Lesson 15 – Buchberger's Algorithm

I. Preliminary Discussion

Last lesson we examined "Buchberger's Criterion" – a fairly simple test that will allow you to determine if a given basis is a Groebner basis:

Theorem (Buchberger's Criterion) Let $I \subseteq k[x_1, x_2, \dots, x_n]$ be an ideal of $k[x_1, x_2, \dots, x_n]$. Then $G = \{g_1, g_2, \dots, g_t\}$ is a Groebner basis for I if and only if for all $i \neq j$, the remainder upon division of $S(g_i, g_j)$ by G (in some order) is zero.

So how do we construct a Groebner basis for I? Buchberger's Criterion suggests a way.

Exercise 1 True or False: If we have an ideal with basis $I = \langle f_1, f_2, \dots, f_s \rangle$, then $\text{LT}(S(f_i, f_j)) \in \langle \text{LT}(f_1), \text{LT}(f_2), \dots, \text{LT}(f_s) \rangle$.

To construct a Groebner basis for an ideal $I = \langle f_1, f_2, \dots, f_s \rangle$, here is the idea... the set $G = \{f_1, f_2, \dots, f_s\}$ may not be a Groebner basis, since the basis elements may not generate the leading term ideal. We can get around this by adding in elements that are redundant as generators for the basis (that is, they are already generated by the basis elements), but that add another element to the basis of the leading term ideal. These elements will be precisely the S-polynomials, $S(f_i, f_j)$.

To be more explicit, in "Buchberger's Algorithm", if the remainder of a given $S(f_i, f_j)$ upon division by G is nonzero, then we have found an element $S(f_i, f_j)$ that lies in I and whose leading term is contained in $\langle \text{LT}(I) \rangle$ but not in $\langle \text{LT}(f_1), \text{LT}(f_2), \dots, \text{LT}(f_s) \rangle$. If this happens, we need to add $S(f_i, f_j)$ to our basis, and then check if the new set is now a Groebner basis. Also, note that we could equivalently add just the remainder, $\overline{S(f_i, f_j)}^G$, to the Groebner basis. Since this will usually result in a simpler basis set, this is what we'll generally do. To summarize this process:

- Calculate all S-polynomials
- Reduce each via G and add any nonzero remainders to G
- Repeat until all S-polynomials reduce

Recall in the one variable case, we defined h to be a **reduction** of f by g, i.e. $f \xrightarrow{g} h$, if $h = f - \frac{\text{LT}(f)}{\text{LT}(g)} g$. Here, we are reducing a multivariable polynomial $S(f_i, f_j)$ by a set of polynomials $G = \{f_1, f_2, \dots, f_s\}$. We may write $S(f_i, f_j) \xrightarrow{f_1, f_2, \dots, f_s} \overline{S(f_i, f_j)}^G$ or simply $S(f_i, f_j) \xrightarrow{G} \overline{S(f_i, f_j)}^G$

II. Buchberger's Algorithm

Now let's formalize the process as an algorithm:

Theorem (Buchberger's Algorithm) Let $I = \langle f_1, f_2, \dots, f_s \rangle \neq 0$ be an ideal of $k[x_1, x_2, \dots, x_n]$. Then a Groebner basis for can be constructed in a finite number of steps by the following algorithm:

INPUT: $F = \{f_1, f_2, \dots, f_s\} \subseteq k[x_1, x_2, \dots, x_n]$, $f_i \neq 0$ for all i
INITIAL VALUES: $G{:=}F, \mathcal{G} = \{\{f_i, f_j\} : f_i \neq f_j \in G\}$
ALGORITHM: **While** $\mathcal{G} \neq \emptyset$ **do**

- **Choose** $f, g \in \mathcal{G}$
- $\mathcal{G} \coloneqq \mathcal{G} - \{\{f, g\}\}$
- $S(f, g) \xrightarrow{G} \overline{S(f, g)}^G$
- **IF** $\overline{S(f, g)}^G \neq 0$ **, THEN** $\mathcal{G} = \mathcal{G} \cup \{\{f_i, \overline{S(f, g)}^G\} : f_i \in G\}$
  $G = G \cup \{\overline{S(f, g)}^G\}$

OUTPUT: $G = \{g_1, g_2, \dots, g_t\}$, **a Groebner basis for** I

Let's make sure we understand the algorithm...

A Careful Example

Find a Groebner basis for the ideal generated by

$$f_1(x, y) = y^2 + yx + x^2$$
$$f_2(x, y) = y + x$$
$$f_3(x, y) = y$$

in $\mathbb{Q}[x, y]$ with respect to the lex order with $y > x$.

Let's make sure we *really* understand the algorithm...

Exercise 1 (True or False): The Groebner basis produced by Buchberger's Algorithm, $G = \{g_1, g_2, \dots, g_t\}$, contains the original set of generators, $F = \{f_1, f_2, \dots, f_s\}$.

Exercise 2 Why must the algorithm terminate?

Exercise 3 Why is the terminating set G a Groebner basis?

III. Reduced Groebner Bases

In the last example we applied Buchberger's Algorithm to generate a Groebner basis for the ideal

$$I = \langle y^2 + yx + x^2, y + x, y \rangle$$

using the lex order with $y > x$. The result was

$$G = \{y^2 + yx + x^2, y + x, y, x^2, x\}.$$

Notice that we could, in fact, simply employ the basis $\{x, y\}$. In other words, the algorithm was far from optimal. We can make a number of improvements that will both produce a "better" Groebner basis and do so with greater efficiency.

One clear drawback of the algorithm is that we retain old elements of the basis even when a new one is introduced whose leading term divides its leading term.

Definition A Groebner basis $\{g_1, g_2, \dots, g_s\}$ is **minimal** if

1. For all $i = 1, \dots, s,\ \mathrm{LC}(g_i) = 1$
2. For all $i \neq j,\ \mathrm{LT}(g_i) \nmid \mathrm{LT}(g_j)$

Exercise 4 (Referring to the above example) Which of the following sets are minimal Groebner bases of $I = \langle y^2 + yx + x^2, y + x, y \rangle$?

$G_1 = \{y, x\}$ $G_2 = \{y, x^2\}$ $G_3 = \{y + x, x\}$ $G_4 = \{y + x, y\}$

Exercise 5 Describe a procedure for obtaining a minimal Groebner basis from a given one, say $G = \{g_1, g_2, \dots, g_s\}$.

By the Exercise 4, we can see that minimal Groebner bases are not unique. Nevertheless we do have the following lemma:

Lemma 1 If $G = \{g_1, g_2, \dots, g_s\}$ and $H = \{h_1, h_2, \dots, h_t\}$ are minimal Groebner bases for an ideal I, then $s = t$ and $\{\mathrm{LT}(g_1), \mathrm{LT}(g_2), \dots, \mathrm{LT}(g_s)\} = \{\mathrm{LT}(h_1), \mathrm{LT}(h_2), \dots, \mathrm{LT}(h_t)\}$.

The proof of this lemma will be presented by Group 2 on Friday, February 22.

Question: Which of the Groebner bases, $G_1 = \{y, x\}$ or $G_3 = \{y + x, x\}$, do you believe is a "better" basis of $I = \langle y^2 + yx + x^2, y + x, y \rangle$ and why?

Definition A Groebner basis $G = \{g_1, g_2, \dots, g_s\}$ is **reduced** if

1. For all $i = 1, \dots, s$, $\mathrm{LC}(g_i) = 1$
2. For all $i = 1, \dots, s$, g_i is reduced with respect to $G \setminus \{g_i\}$.
   (i.e., no monomial appearing in g_i is divisible by a $\mathrm{LT}(g_j)$ where $i \neq j$)

Note that a reduced Groebner basis is automatically a minimal one.

Theorem 2 Given an ideal I and a fixed monomial order, there is a unique reduced Groebner basis for I.

Sketch of Proof.

Existence follows from this procedure for generating a reduced basis from a minimal one:

Assume $G = \{g_1, g_2, \dots, g_s\}$ is a minimal basis for an ideal I.

- Let $H_1 = \{g_2, \dots, g_s\}$ and suppose $g_1 \xrightarrow{H_1} h_1$ (so $h_1 = \overline{g_1}^{G\setminus\{g_1\}}$) then
- Let $H_2 = \{h_1, g_3, \dots, g_s\}$ and suppose $g_2 \xrightarrow{H_2} h_2$ and so on...
- Let $H_s = \{h_1, h_2, \dots, h_{s-1}\}$ and reduce $g_s \xrightarrow{H_s} h_s$
- Now $H = \{h_1, h_2, \dots, h_s\}$ is the required reduced Groebner basis.

For uniqueness, suppose $G = \{g_1, g_2, \dots, g_s\}$ and $H = \{h_1, h_2, \dots, h_t\}$ are reduced Groebner bases. Since they are necessarily minimal, Lemma 1 implies that $s = t$ and we may assume $\mathrm{LT}(g_i) = \mathrm{LT}(h_i)$, for each $i = 1, \dots, s$.

Suppose $g_i \neq h_i$ for some i. We know $g_i - h_i \in I$ so for some j, $\mathrm{LT}(h_j) | \mathrm{LT}(g_i - h_i)$, but $\mathrm{LT}(g_i - h_i) < \mathrm{LT}(h_i) = \mathrm{LT}(g_i)$. So clearly $j \neq i$. It follows that $\mathrm{LT}(h_j) = \mathrm{LT}(g_j)$ divides some term of either g_i or h_i, contrary to the assumption that each is reduced. Thus $g_i = h_i$ for all i.