Advanced Studies in Pure Mathematics 77, 2018
The 50th Anniversary of Gröbner Bases
pp. 25–33

Gröbner bases computation by triangularizing Macaulay matrices

Bruno Buchberger

Abstract.

In my PhD thesis 1965 and the subsequent publication 1970 in aequationes mathematicae, I introduced the notion of Gröbner bases and proved a characterization theorem for Gröbner bases on which an algorithm for constructing Gröbner bases can be based. The main idea for the theorem and the algorithm was the notion of "S-polynomials". Most of the subsequent work on the algorithmic theory of Gröbner bases, including the implementation of the Gröbner bases technology in mathematical software systems like Mathematica, Maple, etc. was based on this approach.

In the early eighties, I proposed a completely different strategy for computing Gröbner bases proceeding by the following three steps:

1. Produce the set of all multiples $u.f$ of the polynomials f in the initial basis F by all power products u (which we call "generalized Sylvester matrix" or "Macaulay matrix" of F).

2. Triangularize this matrix.

3. Take the "contour" in the diagonal of the matrix, i.e. the set of all those polynomials in the diagonal whose leading power product is not a multiple of the leading power product of any other polynomial in the diagonal.

It is easy to prove that the above procedure yields a Gröbner basis if one starts with the infinite matrix of *all* shifts $u.f$. However, of course, this is not an algorithm. So I posed the question whether one can give an a-priori bound on D so that, if one puts all shifts $u.f$ with degree of u smaller than D to the initial matrix, the matrix resulting by triangularization and contour formation will be a Gröbner basis for F. Over the years, several people tried to find such a bound but only recently (2014) my PhD student Manuela Wiesinger-Widi was able to establish such a bound combining known bounds by G. Hermann and T. W. Dubé for the ideal membership and the Gröbner bases degree problem, respectively.

Received November 6, 2016.
2010 *Mathematics Subject Classification.* 33F10, 13P10.
Key words and phrases. Gröbner basis, S-polynomial, Macaulay matrix.

§1. Computing Gröbner Bases by S-Polynomials and the Problem of Constructing a Corresponding Macaulay Matrix

My PhD thesis[1, 2] contains the following results (for sets of multivariate polynomials F):

- Introduction of the notion of Gröbner bases: F is Gröbner basis iff reduction w.r.t. F is unique.
- Characterization 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 certain power products u, v.)
  (Note: The Characterization Theorem is an algorithm for deciding whether a given F is a Gröbner basis!)
- Algorithm for constructing Gröbner bases: Iterate the formation of S-polys and add non-zero remainders.
- Correctness of the algorithm: by the Characterization Theorem.
- Termination of the algorithm: by (a re-invention and new proof) of Dixon's Lemma.
- Application: Algorithm for constructing a linearly independent basis for the residue class ring modulo the ideal generated by F.
- Application: Algorithm for constructing the multiplication table for the associative algebra formed by this linearly independent basis.
- Application: Algorithm for deciding the solvability and zero-dimensionality of systems F of algebraic equation and computing all roots with multiplicities (in the zero-dimensional case).
- Application: Computation of the Hilbert function for Ideal(F).
- Complete implementation of the algorithm on the ZUSE Z23 computer and example computations.
- A first complexity analysis of the algorithm for the bivariate case.

Later, in [3], I introduced the technique of "criteria" (in particular, the chain criterion) for eliminating the consideration of (many) unnecessary S-polynomials in the course of computing Gröbner bases. In many cases, this makes the algorithm much faster. In [5], I proposed the technique "first auto-reduce, only then consider S-polynomials". (In the terminology of the current paper, "auto-reduction" basically is triangularization of the coefficient matrix of polynomials that have been computed up to a certain stage of the algorithm.) Many times, after

auto-reduction, no or only a few S-polynomials have to be considered. However, only heuristics are available on when this happens.

There is a huge literature on the theory of Gröbner bases and their computation using the S-polynomials approach, see [6]. The use of S-polynomials was the prevailing approach to algorithmic Gröbner bases theory. However, there were exceptions:

- Gröbner's original 1954 idea [11] for obtaining a multiplication table for the associative algebra modulo Ideal(F). (Termination was a question and this lead to [1].)
- Mayr's approach [14] for obtaining an exponential space upper bound for Gröbner bases computation.
- Faugére's et al. approach (F4, F5) [8, 9]: Termination of F4 was still based on S-polynomials.
- Grigoriev's approach [10] for bounds for the number of vectors in Macaulay-like matrices.

§2. Gröbner Bases and Resultants

I have often been asked about the relation of Gröbner bases with resultants and related notions (Sylvester matrices, Macaulay matrices) and some people thought that the effect of repeated resultants on bivariate polynomials (eliminating variables one by one) is the same as a Gröbner basis computation. However, definitely, this is not the case.

A more appropriate view is the following:

- In the univariate case, an alternative for computing the GCD of a set F of two polynomials by Euclid's algorithm is the triangulariziation of the Sylvester matrix of F and solvability can also be decided by calculating the determinant of the Sylvester matrix (the resultant). By Habicht's theory [12, 15] one can in fact understand Euclid's algorithm as a particular way of triangularizing the Sylvester matrix.
- In the linear multivariate case, an alternative for variable elimination by Gauss' algorithm is the triangularization of the extended coefficient matrix. Solvability can again be decided by calculating the determinant of the coefficient matrix. In this case, Gauss' algorithm on the linear polynomials and triangularization of the coefficient matrix is in fact basically identical.
- In the non-linear multivariate case, we can compute a Gröbner basis of the initial polynomials by my S-polynomial algorithm (which specializes to Euclid and Gauss in the univariate and linear multivariate cases, respectively). Now the question is,

whether there is a corresponding matrix whose triangularization yields a Gröbner basis and whether my S-polynomial algorithm can be considered as just a special way of triangularizing this matrix.

In her PhD thesis, my student M. Wiesinger-Widi [17], solved the first part of the question thoroughly, i.e. we now can construct a matrix from the coefficients of a given set F of polynomials (a "generalized Sylvester matrix" or "Macaulay matrix") whose triangularization contains a Gröbner basis for F. It is not yet clear, though, whether the computation of Gröbner bases by S-polynomials can be considered as just one special way of triangularizing this matrix, i.e. whether a kind of "generalized Habicht's theory" could be established.

§3. An Inconstructive Method for Computing Gröbner Bases by Triangularizing a Macaulay Matrix

In [4], I proved that the following steps yield a Gröbner basis for any polynomial set F. (Note: we use "Sylvester" interchangeably with "Generalized Sylvester" and "Macaulay"):

$S :=$ Sylvester$(F) :=$ set of all multiples $u.f$ of the polynomials f in F with all power products u.

Consider the elements in Sylvester(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 Gröbner basis for F.

$T :=$ Triangularized(S). (In fact this is nothing else but a special kind of auto-reduction in the terminology of [5].)

$C :=$ 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 Gröbner 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)).

The leading power product 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 is only a "method", not 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. The upper bound should be expressed in terms of

n (number of polys in F),
r (number of polynomials in F),
and 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), Manuela Wiesinger-Widi, solved it by combining Hermann's and Dube's bounds in a clever way, see the theorems in the next section.

§4. Turning the Inconstructive Method into an Algorithm

Theorem 4.1. (***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 Gröbner basis will be head-reduced.

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

Theorem 4.2. (***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 **(generalized) Sylvester matrix** is the appropriate analogue to the univariate Sylvester matrix in the general, multivariate, case in the sense I explained in the introduction. The theorems were proved in 2014, the thesis appeared in 2015.

Proof of the Wiesinger-Widi theorems: The proof uses Hermann's and Dube's bound:

Hermann's Bound [13]**:** If g is in Ideal(F) then there exist $q_1, \ldots, q_r$ such that

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

and, for all i,

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

Dubé's Bound [7]: If G is the reduced Gröbner basis of F then, for all g in G,

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

The proof of Wiesinger-Widi's theorems now proceed as follows:

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

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

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

Proof of Lemma: $G \subseteq \text{VectorSpace}(S) = \text{Vectorspace}(\text{Triangularized}(S))$. 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 well-known property of Gröbner bases, all polynomials in G that are not on Contour(T) can be canceled.

Proof of Theorem 4.1:

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

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

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 Theorem 4.2: Similar. Note that $\{1\}$ is a Gröbner basis. Hence degree(g) in the previous proof becomes zero.

§5. Remarks on Applications and Future Research

The method 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 Sylvester(F).

(Example: The Gröbner basis computation of

$$\left\{-x + xy^2,\ x^2y - x\right\}$$

w.r.t. a total degree ordering, 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 [17], in fact, the author gives much lower bounds for the special case of binomials. However, still, concrete computations using S-polynomials typically stay significantly below these bounds.)

In other words, my 1965 Gröbner bases algorithm based on S-polynomials 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 Sylvester matrices.

Anyway, the above results can be seen as a theoretical frame for the Gröbner 1954 approach and more recent algorithms for constructing Gröbner bases ([8, 9, 10]).

Also, the above theorem and algorithm suggests to extend Habicht's 1948 theory of subresultants (introduced for the univariate case) to the general case of Gröbner bases. Habicht gives a priori estimates on the coefficients that may appear in GCD computations, see also [15]. A general Habicht theory could also have applications for the numeric computation of Gröbner bases: If we knew exactly, which subdeterminants

of the generalized Sylvester matrices may occur in the computation of Gröbner bases, we could derive lower bounds for the size of possible coefficients in the computation and distinguish between "very small" and "zero" in numerical computation. In addition, Habicht's theory gives very subtle predictive information on common factors in the coefficients of polynomials occuring in GCD computation. Similar results can be expected from a detailed study of the generalized Sylvester matrices. This study is not yet undertaken but I think it would be worthwhile. These investigations are quite demanding in terms of proof technology and, for me, were an important motivation for initiating the Theorema project on automated theorem proving in 1995. A recent PhD thesis of another student of mine [16] in the frame of the Theorema project gives some impression about how formalization and automated theorem proving could help in such investigations.

References

[1] 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, **41**, 2006, pp. 475–511.)

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

[3] B. Buchberger, A Criterion for Detecting Unnecessary Reductions in the Construction of Gröbner Bases, In: Proceedings of EUROSAM' 79, Springer LNCS, **72**, 1979, pp. 3–21.

[4] B. Buchberger, Miscellaneous Results on Gröbner-Bases for Polynomial Ideals II, Technical Report 83-1, Department of Computer And Information Sciences, University of Delaware, 1983.

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

[6] B. Buchberger, M. Rady, H. Rahkooy, T. Vo Ngoc, M. Wiesinger-Widi, W. Windsteiger, and A. Zapletal, Gröbner Bases Bibliography, http://www.risc.jku.at/Groebner-Bases-Bibliography/.

[7] T.W. Dubé, The Structure of Polynomial Ideals and Gröbner Bases, SIAM Journal on Computing, **19/4**, 1990, pp. 750–773.

[8] J.C. Faugére, A New Efficient Algorithm for Computing Groebner Bases (F4), Journal of Pure and Applied Algebra, **39**, 1999, pp. 61–88.

[9] J.C. Faugére, A New Efficient Algorithm for Computing Groebner Bases Without Reductions to Zero (F5), Proceedings of ISSAC 2002, pp. 75–83.

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

[11] W. Gröbner, Über die Eliminationstheorie (On Elimination Theory), Monatshefte für Mathematik, **55**, 1950, pp. 71–78.
(English translation by M. Abramson in ACM SIGSAM Bulletin, **32/2**, 1998, pp. 40–46.)

[12] W. Habicht, Eine Verallgemeinerung des Sturmschen Wurzelzählverfahrens (A Generalization of Sturm's Method for Root Counting), Comm. Math. Helvetici, **21**, 1948, pp. 99–116.

[13] G. Hermann, The Question of Finitely Many Steps in Polynomial Ideal Theory (German), Mathematische Annalen, **95**, 1926, pp. 736–788.
(English translation in ACM SIGSAM Bull., **39/3**, 1998, pp. 8–30.)

[14] K. Kühnle, and E.W. Mayr, Exponential Space Computation of Gröbner Bases, Proceedings of ISSAC'96, Zürich, ACM, pp. 63–71.

[15] R. Loos, Generalized Polynomial Remainder Sequences, In: Computer Algebra - Symbolic and Algebraic Computation, (eds. B. Buchberger, G.E. Collins, and R. Loos), Springer Verlag, Wien, 1982, pp. 115–137.

[16] A. Maletzky, Computer-Assisted Exploration of Gröbner Bases Theory in Theorema, PhD Thesis, Johannes Kepler University, Research Institute for Symbolic Computation, Linz / Hagenberg, Austria, 2016.

[17] M. Wiesinger-Widi, Gröbner Bases and Generalized Sylvester Matrices, Ph.D. Thesis, Johannes Kepler University, Research Institute for Symbolic Computation, Linz / Hagenberg, Austria, 2015.

Research Institute for Symbolic Computation (RISC),
Johannes Kepler University, Linz, Austria
E-mail address: bruno.buchberger@risc.jku.at