Lecture LX: Computing Gröbner bases (Buchberger's Algorithm)

Recall: Last time we saw Buchberger's criterion for testing for GB:

Theorem (Buchberger) Let $I = (g_1, \dots, g_m) \subseteq R$ be an ideal. Then:

$G = \{g_1, \dots, g_m\}$ is a Gröbner basis of I $\iff$ $\forall i,j$ $S(g_i, g_j) \equiv 0 \mod G$.

(meaning: remainder 0 when dividing by G)

Recall: $S(g_i, g_j) = \dfrac{M}{L(g_i)} g_i - \dfrac{M}{L(g_j)} g_j$ $\qquad M = \operatorname{lcm}(LT(g_i), LT(g_j))$

§60.1 Examples:

Example 1: $R = K[x,y]$, $\leq$ = lexicographic order with $x > y$.

$I = (f_1, f_2)$ where $f_1 = \underline{x^3 y} - xy^2 + 1$

$f_2 = \underline{x^2 y^2} - y^3 - 1$ (we underline the leading terms)

$G_0 = \{f_1, f_2\}$ $\qquad M = x_1^3 y^2$

$$S(f_1, f_2) = \frac{x_1^3 y^2}{x^3 y} f_1 - \frac{x_1^3 y^2}{x_2^2 y^2} f_2 = y f_1 - x f_2 = y + x \equiv x + y \mod G$$

$\Rightarrow \{f_1, f_2\}$ is not a GB by Buchberger's Theorem.

Example 2: Take $R, I, \leq$ as above, but now $G_1 = \{f_1, f_2, \underbrace{\underline{x}+y}_{=: f_3}\}$

$S(f_1, f_2) = x + y \equiv 0 \mod G_1$.

$M_{13} = x^3 y$, $\quad M_{23} = x^2 y^2$

$S(f_2, f_3) = f_2 - xy^2(x+y) = -y^3 - 1 - \underline{x}y^3 \equiv y^4 - y^3 - 1 \mod (G_1) \Rightarrow$ not GB

We perform the division algorithm:

$q_1 = 0$

$q_2 = 0$

$q_3 = -y^3$

$$\begin{array}{l|l}
f_1 = \underline{x^3}y - xy^2 + 1 & -\underline{x}y^3 - y^3 - 1 \quad = S(f_2, f_3) \\
f_2 = \underline{x^2}y^2 - y^3 - 1 & - \quad -xy^3 - y^4 \quad = -y^3 f_3 \\
f_3 = \underline{x} + y & \overline{\quad y^4 - y^3 - 1}
\end{array}$$

no monomial is divisible by $LT(f_i)$ $i = 1,2,3$

Example 3: Take $R, I, \leq$ as above, but now $G_2 = \{f_1, f_2, \overset{=:f_3}{\underline{x}+y}, \overset{=:f_4}{\underline{y^4}-y^3-1}\}$

We know $S(f_1,f_2) \equiv S(f_2,f_3) \equiv 0 \pmod{G_2}$ by construction

$$S(f_1,f_3) = f_1 - x^2y(x+y) = -xy^2+1-\underline{x^2y^2} \equiv 0 \mod G_2.$$

$$S(f_1,f_4) = y^3f_1 - x^3(y^4-y^3-1) = -xy^5+y^3+\underline{x^3y^3}+x^3 \equiv 0 \mod G_2$$

$$S(f_2,f_4) = y^2f_2 - x^2(y^4-y^3-1) = -y^5-y^2+\underline{x^2y^3}+x^2 \equiv 0 \mod G_2$$

$$S(f_3,f_4) = y^4(x+y) - x(y^4-y^3-1) = y^5+xy^3+x \equiv 0 \mod G_2.$$

$q_1 = 0$
$q_2 = -1$
$q_3 = -y^2$
$q_4 = 0$

$f_1 = \underline{x^3}y - xy^2+1$
$f_2 = \underline{x^2}y^2-y^3-1$
$f_3 = \underline{x}+y$
$f_4 = \underline{y^4}-y^3-1$

$$\begin{array}{rl}
 -\underline{x}y^2 - xy^2 + 1 & = S(f_1,f_3) \\
 - \quad -x^2y^2 + y^3 + 1 & = -f_2 \\ \hline
 -xy^2 - y^3 & \\
 - \quad -xy^2 - y^3 & = -y^2 f_3 \\ \hline
 0 &
\end{array}$$

$q_1 = 0$
$q_2 = 0$
$q_3 = y^3+1$
$q_4 = y$

$f_1 = \underline{x^3}y - xy^2+1$
$f_2 = \underline{x^2}y^2-y^3-1$
$f_3 = \underline{x}+y$
$f_4 = \underline{y^4}-y^3-1$

$$\begin{array}{rl}
 y^5 + xy^3 + x & = S(f_3,f_4) \\
 - \quad y^5 - y^4 - y & = y f_4 \\ \hline
 y^4 + y + \underline{x}y^3 + x & \\
 - \quad y^4 + xy^3 & = y^3 f_3 \\ \hline
 y + x & \\
 - \quad y + x & = f_3 \\ \hline
 0 &
\end{array}$$

$$S(f_1,f_4) = y^2f_1 + 0f_2 + (x^2-xy-y^5+y^4+y^2)f_3 + y^2f_4 + 0$$

$$S(f_2,f_4) = 0f_1 + yf_2 + (x-y)f_3 + (-y)f_4 + 0$$

(These formulas come from the long division computations on the next page)

Conclusion: G_2 is a GB for I.

In particular $LT(I) = (\underset{x^3y}{\underset{\shortparallel}{LT(f_1)}}, \underset{x^2y^2}{\underset{\shortparallel}{LT(f_2)}}, \underset{x}{\underset{\shortparallel}{LT(f_3)}}, \underset{y^4}{\underset{\shortparallel}{LT(f_4)}}) = (x, y^4)$

So $\{f_3, f_4\}$ is already a GB. This is a minimal one ($\{f_3\}$, $\{f_4\}$ are not GB)

Remark: This example shows how we can obtain a GB from successive S-polynomial & remainder computations. This is precisely what Buchberger's Algorithm will do (we'll see this next).

Auxiliary calculations:

$q_1 = y^2$

$q_2 = 0$

$q_3 = x^2 - xy - y^5 + y^4 + y^2$

$q_4 = y^2$

$f_1 = x^3y - xy^2 + 1$

$f_2 = x^2y^2 - y^3 - 1$

$f_3 = x + y$

$f_4 = y^4 - y^3 - 1$

$$
\begin{array}{rl}
& x^3y^3 + x^3 - xy^5 + y^3 = S(f_1, f_4) \\
- & x^3y^3 - xy^4 + y^2 = y^2 f_1 \\
\hline
& x^3 - xy^5 + xy^4 + y^3 - y^2 \\
- & x^3 + x^2y = x^2 q_3 \\
\hline
& -x^2y - xy^5 + xy^4 + y^3 - y^2 \\
- & -x^2y - xy^2 = -xy q_3 \\
\hline
& -xy^5 + xy^4 + xy^2 + y^3 - y^2 \\
- & -xy^5 - y^6 = -y^5 q_3 \\
\hline
& xy^4 + xy^2 + y^6 + y^3 - y^2 \\
- & xy^4 + y^5 = y^4 q_3 \\
\hline
& xy^2 + y^6 - y^5 + y^3 - y^2 \\
- & xy^2 + y^3 = y^2 q_3 \\
\hline
& y^6 - y^5 - y^2 \\
- & y^6 - y^5 - y^2 = y^2 f_4 \\
\hline
& 0 \checkmark
\end{array}
$$

$q_1 = 0$

$q_2 = y$

$q_3 = x - y$

$q_4 = -y$

$f_1 = x^3y - xy^2 + 1$

$f_2 = x^2y^2 - y^3 - 1$

$f_3 = x + y$

$f_4 = y^4 - y^3 - 1$

$$
\begin{array}{rl}
& x^2y^3 + x^2 - y^5 - y^2 = S(f_2, f_4) \\
- & x^2y^3 - y^4 - y = y f_2 \\
\hline
& x^2 - y^5 + y^4 - y^2 + y \\
- & x^2 + xy = x f_3 \\
\hline
& -xy - y^5 + y^4 - y^2 + y \\
- & -xy - y^2 = -y f_3 \\
\hline
& -y^5 + y^4 + y \\
- & -y^5 + y^4 + y = -y f_4 \\
\hline
& 0 \checkmark
\end{array}
$$

§60.2 Buchberger's Algorithm:

INPUT: $f_1, \dots, f_s \in R = K[x_1, \dots, x_n]$ non-zero polynomials, $>$ a term order

OUTPUT: $G = \{g_1, \dots, g_m\} \supseteq F = \{f_1, \dots, f_s\}$ a Gröbner basis for $I = (f_1, \dots, f_s)$ wrt $>$.

PROCEDURE:

Initialize: $G \longmapsto F$

$G_{temp} = \emptyset$

While $G \neq G_{Temp}$:

- Set $G_{temp} = G$
- For every $p \neq q$ in G_{temp}

  $r := S(p, q) \mod G_{temp}$

  if $r \neq 0$, $G \longmapsto G \cup \{r\}$

Return G

Extra step: Remove elements from G to get a minimal GB by looking at those elements of G whose leading terms generate $(LT(g) : g \in G)$.

§60.3 An application: elimination of variables:

Theorem: If G is a Gröbner basis for a non-zero ideal $I \subseteq K[x_1, \dots, x_n]$ with respect to the lexicographic order with $x_1 > \dots > x_n$, then $G_i := G \cap K[x_i, x_{i+1}, \dots, x_n]$ generates the "ith elimination ideal" $I_i := I \cap K[x_i, x_{i+1}, \dots, x_n]$ (ideal of $K[x_i, \dots, x_n]$). Moreover, G_i is a GB for I_i

Example: $I = (2x^2 + 2xy + y^2 - 2x - 2y,\ x^2 + y^2 - 1) \subseteq \mathbb{R}[x,y]$

Problem: Find all (x,y) with $\begin{cases} 2x^2 + 2xy + y^2 - 2x - 2y = 0 \\ x^2 + y^2 - 1 = 0 \end{cases}$

A Gröbner basis for $>_{lex}$ with $x > y$ can be computed with a machine (eg Macaulay2, Sage):

$$g_1 = 2x + y^2 + 5y^3 - 2 \qquad \& \qquad g_2 = 5y^4 - 4y^3 = y^3(5y - 4)$$

$g_2 = 0 \Rightarrow y = 0$ or $y = 4/5$

- $g_1|_{y=0} = 2x - 2 = 0 \Rightarrow x = 1$
- $g_1|_{y=4/5} = 0$ gives $x = -3/5$

Answer: Only solutions are $(1,0)$, $(-\frac{3}{5}, \frac{4}{5})$.

Proof of Theorem: It is enough to show G_i is a GB for $I_i \subseteq K[x_{i+1}, \dots, x_n]$. Thus, we need to show $LT(I_i)$ is generated by $LT(G_i)$. Write $G = \{g_1, \dots, g_m\}$

Since $G_i \subseteq I_i$, we have $(LT(G_i)) \subseteq LT(I_i)$. For the other containment, let $f \in I_i$ with $f \neq 0$. Then $f \in I$ so $LT(f) \in (LT(g_1), \dots, LT(g_m))$ ie $\exists h_1, \dots, h_m \in K[x_1, \dots x_n]$ with $LT(f) = \sum_{j=1}^{m} h_j\, LT(g_j)$

Writing each h_j as a sum of monomials, we see that $LT(f)$ is a sum of terms of the form $a_{\alpha,j}\, \underline{x}^{\alpha}\, LT(g_j)$. Now, the monomials containing any of the variables $x_1, \dots, x_{i-1}$ should cancel out because $LT(f)$ does not contain any of these variables. From here it follows that we can rewrite $LT(f)$ as

$$LT(f) = \sum_{g \in G_i} h_g\, LT(g) \qquad \text{with } h_g \in K[x_{i+1}, \dots, x_n].$$

This shows $LT(f) \in (LT(G_i)) \subseteq K[x_{i+1}, \dots, x_n]$, as we wanted. $\square$