Gröbner Bases:

A Short Introduction for Systems Theorists

Bruno Buchberger

Research Institute for Symbolic Computation
University of Linz, A4232 Schloss Hagenberg, Austria
Buchberger@RISC.Uni-Linz.ac.at

Abstract. In this paper, we give a brief overview on Gröbner bases theory, addressed to novices without prior knowledge in the field. After explaining the general strategy for solving problems via the Gröbner approach, we develop the concept of Gröbner bases by studying uniquenss of polynomial division ("reduction"). For explicitly constructing Gröbner bases, the crucial notion of S-polynomials is introduced, leading to the complete algorithmic solution of the construction problem. The algorithm is applied to examples from polynomial equation solving and algebraic relations. After a short discussion of complexity issues, we conclude the paper with some historical remarks and references.

1 Motivation for Systems Theorists

Originally, the method of Gröbner bases was introduced in [3, 4] for the algorithmic solution of some of the fundamental problems in commutative algebra (polynomial ideal theory, algebraic geometry). In 1985, on the invitation of N. K. Bose, I wrote a survey on the Gröbner bases method for his book on n-dimensional systems theory, see [7]. Since then quite some applications of the Gröbner bases method have been found in systems theory. Soon, a special issue of the Journal of Multidimensional Systems and Signal Processing will appear that is entirely devoted to this topic, see [11]. Reviewing the recent literature on the subject, one detects that more and more problems in systems theory turn out to be solvable by the Gröbner bases method:

- factorization of multivariate polynomial matrices,
- solvability test and solution construction of unilateral and bilateral polynomial matrix equations, Bezout identity,
- design of FIR / IIR multidimensional filter banks,

- stabilizability / detectability test and synthesis of feedback stabilizing
- compensator / asymptotic observer,
- synthesis of deadbeat or asymptotic tracking controller / regulator,
- constructive solution to the *n*D polynomial matrix completion problem,
- computation of minimal left annhilators / minimal right annhilators,
- elimination of variables for latent variable representation of a behaviour,
- computation of controllable part; controllability test,
- observability test,
- computation of transfer matrix and "minimal realization",
- solution of the Cauchy problem for discrete systems,
- testing for inclusion; addition of behaviors,
- test zero / weak zero / minor primeness,
- finite dimensionality test,
- computation of sets of poles and zeros; polar decomposition,
- achievability by regular interconnection,
- computation of structure indices.

In [11], I gave the references to these applications and I also presented an easy introduction to the theory of Gröbner bases by giving a couple of worked-out examples. In this paper, I will give an introduction to Gröbner bases in the style of a flyer for promotion that just answers a couple of immediate questions on the theory for newcomers. Thus, [11] and the present paper are complementary and, together, they may provide a quick and easy introduction to Gröbner bases theory, while [7] provides a quick guide to the application of the method to fundamental problems in commutative

2 Why is Gröbner Bases Theory Attractive?

Gröbner bases theory is attractive because

- the main *problem* solved by the theory can be explained in five minutes (if one knows the operations of addition and multiplication on polynomials),
- the *algorithm* that solves the problem can be learned in fifteen minutes (if one knows the operations of addition and multiplication on polynomials),

- the *theorem* on which the algorithm is based is nontrivial to (invent and to) prove,
- many *problems* in seemingly quite different areas of mathematics can be reduced to the problem of computing Gröbner bases.

3 What is the Purpose of Gröbner Bases Theory?

The method (theory plus algorithms) of Gröbner bases provides a uniform approach to solving a wide range of problems expressed in terms of *sets of multivariate polynomials.* Areas in which the method of Gröbner bases has bee applied successfully are:

- algebraic geometry, commutative algebra, polynomial ideal theory,
- invariant theory,
- automated geometrical theorem proving,
- coding theory,
- integer programming,
- partial differential equations,
- hypergeometric functions,
- symbolic summation,
- statistics,
- non-commutative algebra,
- numerics (e.g. wavelets construction), and
- systems theory.

The book [9] includes surveys on the application of the Gröbner bases method for most of the above areas. In commutative algebra, the list of problems that can be attacked by the Gröbner bases approach includes the following:

- solvability and solving of algebraic systems of equations,
- ideal and radical membership decision,
- effective computation in residue class rings modulo polynomial ideals,
- linear diophantine equations with polynomial coefficients ("syzygies"),
- Hilbert functions,

- algebraic relations among polynomials,
- implicitization,
- inverse polynomial mappings.

4 How Can Gröbner Bases Theory be Applied?

The general strategy of the Gröbner bases approach is as follows: Given a set F of polynomials in $K[x_1, \ldots, x_n]$ (that describes the problem at hand)

- we *transform* F into another set G of polynomials "with certain *nice properties*" (called a "Gröbner basis") such that
- F and G are "*equivalent*" (i.e. generate the same ideal).

From the theory of GB we know:

- Because of the "nice properties of Gröbner bases", many *problems that are difficult for general F are "easy" for Gröbner bases G*.
- There is an *algorithm* for transforming an arbitrary F into an equivalent Gröbner basis G.
- The solution of the problem for G can often be easily *translated back* into a solution of the problem for F.

Hence, by the properties of Gröbner bases and the possibility of transforming arbitrary finite polynomial sets into Gröbner bases, a whole range of problems definable in terms of finite polynomial sets becomes algorithmically solvable.

5 What are Gröbner Bases?

5.1 Division ("Reduction") of Multivariate Polynomials

We first need the notion of division (or "reduction") for multivariate polynomials. Consider, for example, the following bivariate polynomials g, f_1, and f_2, and the following polynomial set F:

$$g = x^2 y^3 + 3 x y^2 - 5 x, \tag{1}$$

$$f_1 = x y - 2 y, \quad f_2 = 2 y^2 - x^2, \tag{2}$$

$$F = \{f_1, f_2\}. \tag{3}$$

The monomials in these polygonomials are ordered. There are infinitely many orderings that are "admissible" for Gröbner bases theory. The most important ones are the lexicographic orderings and the orderings that, first, order power products by their degree and, then, lexicographically. In the example above, the monomials are ordered lexicographically with y ranking higher than x and are presented in descending order from left to right. The highest (left-most) monomial in a polynomial is called the "leading" monomial in the polynomial.

One possible division ("reduction") step that "reduces the polymomial g modulo f_1 " proceeds as follows:

$$h = g - (3\,y)\,f_1 \;=\; -5\,x + 6\,y^2 + x^2\,y^3, \tag{4}$$

i.e. in a reduction step of g modulo f_1, by subtracting a suitable monomial multiple of f_1 from g, one of the monomials of g should cancel against the leading monomial of $-(3\,y)\,f_1$. We write

$$g \;\longrightarrow_{f_1}\; h \tag{5}$$

for this situation (read: "g reduces to h modulo f_1 ").

5.2 In General, Many Reductions are Possible

Given a set F of polynomials and a polynomial g, many different reductions of g modulo polynomials in F may be possible. For example, for g and F as above, we also have

$$h_2 = g - (x\,y^2)\,f_1 \;=\; -5\,x + 3\,x\,y^2 + 2\,x\,y^3, \tag{6}$$

$$h_3 = g - \left(\frac{1}{2}\,x^2\,y\right) f_2 \;=\; -5\,x + \frac{x^4\,y}{2} + 3\,x\,y^2, \tag{7}$$

and, hence,

$$g \;\longrightarrow_{f_1}\; h_2, \tag{8}$$

$$g \;\longrightarrow_{f_2}\; h_3. \tag{9}$$

5.3 Multivariate Polynomial Division Always Terminates But is Not Unique

We write

$$g \;\longrightarrow_{F}\; h \tag{10}$$

if

$$g \longrightarrow_f h \tag{11}$$

for some $f \in F$, and we write

$$g \longrightarrow^*_F h \tag{12}$$

if g reduces to h by finitely many reduction steps w.r.t. F. Also, we write

$$\underline{h}_F \tag{13}$$

if h cannot be reduced further (is "in reduced form") w.r.t. F. Here are a couple of fundamental facts on the notion of reduction:

Fact (Termination): For any g and F, there are no infinite chains of reduction steps modulo F starting from g.

Fact (Reduction is Algorithmic): There is an algorithm RF that produces a reduced form w.r.t. F for any given polynomial g, i.e., for all g and F,

$$g \longrightarrow_F^* \underline{\mathrm{RF}(F, g)}_F. \tag{14}$$

An example of such an algorithm is the iteration of the following operation: Given g, consider the polynomials $f \in F$ until you find one whose leading power product divides one of the power products in g. If you found such an f and power product in g execute the corresponding reduction step. If not, stop.

Fact (Non-uniqueness): Given g and F, there may exist h and k, such that

$$\underline{h}_F \longleftarrow_F^* g \longrightarrow_F^* \underline{k}_F \tag{15}$$

but $h \neq k$.

5.4 Definition of Gröbner Bases

Now we define Gröbner bases to be sets of polynomials whose corresponding reduction is unique:

Definition:

F is a *Gröbner basis* $:\Longleftrightarrow$ $\longrightarrow_F$ is unique, i.e.

$$\forall_{g,h,k} \left(\underline{h}_F \longleftarrow_F^* g \longrightarrow_F^* \underline{k}_F \implies h = k \right).$$

5.5 The "Application Theory of Gröbner Bases"

At first sight, one may not see why the defining property of Gröbner bases should play any fundamental role. The importance of this property stems from the the following facts:

Fact: Gröbner bases have many "nice properties" and hence, for Gröbner bases, many fundamental problems can be solved by "easy" algorithms.

Example (The "Main Problem of Polynomial Ideal Theory"):

Let F be a set of polynomials:

If F is a Gröbner basis, then:

$f \in \text{Ideal}(F) \iff f \longrightarrow^*_F 0$.

Here, $\text{Ideal}(F)$ is the ideal generated by F, i.e. the set of all polynomials of the form $\sum_{i=1}^{m} p_i . f_i$ with f_i in F and arbitrary polynomials p_i. As a consequence of the above property, the question whether or not $f \in \text{Ideal}(F)$, for Gröbner bases F, can be decided by just reducing f modulo F and checking whether or not the result of the reduction is 0. For general F, this question is very hard to decide and, in fact, in the older literature on polynomial ideal theory was called the "main problem of polynomial ideal theory".

Example (The "Elimination Problem"):

Let F be a set of polynomials in the indeterminates $x_1, \ldots, x_n$, and let $i \leq n$:

If F is a Gröbner basis, then:

$\text{Ideal}(F) \cap K[x_1, \ldots, x_i] = \text{Ideal}\,(F \cap K[x_1, \ldots, x_i])$.

As a consequence, a basis for the "i-th elimination ideal" $\text{Ideal}(F) \cap K[x_1, \ldots, x_i]$ of a finite Gröbner basis F can be obtained by just taking those polynomials in F that depend only on the first i indeterminates. Again, this problem is very hard for general F. Having bases for all elimination ideals of a the ideal generated by a given F, one can now find all the solutions of the system of equations determined by F. One just starts by finding all the solutions of the univariate polynomial that forms the basis of the first elimination ideal and then proceeds by substituting these solutions into the bivariate basis polynomials of the second elimination ideal etc.

6 How Can GB be Constructed?

6.1 The Main Problem

The main problem now is how, given an arbitrary finite set F of (multivariate) polynomials, one can find a set of polynomials G such that Ideal(F) = Ideal(G) and G is a Gröbner basis.

6.2 An Algorithm

This problem can be solved by the following algorithm:

> Start with $G := F$.
> For any pair of polynomials $f_1, f_2 \in G$:
>
> > Compute the "S-polynomial" of f_1, f_2
> > and reduce it to a reduced form h w.r.t. G.
> >
> > If $h = 0$, consider the next pair.
> >
> > If $h \neq 0$, add h to G and iterate.

6.3 S-Polynomials

The above algorithms needs the computation of "S-polynomials". Again, we give their definition in an example:

$$f_1 := x\,y - 2\,y, \quad f_2 := 2\,y^2 - x^2, \tag{16}$$

$$\text{S-polynomial}[f_1, f_2] = y\,f_1 - \frac{1}{2}\,x\,f_2 = \frac{x^3}{2} - 2\,y^2. \tag{17}$$

Note that the computation of the S-polynomial of two polynomials f_1 and f_2, first, involves multiplication of the two polynomials by such monomial factors that the leading power product of both polynomials becomes equal, namely the least common multiple of the leading power products of the two polynomials. By the subsequent subtraction, this least common multiple power product then vanishes! The intuition behind this notion is the following: The least common multiple of the "leading power products" of f_1 and f_2 is "the first possible polynomial" that allows two essentially different reductions modulo $\{f_1, f_2\}$. The main theorem of Gröbner bases theory then

shows that, given a finite F, if you "master" the finitely many S-polys, then you master the infinitely many polynomials that allow two or more essentially different reductions.

The notion of S-polynomials is the nucleus of *algorithmic* Gröbner bases theory. Note, however, that the notion of Gröbner bases is independent of the notion of S-polynomials and gives many interesting results also for *nonalgorithmic* polynomial ideal theory.

6.4 Specializations

It is interesting to note that the Gröbner bases algorithm,

- for linear polynomials, specializes to Gauss' algorithm, and
- for univariate polynomials, specializes to Euclid's algorithm.

7 Why Does This Work?

7.1 Termination of the Algorithm

Termination of the algorithm is nontrivial: At the beginning, there are only finitely many pairs of polynomials in G for which the corresponding S-polyonomials have to be computed. However, the reduction of some of the S-polynomials may result in a polynomial unequal zero that has to be adjoined to G. Hence, G is growing and, consequently, the number of S-polynomials that have to be considered may also grow. However, by an application of "Dickson's Lemma", [15], it can be shown that, ultimately, this process must always stop.

7.2 Correctness of the Algorithm

The correctness of the algorithm is based on the following **"*Main Theorem of Gröbner Bases Theory*":**

$$F \text{ is a Gröbner basis } \Longleftrightarrow \bigvee_{f_1, f_2 \in F} \text{RF}[F, \text{S-polynomial}[f_1, f_2]] = 0 \quad .$$

The entire power of the Gröbner bases method lies in this theorem and its proof. The proof of this theorem is nontrivial. It proceeds by induction over the ordering of power products and needs a detailed analysis of the cases that may occur when polynomials are reduced, in one step, to different polynomials modulo two polynomials. The proof was first given in the PhD thesis of the author and then published in aequationes

mathematicae, see [3, 4]. An English translation of the 1970 paper is contained in the appendix of [9]. A modern version of the proof is spelled out in [10].

8 Examples

8.1 A Simple Set of Equations

We now show how Gröbner bases can be applied to solving systems of polynomial equations. Let us, first, consider again the example:

$$\begin{aligned} f_1 &= x\,y - 2\,y, \\ f_2 &= 2\,y^2 - x^2, \\ F &= \{f_1, f_2\}. \end{aligned} \tag{18}$$

The Gröbner basis G of F is

$$G := \{-2\,x^2 + x^3,\ -2\,y + x\,y,\ -x^2 + 2\,y^2\}. \tag{19}$$

(If you have a mathematical software system like, for example, Mathematica availabe, you may compute Gröbner bases by just entering

```
GroebnerBasis[F]
```

into the system.)

By the fact that F and G generate the same ideal, F and G have the same solutions. The elimination property of Gröbner bases guarantees that, in case G has only finitely many solutions, G contains a univariate polynomial in x. (Note that, here, we use the lexicographic order that ranks y higher than x. If we used the lexicographic order that ranks x higher than y then, correspondingly, the Gröbner basis would contain a univariate polynomial in y.) In fact, the above Gröbner basis is "reduced", i.e. all polynomials in the basis are reduced modulo the other polynomial in the basis. It can be shown that reduced Gröbner bases (with finitely many solutions) contain exactly one univariate polynomial in the lowest indeterminate. In our example, the univariate polynomial in x contained in G is

$$-2\,x^2 + x^3. \tag{20}$$

We now can solve this polynomial for x, which gives us the possible solutions

```
{{x → 0}, {x → 0}, {x → 2}},
```

that is

$$x_1 = 0,\ x_2 = 0,\ x_3 = 2. \tag{21}$$

If we now plug in, say, x_2 in the second and third polynomial of G, we obtain the two polynomials

$$0 \tag{22}$$

and

$$-4 + 2\,y^2, \tag{23}$$

i.e. two univariate polynomials in y. Theory tells us that, whatever the resulting polynomials in y will be, they will always have a nontrivial greatest common divisor which, in fact, is just the non-vanishing polynomial of lowest degree. In our case, this is the polynomial

$$-4 + 2\,y^2. \tag{24}$$

Now we can solve this polynomial for y, and we obtain the solutions

$$y_{3,1} = \sqrt{2},\ y_{3,2} = -\sqrt{2}. \tag{25}$$

In this way, we can obtain all the solutions of G and, hence, of F.

8.2 A More Complicated Set of Equations

Here is a more complicated set of equations:

$$\begin{gathered} f_1 = x\,y - 2\,y\,z - z, \\ f_2 = y^2 - x^2\,z + x\,z, \\ f_3 = z^2 - y^2\,x + x, \\ \\ F = \{f_1, f_2, f_3\}. \end{gathered} \tag{26}$$

The corresponding Gröbner basis, w.r.t. the lexicographic ordering ranking x higher than y higher and y higher than z, is

$$\begin{gathered} G := \{z + 4\,z^3 - 17\,z^4 + 3\,z^5 - 45\,z^6 + \\ 60\,z^7 - 29\,z^8 + 124\,z^9 - 48\,z^{10} + 64\,z^{11} - 64\,z^{12}, \\ -22001\,z + 14361\,y\,z + 16681\,z^2 + 26380\,z^3 + \\ 226657\,z^4 + 11085\,z^5 - 90346\,z^6 - 472018\,z^7 - \\ 520424\,z^8 - 139296\,z^9 - 150784\,z^{10} + 490368\,z^{11}, \\ 43083\,y^2 - 11821\,z + 267025\,z^2 - 583085\,z^3 + 663460\,z^4 - \\ 2288350\,z^5 + 2466820\,z^6 - 3008257\,z^7 + 4611948\,z^8 - \\ 2592304\,z^9 + 2672704\,z^{10} - 1686848\,z^{11}, \end{gathered} \tag{27}$$

$$43083\,x - 118717\,z + 69484\,z^2 + 402334\,z^3 + 409939\,z^4 + 1202033\,z^5 - 2475608\,z^6 + 354746\,z^7 - 6049080\,z^8 + 2269472\,z^9 - 3106688\,z^{10} + 3442816\,z^{11}\}.$$

You may again observe that G contains a univariate polynomial in the lowest indeterminate z. This time the degree of this polynomial is 12. The roots of this polynomial cannot be expressed by radicals. In principle, one may represent the roots as algebraic numbers (see the literature on computer algebra and the implementations in the various mathematical software systems) and then proceed by substituting the roots of the first polynomial into the other polynomials of the Gröbner basis. In this introductory paper, we rather switch to a numerical approximation of the roots:

$$z_1 = -0.3313043000789449 - 0.5869344538646171\,i \tag{28}$$

$$z_2 = -0.3313043000789449 + 0.5869344538646171\,i \tag{29}$$

$$\vdots \tag{30}$$

If we now substitute, say, z_1 into the other polynomials of G we obtain the three polynomials

$$(-523.5194758552393 - 4967.646241304139\,i) - (4757.861053433728 + 8428.965691949767\,i)\,y, \tag{31}$$

$$(-7846.89647617919 - 8372.055369776885\,i) + 43083\,y^2, \tag{32}$$

$$(-16311.7 + 16611.\,i) + 43083\,x. \tag{33}$$

Theory tells us that the first polynomial is (an approximation to) the greatest common divisor of the first and the second polynomial. Hence, its solution gives us the common solution of the first and the second polynomial. Thus, we obtain

$$y_{1,1} = -0.4735346386353353 - 0.20518443210789426\,i \tag{34}$$

Finally, we can substitute $y_{1,1}$ into the last polynomial (which, in this particular case does not change it since y does not occur as an indeterminate) and we can obtain the solution

$$x_{1,1,1} = 0.3786106927760740 - 0.3855581188501717\,i\,. \tag{35}$$

In this way, we can obtain all the finitely many solutions of G and, hence, of F.

8.3 Algebraic Relations

(27)

The problem of algebraic relations in invariant theory is the problem of asking whether, for example, the polynomial

$$p := x_1^7\, x_2 - x_1\, x_2^7 \tag{36}$$

can be expressed as a polynomial in, for example,

$$\begin{aligned} i_1 &:= x_1^2 + x_2^2 \\ i_2 &:= x_1^2\, x_2^2 \\ i_3 &:= x_1^3\, x_2 - x_1\, x_2^3. \end{aligned} \tag{37}$$

(Note that the polynomials $i_1,\ i_2,\ i_3$ form a system of fundamental invariants for $\mathbb{Z}_4$, i.e. a set of generators for the ring

$$\{f \in \mathbb{C}[x_1, x_2] \mid f(x_1, x_2) = f(-x_2, x_1)\}, \tag{38}$$

i.e. $i_1,\ i_2,\ i_3$ are in this ring and, furthermore, all polynomials in this ring can be expressed as polynomials in $i_1,\ i_2,\ i_3$.

The theory of Gröbner bases tells us now that the above question can be answered by, first, computing a Gröbner basis G of the following polynomial set

$$\{-i_1 + x_1^2 + x_2^2,\ -i_2 + x_1^2\, x_2^2,\ -i_3 + x_1^3\, x_2 - x_1\, x_2^3\} \tag{39}$$

w.r.t. a lexicographic ordering that ranks $x_1,\ x_2$ higher than $i_1,\ i_2,\ i_3$ and by reducing p modulo G and analyzing the result. In our example the (reduced) Gröbner basis is

$$\begin{aligned} G := \{&-i_1^2\, i_2 + 4\, i_2^2 + i_3^2,\ -i_2 + i_1\, x_1^2 - x_1^4, \\ &i_1^2\, i_3\, x_1 - 2\, i_2\, i_3\, x_1 - i_1\, i_3\, x_1^3 + i_1^2\, i_2\, x_2 - 4\, i_2^2\, x_2, \\ &i_1^2\, x_1 - 2\, i_2\, x_1 - i_1\, x_1^3 + i_3\, x_2, \\ &-i_1\, i_3 + 2\, i_3\, x_1^2 - i_1^2\, x_1\, x_2 + 4\, i_2\, x_1\, x_2,\ -i_3\, x_1 - 2\, i_2\, x_2 + i_1\, x_1^2\, x_2, \\ &-i_3 - i_1\, x_1\, x_2 + 2\, x_1^3\, x_2,\ -i_1 + x_1^2 + x_2^2\}, \end{aligned} \tag{40}$$

and reduction of p modulo G yields

$$h := i_1^2\, i_3 - i_2\, i_3. \tag{41}$$

(Please use mathematical software system like Mathematica for carrying out these computations.)

The theory of Gröbner bases now tells us that p can be expressed as a polynomial in $i_1,\ i_2,\ i_3$ if and only if h is a polynomial only in the indeterminates $i_1,\ i_2,\ i_3$, i.e. does not contain the indeterminates $x_1,\ x_2$. This is the case in our example. Thus, we know that p is representable as a polynomial in the polynomials $i_1,\ i_2,\ i_3$ and, furthermore, h gives us the actual representation, namely

$$p = (x_1^2 + x_2^2)^2\, (x_1^3\, x_2 - x_1\, x_2^3) - (x_1^2\, x_2^2)\, (x_1^3\, x_2 - x_1\, x_2^3). \tag{42}$$

9 How Difficult is it to Construct Gröbner Bases?

Very Easy

The structure of the algorithm is easy. The operations needed in the algorithm are elementary: "Every high-school student can execute the algorithm."

Very Difficult

The intrinsic complexity of the problems that can be solved by the Gröbner bases method is proven to be "exponential". Hence, the worst-case complexity of any algorithm that computes Gröbner bases in full generality *must* be high. Thus, examples in three or four variables with polynomials of degree three or four may already fail to terminate in reasonable time or exceed available memory even on very fast machines.

For example, trying to find a Gröbner basis, w.r.t. to a lexicographic ordering, for the set

$$\begin{array}{c} \{x\,y^3 - 2\,y\,z - z^2 + 13, \\ y^2 - x^2\,z + x\,z^2 + 3, \\ z^2\,x - y^2\,x^2 + x\,y + y^3 + 12\} \end{array} \tag{43}$$

may already exhaust your computer resources.

Sometimes Easy

Mathematically interesting examples often have a lot of "structure" and, in concrete examples, Gröbner bases can be computed in reasonably short time. Thus, a lot of interesting new theoretical insight in various areas of mathematics has been obtain by using the Gröbner bases technique for concrete, theoretically interesting, examples. Also, sometimes, it is possible to derive closed formulae for the Gröbner bases of certain ideals that depend on various parameters and, then, various conclusions can be drawn from the form of these Gröbner bases, see for example [8]. Hence, as a first attempt, it is always recommendable to try Gröbner bases if one encounters a problem formulated in terms of multivariate polynomial sets.

Enormous Potential for Improvement

The positive aspect of an intrinsically complex problem as the one of constructing Gröbner bases is that more *mathematical* knowledge can lead to a drastic speed-up. In the literature, the following ideas have led to drastically improved versions of the above Gröbner basis algorithm:

- The use of "criteria" for eliminating the consideration of certain S-polynomials, see [6].
- Several p-adic and floating point approaches, see [21, 20].
- The "Gröbner Walk" approach, see [13].
- The "linear algebra" approach, see [16].

All these approaches do, however, not change the main idea of the algorithmic construction given above based on the fundamental role of the "S-polynomials". For the practical implementation of the Gröbner basis algorithm, *tuning* of the algorithm is also important, for example by

- heuristics and strategies for choosing favorable orderings of power products and for the sequence in which S-polynomials should be selected etc,
- good implementation techniques and data structures.

There is a huge literature on the complexity of Gröbner bases algorithms and on improving the efficiency of these algorithms.

10 Why are Gröbner Bases Called Gröbner Bases?

Professor *Wolfgang Gröbner* was my PhD thesis supervisor in 1965. He gave me the problem of finding a linearly independent basis for the residue class ring modulo an arbitrary polynomial ideal given by finitely many generators. On the way of answering this question, I developed the theory of what I later (1976, see [5]), in honor of my former advisor, called "Gröbner bases". In more detail, in my thesis (1965) and journal publication (1970), I introduced the following notions, theorems, and methods:

- the concept of Gröbner bases and reduced Gröbner bases,
- the concept of S-polynomial,
- the main theorem with proof,
- the algorithm with termination and correctness proof,
- the uniqueness of reduced Gröbner bases,
- first applications (algorithmic computing in residue class rings, Hilbert function computation, solution of algebraic systems),
- the technique of base-change w.r.t. to different orderings,
- a complete running implementation with examples,
- first complexity considerations.

Later, I contributed mainly the following two ideas to the theory of Gröbner bases:

- the technique of criteria for eliminating unnecessary reductions,
- an abstract characterization of rings ("reduction rings") in which a Gröbner bases approach is possible.

In my view, the main additional ideas that have been contributed to the theory of Gröbner bases by other authors are the following:

- Gröbner bases can be constructed w.r.t. arbitrary "admissible" orderings (W. Trinks 1978).
- Gröbner bases w.r.t. to "lexical" orderings have the elimination property (W. Trinks 1978).
- Gröbner bases can be used for computing syzygies, and the S-polys generate the module of syzygies (G. Zacharias 1978).
- A given F, w.r.t. the *infinitely* many admissible orderings, has only *finitely* many Gröbner bases and, hence, one can construct a "universal" Gröbner bases for F (L. Robbiano, V. Weispfenning, T. Schwarz 1988).
- Starting from a Gröbner bases for F for ordering O_1 one can "walk", by changing the basis only slightly, to a basis for a "nearby" ordering O_2 and so on … until one arrives at a Gröbner bases for a desired ordering O_k (Kalkbrener, Mall 1995).
- Numerous applications of Gröbner bases for solving problems in various fields of mathematics that, sometimes, needed ingenious ideas for establishing the reduction of the problems considered to the computation of Gröbner bases.

11 Where Can You Find Information on Gröbner Bases?

11.1 The Gröbner Bases Conference 1998

The proceedings of this conference, [9], contain tutorials on nearly all currently known applications of Gröbner bases in various fields of mathematics. Unfortunately, no tutorial on applications of Gröbner bases in systems theory is contained in these proceedings.

These proceedings contain also a couple of original papers and an introduction to Gröbner bases including a complete formal proof of the main theorem, see [10]. Also, in the appendix, an English translation of the original paper [4] is included.

11.2 On Your Desk

Implementations of the Gröbner basis algorithms and many application algorithms based on Gröbner bases are contained in any of the current mathematical software systems like Mathematica, Maple, Magma, Macsyma, Axiom, Derive, Reduce, etc. Also, there exist special software systems that are mainly based on the Gröbner bases technique, for example, CoCoA [12], Macaulay [17], Singular [18].

11.3 In Your Palm

Gröbner bases are now availabe on the TI-92 (implemented in Derive) and other palm-top calculators so that literally every high-school student has access to the method.

11.4 Textbooks

By now, a couple of very good textbooks are available on Gröbner bases, see for example, [19], [2], [1], [14]. The textbook [19], in the introduction, contains a complete list of all current textbooks.

11.5 In the Web

Searching in the web, for example starting at http://citeseer.nj.nec.com/ with the key word "Grobner" will quickly lead you to hundreds of papers on Gröbner bases and their applications.

11.6 Original Publications

By now, more than 500 papers appeared meanwhile on Gröbner bases. Many of them are appearing in the Journal of Symbolic Computation (Academic Press, London) or at the ISSAC Symposia (International Symposia on Symbolic and Algebraic Computation).

References

1. W. W. Adams, P. Loustaunau. *Introduction to Gröbner Bases*. Graduate Studies in Mathematics, American Mathematical Society, Providence, R.I., 1994.
2. T. Becker, V. Weispfenning. *Gröbner Bases: A Computational Approach to Commutative Algebra.* Springer, New York, 1993.
3. B. Buchberger. *An Algorithm for Finding the Bases Elements of the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal* (German). PhD thesis, Univ. of Innsbruck (Austria), 1965.
4. B. Buchberger. An Algorithmical Criterion for the Solvability of Algebraic Systems of Equations (German). *Aequationes Mathematicae,* **4**(3):374-383, 1970. English translation in [9].
5. B. Buchberger. Some properties of Grobner bases for polynomial ideals. *ACM SIGSAM Bulletin*, **10**(4):19-24, 1976.
6. B. Buchberger. A Criterion for Detecting Unnecessary Reductions in the Construction of Gröbner Bases. In Edward W. Ng, editor, *Proceedings of the International Symposium on Symbolic and Algebraic Manipulation (EUROSAM '79)*, Marseille, France, volume 72 of *Lecture Notes in Computer Science*, pages 3-21. Springer, 1979.
7. B. Buchberger. Gröbner-Bases: An Algorithmic Method in Polynomial Ideal Theory. In N. K. Bose, editor, *Multidimensional Systems Theory*, chapter 6, pages 184-232. Reidel Publishing Company, Dodrecht, 1985.
8. B. Buchberger and J. Elias. Using Gröbner Bases for Detecting Polynomial Identities: A Case Study on Fermat's Ideal. *Journal of Number Theory* **41**:272-279, 1992.
9. B. Buchberger and F. Winkler, editors. *Gröbner Bases and Applications*, volume 251 of *London Mathematical Society Series*. Cambridge University Press, 1998. Proc. of the International Conference ''33 Years of Groebner Bases''.
10. B. Buchberger. *Introduction to Gröbner Bases*, pages 3-31 in [9], Cambridge University Press, 1998.
11. B. Buchberger. Gröbner-Bases and System Theory. To appear as *Special Issue on Applications of Gröbner Bases in Multidimensional Systems and Signal Processing*, Kluwer Academic Publishers, 2001.
12. A. Capani, G. Niesi, and L. Robbiano. *CoCoA: A System for Doing Computations in Commuatative Algebra*, 1998. Available via anonymous ftp from `cocoa.dima.uniqe.it`.
13. S. Collart, M. Kalkbrenner, D. Mall. Converting bases with the Gröbner walk. *Journal of Symbolic Computation*, **24**:465-469, 1997.
14. D. Cox, J. Little, D. O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Springer, New York, 1992.
15. L. E. Dickson. Finiteness of the Odd Perfect and Primitive Abundant Numbers with n Distince Prime Factors. *American Journal of Mathematics*, **35**:413-426, 1913.
16. J. C. Faugère, P. Gianni, D. Lazard, T. Mora. Efficient computation of zero-dimensional Gröbner bases by change of ordering. *Journal of Symbolic Computation*, **16**:377-399, 1993.

17. D. Grayson and M. Stillman. *Macaulay 2: A Software System for Algebraic Geometry and Commutative Algebra*. Available over the web at `http://www.math.uiuc.edu/-Macaulay2`.

18. G.-M. Greuel and G. Pfister and H. Schönemann. *Singular Reference Manual*. Reports On Computer Algebra, Number 12, Centre for Computer Algebra, University of Kaiserslautern, 1997. Available over the web at `http://www.mathematik.uni-kl.de/~zca/Singular`.

19. M. Kreuzer and L. Robbiano. *Computational Commutative Algebra I*. Springer, Heidelberg-New York, 2000. ISBN 3-540-67733-X.

20. F. Pauer. On lucky ideals for Gröbner basis computations. *Journal of Symbolic Computation*, **14**:471-482, 1992.

21. Franz Winkler. A p-adic approach to the computation of Gröbner bases. *Journal of Symbolic Computation*, **6**:287-304, 1988.