suitable polynomials $p_1, \ldots, p_s$ and $q_1, \ldots, q_t$, $r_1 = f - p_1 g_1 - \cdots - p_s g_s$ and $r_2 = f - q_1 h_1 - \cdots - q_t h_t$. Hence, $r_1 - r_2 \in \mathcal{J}$, and so $LT(r_1 - r_2) \in \mathcal{I}(LT(\mathcal{J}))$. However, the leading monomial of $r_1 - r_2$ must be either 0 or be a monomial of either r_1 or r_2. But we know that no terms of r_1 or r_2 are in $\mathcal{I}(LT(\mathcal{J}))$, so $r_1 - r_2 = 0$. ■

5 More Groebner Basis Tricks

One consequence of the existence of finite Groebner Bases (actually just the existence of finite bases) for every ideal in $K[x_1, \ldots, x_n]$ is the Ascending Chain Condition:

Theorem 6 *For every infinite ascending chain of ideals $\mathcal{I}_1 \subset \mathcal{I}_2 \subset \cdots \subset K[x_1, \ldots, x_n]$, there exists an integer N_0 such that for all $n \geq N_0$, $\mathcal{I}_n = \mathcal{I}_{N_0}$.*

Rings satisfying this condition are called Noetherian rings. We show that $K[x_1, \ldots, x_n]$ is Noetherian:
Proof Let $\mathcal{J} = \bigcup_{i=1}^{\infty} \mathcal{I}_i$. Let $g_1, \ldots, g_t$ be a finite basis for $\mathcal{J}$. For each g_i, since $g_i \in \mathcal{J}$, there must exist some $\mu(i)$ such that $g_i \in \mathcal{I}_{\mu(i)}$. Let $N_0 = \max_i(\mu(i))$. We must have that $g_1, \ldots, g_t \in \mathcal{I}_{N_0}$. Hence $\mathcal{J} = \mathcal{I}_{N_0}$, and the theorem is proved. ■

Now we examine the question of uniqueness for Groebner Bases. Certainly Groebner bases need not be unique, since one can always add more elements of the ideal to a Groebner Basis. Suppose therefore we restrict ourselves to *minimal* Groebner bases, *i.e.* a Groebner basis $g_1, \ldots, g_t$ such that for all i, $LT(g_i) \notin \mathcal{I}(LT(g_1), \ldots, LT(g_{i-1}), LT(g_{i+1}), \ldots, LT(g_t))$. Note that if we start with a Groebner basis and eliminate all polynomials that do not satisfy the minimality constraint, by Lemma 4, what remains is still a Groebner basis. Since we are working in a field, we also adopt a convention requiring that the leading coefficients of polynomials in our bases be 1. This is still not enough to guarantee uniqueness, as $\{x + y, y\}$ and $\{x, y\}$ are both minimal Groebner bases for $\mathcal{I}(x, y)$. This leads us to the definition of a reduced Groebner basis:

Definition 7 *A* reduced Groebner basis *$g_1, \ldots, g_t$ is a minimal Groebner Basis that also satisfies the property that for all pairs i, j with $i \neq j$, we have that no term of g_i is divisible by $LT(g_j)$.*

Now we can prove uniqueness:

Theorem 8 *Every polynomial ideal $\mathcal{J} \subset K[x_1, \ldots, x_n]$ has a unique reduced Groebner basis.*

Proof First, we note that by definition, the leading terms of any minimal Groebner basis must be distinct. Moreover, we have the following:

Claim 9 *For any two minimal Groebner bases G and G', the set $LT(G)$ of leading terms of G must equal the set $LT(G')$ of leading terms of G'.*

Proof Suppose not. Let m be the minimal monomial such that m is in one set of leading terms but not the other. Without loss of generality, assume $m \in LT(G)$. Then $m \in \mathcal{I}(LT(G)) = \mathcal{I}(LT(G'))$, and hence by Claim 3, there must be some monomial a in $LT(G')$ such that a divides m. But since a divides m, by the minimality of G, it cannot be that $a \in LT(G)$. Hence a is in $LT(G')$ but not in $LT(G)$, contradicting the minimality of m. ■

In particular, this claim implies that all minimal Groebner bases of an ideal $\mathcal{J}$ have the same cardinality N, and in fact any Groebner basis of cardinality N must be a minimal Groebner basis. Now we can easily show existence of a reduced Groebner basis by the following algorithm:

Let $g_1, \ldots, g_t$ be any minimal Groebner basis. For $i = 1$ to t, let g'_i be the remainder when dividing g_i by $g'_1, \ldots, g'_{i-1}, g_{i+1}, \ldots, g_t$. Output $g'_1, \ldots, g'_t$.

Since at each stage g'_i is set equal to $g_i - q_1 g'_1 - \cdots - q_{i-1} g'_{i-1} - q_{i+1} g_{i+1} - \cdots - q_t g_t$ for some $q_1 \ldots q_t$, yet by the Remainder Property no leading term of $g'_1, \ldots, g'_{i-1}, g_{i+1}, \ldots, g_t$ can divide the leading term of g'_i, it must be that $LT(g'_i) = LT(g_i)$. Also, the span of $g'_1, \ldots, g'_i, g_{i+1}, \ldots, g_t$ is the same as the span of $g'_1, \ldots, g'_{i-1}, g_i, g_{i+1}, \ldots, g_t$. Hence $g'_1, \ldots, g'_t$ remain a basis for $\mathcal{J}$, and since the leading terms do not change, it remains a minimal Groebner basis. However, now also, since the leading terms do not change, by the Remainder Property, no term of g'_i is divisible by the leading term of g_j for all $j \neq i$, so the basis $g'_1, \ldots, g'_t$ is reduced.

We will now show that any two reduced bases must be the same. Suppose $g_1, \ldots, g_t$ and $g'_1, \ldots, g'_t$ were two reduced bases. Since they are minimal, their set of leading terms must be the same, so we may assume that $LT(g_i) = LT(g'_i)$ for all i. Suppose $g_i \neq g'_i$ for some i. Now, $g_i - g'_i \in \mathcal{J}$. But on the other hand, by the reduced property, $LT(g_i - g'_i)$ cannot be divisible by any $LT(g_j)$, and hence by Claim 3 and the definition of a Groebner basis, $LT(g_i - g'_i)$ cannot be in the ideal $\mathcal{I}(LT(\mathcal{J}))$, a contradiction. ■

6 An Algorithm for computing Groebner Bases

In this section we will give a simple condition which allows us to check if a given generating set is a Groebner basis. First we define the Syzygy polynomial $S(f, g)$:

Definition 10 *For two monomials $m_1 = x^\alpha$ and $m_2 = x^\beta$, we define $LCM(m_1, m_2) := x^\gamma$, where $\gamma_i = \max(\alpha_i, \beta_i)$.*

Definition 11 *For two polynomials f and g, we define the* Syzygy polynomial $S(f, g)$ of f and g *to be* $\frac{LC(g) \cdot LCM(LM(f), LM(g))}{LM(f)} \cdot f - \frac{LC(f) \cdot LCM(LM(f), LM(g))}{LM(g)} \cdot g$.

Note that the definition of $S(f, g)$ implies that $LM(S(f, g)) < LCM(LM(f), LM(g))$, since the highest order monomials will cancel out.

Given this definition, we can establish the following theorem:

Theorem 12 *$G = \{g_1, \ldots, g_t\}$ form a Groebner basis for $\mathcal{J} = \mathcal{I}(g_1, \ldots, g_t)$ iff for all pairs i, j, the remainder after executing* `Divide`$(S(g_i, g_j);\ g_1, \ldots, g_t)$ *is 0.*

Before we proceed with the proof of the theorem, we first examine our algorithm `Divide` more closely. We simply make the observation:

Claim 13 *If* `Divide`$(f;\ g_1, \ldots, g_s)$ *outputs a remainder r and quotients $q_1, \ldots, q_s$, then we always have that $LM(r) \leq LM(f)$ and $LM(q_i g_i) \leq LM(f)$ for each i.*

Proof Obvious from description of algorithm. ■

We also observe:

Claim 14 *Let $i > j$ and suppose the remainder after executing* $\texttt{Divide}(S(g_i, g_j);\ g_1, \ldots, g_t)$ *is* 0 *and leads to quotients* $q_1, \ldots, q_t$.

Then executing $\texttt{Divide}(\frac{LC(g_j)\cdot LCM(LM(g_i),LM(g_j))}{LM(g_i)} \cdot g_i;\ g_1, \ldots, g_t)$ *will lead to a remainder of* 0 *and quotients* $q'_1, \ldots, q'_t$ *where* $q'_k = q_k$ *for all* k *except* $q'_j = q_j + \frac{LC(g_i)\cdot LCM(LM(g_i),LM(g_j))}{LM(g_j)}$.

Proof This is immediate from the description of the divison algorithm and the fact that $LM(S(g_i, g_j)) < LM(\frac{LC(g_j)\cdot LCM(LM(g_i),LM(g_j))}{LM(g_i)} \cdot g_i)) = LCM(LM(g_i), LM(g_j))$. ■

Now we begin the proof of the theorem:

Proof (of Theorem 12) Clearly, $S(g_i, g_j) \in \mathcal{J}$, so by Lemma 4, if G is a Groebner basis, then all the remainders will be 0.

Suppose now that for each i, j the remainder after executing $\texttt{Divide}(S(g_i, g_j);\ g_1, \ldots, g_t)$ is 0. To show that G is a Groebner basis, we must show that for all $f \in \mathcal{J}$, we have that $LM(f)$ is divisible by $LM(g_i)$ for some i. Let us write $f = \sum m_{i,k} g_i$ for monomials $m_{i,k}$. We say that a term mg_i is *reducible* if we can write it as $mg_i = hg_j + \sum \mu_k g_k$ where h and μ_k are monomials, and $j < i$, and $LM(hg_j) = LM(mg_i)$ while $LM(\mu_k g_k) < LM(mg_i)$. Here we call $hg_j + \sum \mu_k g_k$ the *reduction* of mg_i. Now, we take our representation of f as $\sum m_{i,k} g_i$ and replace each reducible term $m_{i,k} g_i$ with its reduction, to obtain a new representation of f as $\sum h_{i,k} g_i$, where now no term is reducible. Now, we consider the terms $h_{i,k} g_i$ such that $LM(h_{i,k} g_i)$ has maximum degree. If there is only one such term, then it must be that $LM(f) = LM(h_{i,k} g_i)$, and hence $LM(g_i)$ divides $LM(f)$. Otherwise, suppose there are at least two terms hg_i and $h'g_j$ with $j < i$ such that their leading monomials are of the same degree. So we have that $LM(h)LM(g_i) = LM(h')LM(g_j)$. This implies that $LM(h)LM(g_i) = w \cdot LCM(LM(g_i), LM(g_j))$ for some monomial w. Hence, $LM(h) = w \cdot \frac{LCM(LM(g_i),LM(g_j))}{LM(g_i)}$. Let the leading coefficient of h be written as $c \cdot LC(g_j)$. Hence, finally we have that

$$hg_i = cw \cdot \frac{LC(g_j) \cdot LCM(LM(g_i), LM(g_j))}{LM(g_i)} \cdot g_i$$

By Claims 14 and 13 and our assumption, we have that hg_i is in fact reducible, a contradiction. Hence, after reducing all terms, we must have a single term with the highest degree monomial, implying that $LM(f) \in \mathcal{I}(LM(G))$, and completing the proof. ■

This characterization of Groebner basis immediately implies that the following algorithm will eventually terminate and produce a Groebner basis.

$\texttt{Groebner} - \texttt{Basis}(g_1, \ldots, g_t)$:

1. For each i, j execute $\texttt{Divide}(S(g_i, g_j);\ g_1, \ldots, g_t)$.

2. If all remainders are 0, return $g_1, \ldots, g_t$.

3. Otherwise, return $\texttt{Groebner} - \texttt{Basis}(g_1, \ldots, g_t, r)$, where r is one of the non-zero remainders found in Step 1.

A remainder is guaranteed to be such that $LM(r)$ is not in the ideal generated by $LM(g_1), \ldots, LM(g_t)$, so each recursion causes the ideal generated by the leading terms of the basis to become strictly larger. On the other hand, by Theorem 6, this ascending chain of ideals must eventually stop growing, and at that point, by Theorem 12 the algorithm must terminate with a Groebner basis.

Unfortunately, we have no bound, except for finiteness, on the running time of this algorithm or on the Groebner basis produced.