Monomial Ideals and Gröbner Bases

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

Last time we introduced the division algorithm for polynomials in several variables. We noted that the result of the procedure was dependent on the order of the polynomials. That is, suppose we want to divide the polynomial f by the set of polynomials, $\{g_1,\, g_2, \ldots, g_k\}$ then the division algorithm will give a sequence of polynomials $h_1,\, h_1, \ldots, h_k, r$ such that,

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

But if we reorder the polynomials that we are dividing by then the results will, in general, be different,

$$f = h'_k g_k + h'_1 g_1 + \cdots + h'_2 g_2 + r'.$$

In particular the remainder term r could be different, this is important because if $r = 0$ we may conclude that f lies in the ideal generated by the dividing polynomials, $r = 0 \Rightarrow f \in < g_1, g_2, \ldots g_k >$. However, because of the non-uniqueness of the remainder we cannot infer that if the remainder is non-zero then the polynomial f is not in the ideal $< g_1, g_2, \ldots g_k >$. Perhaps there is a reordering of the basis for the ideal that gives a zero remainder.

This difficulty can be overcome by introducing a Gröbner basis for the ideal. Before we introduce a definition of such a basis we need just a couple more ideas.

1 Monomial Ideals from General Ideals

There are two ways to produce a monomial ideal from a given set of polynomials, $\{g_1,\, g_2, \ldots, g_k\}$. The first is to is to take the leading terms of the polynomials and then use these monomials to generate an ideal,

$$< \mathrm{LT}(g_1),\, \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_k) > .$$

The second method can be applied to any ideal I. We take the leading terms of every polynomial in I, this can be written $\mathrm{LT}(I) = \{cx^\alpha : c \in K, cx^\alpha = \mathrm{LT}(f) \text{ for some } f \in I\}$. Now we take the ideal generated by this (usually infinite) set of monomials. This ideal is written, as $< \mathrm{LT}(I) >$. It is easy to see that, if $I =< g_1, g_2, \ldots g_k >$, then

$$< \mathrm{LT}(g_1),\, \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_k) > \subseteq < \mathrm{LT}(I) >,$$

since certainly each $g_i \in I$. Now, in general, these two ideals are different. This can be demonstrated with an example, consider the ideal generated by the polynomials $g_1 = xy + 1$ and $g_2 = y^2 - 1$. Using the deglex order we can find,

$$yg_1 - xg_2 = (xy^2 + y) - (xy^2 - x) = x + y \in I =< g_1, g_2 > .$$

So clearly $x \in < \mathrm{LT}(I) >$ but x is not an element of $< \mathrm{LT}(g_1), \mathrm{LT}(g_2) >=< xy, y^2 >$.

However, under some circumstances it is possible to find a set of generators for an ideal such that,

$$< \mathrm{LT}(g_1), \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_k) >=< \mathrm{LT}(I) >,$$

such a set of generators is usually called a **Gröbner basis** (or sometimes a **standard basis**) for the ideal. The rest of this talk will be concerned with showing that such bases do indeed exist and exploring some of their properties. Next time we will see that such bases can be found for every ideal and an algorithm will be given which can construct such a basis.

The first property we can show is that the remainder of a polynomial with respect to a Gröbner basis is uniquely defined. Suppose this was not the case, say that different orderings of the basis elements in the division algorithm gave,

$$f = h_1 g_1 + h_2 g_2 + \cdots + h_k g_k + r \text{ and } f = h'_1 g_1 + h'_2 g_2 + \cdots + h'_k g_k + r'.$$

Note that, none of the terms of r nor r' will be divisible by any of the leading terms of the g_is, $\mathrm{LT}(g_i)$. Subtracting we have that,

$$r - r' = (h_1 - h'_1)g_1 + (h_2 - h'_2)g_2 + \cdots + (h_k - h'_k)g_k \in < g_1, g_2, \ldots, g_k >= I.$$

So that $\mathrm{LT}(r - r') \in < \mathrm{LT}(I) >$, but if $< \mathrm{LT}(I) >=< \mathrm{LT}(g_1), \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_k) >$, then $\mathrm{LT}(r - r') \in < \mathrm{LT}(g_1), \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_k) >$. So there are terms in $\mathrm{LT}(r - r')$ divisible by some $\mathrm{LT}(g_i)$, contradicting our hypothesis. Hence $r - r' = 0$ and the remainder is unique.

Perhaps we are getting a little ahead of ourselves here since we haven't even shown that such a basis can exist. In the next few sections we will show that every ideal has a Gröbner basis.

2 Properties of Monomial Ideals

One small point glossed over at the end of the last section was that any monomial in a monomial ideal must be divisible by some of the basis monomials. This is simple to show. Let us write a monomial ideal as $I =< x^\alpha : \alpha \in A >$; the set of multi-indices A is finite. Now consider another monomial $x^\beta \in I$ so that we may write,

$$x^\beta = \sum_{\alpha \in A} h_\alpha x^\alpha$$

expanding the right-hand side of the above equation gives a sum of monomials each divisible by some x^α, hence the left-hand side must also be divisible by some x^α. Notice that this reasoning also applies to any element of a monomial ideal, say $f \in < x^\alpha : \alpha \in A >$, then every term of f must be divisible by some x^α.

In the above we restricted the monomial ideal to be generated by a finite set of generators, but ideals like $< \mathrm{LT}(I) >$ for some ideal I don't look like they are finitely generated. In fact they are, this is guaranteed by Dickson's lemma. Dickson's lemma states that every monomial ideal of $K[x_1, x_2, \ldots, x_n]$ is finitely generated by monomials. That is, we can always find a finite set of monomials that generate the ideal. Traditionally this is proved by induction on the number of variables. For one variable we have already seen in a previous lecture that all ideals in $K[x]$ are principal and can be generated by the greatest common divisor of the elements in the ideal. For a monomial ideal in one variable, the greatest common divisor of a set of monomials will be a monomial itself. Then we assume the lemma is true up to some number $n-1$ variables and extend the result to the n variable case. However, the lemma is an obvious consequence of theorem of G. Higman concerning "Ordering by divisibility in abstract algebras". The following statement of the theorem is taken from [2],

(i) In any set S of words (read monomials here), the set of minimal words, those not divisible by another member of S, is finite.

(ii) In any infinite sequence $w_1, w_2, \ldots$ of words there is an infinite subsequence $w_i, w_j, w_k, \ldots$ with $w_i \mid w_j \mid w_k \mid \cdots$ and $i < j < k < \cdots$.

(iii) There does not exist an infinite division-free sequence $w_1, w_2, \ldots$. That is one for which $i < j$ implies $w_i \nmid w_j$.

Notice that any monomial order $>$, if $w_i \mid w_j$ then $w_j > w_i$. Conway's proof is as follows,

Proof The equivalence of the three properties is fairly obvious, so we tackle only form (iii). Supposing that division-free sequences exist, we select an 'earliest' one $w_1, w_2, \ldots$ by the conditions:

w_1 is a shortest word beginning an infinite division-free sequence.

w_2 is a shortest word such that w_1, w_2 begins such a sequence.

w_3 is shortest such that w_1, w_2, w_3 begins such a sequence, and so on.

Then infinitely many of the w_i begin with the same letter, say $w_i = av_i$, $w_j = av_j$, $w_k = av_k, \ldots$ for $i < j < k < \cdots$. Unfortunately, we then have the infinite division-free sequence $w_1, \ldots, w_{i-1}, v_i, v_j, v_k, \ldots$ which is 'earlier' than the one we chose.

Both Dickson's lemma and Higman's theorem seem to be examples of a basic theorem about well-quasi-ordered sets, see [3]. Other examples of well-quasi-oredered sets include finite graphs ordered by graph minors and embedding between finite trees with labeled vertices. (Thanks to Roboin for pointing this out to me.)

3 The Existence of Gröbner Bases

We now have the ingredients required to show that a Gröbner basis exists for any ideal $I \in K[x_1, x_2, \ldots, x_n]$. First of all the ideal $< \mathrm{LT}(I) >$ is a monomial ideal, this is not completely straightforward since it is generated by terms rather than monomials but the difference is only a non-zero multiplicative constant. Using the monomials $\mathrm{LM}(g)$, rather that the leading terms $\mathrm{LT}(g)$ such that $g \in I$ clearly makes no difference if K is a field. Now by Dickson's lemma, this monomial ideal is finely generated by a finite set of monomials $m_1,\ m_2, \ldots, m_s$. That is, $< \mathrm{LT}(I) >=< m_1,\ m_2, \ldots, m_s >$. Now we can show that each monomial m_i is the leading term for some $g_i \in I$. Certainly $m_i = h_1 \mathrm{LT}(g_1) + h_2 \mathrm{LT}(g_2) + \cdots + h_t \mathrm{LT}(g_t)$ for some finite set of $g_j \in I$. So $m_i \in < \mathrm{LT}(g_1), \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_t) >$ and hence m_i will be divisible by one of the monomials, say $\mathrm{LT}(g_j)$, see above. This means that $m_i = x^\alpha \mathrm{LT}(g_j)$ for some monomial x^α. By the properties of a monomial order $x^\alpha \mathrm{LT}(g_j) = \mathrm{LT}(x^\alpha g_j)$ and $x^\alpha g_j \in I$. So we see that $m_i = \mathrm{LT}(g_i)$ for some $g_i \in I$.

So far we have shown that, $< \mathrm{LT}(I) >=< \mathrm{LT}(g_1), \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_s) >$ for some finite set of polynomials $g_1, \ldots, g_s \in I$. Finally we must show that the set of polynomials in the original ideal do in fact generate the ideal. Clearly, $< g_1,\ g_2, \ldots, g_s > \subseteq I$ since each $g_i \in I$. Now suppose there is an $f \in I$ but not in $< g_1,\ g_2, \ldots, g_s >$. Dividing this f by the set of g_is gives,

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

where the remainder r, has no terms divisible by any $\mathrm{LT}(g_i)$. Now,

$$r = f - h_1 g_1 - h_2 g_2 - \cdots - h_s g_s,$$

so that the leading term of the remainder is in the ideal $< \mathrm{LT}(I) >$ and hence $\mathrm{LT}(r) \in < \mathrm{LT}(g_1), \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_s) >$ this gives a contradiction unless $r = 0$. Of course when $r = 0$ we have that $f \in < g_1,\ g_2, \ldots, g_s >$ and so we may conclude that $I =< g_1,\ g_2, \ldots, g_s >$.

Hilbert's basis theorem (Basissatz) states that any ideal of $K[x_1, x_2, \ldots, x_n]$ is finitely generated. This is now a very simple consequence of the above since for any ideal $I \in K[x_1, x_2, \ldots, x_n]$, there is a Gröbner basis which finitely generated.

The ascending chain condition (ACC) for polynomial ideals can be proved using the Hilbert basis theorem. Traditionally, the ascending chain condition was used to prove Hilbert's basis theorem. This shows that the two are equivalent. For completeness, the ascending chain condition states that for any sequence of ideals $I_j \in K[x_1, x_2, \ldots, x_n]$ such that,

$$I_1 \subset I_2 \subset I_3 \subset \cdots \subset I_j \subset \cdots$$

there is an integer, say N such that $I_N = I_{N+1} = I_{N+2} + \cdots$. That is the ascending chain of ideal will eventually stabalise.

In the next talk we will look at ways to find a Gröbner basis in any given ideal, until then it is difficult to give concrete examples. However, linear polynomials can just about be understood. For example, consider the ideal $< g_1,\ g_2 >$ where the generators are the linear polynomials $g_1 = x - z$ and $g_2 = y + z$. The polynomials g_1 and g_2 form

a Gröbner basis for the ideal $< g_1, g_2 > \in \mathbb{C}[x, y, z]$ using the lex monomial order where $x >_{\text{lex}} y >_{\text{lex}} z$. To see this first note that $< \text{LT}(g_1), \text{LT}(g_2) > = < x, y >$. To show that this is indeed a Gröbner basis we must show that the leading term of any polynomial in the ideal is divisible by x or y. So let $f = h_1 g_1 + h_2 g_2$, and assume that the leading term of f is not divisible by x or y, that is $\text{LT}(f) = cz^n$ for some coefficient c and exponent n. In lex order any monomial divisible by x or y is greater than any z^n so we can conclude that f must be a function of z only. In particular the zero set of f must be independent of x and y but since f lies in the ideal generated by the linear functions $g_1 = x - z$ and $g_2 = y + z$ it will be zero along the line $z = x = -y$. This gives a contradiction and hence we can conclude that no such non-zero f can exist, or rather that any $f \in < g_1, g_2 >$ must have a leading term in $< \text{LT}(g_1), \text{LT}(g_2) >$. So g_1, g_2 form a Gröbner basis. In fact for linear functions under lex order, the Gröbner basis corresponds to the row echelon form usually found using Gaussian elimination.

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.

[2] Conway, J.H., 1971, "Regular Algebra and Finite Machines", Chapman and Hall, London.

[3] Wikipedia "Well-quasi-ordering" `http://http://en.wikipedia.org/wiki/Well-quasi-ordering` Last access 12/6/2011.