Lecture 15:

Monday, October 05, 2020

Recall the Buchberger criterion, which says that G is Gröbner iff $S(g, g') \mod G = 0$, $\forall g, g' \in G$.

How does $S(x^{alpha} f, f')$ relate to $S(f, f')$? Clearly $\mathrm{LT}(x^\alpha f) = x^\alpha \mathrm{LT}(f)$. The new M will be $x^\beta M$ for some $x^\beta \mid x^\alpha$, so $S(x^\alpha f, f') = x^\beta (f, f')$.

Given $f \in (G)$, we want to show that $\mathrm{LT}(f) in (\mathrm{LT}(G))$. The S polynomials are the only ways to get cancellations between elements of the basis.

If we write $f = \sum h_i g_i$ where $h_i \in F[X]$, suppose $x^\alpha = \max(\mathrm{LM}(h_i g_i))$. Then

$$
\begin{aligned}
f = \sum_{\mathrm{LM}(h_i g_i)} &= x^\alpha h_i g_i + \sum_{\mathrm{LM}(h_i g_i) < x^\alpha} h_i g_i \\
&= \underbrace{\sum_{\mathrm{LM}(h_i g_i) = x^\alpha} \mathrm{LT}(h_i) g_i}_{\sum_1} + \underbrace{\sum_{\mathrm{LM}(h_i g_i) = x^\alpha} (h_i - \mathrm{LT}(h_i)) g_i}_{\sum_2} + \underbrace{\sum_{\mathrm{LM}(h_i g_i) < x^\alpha} h_i g_i}_{\sum_3}
\end{aligned}
$$

Suppose $\mathrm{LM}(f) < x^\alpha$. All polynomials in that first term have the same degree. Let's write $\mathrm{LT}(h_i) = \mathrm{LC}(h_i)\mathrm{LM}(h_i)$ and define $h_i' = \mathrm{LM}(h_i)$. By our lemma, the first sum can be written as

$$
\sum_1 = \sum_i b_i S(h_i' g_i, h_{i+1}' g_{i+1})
$$

since $S(h_i' g_i, h_{i+1}' g_{i+1})$ is a monomial multiple of $S(g_i, g_{i+1})$. We know that $S(g_i, g_{i+1}) \mod G = 0$, so it must be a linear combination of the form $\sum_{g_j \in G} q_j g_j$ and $\mathrm{LM}(q_j g_j) \leq \mathrm{LM}(g_i, g_{i+1})$.

This means that $s = S(h_i' g_i, h_{i+1}' g_{i+1})$ are sums of the form $\sum q_j' g_j$ where $\mathrm{LM}(s) \leq \mathrm{LM}(q_j g_j)$.

So suppose next that $\mathrm{LM}(f) \geq x^\alpha$. Since $f = \sum h_i g_i$, $\mathrm{LT}(f) = \sum_{\mathrm{LM}(h_i g_i) = x^\alpha} \mathrm{LT}(h_i g_i) = \sum \mathrm{LT}(h_i)\mathrm{LT}(g_i)$. This concludes the proof.

Now we have a practical way of determining if something is a Gröbner basis. Next, we want to find a way to generate one.

Input: some set G_0. Output: a set G such that $(G) = (G_0)$ and G is Gröbner.

If G_i is Gröbner, we are done. Else, $S(g, g') \mod G_i \neq 0$ for some $g, g' \in G_i$. Note that $g, g' \in (G_i) \implies S(g, g') \in (G_i)$ so $r \in (G_i)$. By the division algorithm, $\mathrm{LT}(r) \notin (\mathrm{LT}(G_i))$.

Define $G_{i+1} = G_i \cup \{r\}$. $(\mathrm{LT}(G_{i+1})) \supsetneq (\mathrm{LT}(G_i))$.

Claim. If R is Noetherian, then every sequence of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ stabilizes (i.e. $I_j = I_{j+1} = \cdots$ from some point on).