Gröbner Bases and Macaulay Matrices

Bruno Buchberger

Research Institute for Symbolic Computation
Johannes Kepler University, Linz, Austria

Talk at SYNASC 2017
Sep 23, 2017, Timisoara

Computing Gröbner Bases by S-Polynomials

An Inconstructive Method for Computing Gröbner Bases

Turning the Inconstructive Method into an Algorithm

Experiments

Computing Gröbner Bases by S-Polynomials

An Inconstructive Method for Computing Gröbner Bases

Turning the Inconstructive Method into an Algorithm

Experiments

Gröbner Bases Introduction

In BB's PhD thesis 1965 (and aequ math 1970):

- Introduction of the **Notion** of Gröbner bases: F is **Gröbner basis** iff reduction w.r.t. F is unique.
- **Charaterization** Theorem: F is Gröbner basis iff all **S-polynomials** of F reduce to 0 w.r.t. F.

  S-polynomial of f and g := u . f - v . g (with suitable power products u, v)
- Note: The Charaterization Theorem is an algorithm for deciding whether a given F is a Gröbner basis!
- **Algorithm for constructing Gröbner bases**: Iterate formation of S-polys and add non-zero remainders.
- **Correctness** of algorithm: by the Characterization Theorem.
- **Termination** of algorithm: by (a re-invention) of Dixon's Lemma.

Gröbner Bases Introduction

In BB's PhD thesis 1965 (and aequ math 1970):

- **Applications**:

  linearly independent basis for residue class ring modulo Ideal(F),
  multiplication table of associative algebra modulo Ideal(F),
  complete solution of algebraic systems F = 0,
  computation of Hilbert function of F.

- **Complete implementation** of the algorithm on ZUSE Z23 computer and example computations.

- A **first complexity analysis** for the bivariate case.

References:

B. Buchberger.
An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal (German).
PhD thesis, Mathematical Institute, University of Innsbruck, Austria, **1965.**
(English Translation in Journal of Symbolic Computation, Special Issue on Logic, Mathematics, and Computer Science. Vol. 41, pp. 475 - 511, 2006).

B. Buchberger.
An Algorithmic Criterion for the Solvability of Algebraic Systems of Equations (German). Aequationes Mathematicae, Vol. 3, pp. 374–383, 1970.
(English translation in B.Buchberger, F.Winkler eds.: Gröbner Bases and Applications, London Math.Society Lecture Note Series. Vol 251, pp. 535–545, Cambridge University Press.1998.

Improvements

BB 1979: Introduction of **chain criterion** for eleminating the consideration of (many) unnecessary S-polynomials. Makes algorithm, in many cases, much more efficient.

BB 1985: Good strategy (in many, not in all cases): **First, completely "auto-reduce" (= "Gauß'schen elimination")** . Then only S-polynomials! (Sometimes, not necessary any more!)

Huge literature on the subject :

Many (approx. 2000) **papers** on theory, algorithmic improvements, complexity of Gröbner bases.

Many (approx. 30) **textbooks**.

Many **implementations** (*Mathematica*, Maple, Singular, CoCoA, ...)

Most algorithms and implementations for Gröbner bases **based on S-polynomials approach.**

Approaches Not Based on S-Polynomials (but, rather on "Linear Algebra on Power Products")

- **Gröbner's original 1954 idea** for obtaining a multiplication table for the associative algebra modulo Ideal(F). (Termination was a question and this lead to BB 65.)
- **Mayr's approach 1996:** for obtaining an exponential space upper bound for Gröbner bases computation.
- **Faugére's et al 1999, 2002 approach**: F4, (termination still based on S-polynomials ?), F5 (termination based on ?)
- **Grigoriev approach 2000:** for results on complexity.

References:

B. Buchberger.
A Criterion for Detecting Unnecessary Reductions in the Construction of Gröbner Bases. In Proceedings of EUROSAM' 79, Springer LNCS, pp. 3–21, 1979.

B. Buchberger
Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory.
Chapter 6 in: N.K. Bose (ed.), Multidimensional Systems Theory - Progress, Directions and Open Problems in Multidimensional Systems Theory, Reidel Publishing Company, Dodrecht - Boston - Lancaster, 1985, pp. 184-232.

K. Kühnle, E.W. Mayr.
Exponential Space Computation of Gröbner Bases. Proceedings of ISSAC'96, Zurich, ACM, pp. 63 - 71.

J.C. Faugére.
A New Efficient Algorithm for Computing Groebner Bases (F4). h
Journal of Pure and Applied Algebra, 139 : 61–88, 1999.

J.C. Faugére.
A New Efficient Algorithm for Computing Groebner Bases Without Reductions to Zero (F5).
ISSAC 2002, pages 75–83, 2002.

D. Grigoriev.
Bounds on Numbers of Vectors of Multiplicities for Polynomials which are Easy to Compute.
Proc.ACM Intern.Conf.Symbolic and Algebraic Computations, Scotland, 2000, p .137 - 145.

Connection to "Linear Algebra on Power Products"

I have often been asked what is the **relation of Gröbner bases with resultants**.

Repeated resultants (eliminating variables one by one) for solving systems is **not the same** as computing Gröbner bases!

More appropriate view:

Univariate case:

GCD by **Euclid** versus GCD by triangularizing the **Sylvester matrix** (solvability by determinant criterion).

Linear multivariate case:

decoupled by **Gauß** versus **decoupled** by triangularizing the **coefficient matrix** (solvability by determinant criterion).

Non-linear multivariate case:

Gröbner basis by **S-polys** versus **Gröbner basis** by triangularizing which (?) **matrix** (solvability by determinant criterion).

Computing Gröbner Bases by S-Polynomials

An Inconstructive Method for Computing Gröbner Bases

Turning the Inconstructive Method into an Algorithm

Experiments

Macaulay - Triangularize - Contour: A Method but Not an Algorithm

In 1983, I proved that the following steps yield a Gröbner basis for any polynomial set F:

S:= Macaulay(F):= set of all multiples u . f ("shifts") of the polynomials f in F with all power products u.

Consider the elements in Macaulay(F) as rows of an (infinite) matrix with the columns numbered by the power products and ordered according to the admissible ordering of power products w.r.t. to which one wants to find the Groebner basis for F.

T:= Triangularized(S). (In fact this is nothing else then a special kind of auto-reduction of the polynomials in the matrix.)

C:= Contour(T) := the set of those polynomials in T whose leading power products are not multiple of the leading power product of any other polynomial in T.

Then C is a finite Groebner basis of the original set F. (Finiteness can be proved, again, by applying Dixon's lemma.)

Proof Sketch:

VectorSpace(Sylvester (F)) = Ideal(F).

VectorSpace(Sylvester (F)) = VectorSpace(Triangularized(Sylvester (F)).

Leading powerproduct of any f in Ideal(F) must occur in Triangularized(Sylvester(F)) and, hence can be reduced by a polynomial in

Contour (Triangularized(Sylvester(F))).

In fact, I had this result much earlier but I did not think it was worth publishing because it only a "method", not an algorithm.

Reference:

B. Buchberger.
Miscellaneous Results on Groebner Bases for Polynomial Ideals II.
Technical Report 83/1, University of Delaware, Department of Computer and Information Sciences, 1983.

Upper Bound Would Lead to an Algorithm

If we knew a **finite a priori bound on the degrees** of the multiplies u . f that have to go into Sylvester(F) in order to guarantee that

Contour (Triangularized (Sylvester(F)))

is a Gröbner basis for F, then **the above method would be an algorithm.**

Upper bound in terms of

n (number of polys in F),
r (number of polynomials in F),
d (maximum degree of polynomials in F).

Over the years, I proposed this problem of finding such an upper bound a couple of times to my PhD students. However, only recently (2014) one of them, **Manuela Wiesinger-Widi,** stayed with this problem and solved it by combining Hermann's and Dube's bounds in a clever way.

Computing Gröbner Bases by S-Polynomials

An Inconstructive Method for Computing Gröbner Bases

Turning the Inconstructive Method into an Algorithm

Experiments

Two Known Bounds

Hermann Bound: If g is in Ideal(F) then there exist $q_1, ..., q_r$ such that

$$g = \sum_{i=1}^{r} (q_i \cdot F_i)$$

and, for all i,

$$\text{degree}(q_i) \leq \text{degree}(g) + \sum_{j=0}^{n-1} (r\,d)^{2^j}.$$

Dubé Bound: If G is the reduced Gröbner basis of F then, for all g in G,

$$\text{degree(g)} \leq 2\left(\frac{d^2}{2} + d\right)^{2^{n-1}}.$$

References:

T.W. Dubé.
The Structure of Polynomial Ideals and Gröbner Bases.
SIAM Journal on Computing, 19 (4) : 750–773, 1990.

G. Hermann.
The Question of Finitely Many Steps in Polynomial Ideal Theory (German).
Mathematische Annalen, 95 : 736–788, 1926.
(English translation in ACM SIGSAM Bull.32 (3), pages 8–30, 1998.)

Wiesinger's Theorem

Theorem (Manuela Wiesinger-Widi 2014): In the above procedure, it suffices to take the power products u with degree less or equal to

$$2\left(\frac{d^2}{2}+d\right)^{2^{n-1}}+\sum_{j=0}^{n-1}(r\,d)^{2^j}.$$

In fact, the resulting Groebner basis will be head-reduced.

Also, by the same approach, the following theorem can be proved.

Theorem (Manuela Wiesinger-Widi 2014): If, in the above procedure, one considers the matrix of multiples u . f with power products u whose degree is less or equal

$$\sum_{j=0}^{n-1}(r\,d)^{2^j}$$

then 1 is in Ideal(F) if and only if the above procedure yields a matrix containing a polynomial with leading power product 1.

Note: The above **Macaulay matrix** seems to be the appropriate analogue to the univariate Sylvester matrix in the univariate case.

Reference:

M. Wiesinger-Widi.
Gröbner Bases and Generalized Sylvester Matrices.
Ph.D. Thesis, Johannes Kepler University, Institute for Symbolic Computation, submitted 2014.

Proof of Wiesinger's Theorem

Lemma: If G is a finite Gröbner basis for F and the finite (truncated Sylvester) matrix S that contains all the multiples u . f with f in F and the power product u occuring in one of the q_i of the presentations

$$g = \sum_{i=1}^{r} (q_i \cdot F_i)$$

of the polynomials in G, and T = Triangularized(S), then Contour(T) is also a (head-reduced) Gröbner basis of F.

Proof of Lemma: G ⊆ VectorSpace(S) = Vectorspace (Triangularized(S)). Every leading power product of a polynomial g in G must occur among the leading power products of T since T is triangularized. By a wellknown property of Gröbner bases, all polys in G that are not on Contour(T) can be canceled.

Proof of First Theorem :
By Dubé, we know that there exists a Gröbner basis G for F with

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

for all g in G.
By Hermann, each of these g has a presentation

$$g = \sum_{i=1}^{r} (q_i \cdot F_i)$$

such that, for all i,

$$\text{degree}(q_i) \leq \text{degree}(g) + \sum_{j=0}^{n-1} (r\,d)^{2^j}.$$

Hence, if we take all the multiples u . f described in the Theorem into the initial (truncated) Sylvester matrix, by the above Lemma, the contour of the triangularized matrix is a (head-reduced) Gröbner basis.

Proof of Second Theorem : Similar. Note that { 1} is a Gröbner basis. Hence degree(g) in the previous proof becomes zero.

Is the Macaulay / Triangularize / Contour Algorithm Practical?

The method, at first sight, is **not "practical"** for computing a Gröbner basis of F:

- The polys in the S-poly algorithm for Gröbner bases, typically, stay way below the above upper degree bounds!
- The S-poly algorithm for Gröbner bases, typically, only produces very few of the rows in Macaulay(F).

(Example: The Gröbner basis computation of

$$\{-x + x\,y^2,\ x^2\,y - x\}$$

by S-polynomials does not exceed degree four whereas the above bound, for this case, would request us to first set up a matrix with polynomials of up to degree 155.)

In other words, BB 1965 **S-poly algorithm** can be considered as an efficient way of **avoiding** to work with big Macaulay matrices.

Analogy in case n=2: **Euclid's algorithm** can be considered as an efficient way of **avoiding** to work with big Macaulay matrices.

A Frame for Faugére's et al. and Habicht's Approach

Anyway, the above results can be seen as a **theoretical frame for the Gröbner 1954 approach and more recent algorithms** for constructing Gröbner bases (Faugére F4 and F5, Grigoriev 2000).

Also, the above theorem and algorithm suggests to **extend Habicht's 1948 theory of subresultants (**for the univariate case), which gives a priori estimates on the coefficients that may appear in GCD computations, to the general case of Gröbner bases. This could also have relevance for the **numeric computation** of Gröbner bases.

A Side-Step: Automated Proofs in Gröbner Bases Theory

In the **Theorema** Project (see today **Wolfgang Windsteiger's** talk), we take Gröbner bases theory as a benchmark for automated formal proving.

My former PhD student **Alexander Maletzky** did a complete implementation of Gröbner bases theory and is now working on the Macaulay-based theory.

Computing Gröbner Bases by S-Polynomials

An Inconstructive Method for Computing Gröbner Bases

Turning the Inconstructive Method into an Algorithm

Experiments

See Groebner / Macaulay Laboratory.

One sees that the Macaulay / Triangularize / Contour may be practically interesting but much more theory and experimenting is necessary.