London Mathematical Society Lecture Note Series. 251

Gröbner Bases and Applications

Edited by

B. Buchberger & F. Winkler
Johannes Kepler University of Linz

CAMBRIDGE
UNIVERSITY PRESS

PUBLISHED BY THE PRESS SYNDICATE OF THE UNIVERSITY OF CAMBRIDGE
The Pitt Building, Trumpington Street, Cambridge CB2 1RP, United Kingdom

CAMBRIDGE UNIVERSITY PRESS
The Edinburgh Building, Cambridge, CB2 2RU, United Kingdom
40 West 20th Street, New York, NY 10011-4211, USA
10 Stamford Road, Oakleigh, Melbourne 3166, Australia

First published 1998

Printed in the United Kingdom at the University Press, Cambridge

A catalogue record for this book is available from the British Library

ISBN 0 521 63298 6 paperback

Introduction to Gröbner Bases[1]

Bruno Buchberger

Research Institute for Symbolic Computation
Austria-4232, Schloss Hagenberg
Bruno.Buchberger@RISC.uni-linz.ac.at

Outline

A comprehensive treatment of Gröbner bases theory is far beyond what can be done in one article in a book. Recent text books on Gröbner bases like (Becker, Weispfenning 1993) and (Cox, Little, O'Shea 1992) present the material on several hundred pages. However, there are only a few key ideas behind Gröbner bases theory. It is the objective of this introduction to explain these ideas as simply as possible and to give an overview of the immediate applications. More advanced applications are described in the other tutorial articles in this book.

The concept of Gröbner bases together with the characterization theorem (by "S-polynomials") on which an algorithm for constructing Gröbner bases hinges has been introduced in the author's PhD thesis (Buchberger 1965), see also the journal publication (Buchberger 1970). In these early papers we also gave some first applications (computation in residue class rings modulo polynomial ideal congruence, algebraic equations, and Hilbert function computation), a computer implementation (in the assembler language of the ZUSE Z23V computer), and some first remarks on complexity. Later work by the author and by many other authors has mainly added generalizations of the method and quite a few new applications for the algorithmic solution of various fundamental problems in algebraic geometry (polynomial ideal theory, commutative algebra). Also, complexity issues have been treated extensively. The field is still under active development both into the direction of improving the method by new theoretical insights and by finding new applications.

This article is structured as follows:

In the first section we give a variety of examples demonstrating the versatility of the method of Gröbner bases for problems that involve finite sets of multivariate polynomials.

In the second section, the main idea contained in the notion of Gröbner bases and the main theorem about them, which also leads to an algorithmic

[1]An earlier version of this paper appeared in the Proceedings of the Marktoberdorf Summer School 1995, published by Springer Heidelberg, 1997.

construction of Gröbner bases, is explained. The proof of the main theorem is spelled out in detail.

The third section systematically summarizes the most important immediate applications of Gröbner bases.

1 Gröbner Bases at Work

1.1 Example: Fermat Ideals

The following polynomials are called Fermat polynomials:

$$F_n := x^n + y^n - z^n \ (n \geq 1).$$

Question: Can, from some k on, F_n be expressed as a linear combination

$$F_n = \sum_{1 \leq i \leq k} h_{n,i} \cdot F_i$$

with $h_{n,i} \in \mathbb{Q}[x, y, z]$? In other words: Is F_n in Ideal$(F_1, \ldots, F_k)$, the ideal generated by $F_1, \ldots, F_k$? (This question was raised in connection with possible approaches to solving the Fermat problem. An affirmative but inconstructive answer, i.e. an answer that did not explicitly construct the $h_{n,i}$, was given in (Elias 88). This answer used quite heavy machinery from algebraic geometry.)

Solution by the Gröbner bases method: We compute a Gröbner basis G for Ideal(F_1, F_2, F_3) and check, by "reduction of F_4 modulo G", whether or not $F_4 \in$ Ideal(F_1, F_2, F_3). It turns out the answer is "yes", which can be seen from the fact that the reduction of F_4 modulo G yields 0. During the reduction we "collect the cofactors", which yields the representation

$$F_4 = S_0 \cdot F_1 - S_1 \cdot F_2 + S_2 \cdot F_3,$$

where the S_i are the elementary symmetric polynomials in x, y, z. ($S_0 := x\,y\,z$, $S_1 := x\,y + x\,z + y\,z$, $S_2 := x + y + z$.)

By the same method, we can now check whether $F_5 \in$ Ideal(F_1, F_2, F_3, F_4). It turns out that, even, $F_5 \in$ Ideal(F_2, F_3, F_4) and, surprisingly, again

$$F_5 = S_0 \cdot F_2 - S_1 \cdot F_3 + S_2 \cdot F_4.$$

This leads immediately to the conjecture that, for arbitrary $n \geq 1$,

$$F_{n+3} = S_0 \cdot F_n - S_1 \cdot F_{n+1} + S_2 \cdot F_{n+2}. \qquad (\text{identity}_3)$$

This conjecture can be verified easily by elementary formula manipulation. (One may want to use a symbolic computation software system for this verification!)

This identity yields the by-product that the "Fermat ideal" generated by the infinitely many F_n $(n \geq 1)$ is already generated by the first three Fermat polynomials. Of course, one can now go immediately one step further and may conjecture that, for the "generalized Fermat polynomials"

$$F_{m,n} := {x_1}^n + \ldots + {x_{m-1}}^n - {x_m}^n \quad (m, n \geq 1)$$

the following identity holds

$$F_{m,n+m} = \sum_{0 \leq k < m} (-1)^{m+k+1} \cdot S_{m,k} \cdot F_{m,n+k} \qquad (\text{identity}_m)$$

where the $S_{m,k}$ are the elementary symmetric polynomials in $x_1, \ldots, x_m$. This formula can be proved by straight-forward induction on m or by generating functions. The details can be found in (Buchberger, Elias 1992). Note that the same identity holds for the symmetric "exponential sums". However, the $F_{m,n}$ are not symmetric and this could be the reason why (identity_m) seems to have gone unnoticed in the literature.

1.2 Example: Geometry Theorem Proving

(This example is taken from (Buchberger, Kutzler 1986).)

Question: Is the following proposition true?

"In an arrangement of the form shown in the Figure 1, K, L, M are collinear."

(In the drawing, A$< 0, y_1 >$ etc. denotes the point A with coordinates 0 and y_1, etc.)

(The above statement is *Pappus' Theorem* and it is well known that it is true. The point is that one can ask this question about any geometric proposition whose premises and conclusion, after being described in Cartesian coordinates, can be expressed by multivariate polynomials, and the method given below will answer the question automatically.)

Solution by the Gröbner basis algorithm: An algebraic formulation of the problem is as follows:

$$\forall y_1, \ldots, y_{12}$$
$$(p_1(y_1, \ldots, y_{12}) = 0 \wedge \ldots \wedge p_6(y_1, \ldots, y_{12}) = 0 \Longrightarrow c(y_1, \ldots, y_{12}) = 0)$$

where $p_1, \ldots, p_6$, and c are non-linear polynomials in the variables $y_1, \ldots, y_{12}$ that express the premises and the conclusion of the theorem. For example, p_1 expresses the condition that K is on the line $\overline{AE}$ and has the following form

$$p_1(y_1, \ldots, y_{12}) := (y_7 - y_1)y_5 + y_8\, y_1 .$$

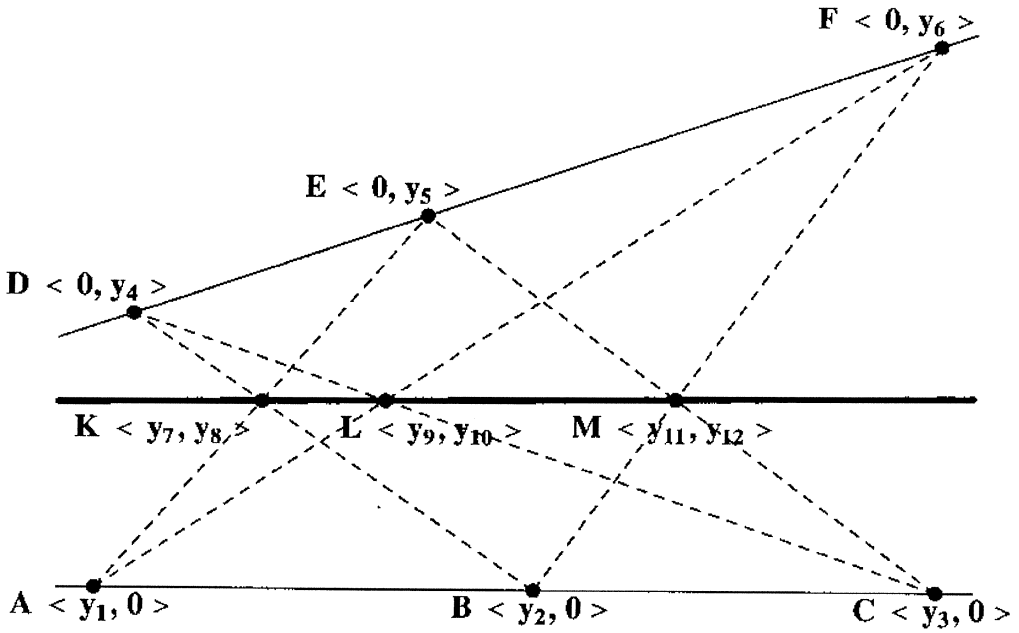

Figure 1: Pappus' Theorem

In our example, the other polynomials are

$$\begin{aligned}
p_2(y_1,\ldots,y_{12}) &:= (y_7 - y_2)y_4 + y_8\,y_2,\\
p_3(y_1,\ldots,y_{12}) &:= (y_9 - y_1)y_6 + y_{10}\,y_1,\\
p_4(y_1,\ldots,y_{12}) &:= (y_9 - y_2)y_4 + y_{10}\,y_3,\\
p_5(y_1,\ldots,y_{12}) &:= (y_{11} - y_2)y_6 + y_{12}\,y_2,\\
p_6(y_1,\ldots,y_{12}) &:= (y_{11} - y_3)y_5 + y_{12}\,y_3,\\
c(y_1,\ldots,y_{12}) &:= (y_9 - y_7)(y_{12} - y_8) + (y_{10} - y_8)(y_{11} - y_7).
\end{aligned}$$

We now input the following system of polynomials to the Gröbner basis algorithm:

$$\{p_1,\ldots,p_6, c\cdot y - 1\},$$

where y is a new variable. It can be shown that a theorem of the above form is true iff the Gröbner basis produced for the above input contains the polynomial 1. This is the case in our example and, hence, we know that the theorem is true.

1.3 Example: Invariant Theory

(This example is taken from (Sturmfels 1993).)

Question: Compute all algebraic relations between the fundamental invariants for the invariant ring of the cyclic group Z_4 of order 4, i.e. a set of

generators for the ring

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

and represent the invariant $x_1^7 x_2 - x_1 x_2^7$ by the fundamental invariants.

Solution by the Gröbner basis method: The following polynomials

$$I_1 := x_1^2 + x_2^2,\ I_2 := x_1^2 x_2^2,\ I_3 := x_1^3 x_2 + x_1 x_2^3$$

form a system of fundamental invariants for Z_4. Now we compute the Gröbner basis of

$$\{-I_1 + x_1^2 + x_2^2, -I_1 + x_1^2 x_2^2, -I_3 + x_1^3 x_2 + x_1 x_2^3\}$$

(in the polynomial ring with added slack variables I_1, I_2, I_3) with respect to the lexical ordering determined by $I_1 < I_2 < I_3 < x_1 < x_2$. In our case this yields the set

$$\{I_1^2 I_2 - 4I_2^2 - 4I_3^2, I_2 - I_1 x_2^2 + x_2^4,$$
$$\ldots \text{ (6 other polynomials in which } x_1 \text{ and } x_2 \text{ occur)}\ldots\}$$

Now, those polynomials in this Gröbner basis that depend only on I_1, I_2, and I_3 generate the ideal of all algebraic relations between I_1, I_2, and I_3. In our case this ideal is, hence, generated by

$$I_1^2 I_2 - 4I_2^2 - 4I_3^2.$$

Furthermore, by reducing any given polynomial g in x_1, x_2 modulo $\{I_1^2 I_2 - 4I_2^2 - 4I_3^2, \ldots\}$ one can check whether or not g is invariant (iff the reduction yields a polynomial that does not contain x_1, x_2 anymore) and, if it is invariant, this reduction yields a representation of g in terms of the fundamental invariants. In our example, the reduction of $x_1^7 x_2 - x_1 x_2^7$ yields $I_1^2 I_3 - I_2 I_3$.

1.4 Example: Systems of Polynomial Equations

(This example is taken from (Buchberger, Kutzler 1986)).

Systems of multivariate polynomial equations are pervasive in all areas of engineering. For example, consider the simple robot from Figure 2.

After appropriate coordinatization (using the Denavit-Hartenberg approach), the relation between the angles d_1 and d_2 at the links of the robot and the position of the gripper (described by the coordinates p_x, p_y, p_z) and its orientation (described, for example, by the Euler angles φ, θ, ψ) can be characterized

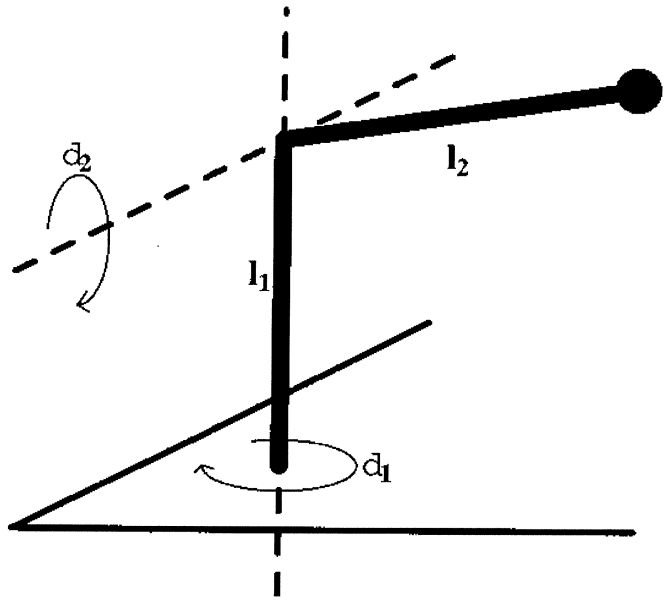

Figure 2: Simple Robot.

by the following system of polynomial equations:

$$\begin{aligned}
c_1c_2 - c_fc_tc_p - s_fs_p &= 0,\\
s_1c_2 - s_fc_ts_p - c_fs_p &= 0,\\
s_2 + s_tc_p &= 0,\\
-c_1s_2 - c_fc_ts_p + s_fc_p &= 0,\\
-s_1s_2 + s_fc_ts_p - c_fc_p &= 0,\\
c_2 - s_ts_p &= 0,\\
s_1 - c_fs_t &= 0,\\
c_1 + s_fs_t &= 0,\\
c_t &= 0,\\
l_2c_1c_2 - p_x &= 0,\\
l_2s_1c_2 - p_y &= 0,\\
l_2s_2 + l_1 - p_z &= 0,\\
c_1^2 + s_1^2 - 1 &= 0,\\
c_2^2 + s_2^2 - 1 &= 0,\\
c_f^2 + s_f^2 - 1 &= 0,\\
c_t^2 + s_t^2 - 1 &= 0,\\
c_p^2 + s_p^2 - 1 &= 0.
\end{aligned}$$

Here, $c_1, s_1, c_2, s_2, c_f, s_f, c_t, s_t, c_p, s_p$ are the cosines and sines of the angles d_1, d_2, φ, θ, ψ, respectively. These values are algebraically related by the last

five additional equations. The arm lengths l_1 and l_2 are parameters. The kinematics problem asks for finding the value of some of these variables if the value of the rest of the variables is given. Because of the limited degree of freedom, in this example, we can only give the value of two of these variables. The others will then be determined. For example, we may fix p_x and p_y and ask for suitable values for the other variables.

Solution by the Gröbner basis algorithm: If we input this system of polynomials to the Gröbner basis algorithm (setting the "ordering parameter" to the "lexical ordering" determined by $c_1 < c_2 < s_1 < s_2 < p_y < c_f < c_t < c_p < s_f < s_t < s_p$ and taking p_x, p_z, l_1, and l_2 as parameters), we obtain the following output:

$$\begin{aligned}
c_1^2 + Q_1 &= 0,\\
c_2 + Q_2 c_1 &= 0,\\
s_1^2 + Q_3 &= 0,\\
s_2 + Q_4 &= 0,\\
p_y + Q_5 c_1 s_1 &= 0,\\
c_f^2 + Q_6 &= 0,\\
c_t &= 0,\\
c_p + Q_7 s_1 c_f &= 0,\\
s_f + Q_8 c_1 s_1 c_f &= 0,\\
s_t + Q_9 s_1 c_f &= 0,\\
s_p + Q_{10} c_1 s_1 c_f &= 0,
\end{aligned}$$

where the Q_i are rational functions in p_x, p_z and the parameters l_1, l_2. The Gröbner basis produced has the remarkable and useful property that it is "triangularized", i.e. its first equation is univariate in the lowest variable c_1, i.e. all the possible values for c_1 can be determined from this equation. The second equation contains c_1 and c_2 and, in fact, c_2 is "explicit". Thus, for each value of c_1 a corresponding value for c_2 can be determined and so on. Also, the Gröbner basis still contains p_x, p_z and the parameters l_1, l_2 in "symbolic form".

Of course, in this simple example, the "symbolic solution" could also be derived by a reasonably skillful analysis of the drawing. However, the Gröbner basis algorithm works in all situations and always results in a "triangularized" system.

2 The Main Theorem on Gröbner Bases

2.1 Polynomials

Let $\mathbb{N}$ be the set of natural numbers including zero. The variables i ,j, k, l, m, n will range over $\mathbb{N}$. Let $(\mathbf{K}, +, 0, -, \cdot, 1, /)$ be a field, let $n \in \mathbb{N}$, and let $x_1, \ldots, x_n$ be indeterminates. By $(\mathbf{K}[x_1, \ldots, x_n], +, 0, -, \cdot, 1)$ we denote (any of the infinitely many isomorphic representations of) the ring of polynomials over $\mathbf{K}$ with indeterminates $x_1, \ldots, x_n$. Furthermore, $[x_1, \ldots, x_n]$ will denote the set of power products (i.e. monomials with coefficient 1) over the indeterminates $x_1, \ldots, x_n$. Throughout this paper, $(\mathbf{K}, +, 0, -, \cdot, 1, /)$, n, and $x_1, \ldots, x_n$ will be fixed and we will also use the abbreviations

$$\begin{aligned} \mathbf{T} &:= [x_1, \ldots, x_n], \\ \mathbf{P} &:= \mathbf{K}[x_1, \ldots, x_n]. \end{aligned}$$

Note that, in this paper, we use the symbols "+", "0" etc. both for the operations in the original field and for the operations in the polynomial ring. In addition, we will use "$\cdot$" also for scalar multiplication between field elements and polynomials. (In fact, with this additional operation, the polynomial ring becomes a vector space and even an associative algebra over the field.) This overloading of operation symbols will not cause any confusion since we will stick to the following additional type convention: The variables a, b, c will range over $\mathbf{K}$; p, q, r, but also f, g, h will range over $\mathbf{P}$; and t, u, v will range over $\mathbf{T}$. The variables F and G will be used for subsets of $\mathbf{P}$.

With some care, all these variables will also be used for ranging over finite sequences of elements from the respective sets. For any set Y, Y^* will denote the set of finite sequences over Y. If $y \in Y^*$, y_i is the i-th element and $|y|$ is the length of y, respectively. Of course, if $y \in Y^*$ then $y_i \in Y$.

On $\mathbf{T}$, we consider the following three additional operations:

$$\begin{aligned} t|u \quad &:\Longleftrightarrow \quad u \text{ is a multiple of } t, \\ t/u \quad &:= \quad t \text{ divided by } u \text{ (in case } u|t), \\ \mathrm{LCM}(t,u) \quad &:= \quad \text{the least common multiple of } t \text{ and } u. \end{aligned}$$

On $\mathbf{P}$ we introduce the following structural operations:

$$\begin{aligned} \mathrm{C}(p,\, t) \quad &:= \quad \text{the coefficient at } t \text{ in } p, \\ \mathrm{M}(p,\, t) \quad &:= \quad \mathrm{C}(p,t) \cdot t, \\ \mathrm{S}(p) \quad &:= \quad \{t \mid \mathrm{C}(p,t) \neq 0\}. \end{aligned}$$

(For $\mathrm{M}(p,\, t)$ and $\mathrm{S}(p)$ read "the monomial at t in p" and "the support of p", respectively.)

The theory of Gröbner bases will be formulated independently of any particular representation of the domain of polynomials. However, in our examples we will always use the "ordinary" representation of polynomials as arithmetical terms in "fully expanded form" as, for example, "$-3xy^2z + 3/2x^2y + 5/3yz^2$".

Formal text (definitions, theorems, proofs) that is followed by informal text will be terminated by the symbol □.

2.2 Polynomial Ideals

Definition (Congruence and Ideals):

$$g \equiv_F h \quad :\Longleftrightarrow \quad \exists p \in \mathbf{P}^* \, \exists f \in F^* (|p| = |f| \wedge g = h + \sum_{1 \le i \le |p|} p_i \cdot f_i).$$

$$\mathrm{Ideal}(F) \quad := \quad \{g \mid g \equiv_F 0\}.$$

(For $f \equiv_F g$ read "f is congruent g modulo F". For Ideal(F) read "the ideal generated by F".)

2.3 Admissible Orderings on Power Products

Congruence modulo an F is a nonalgorithmic notion: For deciding whether or not $g \equiv_F h$, one could try to compare coefficients in the presentation $g = h + \sum p_i \cdot f_i$ and then use linear algebra. However, a priori, it is not clear how big the degrees of appropriate p_i might become. In (Hermann 1926) bounds for the degrees were derived and, thus, in principle, $g \equiv_F h$ could be decided algorithmically.

However, we are heading for a different approach which will allow us to solve a broader class of problems in polynomial ideal theory and yields algorithmic decidability of congruence modulo arbitrary F as a by-product. The first step towards this goal is to replace congruence by "reduction", which can be viewed as a kind of "directed congruence". For this purpose, we order the power products (and thereby also the polynomials) so that we will later be able to replace power products by "lower" polynomials modulo F. Certain special orderings ("total degree" orderings) on power products were used in algebra already at the beginning of this century, for example by F. S. Macaulay. Gröbner basis theory works, however, with respect to any "admissible" ordering, as has been noticed first in (Trinks 1978).

Definition (Admissible Ordering): Let $\prec$ be a total ordering on $\mathbf{T}$. Then,

$$\prec \text{ is admissible} \quad :\Longleftrightarrow \quad \forall t \neq 1 \; (1 \prec t),$$

$$\forall t, u, v \; (t \prec u \Longrightarrow t \cdot v \prec u \cdot v). \quad \text{(monotonicity)}$$

Examples of Admissible Orderings: The "lexical" ordering defined by $x \prec y$ orders the power products in $[x, y]$ in the following way: $1 \prec x \prec x^2 \prec x^3 \prec \ldots \prec y \prec xy \prec x^2y \prec \ldots \prec y^2 \prec xy^2 \prec x^2y^2 \prec \ldots$.

The "total degree" ordering defined by $x \prec y$ orders the power products in $[x, y]$ in the following way: $1 \prec x \prec y \prec x^2 \prec xy \prec y^2 \prec x^3 \prec x^2y \prec xy^2 \prec y^3 \prec x^4 \prec \ldots$.

Admissible orderings on **T** have two important properties:

Proposition (Properties of Admissible Orderings): Let $\prec$ be an admissible ordering on T. Then,

$\forall t, u \; (t \mid u \Longrightarrow t \preceq u)$, (|-compatibility)

$\prec$ is Noetherian.

(A relation is Noetherian iff there are no infinite descending chains w.r.t. the relation.)

Proof: The proof of |-compatibility is immediate using the definition of admissibility. The proof of Noetherianity can be given by using a combinatorial lemma known as Dickson's lemma introduced in (Dickson 1913), see for example (Becker, Weispfenning 1993), p. 163.

2.4 Order Dependent Decomposition of Polynomials

Given an admissible ordering $\prec$ on **T**, we can now introduce a couple of operations on **P** that decompose polynomials into various constituents:

$$
\begin{aligned}
\mathrm{LPP}_\prec(p) &:= \max_\prec \mathrm{S}(p), \\
\mathrm{LC}_\prec(p) &:= \mathrm{C}(p, \mathrm{LPP}_\prec(p)), \\
\mathrm{LM}_\prec(p) &:= \mathrm{LC}_\prec(p) \cdot \mathrm{LPP}_\prec(p), \\
\mathrm{R}_\prec(p) &:= p - \mathrm{LM}_\prec(p), \\
\mathrm{H}_\prec(p, t) &:= \sum_{u \in \mathrm{S}(p) \wedge u \succ t} \mathrm{C}(p, u) \cdot u, \\
\mathrm{L}_\prec(p, t) &:= \sum_{u \in \mathrm{S}(p) \wedge t \succ u} \mathrm{C}(p, u) \cdot u, \\
\mathrm{B}_\prec(p, t_1, t_2) &:= \sum_{u \in \mathrm{S}(p) \wedge t_1 \succ u \succ t_2} \mathrm{C}(p, u) \cdot u,
\end{aligned}
$$

(If $\prec$ is clear from the context, we will omit the subscript $\prec$ at these operations. For LPP(p) etc. read "the Leading Power Product of p", "the Leading Coefficient of p", "the Leading Monomial of p", "the Remaining part of p",

"the part of p Higher than t", "the part of p Lower than t", "the part of p Between t_1 and t_2", respectively.)

Of course, for any p and $t_1 \succ t_2$,

$$p = \mathrm{H}(p, t_1) + \mathrm{C}(p, t_1) \cdot t_1 + \mathrm{B}(p, t_1, t_2) + \mathrm{C}(p, t_2) \cdot t_2 + \mathrm{L}(p, t_2).$$

2.5 Admissible Orderings on Polynomials

Any admissible ordering $\prec$ on power products can be extended to a partial ordering on polynomials in the following way.

Definition (Extension of Admissible Ordering): Let $\prec$ be an admissible ordering on $\mathbf{T}$.

$$p \prec q :\Longleftrightarrow \exists t \; (\mathrm{H}_\prec(p, t) = \mathrm{H}_\prec(q, t) \wedge t \notin \mathrm{S}(p) \wedge t \in \mathrm{S}(q)). \; \square$$

In general, the extension of $\prec$ is not any more a total ordering. However, it is Noetherian, which is important for our algorithmic perspective:

Proposition (Properties of Admissible Orderings): Let $\prec$ be the extension of an admissible ordering to $\mathbf{P}$. Then,

$\prec$ is a partial ordering,

$\prec$ is Noetherian,

$\forall p \neq 0 \; (\; \mathrm{p} \succ 0 \;)$.

Proof: Easy from the definitions. For proving Noetherianity of $\prec$ on $\mathbf{P}$, one uses Noetherian induction w.r.t. $\prec$ on $\mathbf{T}$.

2.6 Reduction Modulo Polynomials

From now on, let an admissible ordering $\prec$ on $\mathbf{T}$ (and, hence, on $\mathbf{P}$) be fixed. We will now define a binary relation "reduction modulo a set F of polynomials" and a corresponding reduction algorithm that reduces a given "reducible" polynomial, modulo F to a polynomial which is smaller w.r.t. $\prec$. It will turn out that the reflexive, symmetric, transitive closure of this reduction relation is identical to ideal congruence modulo F. However, reduction brings in an algorithmic flavor. Reduction modulo F can also be viewed as a sort of generalized polynomial division with respect to divisors in F.

Definition (Reduction Modulo Polynomials):

$$\begin{aligned} g \to_{f,t} h &:\Longleftrightarrow t \in \mathrm{S}(g) \wedge \mathrm{LPP}(f) \mid t \wedge h = g - (\mathrm{M}(g,t)/\mathrm{LM}(f)) \cdot f. \\ g \to_f h &:\Longleftrightarrow \exists t \in \mathrm{S}(g)\ (g \to_{f,t} h). \\ g \to_F h &:\Longleftrightarrow \exists f \in F\ (g \to_f h). \\ \underline{g}_F &:\Longleftrightarrow \neg\exists h\ (g \to_F h). \end{aligned}$$

(For $g \to_{f,t} h$, $g \to_f h$, $g \to_F h$ and $\underline{g}_F$ read "g reduces to h modulo f using t","g reduces to h modulo f", "g reduces to h modulo F" and "g is reduced modulo F", respectively.)

Example: Let $\prec$ be the total degree ordering defined by $x \prec y$ and let $g := x^2y^3 + 3xy^2 - 5x$, $f_1 := xy - 2y$, $f_2 := 2y^2 - x^2$. Then, for example

$$g \to_{f_1,xy^2} h_1 := g - (3xy^2/xy) \cdot f_1 = x^2y^3 + 6y^2 - 5x$$

but also

$$g \to_{f_1,x^2y^3} h_2 := g - (x^2y^3/xy) \cdot f_1 = 2xy^3 + 3xy^2 - 5x$$

and also

$$g \to_{f_2,x^2y^3} h_3 := g - (x^2y^3/2y^2) \cdot f_2 = 1/2x^4y + 3xy^2 - 5x.$$

We will now show that reduction is Noetherian, which is important for obtaining an algorithm that computes reduced polynomials modulo a polynomial set F.

Proposition (Noetherianity of Reduction Modulo Polynomials):

$g \to_F h \Longrightarrow g \succ h$.

$\to_F$ is Noetherian.

Proof: If $g \to_{f,t} h$, then $h = \mathrm{H}(g,t) + 0 \cdot t + r$, where $r := \mathrm{L}(g,t) - (\mathrm{M}(g,t)/\mathrm{LM}(f)) \cdot R(f)$. By |-compatibility and monotonicity of $\prec$, $\mathrm{LPP}(r) \prec t$. Hence, $\mathrm{H}(g,t) = \mathrm{H}(h,t)$. Furthermore, $t \in \mathrm{S}(g)$ but $t \notin \mathrm{S}(h)$ and, thus, $g \succ h$. Now, since $\prec$ is Noetherian, also $\to_F$ must be Noetherian.

Let $\to_F^*$ be the reflexive and transitive closure of $\to_F$. By the Noetherianity of $\to_F$ and by the fact that the existence and selection of suitable t and f in the definition of $\to_F$ can of course be handled algorithmically, "by iteration of this selection process", we can easily design an algorithm "RF" with the property stated in the following proposition. We omit the straight-forward details of this algorithm.

Proposition (Property of Reduction Algorithm):

$$g \to_F^* \mathrm{RF}(F,g),$$

$$\underline{\mathrm{RF}(F,g)}_F.$$

(For $\mathrm{RF}(F,g)$ read "a Reduced Form of g modulo F".) □

In fact, we can get out more information from these iterated selection steps. Namely, we can collect the appropriate multiples of the polynomials in F that were selected in the individual reduction steps so that, at termination of RF, we will also have accumulated polynomial "cofactors" available such that $\mathrm{RF}(F,g)$ can be represented as g plus a linear combination of the cofactors with the polynomials in F. More formally, we have an algorithm "Cofactors" that satisfies the following property:

Proposition (Property of Cofactor Algorithm):

$$\mathrm{RF}(F,g) = g + \sum_{f \in F} \mathrm{Cofactors}(F,g)_f \cdot f.$$

(For $\mathrm{Cofactors}(F,g)$ read "the cofactors of the reduced form of g modulo F".) □

Reduction modulo polynomials has a couple of useful elementary properties that will play a crucial role in Gröbner bases construction.

Proposition (Compatibility of Reduction):

$$a \neq 0 \wedge f_1 = a \cdot f_2 \implies \to_{f_1} = \to_{f_2}, \qquad \text{(monicity)}$$

$$g \to_f h \implies a \cdot t \cdot g \to_f a \cdot t \cdot h, \qquad \text{(product compatibility)}$$

$$g \to_f h \implies \exists q (g + p \to_f^* q \leftarrow_f^* h + p). \qquad \text{(sum semi-compatibility)}$$

Proof: Monicity and product compatibility are straight-forward from the definitions. Because of monicity, in the sequel we will be able to restrict our considerations to monic polynomials f, i.e. polynomials whose leading coefficient is 1. This will make the presentation slightly simpler.

Now assume that $g \to_{f,t} h$, and consider an arbitrary p. Define $u := t/\mathrm{LPP}(f)$. Of course, $h = g - \mathrm{C}(g,t) \cdot u \cdot f$. Now

$$\begin{aligned} f &= \mathrm{LPP}(f) + \mathrm{R}(f), \\ g &= \mathrm{H}(g,t) + \mathrm{C}(g,t) \cdot t + \mathrm{L}(g,t), \\ h &= \mathrm{H}(g,t) + 0 \cdot t + \mathrm{L}(g,t) - \mathrm{C}(g,t) \cdot u \cdot \mathrm{R}(f), \\ p &= \mathrm{H}(p,t) + \mathrm{C}(p,t) \cdot t + \mathrm{L}(p,t). \end{aligned}$$

We now have three cases:

Case $\mathrm{C}(p,t) = 0$: In this case, $g + p \rightarrow_{f,t} g + p - \mathrm{C}(g,t) \cdot u \cdot f = h + p$.

Case $0 \neq \mathrm{C}(p,t) = -\mathrm{C}(g,t)$: In this case, $g+p = h+p+\mathrm{C}(p,t)\cdot u\cdot f \leftarrow_{f,t} h+p$.

Case $0 \neq \mathrm{C}(p,t) \neq -\mathrm{C}(g,t)$: In this case,

$g+p \rightarrow_{f,t} g+p-(\mathrm{C}(g,t)+\mathrm{C}(p,t))\cdot u\cdot f = h+p-\mathrm{C}(p,t)\cdot u\cdot f \leftarrow_{f,t} h+p$.□

Note that sum compatibility, i.e.

$$g \rightarrow_f h \Longrightarrow g + p \rightarrow_f h + p,$$

does not hold in general. This fact is the reason for additional technical difficulties encountered in the proof of the main theorem for Gröbner bases (in comparison with analogous situations in general rewriting).

Congruence and reduction are intimately related. For expressing the relation, let now $\longleftrightarrow_F^*$ denote the reflexive, symmetric, and transitive closure of $\rightarrow_F$.

Proposition (Relation Between Reduction and Congruence):

$$g \equiv_F h \Longleftrightarrow g \longleftrightarrow_F^* h.$$

Proof: "$\Longleftarrow$": This direction is easy. Just notice that, if $g \rightarrow_f h$, then h results from g by subtracting a multiple of f.
"$\Longrightarrow$": For this direction we observe, first, that $g \equiv_F h$ implies that, for certain $a \in \mathbf{K}^*$, $t \in \mathbf{T}^*$, $f \in F^*$ with $|a| = |t| = |F|$,

$$g = h + \sum_{1 \leq i \leq |a|} a_i \cdot t_i \cdot f_i.$$

Now one can proceed by induction on $|a|$ using sum semi-compatibility. □

(If you have the feeling that the direction "$\Longrightarrow$" in the above proposition, and sum semi-compatibility, is trivial then you should better go back to the definition of $\rightarrow_F$ and study it carefully. The point is that $g \rightarrow_f h$ entails that $h = g + a \cdot u \cdot f$ for some a and u with the additional property that a power product $t \in \mathrm{S}(g)$ is "cancelled" and $g \succ h$. In contrast, if $h = g + a \cdot u \cdot f$ for some general a and u, we cannot conclude at all that any cancellation takes place nor that $g \succ h$. Therefore the above lemma is non-trivial.)

The above relation does not yet help us deciding whether or not $g \equiv_F h$. We were much better off if we could prove, for example,

$$g \equiv_F h \iff \exists p \, (g \rightarrow_F^* p \leftarrow_F^* h)$$

because this equivalence would allow a "directed" search for an appropriate p in order to decide whether or not $g \equiv_F h$.

However, this equivalence is not true in general.

Now, those sets F for which the above property is true are called *Gröbner bases*. Those are the sets for which $g \longleftrightarrow_F^* h$ (and, hence, $g \equiv_F h$) can be decided by a directed search. Fortunately, we will be able to prove that any F that does not satisfy the above property can be transformed (algorithmically) into an "equivalent" Gröbner basis G, i.e. into a Gröbner basis G for which $\equiv_G = \equiv_F$. This will provide a uniform methodology for tackling quite a few fundamental problems in polynomial ideal theory by structurally simple algorithms.

Before we go into the details of this program, we will summarize a few fundamental properties of general reduction relations that do not depend on the special context of polynomials.

2.7 Some General Properties of Noetherian Reduction Relations

In this subsection, the variables x, y, z, w range over an arbitrary set X. Let $\rightarrow$ be a binary relation on X. Let $\longleftrightarrow$, $\rightarrow^*$ and $\longleftrightarrow^*$ denote the symmetric, the reflexive-transitive, and the reflexive-symmetric-transitive closure of $\rightarrow$, respectively. Furthermore, $\underline{x} :\Longleftrightarrow \neg\exists\, y\,(x \rightarrow y)$. Furthermore, let NF be a function on X such that $\forall\, x\,(x \rightarrow^* \mathrm{NF}(x))$ and $\forall\, x\,(\underline{\mathrm{NF}(x)})$. For "NF$(x)$" read "the Normal Form of x produced by $\rightarrow$". Finally, $x \downarrow^* y :\Longleftrightarrow \exists\, z\,(x \rightarrow^* z \leftarrow^* y)$. (For $x \downarrow^* y$ read "x and y have a common $\rightarrow$ successor".)

Proposition (Church-Rosser Property, Confluence, and Local Confluence): Let $\rightarrow$ be Noetherian. Then the following properties are equivalent:

$\forall x, y\,(x \longleftrightarrow^* y \Longrightarrow x \downarrow^* y)$, (Church-Rosser property)
$\forall x, y\,(x \longleftrightarrow^* y \Longrightarrow \mathrm{NF}(x) = \mathrm{NF}(y))$, (Church-Rosser normal form property)
$\forall x, y, z\,(x \leftarrow^* z \rightarrow^* y \Longrightarrow x \downarrow^* y)$, (confluence)
$\forall x, y, z\,(x \leftarrow z \rightarrow y \Longrightarrow x \downarrow^* y)$. (local confluence)

Proof: The equivalence of the first three properties is easy and, of course, confluence implies local confluence. The converse is the so-called Newman-Lemma introduced in (Newman 1942) whose proof, by Noetherian induction, can be found for example in (Becker, Weispfenning 1993). □

The test for checking the Church-Rosser property can be simplified further. For this, let $<$ be a partial ordering on X.

Definition (Connectibility):

$$x \overset{<w}{\longleftrightarrow}{}^{*} y \iff \exists z \in X^{*} \; (x = z_1 < w \wedge \forall 1 \leq i < |z| \, (z_i \longleftrightarrow z_{i+1} < w) \wedge z_{|z|} = y < w).$$

(For $x \overset{<w}{\longleftrightarrow}{}^{*} y$ read "x can be connected with y by $\rightarrow$ staying $< w$".)

Proposition (Generalized Newman Lemma): Let $<$ be Noetherian and $\rightarrow \subseteq >$. Then the following two properties are equivalent:

$$\forall x, y, z \, (x \leftarrow z \rightarrow y \Longrightarrow x \downarrow^{*} y), \qquad \text{(local confluence)}$$

$$\forall x, y, z \, (x \leftarrow z \rightarrow y \Longrightarrow x \overset{<z}{\longleftrightarrow}{}^{*} y). \qquad \text{(local connectibility)}$$

Proof: This version of Newman's lemma and its proof, by Noetherian induction, is implicit in (Buchberger 1979). I formulated and proved the lemma explicitly in (Winkler, Buchberger 1983). □

When we apply the above proposition to the case of reductions modulo polynomial sets F, we see that "$g \longleftrightarrow_F^{*} h$" and, hence, "$g \equiv_F h$" could be decided algorithmically by checking whether or not $\mathrm{RF}(F, g) = \mathrm{RF}(F, h)$ if $\rightarrow_F$ had the Church-Rosser property. This motivates the following definition of the concept of *Gröbner basis*.

2.8 Gröbner Bases

Definition (Gröbner Basis):

F is a Gröbner basis $\iff$ $\rightarrow_F$ has the Church-Rosser property
(i.e. $\forall g, h \, (g \longleftrightarrow_F^{*} h \Longrightarrow g \downarrow_F^{*} h)$. □

It is relatively easy to give an inconstructive proof that

$$\forall F \, \exists G \, (G \text{ is a Gröbner basis and } \longleftrightarrow_F^{*} = \longleftrightarrow_G^{*}).$$

However, what we want is an *algorithm* that constructs G from F. For this we first try to develop an algorithmic test for deciding whether or not a given F *is* a Gröbner basis. By Newman's lemma, for this it is sufficient to test, for all g, h, and q with $g \leftarrow_F q \rightarrow_F h$, whether or not there exists a p such that $g \rightarrow_F^{*} p \leftarrow_F^{*} h$. However, still, this requires infinitely many tests.

The crucial idea in Gröbner basis theory is the observation that these infinitely many tests can be replaced by the consideration of finitely many "critical situations" that can be characterized by the so-called "S-polynomials" of F.

2.9 S-Polynomials

Definition (S-Polynomials): Let f_1, f_2 be monic polynomials. Then,

$$\mathrm{SP}(f_1, f_2) := u_1 \cdot f_1 - u_2 \cdot f_2,$$

where $u_1 := w/\mathrm{LPP}(f_1)$, $u_2 := w/\mathrm{LPP}(f_2)$, $w := \mathrm{LCM}(\mathrm{LPP}(f_1), \mathrm{LPP}(f_2))$. (For $\mathrm{SP}(f_1, f_2)$ read "the S-polynomials of f_1 and f_2".) □

The intuition behind considering S-polynomials is that LCM($\mathrm{LPP}(f_1)$, $\mathrm{LPP}(f_2)$) is the first power product (in the divisibility ordering) that can be reduced both modulo f_1 and modulo f_2, i.e. where reduction may "diverge" and, hence, an injury of the Church-Rosser property may occur. In the proof of the main theorem we will then see the surprising fact that, fortunately, if for a given (finite) set F no divergence is detected at any of the finitely many $\mathrm{LCM}(\mathrm{LPP}(f_1), \mathrm{LPP}(f_2))$ $(f_1, f_2 \in F)$ then no divergence can occur at any point in the infinite "reduction graph" of $\rightarrow_F$, i.e. $\rightarrow_F$ has the Church-Rosser property or, in other words F is a Gröbner basis. Thus, by considering S-polynomials we obtain a finite algorithmic check for testing whether or not a given F is a Gröbner basis.

2.10 The Main Theorem: Algorithmic Characterization of Gröbner Bases by S-Polynomials

In the sequel, by the property (monicity), we may assume without loss of generality that all polynomials in F are monic.

Theorem (Main Theorem of Gröbner Basis Theory):

$$F \text{ is a Gröbner basis} \iff \forall f_1, f_2 \in F\,(\mathrm{RF}(F, \mathrm{SP}(f_1, f_2)) = 0).$$

Proof: The direction "$\Longrightarrow$" is easy. Namely, if $f_1, f_2 \in F$, then $\mathrm{SP}(f_1, f_2) \in \mathrm{Ideal}(F)$, i.e. $\mathrm{SP}(f_1, f_2) \equiv_F 0$. By the relation between reduction and congruence this implies that $\mathrm{SP}(f_1, f_2) \longleftrightarrow_F^* 0$. Hence, RF(F, $\mathrm{SP}(f_1, f_2)$) = $\mathrm{RF}(F, 0) = 0$ because F is a Gröbner basis (and because of the equivalence between the Church-Rosser property and the normal form Church-Rosser property).

For the direction "$\Longleftarrow$", by the generalized Newman lemma and the fact that $\rightarrow_F \subseteq \succ$, it suffices to prove local connectibility, i.e. it suffices to prove that under the assumption

$$g_1 \leftarrow_F h \rightarrow_F g_2$$

we have

$$g_1 \overset{\prec h}{\longleftrightarrow}{}^*_F g_2.$$

By the assumption, there exist $f_1, f_2 \in F$ and $t_1, t_2 \in \mathrm{S}(h)$ with $\mathrm{LPP}(f_1) \mid t_1$ and $\mathrm{LPP}(f_2) \mid t_2$, such that $h \rightarrow_{f_1,t_1} g_1$ and $h \rightarrow_{f_2,t_2} g_2$.

Now we have three cases.

Case $t_1 \succ t_2$: In this case,

$$g_1 = \mathrm{H}(h,t_1) + 0 \cdot t_1 + \mathrm{B}(h,t_1,t_2) + \mathrm{C}(h,t_2) \cdot t_2 + \mathrm{L}(h,t_2) - \\ - \mathrm{C}(h,t_1) \cdot u_1 \cdot \mathrm{R}(f_1)$$

and

$$g_2 = \mathrm{H}(h,t_1) + \mathrm{C}(h,t_1) \cdot t_1 + \mathrm{B}(h,t_1,t_2) + 0 \cdot t_2 + \mathrm{L}(h,t_2) - \\ - \mathrm{C}(h,t_2) \cdot u_2 \cdot \mathrm{R}(f_2),$$

where $u_1 := t_1/\mathrm{LPP}(f_1)$, $u_2 := t_2/\mathrm{LPP}(f_2)$.

Furthermore,

$$g_2 \rightarrow_{f_1} g_{1,2} := \mathrm{H}(h,t_1) + 0 \cdot t_1 + \mathrm{B}(h,t_1,t_2) + 0 \cdot t_2 + \mathrm{L}(h,t_2) - \\ - \mathrm{C}(h,t_1) \cdot u_1 \cdot \mathrm{R}(f_1) - \\ - \mathrm{C}(h,t_2) \cdot u_2 \cdot \mathrm{R}(f_2).$$

Now, $g_1 = h - \mathrm{C}(h,t_1) \cdot u_1 \cdot f_1$ and $g_{1,2} = g_2 - \mathrm{C}(h,t_1) \cdot u_1 \cdot f_1$ and, by assumption, $h \rightarrow_F g_2$. Hence, by sum semi-compatibility, $g_1 \downarrow_F^* g_{1,2}$ and, hence, $g_1 \overset{\prec h}{\longleftrightarrow}{}^*_F g_2$. (Note that, in general, $g_1 \rightarrow_{f_1} g_{1,2}$ need not be the case. Why not?)

Case $t_1 \prec t_2$: Analogous.

Case $t := t_1 = t_2$: In this case,

$$g_1 = \mathrm{H}(h,t) + 0 \cdot t + \mathrm{L}(h,t) - \\ - \mathrm{C}(h,t) \cdot u_1 \cdot \mathrm{R}(f_1)$$

and

$$g_2 = \mathrm{H}(h,t) + 0 \cdot t + \mathrm{L}(h,t) - \\ - \mathrm{C}(h,t) \cdot u_2 \cdot \mathrm{R}(f_2).$$

Hence,

$$\begin{aligned} g_1 - g_2 &= -\mathrm{C}(h,t) \cdot (u_1 \cdot R(f_1) - u_2 \cdot R(f_2)) = \\ &= -\mathrm{C}(h,t) \cdot (u_1 \cdot f_1 - u_2 \cdot f_2) = -\mathrm{C}(h,t) \cdot v \cdot SP(f_1,f_2), \end{aligned}$$

where $v := t/\ \mathrm{LCM}(\ \mathrm{LPP}(f_1), \mathrm{LPP}(f_2)\ )$.

We have assumed that $\mathrm{RF}(F,\mathrm{SP}(f_1,f_2)) = 0$, i.e. $\mathrm{SP}(f_1,f_2) \to_F^* 0$. Hence, by product compatibility, $g_1 - g_2 = -\mathrm{C}(h,t)\cdot v \cdot SP(f_1,f_2) \to_F^* 0$. This means that there exists a sequence $p \in \mathbf{P}^*$ such that

$$\begin{aligned} p_1 &= g_1 - g_2, \\ \forall 1 \leq i < |p|\ (p_i &\to_F p_{i+1}), \end{aligned} \qquad (*)$$

and

$$p_{|p|} = 0.$$

Furthermore note that, because of $\to_F \subseteq \succ$,

$$\forall 1 \leq i \leq |p|\ (\, p_i \preceq g_1 - g_2 \prec h).$$

Thus, by sum semi-compatibility applied to (*),

$$\begin{aligned} g_1 &= p_1 + g_2, \\ \forall 1 \leq i < |p|\ (p_i + g_2 &\downarrow_F^* p_{i+1} + g_2), \\ g_2 &= p_{|p|} + g_2. \end{aligned}$$

Also, we have

$$\forall 1 \leq i \leq |p|\ (\, p_i + g_2 \prec h)$$

because

$$\forall 1 \leq i \leq |p|\ (\, \mathrm{H}(p_i + g_2, t) = \mathrm{H}(h,t) \wedge \mathrm{C}(p_i + g_2, t) = 0).$$

Thus, summarizing, $g_1 \overset{\prec h}{\longleftrightarrow}{}^*_F\, g_2$ also in this case.

2.11 An Algorithm for Constructing Gröbner Bases

The main theorem can immediately be read as an algorithm for testing whether or not a given *finite* F is a Gröbner basis. However, it can also be used to show that the following, structurally simple, algorithm "Gröbner-Basis" (formulated here in a functional style) meets the specification given in the proposition below.

Algorithm (Construction of a Gröbner Basis):

$\mathrm{Gröbner\text{-}Basis}(F) := \mathrm{GB}(F, \{\{f_1, f_2\} \mid f_1, f_2 \in F\})$.

$\mathrm{GB}(F, \emptyset) := F$,

$\mathrm{GB}(F, \{f_1, f_2\} \smile B) :=$

$\mathrm{GB}(F, B)$, if $h = 0$,

$\mathrm{GB}(F \cup \{h\}, B \cup \{\{h, f\} \mid f \in F\})$, otherwise,

where $h := \mathrm{RF}(F, \mathrm{SP}(f_1, f_2))$.□

(Here, $\smile$ is a constructor for finite sets such that $x \smile X = Y$ iff $\{x\} \cup X = Y$ and $x \notin X$.)

Proposition (Correctness of the Gröbner-Basis Algorithm): For finite sets F:

$$\text{Gröbner-Basis}(F) \text{ is a Gröbner basis,}$$

$$\text{Ideal}(F) = \text{Ideal}(\text{ Gröbner-Basis}(F)).$$

Proof (Sketch): (The algorithm always terminates by Dickson's lemma because the leading power product of a polynomial h that gets adjoined to an intermediate set F is not a multiple of the leading power product of any $f \in F$.) The final set F clearly satisfies the condition in the main theorem and, hence, is a Gröbner basis. Furthermore, any h that gets adjoined to an intermediate F is in Ideal(F) and hence in the ideal generated by the input set. □

Gröbner bases can be made unique by "interreducing" them:

Definition (Reduced Gröbner Bases):

$$F \text{ is a reduced Gröbner basis} \quad :\Longleftrightarrow \quad F \text{ is a (monic) Gröbner basis,}$$
$$\forall f \in F\,(\underline{f}_{(F-\{f\})}).\ \square$$

The above algorithm can be easily converted into an algorithm "Reduced-Gröbner-Basis" that yields a reduced Gröbner basis and it is easy to show that these bases are unique in the following sense:

Proposition (Canonicality):

$$\text{Ideal}(F) = \text{Ideal}(G) \Longrightarrow$$

$$\text{Reduced-Gröbner-Basis}(F) = \text{ Reduced-Gröbner-Basis}(G).\ \square$$

The above crude form of the algorithm can be made much more efficient by introducing "criteria" by which one can predict that certain S-polynomials reduce to zero without actually carrying out the reduction. This idea was introduced in (Buchberger 1979) and is an easy consequence of the main theorem in the form given above using our generalized Newman lemma. The strategy of using "criteria" later was carried over and proved useful also in the Knuth-Bendix completion algorithm in the area of rewriting.

In fact, the above algorithms Gröbner-Basis and Reduced-Gröbner-Basis should be indexed by one more parameter, namely the admissible ordering $\prec$ used. When, in the applications below, indication of the ordering used is important we will therefore write "Gröbner-Basis$_\prec$" etc.

2.12 Other Characterizations of Gröbner Bases

Gröbner bases can also be characterized by quite a few other properties, see the text books on the subject. The equivalence proofs are quite simple except the one that relates Gröbner bases F to "syzygies", i.e. to the solutions of linear diophantine equations with coefficients from F.

3 Applications of Gröbner Bases

3.1 Overview

Over the years, literally dozens of applications have been found for the Gröbner bases algorithm, see the recent text books, for example (Becker, Weispfenning 1993), (Cox et al. 1992) and the papers on applications in this book. In this section, we only briefly summarize the most fundamental problems to which the Gröbner bases algorithm can be applied.

We present most of these problems and their algorithmic solutions by formulating a mathematical theorem whose left-hand side defines a problem and whose right-hand describes the algorithmic solution. The proofs of most of these theorems are easy consequences of the main theorem and the various equivalent forms of it. Some of the applications need additional knowledge for which we refer to the text books.

3.2 Ideal Membership, Canonical Simplification, Ideal Identity

$f \in \text{Ideal}(F) \Longleftrightarrow \text{RF}(\text{Gröbner-Basis}(F), f) = 0.$
(This problem is sometimes called the "main problem of polynomial ideal theory".)

$f \equiv_F g \Longleftrightarrow \text{RF}(\text{Gröbner-Basis}(F), f) = \text{RF}(\text{Gröbner-Basis}(F), g),$

$f \equiv_F \text{RF}(\text{Gröbner-Basis}(F), f).$

(The last two properties show that "RF" modulo a Gröbner-Basis(F) is a canonical simplifier for $\equiv_F$. For the notion of "canonical simplifier" see (Buchberger, Loos 1982).)

$\text{Ideal}(F) \subseteq \text{Ideal}(G) \Longleftrightarrow \forall f \in F\,(\text{RF}(\text{Gröbner-Basis}(G), f) = 0).$

$\text{Ideal}(F) = \text{Ideal}(G) \Longleftrightarrow$
$\text{Reduced-Gröbner-Basis}(F) = \text{Reduced-Gröbner-Basis}(G).$

Ideal(F) = Ideal(Reduced-Gröbner-Basis(F)).

(The last two properties show that "Reduced-Gröbner-Basis" is a canonical simplifier for the equivalence $\sim$ defined by $F \sim G :\Longleftrightarrow$ Ideal(F) = Ideal(G) on the set of subsets of $\mathbf{P}$.)

3.3 Radical Membership

f $\in$ Radical(F) $\Longleftrightarrow$ 1 $\in$ Gröbner-Basis($F \cup \{y \cdot f - 1\}$) (where y is a new indeterminate). □

(On this test, a systematic method for deciding a large class of geometrical propositions can be based, see the example in the first section. It is much harder to compute, by Gröbner bases, a basis for the radical of an ideal because one must have a means of factorization in extension fields. Even harder is the determination of a complete "primary decomposition" of an ideal that, roughly, corresponds to a decomposition of algebraic varieties into irreducible varieties, see (Becker, Weispfenning 1993).)

3.4 Computation in Residue Class Rings Modulo Ideals

Let $(\mathbf{P}_F, +_F, 0_F, -_F, \cdot_F, 1_F)$ be the residue class ring of $(\mathbf{P}, +, 0, -, \cdot, 1)$ modulo Ideal(F).

Let $\underline{F}$:= Gröbner-Basis(F) and $(\underline{\mathbf{P}}, \underline{+}, \underline{0}, \underline{-}, \underline{\cdot}, \underline{1})$ be the following structure:

$$\begin{aligned} \underline{\mathbf{P}} &:= \{f \in \mathbf{P} | \underline{f}_{\underline{F}}\}, \\ f \underline{+} g &:= \mathrm{RF}(\underline{F}, f + g), \\ \underline{0} &= 0, \\ \underline{-} f &:= \mathrm{RF}(\underline{F}, -f), \\ f \underline{\cdot} g &:= \mathrm{RF}(\underline{F}, f \cdot g), \\ \underline{1} &= 1, \end{aligned}$$

Then $(\mathbf{P}_F, +_F, 0_F, -_F, \cdot_F, 1_F)$ is isomorphic to $(\underline{\mathbf{P}}, \underline{+}, \underline{0}, \underline{-}, \underline{\cdot}, \underline{1})$ by the following isomorphism i:

$$i(f) := \text{ the residue class of } f \text{ modulo Ideal}(F) \text{ (for all} f \in \underline{\mathbf{P}}).$$

$\mathbf{B} := \{ t \in \mathbf{T} \mid \neg\exists f \in \underline{F} \text{ (LPP}(f) \,|\, t) \}$ is a linearly independent basis for the vector space $(\mathbf{K}, \underline{\mathbf{P}}, \underline{+}, \underline{0}, \underline{-}, \underline{\cdot})$.

The following elements in $\mathbf{K}$

$$\mathrm{SC}_{t,u,v} := \mathrm{C}(\mathrm{RF}(\underline{F}, t \cdot u), v),$$

are the "structure constants" of the associative algebra $(\mathbf{K}, \underline{\mathbf{P}}, \underline{+}, \underline{0}, \underline{-}, \underline{\cdot})$, i.e., for all $t, u, v \in \mathbf{B}$,

$$t \underline{\cdot} u = \sum_{v \in \mathbf{B}} \mathbf{SC}_{t,u,v} \cdot v.$$

In other words, having computed a Gröbner basis $\underline{F}$ for a given F, one can master arithmetics in the residue class ring modulo Ideal(F) completely algorithmically. On this method, one can also base algorithms for computing in algebraic extension fields which can be considered as residue class rings modulo polynomial ideals.

3.5 Leading Power Products

$$\{\text{LPP}(f) |\ f \in \text{Ideal}(F)\} = \{u \cdot \text{LPP}(f)\ |\ u \in \mathbf{T} \wedge f \in \text{Gröbner-Basis}(F)\}.$$

Ideal(F) is a principal ideal $\Longleftrightarrow$ Reduced-Gröbner-Basis(F) has exactly one element.

3.6 Polynomial Equations

$$\begin{aligned} \text{Ideal}(F) = \mathbf{P} &\Longleftrightarrow 1 \in \text{Gröbner-Basis}(F) \\ &\Longleftrightarrow \text{Reduced-Gröbner-Basis}(F) = \{1\}. \end{aligned}$$

Let $\mathbf{K}$ be algebraically closed:
F is solvable (i.e. has a solution in $\mathbf{K}$) $\Longleftrightarrow 1 \notin$ Gröbner-Basis(F).

F has only finitely many solutions $\Longleftrightarrow$
$\forall 1 \leq i \leq n\ \exists f \in \text{Gröbner-Basis}(F)\ \exists j\ (\ \text{LPP}(f) = x_i^j\ )$.

For all F with finitely many solutions:
the number of solutions of F (counting multiplicities) =
$|\ \{t \in \mathbf{T} \mid \neg\exists f \in \text{Gröbner-Basis}(F)\ (\ \text{LPP}(f) \mid t\ )\ \}\ |$.

Let $U \subset \mathbf{T}$ be finite:
$\exists\, \text{f} \in \text{Ideal}(F)\ (\ \text{S}(f) \subseteq U) \Longleftrightarrow$
$\{\ \text{RF}(\ \text{Gröbner-Basis}(F),\ u\ ) \mid u \in U\}$ is linearly dependent over $\mathbf{K}$. □

By applying this property successively to the powers $1, x, x^2, x^3, \ldots$, one can algorithmically find, for example, the univariate polynomial in x of minimal degree in Ideal(F) if it exists. Such a polynomial exists iff F has only finitely many solutions, which can be checked algorithmically by the above method. On this algorithm a general method for solving arbitrary systems

of polynomial equations can be based, see (Buchberger 1970), which works for arbitrary term orderings $\prec$ whereas the elimination method mentioned below works only for elimination orderings. Also, this algorithm can be used for transforming a Gröbner basis w.r.t. a given admissible ordering $\prec_1$ into a Gröbner basis w.r.t. $\prec_2$. This is sometimes helpful because the complexity of Gröbner bases computation depends strongly on the term ordering chosen. Basically this idea is used in the recent, most advanced, version of the Gröbner bases algorithm for improving efficiency, see (Collart et al.).

3.7 Linear Syzygies

Let $F \subseteq \mathbf{P}$ be finite and $h : F \to \mathbf{P}$ (i.e. a sequence of polynomials indexed by F).

> h is a (linear) syzygy for $(F, g) :\Longleftrightarrow \sum_{f \in F} h_f \cdot f = g$.
> (For "h is a linear syzygy for (F, g)" we also say "h is a solution of the inhomogeneous diophantine equation given by F and g.").
>
> h is a (linear) syzygy for $F :\Longleftrightarrow h$ is a syzygy for $(F, 0)$ (i.e. $\sum_{f \in F} h_f \cdot f = 0$).
> (For "h is a linear syzygy for F" we also say "h is a solution of the homogeneous diophantine equation given by F.").

Let F be a Gröbner basis:

> The diophantine equation given by (F, g) is solvable (i.e. $\exists h$ (h is a syzygy for (F, g)) $\Longleftrightarrow \mathrm{RF}(F, g) = 0$.
>
> The diophantine equation given by (F, g) is solvable $\Longrightarrow$ Cofactors(F, g) is a syzygy for (F, g).

The following set of sequences is a finite basis for the infinite module of all solutions of the homogeneous diophantine equation given by F:

$$\{S^{f,g} \mid f, g \in F\},$$

where, for arbitrary $f, g \in F$,

$$S^{f,g} : F \to \mathbf{P},$$

$$S_f^{f,g} := u - P_f^{f,g},$$

$$S_g^{f,g} := -v - P_g^{f,g}$$

$$S_h^{f,g} := -P_h^{f,g}, \text{ if } h \in F - \{f, g\},$$

$$u := \mathrm{LCM}(\mathrm{LPP}(f), \mathrm{LPP}(g))/\mathrm{LPP}(f),$$

$v := \mathrm{LCM}(\mathrm{LPP}(f), \mathrm{LPP}(g))/\mathrm{LPP}(g)$,

$P^{f,g} := \mathrm{Cofactors}(F, \mathrm{SP}(f,g))$.□

Thus, essentially, the reduction of all the S-polynomials of F establishes a finite basis for the module of homogeneous syzygies. By adding one solution of the inhomogeneous equations one obtains all the solutions of the inhomogeous diophantine equation.

For obtaining a basis for the syzygies for a diophantine equation with arbitrary F, one first computes $\underline{F} = \text{Gröbner-Basis}(F)$. Then one solves the problem for $\underline{F}$ as above. The solutions found can transformed back to solutions for F by multiplication with matrices with polynomial entries that can be obtained from expressing $\underline{F}$ in terms of F and F in terms of $\underline{F}$ using the Cofactor algorithm.

Systems of linear diophantine equations can be handled by reducing the problem recursively to the case of just one equation.

3.8 Hilbert Functions

Let the term ordering $\prec$ be a total degree ordering. The "Hilbert function" H is defined as follows:

$$\begin{aligned} \mathrm{H}(d,F) \quad := \quad & \text{the number of modulo Ideal}(F) \text{ linearly} \\ & \text{independent polynomials } f \text{ with Degree}(f) \leq d. \end{aligned}$$

(The Hilbert function is important because it allows to read off various structural information on the variety of F.)

Now,

$$\mathrm{H}(d,F) = \binom{d+n}{n} -$$

$$-|\{u \in \mathbf{T} \mid \mathrm{Degree}(u) \leq d \wedge \neg\exists f \in \text{ Gröbner-Basis}(F)\,(\mathrm{LPP}(f) \mid u)\}|.$$

3.9 Elimination Ideals

Let $\prec$ be the lexical term ordering defined by $x_1 \prec x_2 \prec \ldots \prec x_n$. Then,

$$\begin{aligned} &\text{Gröbner-Basis}_{\prec}(F) \cap \mathbf{K}[x_1, \ldots, x_i] \text{ is a Gröbner basis for} \\ &(\text{ Ideal}(F) \cap \mathbf{K}[x_1, \ldots, x_i]). \end{aligned}$$

$$\begin{aligned} &\text{Reduced-Gröbner-Basis}_{\prec}(F) \cap \mathbf{K}[x_1, \ldots, x_i] = \\ &= \text{Reduced-Gröbner-Basis}_{\prec}(\text{Ideal}(F) \cap \mathbf{K}[x_1, \ldots, x_i]). \square \end{aligned}$$

This property leads immediately to a general solution method, by "successive substitution", for arbitrary systems of polynomial equations with finitely many solutions, see the example in the first lecture.

Let $\prec$ be a term ordering in which power products containing no other indeterminates except $x_{i_1}, \ldots, x_{i_m}$ are $\prec$ then all the other power products.

$$\text{Ideal}(F) \cap \mathbf{K}[x_{i_1}, \ldots, x_{i_m}] = \emptyset \iff$$

$$\text{Gröbner-Basis}_{\prec}(F) \cap \mathbf{K}[x_{i_1}, \ldots, x_{i_m}] = \emptyset. \square$$

(In case $\text{Ideal}(F) \cap \mathbf{K}[x_{i_1}, \ldots, x_{i_m}] = \emptyset$ one says that the indeterminates x_{i_1}, $\ldots$, x_{i_m} are algebraically independent modulo $\text{Ideal}(F)$. The above criterion for independence yields an algorithm for determining the dimension of $\text{Ideal}(F)$, i.e. the maximal number of independent indeterminates modulo $\text{Ideal}(F)$.)

3.10 Ideal Operations

Let $\prec$ be an admissible term ordering in which power products containing $x_1, \ldots, x_n$ are $\prec$ than any power product containing the new variable y:

$\text{Gröbner-Basis}_{\prec}(\{y \cdot f \mid f \in F\} \cup \{(1-y) \cdot g \mid g \in G\}) \cap \mathbf{K}[x_1, \ldots, x_n]$ is a Gröbner basis for $\text{Ideal}(F) \cap \text{Ideal}(G)$.

$$\text{Reduced-Gröbner-Basis}_{\prec}(\text{Ideal}(F) \cap \text{Ideal}(G)) =$$
$$= \text{Reduced-Gröbner-Basis}_{\prec}(\{y \cdot f \mid f \in F\} \cup \{(1-y) \cdot g \mid g \in G\})$$
$$\cap \mathbf{K}[x_1, \ldots, x_n].$$

(This property yields also an algorithm for quotients of finitely generated ideals because the determination of such quotients can be reduced to the determination of intersections. Alternatively, quotients of ideals can be computed by using the algorithm for linear syzygies.)

3.11 Algebraic Relations and Implicitization

Let $F = \{f_1, \ldots, f_m\} \subseteq \mathbf{K}[x_1, \ldots, x_n]$, let $y_1, \ldots, y_m$ be new indeterminates and let $\prec$ be an admissible ordering in which power products containing only the y_i are $\prec$ any other power product. Then,

$\text{Gröbner-Basis}_{\prec}(\{y_1 - f_1, \ldots, y_m - f_m\}) \cap \mathbf{K}[y_1, \ldots, y_m]$ is a Gröbner basis for $\{g \in \mathbf{K}[y_1, \ldots, y_m] \mid g(f_1, \ldots, f_m) = 0\}$.

(The set $\{g \in \mathbf{K}[y_1, \ldots, y_m] \mid g(f_1, \ldots, f_m) = 0\}$ is, in fact, an ideal. It is called the "ideal of algebraic relations (or non-linear syzygies) over F".)

Let $R := \text{Gröbner-Basis}_{\prec}(\{y_1 - f_1, \ldots, y_m - f_m\}) \cap \mathbf{K}[y_1, \ldots, y_m]$ and let $\mathbf{K}$ be algebraically closed. Then the variety of R is the smallest variety in $\mathbf{K}$ that contains the set

$$\{(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)) \mid x_1, \ldots, x_n \in \mathbf{K}\}.$$

(This means that R is an "implicit" representation of the set given in "parametric" representation by $f_1, \ldots, f_m$.)

3.12 Inverse Mappings

Let $F = \{f_1, \ldots, f_n\} \subseteq \mathbf{K}[x_1, \ldots, x_n]$, let $y_1, \ldots, y_n$ be new indeterminates and let $\prec$ be an admissible ordering with the property of the previous section. Then,

$$\begin{array}{rcl} \text{the mapping } M : \mathbf{K}^n & \to & \mathbf{K}^n \text{ is bijective} \\ (a_1, \ldots, a_n) & \mapsto & (f_1(a_1, \ldots, a_n), \ldots, f_n(a_1, \ldots, a_n)) \end{array}$$

$$\Longleftrightarrow$$

$$\begin{array}{c} \text{Reduced-Gröbner-Basis}_{\prec}(y_1 - f_1, \ldots, y_n - f_n) \text{ has the form} \\ \{x_1 - g_1, \ldots, x_n - g_n\} \text{ with } \{g_1, \ldots, g_n\} \subseteq \mathbf{K}[y_1, \ldots, y_n]. \end{array}$$

(Moreover, the g_i define the mapping which is inverse to M.)

3.13 Miscellaneous

In fact, by combining the above methods, a big number of particular problems in various areas of mathematics have been attacked in the literature. Some of these applications of Gröbner bases are quite unexpected. For example, geometrical theorem proving, integer programming, integration of rational functions, greatest common divisor and factorization of multivariate polynomials, bases for Bezier splines, bases for Runge-Kutta numerical integration formulae, interpretation of resolution theorem proving in boolean rings etc. have been studied successfully using Gröbner bases, see the other tutorial papers in this book.

Acknowledgement: My sincere thanks to Daniela Văsaru and Wolfgang Windsteiger for carefully checking the paper and preparing the Latex version. Some work on the paper was done during a stay of the author at the University of Tsukuba, chair of Professor Tetsuo Ida, in the frame of the TARA project and an invitation by the Japanese Society for the Promotion of Science.

References

An extensive bibliography on Gröbner bases giving credit also to the original papers on the various applications is contained in the book by Becker and Weispfenning (1993). Below we only list those papers that are explicitly referenced in the present paper.

Becker, T., Weispfenning, V. (1993): Gröbner Bases: A Computational Approach to Commutative Algebra. Springer-Verlag, New York

Buchberger, B. (1965): An Algorithm for Finding a Basis for the Residue Class Ring of a Zero-Dimensional Polynomial Ideal (German). PhD Thesis, University of Innsbruck, Institute for Mathematics

Buchberger, B. (1970): An Algorithmic Criterion for the Solvability of Algebraic Systems of Equations (German). Aequationes Mathematicae 4: 374-383

Buchberger, B. (1979): A Criterion for Detecting Unnecessary Reductions in the Construction of Gröbner bases. In: Ng (ed.): Proceedings of the EUROSAM '79 , Springer, pp. 3-21 (Lecture notes in computer science, vol. 72)

Buchberger, B. (1985): Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory. In: Bose, N. K. (ed): Multidimensional Systems Theory. D. Reidel, Dordrecht, pp. 184-232

Buchberger, B., Elias, J. (1992): Using Gröbner Bases for Detecting Polynomial Identities: A Case Study on Fermat's Ideal. J. Number Theory 41: 272-279

Buchberger, B., Kutzler, B. (1986): Computer-Algebra for the Engineer (German). In: Rechnerorientierte Verfahren, Teubner Verlag, Stuttgart, pp. 11-69

Buchberger, B., Loos, R. (1982): Algebraic Simplification. In: Buchberger, B., Collins, G.E., Loos, R. (eds): Computer Algebra: Symbolic and Algebraic Computation. Springer, Vienna, pp. 11-44

Collart, S., Kalkbrener, M., Mall, D. (1997): Converting Bases with the Gröbner Walk. J. Symb. Comp., to appear.

Cox, D., Little, J., O'Shea, D. (1992): Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra. Springer-Verlag, New York

Dickson, L.E. (1913): Finiteness of the Odd Perfect and Primitive Abundant Numbers With n Distinct Prime Factors. American J. Math. 35: 413-422

Elias, J. (1988): On Fermat's Ideal. Technical Report, Univ. Barcelona, Dept. of Algebra and Geometry

Hermann, G. (1926): The Question of Finitely Many Steps in the Theory of Polynomial Ideals (German). Mathematische Annalen 95: 736-788

Newman, M.H.A. (1942): On Theories with a Combinatorial Definition of Equivalence. Annals of Mathematics 43: 233-243

Sturmfels, B. (1993): Algorithms in Invariant Theory. In: Buchberger, B., Collins, G. (eds.): Texts and Monographs in Symbolic Computation. Springer Verlag Wien

Trinks, W. (1978): On Buchberger's Method for Solving Systems of Algebraic Equations (German). J. Number Theory 10: 475-488

Winkler, F., Buchberger, B. (1983): A Criterion for Eliminating Unnecessary Reductions in the Knuth-Bendix Algorithm. Colloquia Math. Soc. J. Bolyai 42: 849-869