Buchberger's algorithm

From Wikipedia, the free encyclopedia

In computational algebraic geometry and computational commutative algebra, **Buchberger's algorithm** is a method of transforming a given set of generators for a polynomial ideal into a Gröbner basis with respect to some monomial order. It was invented by Austrian mathematician Bruno Buchberger. One can view it as a generalization of the Euclidean algorithm for univariate GCD computation and of Gaussian elimination for linear systems.

A crude version of this algorithm to find a basis for an ideal *I* of a polynomial ring *R* proceeds as follows:

Input A set of polynomials *F* that generates *I*
Output A Gröbner basis *G* for *I*

1. $G := F$
2. For every f_i, f_j in G, denote by g_i the leading term of f_i with respect to the given ordering, and by a_{ij} the least common multiple of g_i and g_j.
3. Choose two polynomials in G and let $S_{ij} = (a_{ij} / g_i)\ f_i - (a_{ij} / g_j)\ f_j$ *(Note that the leading terms here will cancel by construction)*.
4. Reduce S_{ij}, with the multivariate division algorithm relative to the set G until the result is not further reducible. If the result is non-zero, add it to G.
5. Repeat steps 1-4 until all possible pairs are considered, including those involving the new polynomials added in step 4.
6. Output G

The polynomial S_{ij} is commonly referred to as the *S*-polynomial, where *S* refers to *subtraction* (Buchberger) or *Syzygy* (others). The pair of polynomials with which it is associated is commonly referred to as critical pair.

There are numerous ways to improve this algorithm beyond what has been stated above. For example, one could reduce all the new elements of *F* relative to each other before adding them. If the leading terms of f_i and f_j share no variables in common, then S_{ij} will *always* reduce to 0 (if we use only f_i and f_j for reduction), so we needn't calculate it at all.

The algorithm terminates because it is consistently increasing the size of the monomial ideal generated by the leading terms of our set *F*, and Dickson's lemma (or the Hilbert basis theorem) guarantees that any such ascending chain must eventually become constant.

The computational complexity of Buchberger's algorithm is very difficult to estimate, because of the number of choices that may dramatically change the computation time. Nevertheless, T. W. Dubé has been proved[1] that the degrees of the elements of a reduced Gröbner basis are always bounded by

$$2\left(\frac{d^2}{2}+d\right)^{2^{n-1}},$$

where n is the number of variables, and d the maximal total degree of the input polynomials. This allows, in theory, to use linear algebra over the vector space of the polynomials of degree bounded by this value, for getting an algorithm of complexity $d^{2^{n+o(1)}}$.

On the other hand, there are examples[2] where the Gröbner basis contains elements of degree

$$d^{2^{\Omega(n)}},$$

and above upper bound of complexity is almost optimal, up to a constant factor in the second exponent). Nevertheless, such examples are extremely rare.

Since its discovery, many variants of Buchberger's have been introduced to improve its efficiency. Faugère's F4 and F5 algorithms are presently the most efficient algorithms for computing Gröbner bases, and allow to compute routinely Gröbner bases consisting of several hundreds of polynomials, having each several hundreds of terms and coefficients of several hundreds of digits.

See also [edit]

- Quine-McCluskey algorithm (analogous algorithm for Boolean algebra)
- Buchberger's algorithm discussed more extensively on Scholarpedia

References [edit]

- Buchberger, B. (August 1976). "Theoretical Basis for the Reduction of Polynomials to Canonical Forms". *ACM SIGSAM Bull.* (ACM) **10** (3): 19–29. doi:10.1145/1088216.1088219. MR 0463136.
- David Cox, John Little, and Donald O'Shea (1997). *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Springer. ISBN 0-387-94680-2.
- Vladimir P. Gerdt, Yuri A. Blinkov (1998). *Involutive Bases of Polynomial Ideals*, Mathematics and Computers in Simluation, 45:519ff

1. ^ doi:10.1137/0219053
   This citation will be automatically completed in the next few minutes. You can jump the queue or expand by hand
2. ^ doi:10.1016/0001-8708(82)90048-2
   This citation will be automatically completed in the next few minutes. You can jump the queue or expand by hand

External links [edit]

- Hazewinkel, Michiel, ed. (2001), "Buchberger algorithm", *Encyclopedia of Mathematics*, Springer, ISBN 978-1-55608-010-4
- Weisstein, Eric W., "Buchberger's Algorithm", *MathWorld*.

Categories: Computer algebra | Rewriting systems | Algebraic geometry | Commutative algebra