Monomial Orders and the Division Algorithm

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

We start by recalling the familiar algorithm for dividing polynomials in one variable. The idea is that we want to extend this to an analogous algorithm for polynomials in several variables. This is not straightforward, and we will encounter several difficulties which need to be overcome, the final problem is solved by the introduction of Gröbner bases.

1 Division of Polynomials in One Variable

Consider dividing the polynomial $f = x^3 + x^2 + x + 2$ by $g = x - 1$. To do this we can take the leading term of f and divide it by the leading term of g. This will be written $\mathrm{LT}(f) = x^3$, and $\mathrm{LT}(g) = x$ so that $\mathrm{LT}(f)/\mathrm{LT}(g) = x^2$. This quantity is recorded and then we compute,

$$f' = f - \big(\mathrm{LT}(f)/\mathrm{LT}(g)\big)g = (x^3 + x^2 + x + 2) - x^2(x - 1) = 2x^2 + x + 2.$$

Now we repeat this process with f': $\mathrm{LT}(f')/\mathrm{LT}(g) = 2x$ and then,

$$f'' = f' - \big(\mathrm{LT}(f')/\mathrm{LT}(g)\big)g = (2x^2 + x + 2) - 2x(x - 1) = 3x + 2.$$

Repeating once more gives $\mathrm{LT}(f'')/\mathrm{LT}(g) = 3$, so that

$$f''' = f'' - \big(\mathrm{LT}(f'')/\mathrm{LT}(g)\big)g = (3x + 2) - 3(x - 1) = 5.$$

Now the leading term of g doesn't divide the leading term of f''' so we are done, all that remains is to put together the results, let

$$h = \mathrm{LT}(f)/\mathrm{LT}(g) + \mathrm{LT}(f')/\mathrm{LT}(g) + \mathrm{LT}(f'')/\mathrm{LT}(g) = x^2 + 2x + 3$$

and the remainder is $r = f''' = 5$. This means we can write,

$$f = hg + r = (x^2 + 2x + 3)(x - 1) + 5.$$

There are many consequences of this algorithm. In particular it is clear that the results for h and the remainder r are unique and moreover that the degree of the remainder r is strictly less that the degree of g.

The computation can be set down as follows,

$$
\begin{array}{r|rcrcrcr}
 & & & x^2 & + & 2x & + & 3 \\
\cline{2-8}
x-1 & x^3 & + & x^2 & + & x & + & 2 \\
 & x^3 & - & x^2 & & & & \\
\cline{2-8}
 & & & 2x^2 & + & x & + & 2 \\
 & & & 2x^2 & - & 2x & & \\
\cline{2-8}
 & & & & & 3x & + & 2 \\
 & & & & & 3x & - & 3 \\
\cline{2-8}
 & & & & & & & 5
\end{array}
$$

Now suppose we try to imitate the above with polynomials in several variables. Immediately we hit a problem, what is the leading term for a polynomial of several variables? If we assume naively that this is just the term of highest total degree then there maybe several different terms with this degree and it does matter which we choose. For example, suppose $f = x^2 + y^2$ and $g = y + 1$ and say we assume that x^2 is the leading term of f, this would lead to the result,

$$f = 0.g + (x^2 + y^2),$$

on the other hand if we say that y^2 is the leading term for f the we get,

$$f = yg + (x^2 - y).$$

To overcome this problem we need to introduce an ordering on the possible monomials.

2 Orders on Monomials

Certainly we want any order on monomials to be a total order so that any pair of monomials may be compared and which is the 'larger' can be decided. There are a couple of other requirements that are needed of an order on monomials that are needed to make this work. So we define a **monomial ordering** on $K[x_1, x_2, \ldots, x_n]$ to be a relation $>$, on the monomials of the ring, or equivalently on the multi-indices $\alpha \in \mathbb{Z}^n_{\geqslant 0}$ with the following properties,

- $>$ is a total order, that is it is transitive, anti-symmetric and for any pair of elements $\alpha, \beta \in \mathbb{Z}^n_{\geqslant 0}$ either $\alpha > \beta$, $\beta > \alpha$ or $\alpha = \beta$.
- if $\alpha > \beta$ and $\gamma \in \mathbb{Z}^n_{\geqslant 0}$ then $\alpha + \gamma > \beta + \gamma$. This is required to make the algebra consistent with the ordering. Notice that adding multi-indices is equivalent to multiplying monomials.
- $>$ is a well-ordering on $\mathbb{Z}^n_{\geqslant 0}$. This means that ever non-empty subset of $\mathbb{Z}^n_{\geqslant 0}$ (even infinite subsets) has a smallest element. Put another way, any decreasing sequence, $\alpha > \beta > \cdots > \xi > \cdots$ eventually terminates.

There are many possible monomial orderings and it doesn't matter which one we choose, at least not for theoretical purposes. In practice, computations can often be done far more efficiently using the 'correct' monomial ordering. However, we won't concern ourselves with practicalities here.

Our first example of a monomial order will be the lexicographic or lexical ordering $>_{\text{lex}}$. This is supposedly the ordering used in dictionaries, however in any dictionary I have seen 'a' is before 'aardvark' so I don't think this is correct. Once we have decided on an ordering for the variables, (usually $x_1 >_{\text{lex}} x_2 >_{\text{lex}} \cdots >_{\text{lex}} x_n$ or alphabetic order for $x >_{\text{lex}} y >_{\text{lex}} z$ for example). This ordering is most conveniently expressed in terms of multi-indices, $\alpha >_{\text{lex}} \beta$ if the left-most non-zero entry of $\alpha - \beta$ is positive. For example $xy^2z >_{\text{lex}} xz^2$ since $(1,2,1) - (1,0,2) = (0,2,-1)$. To see that this is indeed a monomial ordering as defined above, notice that it is clearly a total order, this follows from the fact that 'greater than' $>$ is a total order on $\mathbb{Z}_{\geqslant 0}$. Next it is clear that $(\alpha+\gamma) - (\beta+\gamma) = \alpha - \beta$ and hence $\alpha + \gamma >_{\text{lex}} \beta + \gamma$ if $\alpha >_{\text{lex}} \beta$. Finally, observe that if this were not a well-ordering there would be an infinite sequence of elements, $\alpha >_{\text{lex}} \beta >_{\text{lex}} \cdots >_{\text{lex}} \xi >_{\text{lex}} \cdots$. Consider the successive differences $\alpha - \beta,\ \beta - \gamma, \ldots$ the left-most non-zero digit will form a decreasing sequence which must terminate in a zero in a finite number of steps. After this the next digit on the right will form a decreasing sequence terminating in a zero in a finite number of steps, and so forth until we run out of digits, again after a finite number of steps. This contradicts the assumption that the sequence is infinite.

The next monomial ordering we look at is called 'degree then lexical' or 'graded lexical' often abbreviated to deglex. Here, monomials are ordered by total degree then any ties are broken by the lexical ordering. The total degree of a multi-index α is given by,

$$|\alpha| = \sum_{i=1}^{n} \alpha_i.$$

So we may define the monomial ordering $>_{\text{deglex}}$ as,

$$\alpha >_{\text{deglex}} \beta \Leftrightarrow |\alpha| > |\beta| \quad \text{or if} \quad |\alpha| = |\beta| \quad \text{then} \quad \alpha >_{\text{lex}} \beta$$

There are several other possible monomial orders and of course we can always permute the order of the variables to start with.

3 The Division Algorithm

Now let us see how the idea of a monomial order helps us to define a division algorithm for polynomials in several variables. First notice that the notion of the leading term is now well defined, presuming we have chosen to work with a definite monomial order. There remains a small problem with simply imitating the one variable case, to see the problem consider the following division: Suppose we divide $f = x^2 + y^2 + x$ by $g = x - 1$ using the deglex ordering. To begin with there is no problem, $\text{LT}(f)/\text{LT}(g) = x$ so that,

$$f' = f - \text{LT}(f)/\text{LT}(g)g = y^2 + 2x.$$

But now the leading term of f' (under the deglex ordering) is y^2 and $\mathrm{LT}(g) = x$ doesn't divide this. With the standard, one variable algorithm, this would mean we are finished and f' would be the remainder. However, it is clear that the next term in f' is divisible by x so we should really keep on dividing, the leading term of f' forming part of the remainder. So the algorithm should be,

Inputs:
Polynomials f and g.

Outputs:
Quotient h and remainder r.

Method:
initialise $h := 0$,
initialise $r := 0$,
while $f \neq 0$ do:
if $\mathrm{LT}(g)$ divides $\mathrm{LT}(f)$ then
$h := h + \mathrm{LT}(f)/\mathrm{LT}(g)$,
$f := f - \mathrm{LT}(f)/\mathrm{LT}(g)g$,
else
$r := r + \mathrm{LT}(f)$,
$f := f - \mathrm{LT}(f)$,
end while
Output h, r.

Note that it is easy to tell if one monomial divides another: α divides β if and only if $\alpha_1 \leqslant \beta_1,\ \alpha_2 \leqslant \beta_2, \ldots, \alpha_n \leqslant \beta_n$.

Applying this algorithm to the example where $f = x^2 + y^2 + x$ by $g = x - 1$ gives $h = (x + 2)$ and $r = (y^2 + 2)$ so that,

$$f = (x + 2)g + (y^2 + 2).$$

The next complication is that we don't just want to divide by single polynomials, we really want to be able to divide by ideals. One possible reason why we want to do this is to solve the so called ideal membership problem. Suppose we are given a polynomial f and an ideal $I =< g_1,\ g_2, \ldots, g_k >$, how could we tell whether or not f is an element of I? One possible answer to this would be to divide f by g_1, then take the remainder r_1 and divide by g_2, then repeating this for all g_i in the basis for I. We will end up with an identity of the form,

$$f = h_1 g_1 + h_2 g_2 + \cdots + h_k g_k + r.$$

Now if the remainder r is zero then we can definitely say that $f \in I$. But if $r \neq 0$ then we cannot exclude the possibility $f \in I$. This is because the result depends, in general, on the order that we divide by basis polynomials. As an example, consider the case where $f = x^2 + y^2 + 2y - 1$ and $I =< x^2 + y^2 - 1,\ y >$. Dividing f by $x^2 + y^2 - 1$, using deglex order, gives $h = 1$ and $r = 2y$. Then dividing r by y gives $h = 2$, $r = 0$, that is,

$$f = 1.(x^2 + y^2 - 1) + 2(y) + 0.$$

So clearly $f \in I$. Now consider dividing f by y first. The first step here would be to add $x^2 = \mathrm{LT}(f)$ to the remainder so that, $h = y + 2$ and the first remainder is $r = x^2 - 1$. Dividing this now by $x^2 + y^2 - 1$ we get $h = 1$ and $r = -y^2$, leading to,

$$f = (y + 2)y + 1(x^2 + y^2 - 1) - y^2.$$

Notice here that the remainder is in fact divisible by the basis element y, so we could have divided by y again to get the same result as before. This is not always the case.

This problem can be partially solved by dividing by the basis polynomials in a more symmetrical fashion, inside a single algorithm,

Inputs:
Polynomials f and $g_1, g_2, \ldots, g_k$.

Outputs:
Quotients $h_1, h_2, \ldots, h_k$ and remainder r.

Method:
initialise $h_1 := 0, h_2 := 0, \ldots, h_k := 0$,
initialise $r := 0$,
while $f \neq 0$ do:
$i := 1$, // loop counter
$s := k$, // exit condition
while $i \leqslant s$ do
if $\mathrm{LT}(g_i)$ divides $\mathrm{LT}(f)$ then
$h_i := h_i + \mathrm{LT}(f)/\mathrm{LT}(g_i)$,
$f := f - \mathrm{LT}(f)/\mathrm{LT}(g_i)g_i$,
$s := 0$, // force exit
else
$i := i + 1$
end while
if $s \neq 0$ then // no division happened
$r := r + \mathrm{LT}(f)$,
$f := f - \mathrm{LT}(f)$,
end while
Output $h_1, h_2, \ldots, h_k, r$.

Notice here how the algorithm steps through all the possible basis elements $g_1, g_2, \ldots, g_k$ in turn until it finds one that divides the current f. If none of them divide f then the leading term of f is moved to the remainder r. Unfortunately this does not completely solve the problem since the result is still sensitive to the order in which the g_is are checked.

To see this consider the following example. Let $f = x^2y + xy^2 + y^2$ and $g_1 = y^2 - 1$, $g_2 = xy - 1$. Using deglex ordering we can see that $\mathrm{LT}(g_1)$ doesn't divide $\mathrm{LT}(f)$ but $\mathrm{LT}(g_2)$ does. So f becomes $f = x^2y + y^2 + x$. Now the leading term of this polynomial is divisible by both $\mathrm{LT}(g_1)$ and $\mathrm{LT}(g_2)$. But the algorithm says we must

divide by $\mathrm{LT}(g_1)$, the result also has a leading term divisible by $\mathrm{LT}(g_1)$ and the final result will be,

$$x^2y + xy^2 + y^2 = (x+1)g_1 + xg_2 + 2x + 1 = (x+1)(y^2-1) + x(xy-1) + 2x + 1.$$

On the other hand if we swap g_1 and g_2 we get,

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

Overcoming this problem leads to the notion of Gröbner bases for ideals.

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.