

Gröbner bases

A micro-introduction.

1 Introduction

Gröbner bases were introduced to solve the ideal membership problem. Given the ideal $I = (f_1, \dots, f_m)$ generated by given functions f_i in the polynomial ring $k[X_1, \dots, X_n]$, how can we test whether some given f belongs to I ?

In the one-variable case that is easy: the ideal I is also generated by a single element (that is, $k[X]$ is a PID, a *Principal Ideal Domain*), namely by the g.c.d. g of the f_i . And f belongs to (g) precisely when g divides f .

Also in the multi-variable case the question can be answered by first picking a suitable basis and then doing a division.

2 One-variable division

Ordinary division of one-variable polynomials works by repeatedly eliminating the term of highest degree: $x^4 + x^3 + x^2 + x + 1$ is divided by $x^2 - x - 2$ by first subtracting $x^2(x^2 - x - 2)$, rest $2x^3 + 3x^2 + x + 1$, then subtracting $2x(x^2 - x - 2)$, rest $5x^2 + 5x + 1$, finally subtracting $5(x^2 - x - 2)$, rest $10x + 11$, so that $x^4 + x^3 + x^2 + x + 1 = (x^2 + 2x + 5)(x^2 - x - 2) + 10x + 11$.

3 Term orders

For polynomials in more than one variable one first needs some ordering on term degrees. Let the term x^3yz^2 have degree $(3,1,2)$. Then degrees are elements of \mathbf{N}^n for functions with n variables, if \mathbf{N} denotes the set of nonnegative integers.

One would like (i) term order is a total order on \mathbf{N}^n , (ii) if $a < b$ then $a + c < b + c$, (iii) there is no infinite strictly decreasing sequence.

Three well-known examples of term orders are

- *lex order*: $a > b$ if we have $a_i > b_i$ when i is the first coordinate where a and b differ. For example, $(3, 1, 2) > (3, 0, 3) > (1, 8, 0) > (1, 4, 1)$.
- *graded lex order*: Let $|a| = \sum a_i$, so that $|(3, 1, 2)| = 6$ ("total degree"). Graded lex order first orders by total degree, and in case of equal total degree the order is using lex. For example, $(1, 8, 0) > (3, 1, 2) > (3, 0, 3) > (1, 4, 1)$.
- *graded reverse lex order*: First order by total degree, and in case of equal total degree say $a > b$ if we have $a_i < b_i$ when i is the last coordinate where a and b differ. For example, $(1, 8, 0) > (1, 4, 1) > (3, 1, 2) > (3, 0, 3)$.

It will follow from the lemma in the proof of Hilbert's Basis Theorem below that (iii) is equivalent to (iii)' $0 < a$ for all $a \neq 0$.

4 Division

Given a term order we have a division algorithm, dividing a given polynomial p by a sequence of polynomials p_1, \dots, p_m : Find the leading term t of p and eliminate it by finding the smallest i for which the leading term of p_i divides t and subtracting the appropriate multiple of p_i from p . When no such i exists, t is eliminated by putting it in the remainder. Stop when $p = 0$.

For example, for lex order, divide $x^3y^2 + x^2y^3 - y^2$ by $xy - 1, y^2$ to find $x^3y^2 + x^2y^3 - y^2 = (x^2y + xy^2 + x + y)(xy - 1) - 1 \cdot y^2 + x + y$ where the remainder is $x + y$. On the other hand, divide by $y^2, xy - 1$ to find $x^3y^2 + x^2y^3 - y^2 = (x^3 + x^2y - 1)y^2$ with zero remainder.

Hmm. This division algorithm is not yet good enough to decide whether $x^3y^2 + x^2y^3 - y^2$ lies in the ideal $(xy - 1, y^2)$ generated by $xy - 1$ and y^2 . Two things are bad: the remainder depends on the ordering of the p_i , and being in the ideal (p_1, \dots, p_m) is not equivalent to having zero remainder.

5 Hilbert basis theorem

Theorem 5.1 *Let k be a field. Every ideal I in $k[x_1, \dots, x_n]$ is finitely generated.*

Proof: Define a partial order \leq on \mathbf{N}^n by letting $a \leq b$ when $a_i \leq b_i$ for all i . For example, $(0, 3, 2) \leq (1, 3, 8)$, but $(0, 3, 2)$ and $(1, 3, 1)$ are incomparable.

Lemma 5.2 *Any subset S of \mathbf{N}^n with pairwise incomparable elements is finite.*

Proof: Induction on n . For $n = 1$ the subset has at most one element, so is finite. If $n > 1$ then let T be the subset of \mathbf{N}^{n-1} obtained from S by deleting the last coordinate from all elements, and removing the elements that are not minimal in the result. By induction T is finite, say $T = \{t_1, \dots, t_m\}$. Each t_i was obtained from some s_i by deleting the last coordinate. If s in S yields t after deleting the last coordinate, and then t is deleted because t_i is smaller, then the last coordinate of s is smaller than that of s_i (since all other coordinates are not smaller, and they are incomparable). This shows that among the $s \in S$ only finitely many last coordinates occur, and for any given value of the last coordinate there are finitely many points in S (by induction), so S is finite. \square

Fix some term order, say lex order. Let $\text{LT}(I)$ be the ideal generated by the leading terms of the elements of I . By the lemma $\text{LT}(I)$ has a finite basis $\{t_1, \dots, t_m\}$ consisting of monomials. Let t_i be the leading term of $f_i \in I$. Then $\{f_1, \dots, f_m\}$ is a basis of I , since if $f \in I$ and we divide f by f_1, \dots, f_m , the remainder lies in I so has leading term divisible by that of one of the f_i , contradiction, unless the remainder is 0. \square

6 Gröbner basis

A *Gröbner basis* of an ideal I is a basis $\{g_1, \dots, g_m\}$ of I such that the leading terms $\text{LT}(g_i)$ of the g_i generate the ideal $\text{LT}(I)$.

Using a Gröbner basis, the remainder after division is uniquely determined, independent of choice or ordering of the basis, and $f \in I$ if and only if the remainder after division of f by g_1, \dots, g_m is zero.

This solves the ideal membership problem, at least when we can find a Gröbner basis.

And one finds a Gröbner basis by repeatedly dividing each basis element found so far by the other elements and adding the remainder to the basis if it is nonzero.

More precisely, one defines so-called *S-polynomials*

$$S(f, g) := \frac{x^\gamma}{\text{LT}(f)}f - \frac{x^\gamma}{\text{LT}(g)}g$$

where x^γ is the least common multiple of the leading monomials of f and g . Now $\{g_1, \dots, g_m\}$ is a Gröbner basis iff the remainder of each $S(g_i, g_j)$ upon division by g_1, \dots, g_m is zero.

A Gröbner basis is large enough, but may be larger than necessary. It is called *minimal* when all of its elements have leading term not divisible by the leading term of one of the other elements. It is called *reduced* when all terms of every element are not divisible by the leading term of one of the other elements.

Theorem 6.1 *Given a term ordering, any ideal I in $k[x_1, \dots, x_n]$ has a unique reduced Gröbner basis.*