S-Polynomials and Buchberger's Algorithm

J.M. Selig
Faculty of Business
London South Bank University,
London SE1 0AA, UK

1 S-Polynomials

As we have seen in previous talks one of the problems we encounter in the division algorithm is if the leading terms of a pair of polynomials cancel. So here we study this phenomenon in some detail.

For any pair of polynomials $f_1,\, f_2 \in K[x_1, x_2, \ldots, x_n]$ and a given monomial order, we can form their S-polynomial which deliberately cancels the leading terms of both polynomials. For example, using deglex order, suppose $f_1 = 3x^3y + 2xy - y^2$ and $f_2 = 2xy^2 - 5y^3$, then we can write,

$$\begin{aligned} S(f_1,\, f_2) &= (1/3)yf_1 - (1/2)x^2 f_2 = (x^3y^2 + \frac{2}{3}xy^2 - \frac{1}{3}y^3) - (x^3y^2 - \frac{5}{2}x^2y^3) \\ &= \frac{5}{2}x^2y^3 + \frac{2}{3}xy^2 - \frac{1}{3}y^3. \end{aligned}$$

This can be written more generally if we introduce the notion of the least common multiple of a pair of monomials. Consider monomials x^α and x^β, where as usual this is short for $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ and similar for the other monomial. It is not too difficult to see that the least common multiple (LCM) of these can be found by taking the maximum of each index,

$$\mathrm{LCM}(x^\alpha,\, x^\beta) = x_1^{\max(\alpha_1,\beta_1)} x_2^{\max(\alpha_2,\beta_2)} \cdots x_n^{\max(\alpha_n,\beta_n)}.$$

Now the definition of the S-polynomial of a pair of polynomials can be written formally as,

$$S(f_1,\, f_2) = \frac{x^\gamma}{\mathrm{LT}(f_1)} f_1 - \frac{x^\gamma}{\mathrm{LT}(f_2)} f_2,$$

where $x^\gamma = \mathrm{LCM}(\mathrm{LM}(f_1), \mathrm{LM}(f_2))$ is the least common multiple of the leading monomials of the polynomials. Note that the leading coefficients are inverted when we do this.

In some sense this is the only way that cancellation can occur.

Consider a polynomial $h = \sum_{i=1}^{t} c_i f_i$ with constant coefficients $c_i \in K$ and $\mathrm{multideg}(f_i) = \delta = (\delta_1, \delta_2, \ldots, \delta_n) \in \mathbb{Z}^n_{\geqslant 0}$, for all i. Now if $\mathrm{multideg}(h) < \delta$ then h can be written as a linear combination (with coefficients from K) of the S-polynomials:

$S(f_j, f_k)$ with $1 \leqslant j,\ k \leqslant t$. Moreover the multidegrees of these S-polynomials will be less than δ; $S(f_j, f_k) < \delta$.

To see this let $p_i = f_i/d_i$ where $d_i \in K$ is the leading coefficient of f_i. Notice that this means that the leading term of any f_i will be $\mathrm{LT}(f_i) = d_i x^\delta$. The sum now becomes, $h = \sum_{i=1}^{t} c_i d_i p_i$. This can be written in terms of differences of the p_is,

$$\begin{aligned} h &= \sum_{i=1}^{t} c_i d_i p_i = c_1 d_1 (p_1 - p_2) + (c_2 d_2 + c_1 d_1)(p_2 - p_3) + \\ &\quad (c_1 d_1 + c_2 d_2 + c_3 d_3)(p_3 - p_4) + \cdots + (c_1 d_1 + c_2 d_2 + \cdots + c_t d_t) p_t \end{aligned}$$

Now, by hypothesis, the multidegree of h is less than δ and this can only happen if the coefficients of x^δ sum to zero. That is, $(c_1 d_1 + c_2 d_2 + \cdots + c_t d_t) = 0$ and hence the final term in the above expansion must vanish.

$$\begin{aligned} h &= \sum_{i=1}^{t} c_i d_i p_i = c_1 d_1 (p_1 - p_2) + (c_2 d_2 + c_1 d_1)(p_2 - p_3) + \\ &\quad (c_1 d_1 + c_2 d_2 + c_3 d_3)(p_3 - p_4) + \cdots \\ &\quad \cdots + (c_1 d_1 + c_2 d_2 + \cdots + c_{t-1} d_{t-1})(p_{t-1} - p_t) \end{aligned}$$

Next observe that

$$S(f_j, f_k) = \frac{x^\delta}{\mathrm{LT}(f_j)} f_j - \frac{x^\delta}{\mathrm{LT}(f_k)} f_k = \frac{x^\delta}{d_j x^\delta} f_j - \frac{x^\delta}{d_k x^\delta} f_k = (pj - p_k).$$

Hence finally we can write,

$$h = \sum_{i=1}^{t} c_i d_i p_i = \sum_{j=1}^{t-1} a_j S(f_j, f_{j+1})$$

where, $a_j = \sum_{i=1}^{j} c_i d_i$.

2 Gröbner Bases in terms of S-polynomials

The key theorem here is a characterisation of a Gröbner basis in terms of these S-polynomials.

Theorem 1 *Let $I \subset K[x_1, x_2, \ldots, x_n]$ be a polynomial ideal with basis $G = \{g_1, g_2, \ldots, g_s\}$ then G is a Gröbner basis for I if and only if the remainder on dividing every S-polynomial $S(g_i, g_j)$ $(i \neq j)$ by G (in any order of the basis elements) is zero.*

One way around this is straightforward, if G is a Gröbner Basis then from what we saw last time, dividing $S(g_i, g_j)$ by G in any order must give 0 since the S-polynomials will all be elements of the ideal generated by G.

The other way around is substantially harder to show. We must show that given the properties of the S-polynomials, G must be a Gröbner basis. That is, we must show

that given the properties of the S-polynomials then the leading term of any $f \in I$ lies in the ideal $< \mathrm{LT}(g_1), \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_s) >$. If $f \in I =< g_1, g_2, \ldots, g_s >$ then there must be polynomials h_i such that,

$$f = h_1 g_1 + h_2 g_2 + \cdots + h_s g_s$$

and moreover, the multidegree of f must be less than or equal to the maximum of the multidegrees of the $h_i g_i$s,

$$\text{multideg}(f) \leq \max(\text{multideg}(h_i g_i))$$

If equality holds then clearly the leading term of f is divisible by the leading term of the generator g_i with the maximal multidegree for $h_i g_i$. So in this case $\mathrm{LT}(f) \in < \mathrm{LT}(g_1), \mathrm{LT}(g_2) \ldots, \mathrm{LT}(g_s) >$. If equality does not hold, then some cancellation must have occurred. This means that, f can be expressed in terms of S-polynomials. Now the hypothesis that the S-polynomials have no remainder when divided by G means that we can 'undo' the cancellation and replace the S-polynomials by expressions involving the g_is. Continuing in this fashion we will eventually find an expression for f in terms of the g_is where the multigegree of f is equal to the maximum multidegree of the terms $h_i g_i$. When this happens the theorem is proved. Full details of the proof can be found in [1, pp.82–84].

3 Buchberger's Algorithm

The above considerations lead quite naturally to a fairly simple algorithm for finding a Gröbner basis of an ideal. In essence, we repeatedly compute the S-polynomials of pairs of generators and then divide by the set of generators. If the remainder of this division is non-zero then we extend the set of generators by adding the remainder. Formally this can be written,

Inputs:
$F = (f_1, f_2, \ldots, f_s)$, a list of generators for a non-zero ideal.

Outputs:
$G = (g_1, g_2, \ldots, g_t)$, a Gröbner basis for the ideal with $F \subset G$.

Method:
Initialise $G := F$,
Repeat $G' := G$
For every pair $\{g_i,\ g_j\} \quad i \neq j$ Do,
compute the remainder S on dividing $S(g_i, g_j)$ by G',
If $S \neq 0$ then $G := G \cup \{S\}$,
end for
Until $G = G'$
Output G.

The fact the algorithm will terminate is guaranteed by the ascending chain condition (ACC). Each iteration of the central loop increases the monomial ideal generated by

the leading terms of the generators $< \mathrm{LT}(g_1), \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_t) >$. Each of these ideas is a sub-ideal of the following iteration and by ACC this sequence will eventually stabalise.

Again, for a detailed proof that the algorithm is correct see [1, p. 88].

This algorithm is simple to describe but it is not very efficient, there are now many modifications of this basic routine which make it quicker. However, notice that the above algorithm must repeatedly examine all possible pairs of polynomials in a list, so it is never going to be particularly quick.

Groöbner bases for an ideal are not unique, and this can cause difficulties in some circumstances. By imposing more constraints on the possible generators it is possible to define minimal and then reduced Gröbner bases. The reduced Gröbner basis of an ideal is unique and hence can be used to solve the ideal identity problem for example. Given two ideals in terms of a set of generators, how can we tell if they are actually the same ideal? A possible solution is to compute the reduced Gröbner basis for each and compare. If the generators of the reduced Gröbner basis differ then so do the ideals they generate.

4 Example: Solving Systems of Polynomial Equations

Consider the problem of finding the points of intersection between two ellipses defined by the equations,

$$\begin{aligned} 2x^2 - 4x + y^2 - 4y + 3 &= 0, \\ x^2 - 2x + 3y^2 - 12y + 9 &= 0. \end{aligned}$$

To do this we consider the ideal generated by the two polynomials $< f_1,\ f_2 >$ where, $f_1 = 2x^2 - 4x + y^2 - 4y + 3$ and $f_2 = x^2 - 2x + 3y^2 - 12y + 9$. The lexical order with $x > y$ will be used in the following. First the S-polynomial,

$$S(f_1,\ f_2) = \frac{-5}{2}y^2 + 10y - \frac{15}{2}.$$

It is easy to see that the remainder on dividing this by (f_1, f_2) is just all of $S(f_1,\ f_2)$. Write this as $f_3 = \frac{-5}{2}y^2 + 10y - \frac{15}{2}$. So we add this to the list of generators to get $G_1 = (f_1,\ f_2,\ f_3)$. Next we don't have to work out $S(f_1,\ f_2)$ again, it doesn't change, but we do need to find the other two S-polynomials,

$$\begin{aligned} S(f_1,\ f_3) &= 4x^2y - 3x^2 - 2xy^2 + \frac{1}{2}y^4 - 2y^3 + \frac{3}{2}y^2, \\ S(f_2,\ f_3) &= 4x^2y - 3x^2 - 2xy^2 + 3y^4 - 12y^3 + 9y^2. \end{aligned}$$

Now we divide these S-polynomials by G_1 we get,

$$\begin{aligned} S(f_1,\ f_3) &= (2y - \frac{3}{2})f_1 + (\frac{4}{5}x - \frac{1}{5}y^2 + \frac{4}{5}y - \frac{3}{5})f_3, \\ S(f_2,\ f_3) &= (2y - \frac{3}{2})f_1 + (\frac{4}{5}x - \frac{6}{5}y^2 + \frac{4}{5}y - \frac{3}{5})f_3. \end{aligned}$$

No remainders, so we are done!

Now solving $f_3 = 0$ gives two solutions for y, $y = 3$ or $y = 1$. Substituting either of these solutions into f_1 or f_2 gives $x = 0$ or $x = 2$. This gives four possible solutions, $(x, y) = (0, 1),\ (2, 1),\ (0, 3)$ and $(2, 3)$, the vertices of a square.

References

[1] Cox, D. Little, J. and O'Shea, D., 1996, "Ideals, Varieties, and Algorithms an Introduction to Algebraic Geometry and Commutative Algebra (second ed.)", Springer Verlag, Berlin.