Gröbner Bases

Holly Cook ⇔ cookh@appstate.edu
Michael Kelley ⇔ kelleyma1@appstate.edu
Woody Madison ⇔ madisonrt@appstate.edu
Samwise Migirditch ⇔ migirditchsv@appstate.edu
Elisabeth Moore ⇔ mooreej@appstate.edu

[Please, no unsolicited emails.]

Thursday, May 1st 2014

In 1965 Bruno Buchberger introduced the notion of a Gröbner basis as well as his algorithm for computing them. Gröbner bases are incredibally useful tools for solving all sorts of algebraic problems. They are used in a wide variety of applications in areas such as computational biology and are even used in encryption schemes for many cell phones.

To indicate how important Buchberger's algorithm is, this algorithm simulataneously generalizes both the Euclidean algorithm (for finding GCD's of polynomials) and Gauss-Jordan elimination (for solving linear systems).

Although Gröbner bases can be discussed in a very general context, we will primarily stick to polynomials with complex coefficients in 3 variables: $\mathbb{C}[x, y, z]$.

Definition: A monomial ordering on $\mathbb{C}[x, y, z]$ is a linear orderings (think "less than") such that if $A < B$ for monomials A and B, then $CA < CB$ for any monomial C and in addition $1 < A$ for all monomials $A \neq 1$.

Two popular monomial orderings are the lexicographic and total degree orderings.

Lexicographic This is essentially alphabetic ordering:
$x^2y > xy^2 > xyz > xy > x > y^2 > z^3$.

Degree Lex This ordering first considers the total degree and then defaults to lexicographic ordering:
$x^2y > xy^2 > xyz > z^3 > xy > y^2 > x$.

Multivariate division extends standard single variable polynomial division.

We can reduce f by g to h, written as $f \underset{g}{\to} h$ if f contains a term which is a multiple of the leading term of g, say mg's leading term appears in f, and $h = f - mg$.

Given a set S of polynomials, we write $f \underset{S}{\to} h$ if $f \underset{g}{\to} h$ for some $g \in S$.

Finally, we write $f \underset{S}{\to}_+ h$ if $f \underset{g_1}{\to} h_1 \underset{g_2}{\to} h_2 \cdots \underset{g_\ell}{\to} h_\ell = h$ for some $g_1, \ldots, g_\ell \in S$ and polynomials $h_1, \ldots, h_\ell$.

If there is no $g \in S$ and polynomial h such that $f \underset{g}{\to} h$, we say f is reduced (mod S).

If f reduces to r (mod S), we call r a remainder of division of f by S.

Definition: A Gröbner basis S is a collection of polynomials such that division by S yields unique remainders.

Buchberger's algorithm allows one to take an arbitrary finite set of polynomials and find an equivalent Gröbner basis. (By equivalent we mean that they share a common solution set when treated as polynomial equations.)

Example of division: Let's divide $f = x^3y^3 + 2y^2$ by $S = \{g_1 = 2xy^2 + 4y^2 + 3x, g_2 = y^2 - 2y - 2\}$.

- $f - \frac{1}{2}x^2yg_1 = -2x^2y^3 - \frac{3}{2}x^3y + 2y^2 = h_1$
- $h_1 + xyg_1 = -\frac{3}{2}x^3y + 4xy^3 + 3x^2y + 2y^2 = h_2$
- $h_2 - 2yg_1 = -\frac{3}{2}x^3y + 3x^2y - 8y^3 - 6xy + 2y^2 = h_3$
- $h_3 + 8yg_2 = -\frac{3}{2}x^3y + 3x^2y - 6xy + 18y^2 + 16y = h_4$
- $h_4 - 18g_2 = -\frac{3}{2}x^3y + 3x^2y - 6xy + 52y + 36 = r$

Therefore, $f \underset{g_1}{\to} h_1 \underset{g_1}{\to} h_2 \underset{g_1}{\to} h_3 \underset{g_2}{\to} h_4 \underset{g_2}{\to} r.$

So $f \underset{S}{\to}_+ r$ where r is reduced mod S.

An application: Making change. $p^5 = n$, $p^{10} = d$, $p^{25} = q$, $p^{100} = b$. Then the Gröbner basis equivalent to $S = \{p^5 - n, p^{10} - d, p^{25} - q, p^{100} - b\}$ is $B = \{p^5 - n, d - n^2, nq - d^3, q - d^2n, q^4 - b\}$ (using the degree lex ordering).

Then 2 bucks (i.e. dollars), 5 quarters, 2 dimes, 3 nickels, and 8 pennies. Are represented by $f = b^2q^5d^2n^3p^8$.

f divided by B is $r = b^3q^2dnp^3$ which is 3 bucks, 2 quarters, 1 dime, 1 nickel, and 3 pennies (equivalent change with fewer "coins").

If we change to pure lexicographic ordering, we get $B = \{p^5 - n, n^2 - d, d^2n - q, nq - d^3, bn - d^3q^3, d^5 - q^2, q^4 - b\}$. When f is divided by this Gröbner basis, we get $r = b^3qd^4p^3$. This is 3 bucks, 1 quarter, 4 dimes, no nickels, and 3 pennies. Again we have equivalent change, but we used more "coins". However, we avoided the use of lower denomination coins *if possible*. In particular, we have no nickels.

We also discussed Gröbner bases for non-commutative rings and how these can be used to "compute proofs" of otherwise difficult statements.

We also discussed doomsday weapons and our future red-headed overlords.

References:

- *Ideals, Varieties, and Algorithms* by Cox, Little, and O'Shea
- *A First Course in Abstract Algebra* by Fraleigh (7^{th} edition)
- *An Introduction to Gröbner Bases* by Adams and Loustaunau
- *Commutativity Theorems: Examples in Search of Algorithms* by Wavrik
- *An Introduction to Commutative and Non-Commutative Gröbner Bases* by Mora

Thank you Cobra Commander!

Any Questions?