Groebner Bases

Tracy Chin

April 19, 2019

1 Motivation

Recall that $k[x]$, the ring of single variable polynomials, is a Euclidean domain, and has a division algorithm so that for any $f, g \in k[x]$, there exist $q, r \in k[x]$ such that

$$g = q \cdot f + r$$

where either $r = 0$, or $\deg(r) < \deg(f)$.

Since $k[x]$ is a Euclidean domain, it is also a PID. The division algorithm allows us to easily check if $g \in (f)$. Specifically, $g \in (f)$ if and only if $r = 0$ when we write $g = qf + r$ as above.

However, the ideal membership problem is more difficult to answer in multivariate polynomial rings. To start, $k[x_1, \dots, x_n]$ is no longer a PID. One might naturally try to extend the division algorithm to dividing by multiple polynomials by using, at any given step, any polynomial whose leading term divides the current leading term, and terminate when no polynomial divides any of the remaining terms.

Unlike the one variable case, this can lead to inconsistent remainders, and even give non-zero remainders when a zero remainder is possible.

Consider, for example, $g = xy^2 - x$, $f_1 = xy + 1$, $f_2 = y^2 - 1$, and suppose we want to check if $g \in (f_1, f_2)$. The leading term of g is divisible by both the leading term of f_1 and of f_2. If we divide by f_1 first, then we get

$$xy^2 - x = y(xy + 1) - x - y$$

which has nonzero remainder. However, if we divide by f_2 first, we see that

$$xy^2 - x = x(y^2 - 1)$$

so in fact $g \in (f_1, f_2)$.

Groebner bases allow us to guarantee a consistent remainder in polynomial division, and thus solve the ideal membership problem for multivariate polynomials rings.

2 Definition and Properties

2.1 Preliminaries

Fix $R = k[x_1, \dots, x_n]$, where k is a field.

For simplicity, we will mostly gloss over the idea of monomial orderings. In class, we already saw the example of lexicographic ordering. For the purposes of Groebner bases, we only require monomial orderings in order to have a well-defined notion of a leading term. Namely, $\textsc{lt}(f)$ is the term of the polynomial f that comes first in the monomial order.

For an ideal $I \subset R$, define

$$\textsc{lt}(I) = \{\textsc{lt}(f) : f \in I \setminus \{0\}\}$$

As shorthand, we will also write x^α to mean $x_1^{\alpha_1} \dots x_n^{\alpha_n}$, where $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$.

2.2 Groebner Bases

Let $I \subset R$ be an ideal.

Definition (Groebner Basis)**.** A set $G = \{g_1, \dots, g_t\} \subset I$ is a *Groebner basis* of I if

$$(\textsc{lt}(G)) = (\textsc{lt}(I))$$

That is, the leading terms of the g_i generate the same ideal as the leading terms of I.

In order to prove the desired properties of Groebner bases, we will use the following lemma.

Lemma. *Let $I \subset R$ be an ideal generated by monomials $I = (x^{\alpha_1}, \dots, x^{\alpha_k})$. Then a monomial $x^\beta \in I$ if and only if x^β is divisible by some x^{α_i}.*

Proof. First, if $x^{\alpha_i} | x^\beta$, then x^β is a multiple of a generator of I and so in I.

Now, suppose $x^\beta \in I$. Then we must have

$$x^\beta = \sum_{i=1}^{k} h_i x^{\alpha_i}$$

for some $h_i \in k[x_1, \dots, x_n]$.

Each term on the right is divisible by some x^{α_i}, so each term on the left must also be divisible by some x^{α_i}, so $x^{\alpha_i} | x^\beta$ for some i, as desired. □

Now, we show that Groebner bases allow us to solve the ideal membership problem.

Theorem. *If $G = \{g_1, \dots, g_t\} \subseteq I$ is a Groebner basis for an ideal I, then G generates I.*

Proof. First, since $G \subseteq I$, we know that $(g_1, \dots, g_t) \subseteq I$.

Now, pick any $f \in I$. Using the division algorithm, we can write

$$f = a_1 g_1 + \dots + a_t g_t + r$$

where $a_i \in R$ and no term of r is divisible by the leading term of any g_i.

Suppose $r \neq 0$. Then, since $f \in I$ and each $g_i \in I$,

$$r = f - a_1 g_1 - \cdots - a_t g_t \in I$$

so $\text{LT}(r) \in \text{LT}(I) \subset (\text{LT}(g_1), \ldots, \text{LT}(g_t))$. By the lemma, this means that some $\text{LT}(g_i)$ divides $\text{LT}(r)$, which is impossible since no term of r is divisible by any leading term of a g_i. Thus, we must have $r = 0$ and so $f \in (G)$.

Thus, G generates I, as desired. □

Theorem. *Let G be a Groebner basis for an ideal I. Then for any $f \in R$, there exists a unique $r \in R$ such that*

(i) No term of r is divisible by any $\text{LT}(g_i)$, and

(ii) there exists $g \in I$ such that $f = g + r$.

Proof. By running the division algorithm, such an r certainly exists.

Suppose $f = g + r = g' + r'$, where $g, g' \in I$ and no term of r or r' is divisible by any $\text{LT}(g_i)$. Then $r - r' = g' - g \in I$, so $\text{LT}(r - r') \in \text{LT}(I) \subset (\text{LT}(g_1), \ldots, \text{LT}(g_t))$.

Since no term of r or r' is divisible by any $\text{LT}(g_i)$, we must have $r - r' = 0$, so the remainder r is indeed unique. □

Therefore, the remainder of division by a Groebner basis is does not change if we divide by the elements of G in a different order. In particular, this means that $f \in I$ if and only if the remainder of f divided by a Groebner basis G is 0.