COMPUTERS IN MATHEMATICS

Edited by

DAVID V. CHUDNOVSKY
Columbia University
New York, New York

RICHARD D. JENKS
IBM Thomas J. Watson Research Center
Yorktown Heights, New York

MARCEL DEKKER, INC. New York and Basel

LIBRARY OF CONGRESS CATALOGING-IN-PUBLICATION DATA

Computers in mathematics / edited by David V. Chudnovsky, Richard D. Jenks.
p. cm. --(Lecture notes in pure and applied mathematics ; 125)
Talks from the International Conference on Computers and Mathematics which took place July 29-Aug. 1, 1986 on the campus of Stanford University, sponsored by the American Association for Artificial Intelligence and the ACM Special Interest Group on Symbolic and Algebraic Manipulation.
Includes bibliographical references.
ISBN 0-8247-8341-7 (alk. paper)
1. Mathematics--Data processing--Congresses. I. Chudnovsky, David V. II. Jenks, Richard D. III. International Conference on Computers and Mathematics (1986 : Stanford University) IV. American Association for Artificial Intelligence. V. Association for Computing Machinery. Special Interest Group on Symbolic & Algebraic Manipulation. VI. Series: Lecture notes in pure and applied mathematics ; v. 125.
QA76.95.C645 1990
510' .285--dc20 90-34508
CIP

This book is printed on acid-free paper.

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

Current printing (last digit):
10 9 8 7 6 5 4 3 2 1

PRINTED IN THE UNITED STATES OF AMERICA

Solution of Equations I: Polynomial Ideals and Gröbner Bases

FRANZ WINKLER University of Delaware, Newark, Delaware

0. Introduction

The idea of using Gröbner bases for solving equations which arise from a given polynomial ideal is relatively new. Gröbner bases have been introduced by B.Buchberger in his dissertation in 1965, but only about ten years ago has the computer algebra community become aware of them and packages for computing and using Gröbner bases have only recently been added to existing computer algebra systems.

The problems, however, which can be attacked via Gröbner bases have a long history. In [Hilbert 1890] D. Hilbert investigates the problem of computing a basis for the syzygies of a finite set of polynomials over a field. Actually he considers a more general problem, namely solving a system of equations

$$(1) \quad f_{i1}z_1 + \dots + f_{is}z_s = 0 \quad , (i=1,\dots,t).$$

By induction on the number of variables he shows how to construct a basis for the space of all solutions of the system (1). In [Hermann 26] G. Hermann uses Hilbert's method to derive a bound for the degree of a basis for the solutions of (1). After a slight correction, this bound is

$$m(t,q,n) = 1/2 \sum_{i=0}^{n-1} (2qt)^{2^i},$$

where q is the maximal degree of the f_{ij}'s and n is the number of variables. Hermann goes on to show in Satz 4 that for every ideal I there exists a basis $f_1,\dots,f_t$ such that every g in I can be represented by a linear combination

(2) $g = g_1 f_1 + \dots + g_t f_t$

such that the degree of every summand $g_i f_i$ is bounded by the degree of g. She also gives an algorithm for constructing such a basis from an arbitrary basis of the ideal I. The degree of such a distinguished basis can be bounded by $m(1,q,n)$, where q is the maximal degree of the given basis polynomials. A basis for which (2) holds has been called an H-basis in [Macauley 16]. Obviously such a basis immediately leads to an algorithm for deciding the ideal membership problem. In [Buchberger 65] Buchberger introduces the concept of a Gröbner basis, as a basis which allows to reduce all polynomials in the ideal to 0. He also gives an algorithm for constructing such a basis. It turns out that every Gröbner basis is an H-basis, but not vice versa [Buchberger 81]. Hironaka's definition of a standard basis [Hironaka 64] for an ideal in a regular local ring is basically identical to Buchberger's definition of a Gröbner basis. However, Hironaka does not give an algorithm for computing such a basis.

Gröbner bases are useful in computer algebra systems at least in two different ways. First, they allow to find solutions to a number of algebraic problems which are important in their own right. Some of these problems will be discussed in this paper. For a more extensive list of applications we refer to [Buchberger 83], [Buchberger 85], [Winkler et al 85], [Trinks 78], and [Möller/Mora 86]. Secondly, Gröbner bases can be used to simplify complicated partial results with respect to polynomial side relations. Simplification is one of the main problems in computer algebra.

Gröbner bases can be viewed in the context of equational theorem proving. Actually a Gröbner basis gives rise to a canonical reduction relation for the ideal congruence. Buchberger's algorithm for constructing a Gröbner basis is essentially a completion algorithm for the associated equational theory [Llopis 83], [Kandri-Rody/Kapur 83], [Winkler 84]. This correspondence has been helpful in tranferring computational improvements in the construction of a Gröbner basis to the general situation of completing a reduction system for an equational theory [Winkler/Buchberger 83].

In this paper we concentrate on applying Gröbner bases to solving equations that arise from a given set of polynomials. In chapter 1 we specify the problems considered in this paper, in chapter 2 we give the definition of a Gröbner basis and an algorithm for constructing one, and in chapter 3 we describe how a Gröbner basis can be used to solve the problems stated in chapter 1.

1. Problems

In this and the following chapters we assume that K is a field. Whenever we talk about polynomials we mean polynomials over K in the indeterminates $x_1,\dots,x_n$.

1.1. System of algebraic equations

We suppose that we are given polynomials $f_1,\dots,f_s$. We are looking for the common zeros of the given polynomials in the algebraic closure $\bar{K}$ of the field K, i.e. we want to solve the following problem:

(P1) given: a finite set $F=\{f_1(x_1,\dots,x_n),\dots,f_s(x_1,\dots,x_n)\}$ of polynomials,
find: the set of points $(x_1,\dots,x_n)$ in $\bar{K}^n$, for which all the polynomials in F vanish.

1.2. The equational theory associated with a polynomial ideal

For given equations $f_1=0,\dots,f_s=0$ we ask whether another equation $f=0$ can be derived from them, using the following equational calculus:

$$\frac{}{f=g} \qquad \text{for all } f=g \text{ in the set of axioms,}$$

$$\frac{}{f=f}\,,\ \frac{f=g}{g=f}\,,\ \frac{f=g,\ g=h}{f=h} \qquad \text{for all polynomials } f,g,h$$

$$\frac{f=g}{fh=gh}\,,\ \frac{f=g}{f+h=g+h} \qquad \text{for all polynomials } f,g,h,$$

$$\frac{f=f',\ g=g'}{f+g=f'+g'}\,,\ \frac{f=f',\ g=g'}{fg=f'g'} \qquad \text{for all polynomials } f,f',g,g'.$$

$f=0$ can be proved in this equational calculus if and only if f is in the ideal generated by the polynomials $f_1,\dots,f_s$. The provability problem for the equational theory associated with a finite set of polynomials or the membership problem for the ideal generated by a finite set of polynomials is the following:

(P2) given: polynomials $f_1,\dots,f_s$, and f,
decide: whether $f=0$ can be proved in the equational calculus with the axioms $f_1=0,\dots,f_s=0$,
or, stated as an ideal membership problem, whether $f \in ideal(f_1,\dots,f_s)$.

1.3. System of linear equations with coefficients in $K[x_1,\dots,x_n]$

Information about the structure of an ideal given by a basis $f_1,\dots,f_s$ is provided by the syzygies of this basis, i.e. the s-tuples $(z_1,\dots,z_s)$ in $K[x_1,\dots,x_n]^s$, for which

$$f_1 z_1 + \dots + f_s z_s = 0.$$

More generally, we will consider the following problem:

(P3) given: polynomials $f_{11},\dots,f_{1s}, \dots, f_{t1},\dots,f_{ts}$, and $f_1,\dots,f_t$ in $K[x_1,\dots,x_n]$,
find: (a description of) all s-tuples $(z_1,\dots,z_s)$ of polynomials in $K[x_1,\dots,x_n]$, such that

$$\begin{pmatrix} f_{11} & \dots & f_{1s} \\ \vdots & & \vdots \\ f_{t1} & \dots & f_{ts} \end{pmatrix} \cdot \begin{pmatrix} z_1 \\ \vdots \\ z_s \end{pmatrix} = \begin{pmatrix} f_1 \\ \vdots \\ f_t \end{pmatrix}.$$

1.4. Membership in the radical of an ideal

Again we are given a finite set of polynomials $f_1,\dots,f_s$, and an additional polynomial f. We ask whether the conditions $f_1(\bar{x})=0, \dots, f_s(\bar{x})=0$ for an n-tuple $\bar{x}$ in $\bar{K}^n$ imply $f(\bar{x})=0$. That means we want to decide whether the polynomial f vanishes on the variety of $ideal(f_1,\dots,f_s)$, i.e. whether f is contained in the radical of $ideal(f_1,\dots,f_s)$.

(P4) Given: polynomials $f_1,\dots,f_s$, and f,
decide: whether f is contained in the radical of ideal$(f_1,\dots,f_s)$,
or in other words, whether $f_1(\bar{x})=0, \dots, f_s(\bar{x})=0 \Longrightarrow f(\bar{x})=0$ for all n-tuples $\bar{x}$ in $\bar{K}^n$.

2. What is and how can we construct a Gröbner basis?

Before we show how Gröbner bases can be used for solving various problems, let us just say a few words about what a Gröbner basis is and how we can construct one. For further details we refer to [Buchberger 76a,b] and [Buchberger 85].

Let $\gg$ be a linear ordering on the power products of $x_1,\dots,x_n$, such that $1=x_1^0 \dots x_n^0$ is minimal under $\gg$ and multiplication by a power product preserves the ordering. Examples for such an ordering are the lexicographic ordering or the graduated lexico-

graphic ordering. Once the ordering $\gg$ is fixed, every nonzero polynomial f has a greatest power product (with nonzero coefficient) occurring in it, the *leading power product* of f, $lpp(f)$. The coefficient of $lpp(f)$ in f is the *leading coefficient* of f, $lc(f)$. The polynomial which results from f by subtracting the leading power product multiplied by its coefficient is called the *reductum* of f, $red(f)$.

Every nonzero polynomial f gives rise to a *reduction relation* $\rightarrow_f$ on the ring of polynomials in the following way: $g_1 \rightarrow_f g_2$ if and only if there is a power product p with a nonzero coefficient a in g_1, i.e. $g_1 = ap + h$ for some polynomial h which does not contain p, such that $lpp(f)$ divides p, i.e. $p = lpp(f)q$ for some q, and $g_2 = -(a/lc(f))\cdot q\cdot red(f) + h$. If F is a set of polynomials, the *reduction relation* modulo F is defined such that $g_1 \rightarrow_F g_2$ if and only if $g_1 \rightarrow_f g_2$ for some $f \in F$. In this case g_1 *is reducible to* g_2 *by* F. If there is no such g_2, g_1 *is irreducible modulo* F. By $\rightarrow^+$, $\rightarrow^*$, and $\longleftrightarrow^*$ we denote the transitive, reflexive-transitive, and symmetric-reflexive-transitive closure of $\rightarrow$, respectively. For every set of polynomials F the reduction relation $\rightarrow_F$ is Noetherian, i.e. every decreasing chain terminates. We say that g is a *normal form of* f *modulo* F, if $f \rightarrow_F^* g$ and g is irreducible modulo F. In general, normal forms are not unique.

If two polynomials f and g are given, we can reduce the least common multiple (lcm) of $lpp(f)$ and $lpp(g)$ both by $\rightarrow_f$ and by $\rightarrow_g$. The difference of the results is called the *S-polynomial* (*S-pol*) of f and g. I.e.

$$S\text{-}pol(f,g) = lc(g)\cdot(lcm(lpp(f),lpp(g))/lpp(f))\cdot f - lc(f)\cdot(lcm(lpp(f),lpp(g))/lpp(f))\cdot g.$$

A *Gröbner basis* for a polynomial ideal I is a finite set of polynomials G such that I is generated by G, $I = ideal(G)$, and every nonzero polynomial f in I is reducible modulo G. According to a theorem of Buchberger G is a Gröbner basis if and only if $S\text{-}pol(g_1,g_2) \rightarrow_G^* 0$ for all $g_1, g_2 \in G$. Based on this theorem we get (a first, primitive version of) an algorithm for computing a Gröbner basis. For more advanced versions we refer to [Buchberger 76a] and [Buchberger 85].

Gröbner basis algorithm:

input: F, a finite set of polynomials,
output: G, a finite set of polynomials such that G is a Gröbner basis for the ideal generated by F.

$G := F$;

for all pairs $(g_1,g_2) \in G \times G$ **do**
  $h :=$ a normal form of $S\text{-}pol(g_1,g_2)$ modulo G;
  if $h \neq 0$ **then** $G := G \cup \{h\}$ **endif**
endfor •

For every input F the Gröbner basis algorithm will terminate after a finite number of steps [Buchberger 70]. Once a Gröbner basis is computed, the polynomials in the basis can be reduced with respect to each other and the leading coefficients can be normalized to 1, leading to a uniquely defined *minimal reduced Gröbner basis*. Wheras in general normal forms modulo a basis F are not unique, every polynomial f has a unique normal form modulo a Gröbner basis G, i.e. the reduction relation $\rightarrow_G$ has the Church-Rosser property.

3. Application of the Gröbner basis method to the solution of equations

3.1. System of algebraic equations

Before we set out to generate the solutions to the problem (P1) for given polynomials $f_1,\ldots,f_s$, we might want to know whether the system of equations

$$f_i(x_1,\ldots,x_n) = 0 \quad (i=1,\ldots,s)$$

has any solutions at all. This question can easily be answered once we have computed a Gröbner basis for the given polynomials.

Theorem 1: Let $F=\{f_1,\ldots,f_s\}$ be a set of polynomials and G the minimal reduced Gröbner basis for $ideal(F)$. Then the system of equations

$$(3) \qquad f_i(x_1,\ldots,x_n) = 0 \quad (i=1,\ldots,s)$$

is unsolvable (in $\bar{K}$) if and only if $1 \in G$.

Proof: If $1 \in G$, then 1 is in $ideal(F)$. So every solution of (3) is a solution of $1=0$. Thus, there is no solution of (3).

On the other hand, assume that (3) is unsolvable. Then 1 vanishes for every root of (3). So by Hilbert's Nullstellensatz [Waerden 37] there exists a positive integer m such that $1^m=1 \in ideal(F)$. So there has to be a polynomial in G which allows to reduce 1, i.e. $1 \in G$.

Now suppose that (3) is solvable. We might want to determine whether there are finitely or infinitely many solutions.

Theorem 2: Let F and G be as in Theorem 1. Then (3) has finitely many solutions if and only if for every i ($i=1,\ldots,n$) there is a polynomial g_i in G such that $lpp(g_i)$ is a power of x_i.

Proof: The system of equations (3) has finitely many solutions if and only if the vector space $K[x_1,\ldots,x_n]/ideal(F)$ has finite vector space dimension [Gröbner 49]. That is the case if and only if the number of irreducible power products modulo G is finite, see lemma 6.7 in [Buchberger 83]. From this condition, the theorem follows immediately.

For really carrying out the elimination process, we compute the Gröbner basis with respect to the lexicographic ordering. The following elimination property of a Gröbner basis w.r.t. the lexicographic ordering has been observed in [Trinks 78]. It means that the i-th elimination ideal of a Gröbner basis G is generated by the polynomials in G that depend only on the variables $x_1,\ldots,x_i$.

Theorem 3: Let G be a Gröbner basis w.r.t. the lexicographic ordering (without loss of generality assume $x_n \gg x_{n-1} \gg \ldots \gg x_1$). Then

$$ideal(G) \cap K[x_1,\ldots,x_i] = ideal(G \cap K[x_1,\ldots,x_i]) \qquad \text{for } i=1,\ldots,n,$$

where the ideal on the right hand side is formed in $K[x_1,\ldots,x_i]$.

Proof: Obviously the right hand side is contained in the left hand side.

On the other hand, assume that $f \in ideal(G) \cap K[x_1,\ldots,x_i]$. Then f can be reduced to 0 modulo G w.r.t. the lexicographic ordering. So all the polynomials occurring in this reduction process depend only on the variables $x_1,\ldots,x_i$, and we get a representation of f as a linear combination of polynomials in G, where all the summands in this representation depend only on the variables $x_1,\ldots,x_i$.

Example 1: Let $F=\{f_1,f_2,f_3\} \subset \mathbf{Q}[x,y,z]$ be the set of polynomials

$$f_1 = xz - xy^2 - 4x^2 - \tfrac{1}{4},$$
$$f_2 = y^2z + 2x + \tfrac{1}{2},$$
$$f_3 = x^2z + y^2 + \tfrac{1}{2}x.$$

Let $\gg$ be the lexicographic ordering with $z \gg y \gg x$. The Gröbner basis algorithm

applied to F generates the minimal reduced Gröbner basis $G=\{g_1,g_2,g_3\}$, where

$$g_1 = z + \frac{64}{65}x^4 - \frac{432}{65}x^3 + \frac{168}{65}x^2 - \frac{354}{65}x + \frac{8}{5},$$
$$g_2 = y^2 - \frac{8}{13}x^4 + \frac{54}{13}x^3 - \frac{8}{13}x^2 + \frac{17}{26}x,$$
$$g_3 = x^5 - \frac{27}{4}x^4 + 2x^3 - \frac{21}{16}x^2 + x + \frac{5}{32}.$$

Applying theorem 1 we see that the system of equations $f_1=0$, $f_2=0$, $f_3=0$ is solvable in the algebraic closure of $\mathbf{Q}$ (the field of algebraic numbers). Furthermore, by theorem 2, this system of equations has finitely many solutions. The variables in the Gröbner basis G are totally separated. An approximation of a root of g_3 up to $\pm\frac{1}{100000}$ is -0.128475. This solution of $g_3=0$ can be continued to solutions of $g_2=0$ and $g_1=0$, yielding the approximation (-0.128475, 0.321145, -2.356718) for the original system of equations. •

Example 2: The same method can be applied to algebraic equations with symbolic coefficients. For example let $F=\{f_1,\ldots,f_4\} \subset \mathbf{Q}(a,b,c,d)$ consist of the polynomials

$$f_1 = x_4 + (b-d),$$
$$f_2 = x_4 + x_3 + x_2 + x_1 + (-a-c-d),$$
$$f_3 = x_3x_4 + x_1x_4 + x_2x_3 + (-ad-ac-cd),$$
$$f_4 = x_1x_3x_4 + (-acd).$$

Let $\gg$ be the lexicographic ordering with $x_4 \gg x_3 \gg x_2 \gg x_1$. The minimal reduced Gröbner basis for $ideal(F)$ is $G=\{g_1,\ldots,g_4\}$, where

$$g_1 = x_4 + (b-d),$$
$$g_2 = x_3 + (-b^2+2bd-d^2)/(acd)x_1^2 + (-abc-abd+acd+ad^2-bcd+cd^2)/(acd)x_1 + (-a-c-d),$$
$$g_3 = x_2 + (b^2-2bd+d^2)/(acd)x_1^2 + (abc+abd-ad^2+bcd-cd^2)/(acd)x_1 + (-b+d),$$
$$g_4 = x_1^3 + (ac+ad+cd)/(b-d)x_1^2 + (a^2cd+ac^2d+acd^2)/(b^2-2bd+d^2)x_1 + (a^2c^2d^2)/(b^3-3b^2d+3bd^2-d^3).$$

Thus, the system has finitely many solutions. A particular solution of $g_4=0$ is $(-ad)/(b-d)$, which can be continued to the solution

$$\left(\frac{-ad}{b-d}, \frac{ab+b^2-bd}{b-d}, c, -b+d\right).$$

3.2. The equational theory associated with a polynomial ideal

Once we have computed a Gröbner basis G for the ideal generated by $F=\{f_1,\ldots,f_s\}$,

the provability of an equation $f=0$ in the equational theory associated with F, or in other words, the membership of f in $ideal(F)$, can be decided by reducing f to the uniquely defined normal form modulo G.

Theorem 4: Let G be a Gröbner basis, f a polynomial. Then $f \in ideal(G)$ if and only if $f \rightarrow_G^* 0$.

Proof: If $f \rightarrow_G^* 0$, then obviously f can be expressed as a linear combination of the elements of G.

On the other hand, if $f \in ideal(G)$ and $f \neq 0$, by the definition of a Gröbner basis f can be reduced modulo G, $f \rightarrow_G f'$, where $f' \in ideal(G)$. f' is also reducible modulo G, leading to f'' and so on. Since $\rightarrow_G$ is Noetherian, this process has to stop, i.e. f has to be reducible to 0. •

Example 3: Let $F=\{ f_1, f_2, f_3 \}$, where

$f_1 = x_2x_3x_4 - x_1x_3x_4 + x_2^2x_4 - 2x_1x_2x_4 + x_2x_3^2$,

$f_2 = x_1x_3^2x_4 - x_2^2x_3x_4 + x_1^2x_3x_4 - x_2^3x_4 + 2x_1x_2^2x_4 + x_2^2x_3^2 - x_1x_2x_3^2$,

$f_3 = x_1x_3x_4 - x_1x_2x_4 - x_1^2x_4 + 2x_2^2x_3 - x_1x_2x_3$.

We want to decide, whether for

$$f = 2x_1x_2^2x_4 - 2x_1^2x_2x_4 - x_1^3x_4 + x_1x_2^2x_3^3 - 2x_2^4x_3^2 + 2x_1x_2^3x_3^2 - 2x_1^2x_2^2x_3^2 + x_1x_2x_3^2 - 2x_2^5x_3 + 5x_1x_2^4x_3 - 2x_1^2x_2^3x_3 - 2x_2^3x_3 + 3x_1x_2^2x_3 - x_1^2x_2x_3$$

the equation $f=0$ is provable in the equational theory associated with F, or whether $f \in ideal(F)$.

A Gröbner basis for $ideal(F)$, w.r.t. the lexicographic ordering $x_4 \gg x_3 \gg x_2 \gg x_1$, is $G=\{ g_1, g_2, g_3, g_4 \}$, where $g_1=f_1$, $g_2=f_3$,

$g_3 = x_1x_2^2x_4 - x_1^2x_2x_4 - \frac{1}{2}x_1^3x_4 + \frac{1}{2}x_1x_2x_3^2 - x_2^3x_3 + \frac{3}{2}x_1x_2^2x_3 - \frac{1}{2}x_1^2x_2x_3$,

$g_4 = x_1x_2x_3^3 - 2x_2^3x_3^2 + 2x_1x_2^2x_3^2 - 2x_1^2x_2x_3^2 - 2x_2^4x_3 + 5x_1x_2^3x_3 - 2x_1^2x_2^2x_3$.

f is reducible to 0 modulo G, so by theorem 4 the equation $f=0$ is provable in the equational theory associated with F. •

3.3. System of linear equations with coefficients in $K[x_1,\dots,x_n]$

Let us first consider the case $t=1$, i.e. only one inhomogeneous equation

$$(3) \qquad f_1 z_1 + \dots + f_s z_s = f.$$

If $G=\{g_1,\dots,g_m\}$ is a Gröbner basis, then a generating set for the solutions of the homogeneous equation

$$(4) \qquad g_1 z_1 + \dots + g_m z_m = 0$$

can be computed by reducing the S-polynomials of G to 0 and storing the multiples of the basis polynomials used in this process ([Buchberger 85]). We provide a correctness proof for this method.

Theorem 5: Let $G=\{g_1,\dots,g_m\}$ be a Gröbner basis. For all $1\le i<j\le m$, let $p_{i,j}$, $q_{i,j}$, $k_{i,j}^1,\dots,k_{i,j}^m$ be such that

$$S\text{-}pol(g_i,g_j) = p_{i,j}g_i - q_{i,j}g_j = k_{i,j}^1 g_1 + \dots + k_{i,j}^m g_m,$$

where $k_{i,j}^1,\dots,k_{i,j}^m$ are the polynomials extracted from the reduction of $S\text{-}pol(g_i,g_j)$ to 0. For $i=1,\dots,m$ let e_i denote the vector $(0,\dots,0,1,0,\dots,0)$, where the 1 occurs at the i-th position. Then

$$S = \{\underbrace{p_{i,j}e_i - q_{i,j}e_j - (k_{i,j}^1,\dots,k_{i,j}^m)}_{S_{i,j}} \mid 1\le i<j\le m\}$$

generates all the syzygies of G, i.e. the solutions of the homogeneous equation

$$g_1 z_1 + \dots + g_m z_m = 0 \ .$$

Proof: Obviously every element of S is a syzygy. On the other hand, let $H=(h_1,\dots,h_m)\neq(0,\dots,0)$ be an arbitrary syzygy, i.e.

$$(*) \quad g_1 h_1 + \dots + g_m h_m = 0.$$

Let $i_1<\dots<i_k$ be those indices such that $lpp(g_{i_j}h_{i_j})=p$, the maximal power product w.r.t. $\gg$ in (*). We have $k\ge 2$. Suppose $k>2$. By subtracting a suitable multiple of S_{i_{k-1},i_k}, we can reduce the number of positions in H that contribute to the highest power product in (*). Iterating this process k-2 times, we finally reach a situation, where only two positions in the syzygy contribute to the highest power p in (*). Now the highest power product in (*) can be decreased by subtracting a suitable multiple of S_{i_1,i_2}. Since $\gg$ is Noetherian, this process has to terminate, leading to an expression of H as a linear combination of elements of S. •

Having solved equation (3) for a Gröbner basis G for the ideal generated by F, we

want to transform this solution to a solution of

$$(5) \qquad f_1 z_1 + \ldots + f_s z_s = 0.$$

Such a transformation algorithm is given in [Buchberger 85]. We provide a correctness proof.

Theorem 6: Let $F=\{f_1,\ldots,f_s\}$ be a set of polynomials and $G=\{g_1,\ldots,g_m\}$ a Gröbner basis for $ideal(F)$. We think of F and G as column vectors, i.e. $F=(f_1,\ldots,f_s)^T$, $G=(g_1,\ldots,g_m)^T$. Let the r rows of the matrix R be a basis for the syzygies of G, and let the matrices X^T, Y^T be such that $G=X^T F$ and $F=Y^T G$. Then the rows of Q are a basis for the syzygies of F, where

$$Q = \begin{pmatrix} I_s - Y^T X^T \\ \ldots\ldots\ldots\ldots \\ RX^T \end{pmatrix}.$$

Proof: Let $b_1,\ldots,b_{s+r}$ be polynomials, $b=(b_1,\ldots,b_{s+r})$.

$$\begin{aligned}
&(b\cdot Q)\cdot F = \\
&(\,(b_1,\ldots,b_s)\cdot(I_s - Y^T X^T) + (b_{s+1},\ldots,b_{s+r})\cdot RX^T\,)\cdot F = \\
&(b_1,\ldots,b_s)\cdot(F - \underbrace{Y^T X^T F}_{F}) + (b_{s+1},\ldots,b_{s+r})\cdot R\underbrace{X^T F}_{G} = 0.
\end{aligned}$$

So every linear combination of the rows of Q is a syzygy of F.

On the other hand, let $H=(h_1,\ldots,h_s)$ be a syzygy of F. Then $H\cdot Y^T$ is a syzygy of G. So for some H', $H\cdot Y^T = H'\cdot R$, and therefore $H\cdot Y^T\cdot X^T = H'\cdot R\cdot X^T$. Thus,

$$H = H\cdot(I_s - Y^T\cdot X^T) + H'\cdot RX^T = (H,H')\cdot Q,$$

i.e. H is a linear combination of the rows of Q. •

What we still need is a particular solution of (3). (3) has a solution if and only if $f \in ideal(F) = ideal(G)$. If the reduction of f to normal form modulo G yields $f\neq 0$, then (3) has no solution (compare Section 3.2). Otherwise one can extract from this reduction polynomials $h_1',\ldots,h_m'$ such that

$$g_1 h_1' + \ldots + g_m h_m' = f.$$

So $h'X^T$ is a particular solution of (3).

LinSolve1:

input: $f_1,\ldots,f_s$, f, polynomials,

output: a polynomial vector $\bar{a}$ of length s and a polynomial matrix A of dimension (s,m) for some m, such that the set of solutions of

$f_1 z_1 + \ldots + {}_s z_s = f$ is $\{\bar{a} + A\cdot(c_1,\ldots,c_m)^T \mid c_1,\ldots,c_m$ polynomials$\}$
or unsolvable.

compute a Gröbner basis $(g_1,\ldots,g_m)$ for $(f_1,\ldots,f_s)$ along with the transformation matrices X^T and Y^T (as in Theorem 6);
let R be a basis for the syzygies of $(g_1,\ldots,g_m)$ as described in Theorem 5;
let Q be the basis for the syzygies of $(f_1,\ldots,f_s)$ constructed from X^T, Y^T and R as described in Theorem 6;
$A := Q^T$;
$f :=$ normal form of f modulo G;
if $f \neq 0$
then **return unsolvable**
else {let $\bar{a}' = (\bar{a}'_1,\ldots,\bar{a}'_m)^T$ be the polynomials used as multiplicands of $g_1,\ldots,g_m$ in the reduction of f to 0;
$\bar{a} := (\bar{a}'^T \cdot X^T)^T$;
return $(\bar{a}, A)$} •

Example 4: Let F and G be as in example 1. We want to compute a basis for the syzygies of F, i.e. a basis for the solutions of the equation

$$f_1 h_1 + \ldots + f_3 h_3 = 0.$$

From the Gröbner basis algorithm we can extract the transformation matrix $X^T = (X_{i,j})_{i=1,\ldots,3,\ j=1,\ldots,3}$.

$$X_{1,1} = -\frac{32}{35}y^2z^2 + \frac{16}{5}xz^2 + \frac{32}{35}y^4z - \frac{96}{35}xy^2z - \frac{8}{5}x^2z - \frac{64}{35}xz + \frac{68}{35}z + \frac{16}{5}xy^4 + \frac{8}{5}x^2y^2 + \frac{64}{35}xy^2 - \frac{744}{455}y^2 - \frac{32}{5}x^4 - \frac{8}{5}x^3 - \frac{192}{35}x^2 - \frac{204}{455}x - \frac{32}{5},$$

$$X_{1,2} = \frac{32}{35}x^3z^2 + \frac{32}{35}xz^2 - \frac{32}{35}x^3y^2z - \frac{32}{35}xy^2z - \frac{16}{35}x^4z - \frac{16}{35}x^2z + \frac{104}{35}z - \frac{16}{5}x^4y^2 - \frac{16}{5}x^2y^2 - \frac{104}{35}y^2 - \frac{64}{5}x^5 - \frac{852}{65}x^4 - \frac{5548}{455}x,$$

$$X_{1,3} = -\frac{32}{35}xy^2z^2 - \frac{16}{5}z^2 + \frac{32}{35}xy^4z + \frac{16}{35}x^2y^2z + \frac{16}{5}y^2z - \frac{64}{35}x^2z + \frac{488}{35}xz + \frac{16}{5}x^2y^4 + \frac{64}{5}x^3y^2 + \frac{64}{35}x^2y^2 - \frac{76}{91}xy^2 + \frac{256}{35}x^3 - \frac{32}{7}x^2 - \frac{14}{13},$$

$$X_{2,1} = \frac{4}{13}y^2 - \frac{14}{13}x,$$

$$X_{2,2} = -\frac{4}{13}x^3 - \frac{4}{13}x,$$

$$X_{2,3} = \frac{4}{13}xy^2 + \frac{14}{13},$$

$$X_{3,1} = -\frac{1}{7}y^2z + \frac{1}{2}xz - \frac{1}{2}xy^2 + \frac{7}{4}x^2 - \frac{2}{7}x + \frac{17}{56},$$

$$X_{3,2} = \frac{1}{7}x^3z + \frac{1}{7}xz + \frac{1}{2}x^4 + \frac{1}{2}x^2 + \frac{13}{28},$$

$$X_{3,3} = -\frac{1}{7}xy^2z - \frac{1}{2}z - \frac{1}{2}x^2y^2 - \frac{2}{7}x^2 + \frac{5}{28}x.$$

Reduction of the polynomials of F to 0 modulo G yields the entries for the matrix

$$Y^{\mathrm{T}} = \begin{pmatrix} x & -x & -\frac{8}{5} \\ \frac{8}{13}x^4 - \frac{54}{13}x^3 + \frac{8}{13}x^2 - \frac{17}{26}x & z & -\frac{512}{845}x^3 + \frac{3456}{845}x^2 - \frac{64}{65}x + \frac{16}{5} \\ x^2 & 1 & -\frac{64}{65}x \end{pmatrix}.$$

Reducing the S-polynomials of G to 0 we get the rows R_1, R_2, R_3 of R, which form a basis for the syzygies of G.

$$R_1 = \left(y^2 - \frac{8}{13}x^4 + \frac{54}{13}x^3 - \frac{8}{13}x^2 + \frac{17}{13}x,\ -z - \frac{64}{65}x^4 + \frac{432}{65}x^3 - \frac{168}{65}x^2 + \frac{354}{65}x - \frac{8}{5},\ 0 \right),$$

$$R_2 = \left(x^5 - \frac{27}{4}x^4 + 2x^3 - \frac{21}{16}x^2 + x + \frac{5}{32},\ 0,\ -z - \frac{64}{65}x^4 + \frac{432}{65}x^3 - \frac{168}{65}x^2 + \frac{354}{65}x - \frac{8}{5} \right),$$

$$R_3 = \left(0,\ x^5 - \frac{27}{4}x^4 + 2x^3 - \frac{21}{16}x^2 + x + \frac{5}{32},\ -y^2 + \frac{8}{13}x^4 - \frac{54}{13}x^3 + \frac{8}{13}x^2 - \frac{17}{13}x \right).$$

Now according to theorem 6, the rows $Q_1, \ldots, Q_6$ of

$$Q = \begin{pmatrix} I_3 - Y^{\mathrm{T}}X^{\mathrm{T}} \\ \cdots\cdots\cdots \\ RX^{\mathrm{T}} \end{pmatrix}$$

form a basis for the syzygies of F.

$$\begin{aligned} Q_1 = \quad & (1/35)\,(32\,x\,y^2\,z^2 - 112\,x^2\,z^2 - 32\,x\,y^4\,z + 96\,x^2\,y^2\,z - 8\,y^2\,z + 56\,x^3\,z \\ & + 64\,x^2\,z - 40\,x\,z - 112\,x^2\,y^4 - 56\,x^3\,y^2 - 64\,x^2\,y^2 + 40\,x\,y^2 + 224\,x^5 \\ & + 56\,x^4 + 192\,x^3 + 76\,x^2 + 208\,x + 52, \\ & - 32\,x^4\,z^2 - 32\,x^2\,z^2 + 32\,x^4\,y^2\,z + 32\,x^2\,y^2\,z + 16\,x^5\,z + 24\,x^3\,z - 96\,x\,z \\ & + 112\,x^5\,y^2 + 112\,x^3\,y^2 + 104\,x\,y^2 + 448\,x^6 + 476\,x^4 + 444\,x^2 + 26, \\ & 32\,x^2\,y^2\,z^2 + 112\,x\,z^2 - 32\,x^2\,y^4\,z - 16\,x^3\,y^2\,z - 120\,x\,y^2\,z + 64\,x^3\,z \\ & - 486\,x^2\,z - 28\,z - 112\,x^3\,y^4 - 448\,x^4\,y^2 - 64\,x^3\,y^2 + 12\,x^2\,y^2 - 256\,x^4 \\ & + 160\,x^3 - 16\,x^2 + 10\,x\,) \end{aligned}$$

$$
\begin{aligned}
Q_2 = \; & (1/5915)\,(3328\,x^4 y^2 z^2 - 22464\,x^3 y^2 z^2 + 3328\,x^2 y^2 z^2 - 3536\,x\,y^2 z^2 \\
& - 11648\,x^5 z^2 + 78624\,x^4 z^2 - 11648\,x^3 z^2 + 12376\,x^2 z^2 - 3328\,x^4 y^4 z \\
& + 22464\,x^3 y^4 z - 3328\,x^2 y^4 z + 3536\,x\,y^4 z + 9984\,x^5 y^2 z - 67392\,x^4 y^2 z \\
& + 9472\,x^3 y^2 z - 7152\,x^2 y^2 z - 832\,x\,y^2 z + 864\,y^2 z + 5824\,x^6 z - 32656\,x^5 z \\
& - 44384\,x^4 z + 36108\,x^3 z - 11232\,x^2 z + 4420\,x\,z - 11648\,x^5 y^4 + 78624\,x^4 y^4 \\
& - 11648\,x^3 y^4 + 12376\,x^2 y^4 - 5824\,x^6 y^2 + 32656\,x^5 y^2 + 43264\,x^4 y^2 \\
& - 28548\,x^3 y^2 + 10112\,x^2 y^2 + 3140\,x\,y^2 + 23296\,x^8 - 151424\,x^7 + 3952\,x^6 \\
& - 145808\,x^5 - 17300\,x^4 - 158640\,x^3 - 20570\,x^2 - 17576\,x - 5746, \\
& - 3328\,x^7 z^2 + 22464\,x^6 z^2 - 6656\,x^5 z^2 + 26000\,x^4 z^2 - 3328\,x^3 z^2 + 3536\,x^2 z^2 \\
& + 3328\,x^7 y^2 z - 22464\,x^6 y^2 z + 6656\,x^5 y^2 z - 26000\,x^4 y^2 z + 3328\,x^3 y^2 z \\
& - 3536\,x^2 y^2 z + 1664\,x^6 z - 11232\,x^7 z + 3840\,x^6 z - 16456\,x^5 z - 7808\,x^4 z \\
& + 68900\,x^3 z - 9984\,x^2 z + 10608\,x\,z + 11648\,x^8 y^2 - 78624\,x^7 y^2 + 23296\,x^6 y^2 \\
& - 91000\,x^5 y^2 + 22464\,x^4 y^2 - 85384\,x^3 y^2 + 10816\,x^2 y^2 - 11492\,x\,y^2 \\
& + 46592\,x^9 - 314496\,x^8 + 96096\,x^7 - 383856\,x^6 + 96800\,x^5 - 371846\,x^4 \\
& + 48960\,x^3 - 67854\,x^2 + 2704\,x - 2873, \\
& 3328\,x^5 y^2 z^2 - 22464\,x^4 y^2 z^2 + 3328\,x^3 y^2 z^2 - 3536\,x^2 y^2 z^2 + 11648\,x^4 z^2 \\
& - 78624\,x^3 z^2 + 11648\,x^2 z^2 - 12376\,x\,z^2 - 3328\,x^5 y^4 z + 22464\,x^4 y^4 z \\
& - 3328\,x^3 y^4 z + 3536\,x^2 y^4 z - 1664\,x^6 y^2 z + 11232\,x^5 y^2 z - 13824\,x^4 y^2 z \\
& + 83648\,x^3 y^2 z - 12480\,x^2 y^2 z + 13280\,x\,y^2 z + 6656\,x^6 z - 95680\,x^5 z \\
& + 349232\,x^4 z - 59616\,x^3 z + 66020\,x^2 z - 2912\,x\,z + 3094\,z - 11648\,x^6 y^4 \\
& + 78624\,x^5 y^4 - 11648\,x^4 y^4 + 12376\,x^3 y^4 - 46592\,x^7 y^2 + 307840\,x^6 y^2 \\
& - 416\,x^5 y^2 + 34424\,x^4 y^2 + 7200\,x^3 y^2 + 6234\,x^2 y^2 - 26624\,x^7 + 196352\,x^6 \\
& - 139968\,x^5 + 48560\,x^4 + 2796\,x^3 + 2528\,x^2 + 786\,x)
\end{aligned}
$$

$$
\begin{aligned}
Q_3 = \; & (1/485)\,(\,416\,x^2 y^2 z^2 - 1456\,x^3 z^2 - 416\,x^2 y^4 z + 1248\,x^3 y^2 z - 64\,x\,y^2 z \\
& + 728\,x^4 z + 832\,x^3 z - 660\,x^2 z - 1456\,x^3 y^4 - 728\,x^4 y^2 - 832\,x^3 y^2 \\
& + 320\,x^2 y^2 - 140\,y^2 + 2912\,x^6 + 728\,x^5 + 2496\,x^4 + 988\,x^3 + 2784\,x^2 + 626\,x, \\
& - 416\,x^5 z^2 - 416\,x^3 z^2 + 416\,x^5 y^2 z + 416\,x^3 y^2 z + 208\,x^6 z + 272\,x^4 z \\
& - 1288\,x^2 z + 1456\,x^6 y^2 + 1456\,x^4 y^2 + 1352\,x^2 y^2 + 5824\,x^7 + 6188\,x^5
\end{aligned}
$$

$$+ 3912\, x^{3} + 348\, x,\ 416\, x^{3} y^{2} z^{2} + 1456\, x^{2} z^{2} - 416\, x^{3} y^{4} z - 208\, x^{4} y^{2} z$$

$$- 1520\, x^{2} y^{2} z + 832\, x^{4} z - 6344\, x^{3} z - 224\, x\, z - 1456\, x^{4} y^{4} - 5824\, x^{5} y^{2}$$

$$- 832\, x^{4} y^{2} + 136\, x^{3} y^{2} - 140\, x\, y^{2} - 3328\, x^{5} + 2080\, x^{4} - 128\, x^{3} - 410\, x^{2} - 35)$$

$$Q_4 = (1/455)\ (-416\, y^{4} z^{2} + 256\, x^{4} y^{2} z^{2} - 1728\, x^{3} y^{2} z^{2} + 256\, x^{2} y^{2} z^{2} + 1184\, x\, y^{2} z$$

$$- 896\, x^{5} z^{2} + 6048\, x^{4} z^{2} - 896\, x^{3} z^{2} + 952\, x^{2} z^{2} + 416\, y^{6} z - 256\, x^{4} y^{4} z$$

$$+ 1728\, x^{3} y^{4} z - 256\, x^{2} y^{4} z - 976\, x\, y^{4} z + 768\, x^{5} y^{2} z - 6184\, x^{4} y^{2} z$$

$$+ 768\, x^{3} y^{2} z - 1544\, x^{2} y^{2} z - 832\, x\, y^{2} z + 744\, y^{2} z + 448\, x^{6} z - 2512\, x^{5} z$$

$$- 3552\, x^{4} z + 3708\, x^{3} z - 1088\, x^{2} z + 1088\, x\, z + 1456\, x\, y^{6} - 896\, x^{5} y^{4}$$

$$+ 6048\, x^{4} y^{4} - 896\, x^{3} y^{4} + 1680\, x^{2} y^{4} + 832\, x\, y^{4} - 744\, y^{4} - 448\, x^{6} y^{2}$$

$$+ 2512\, x^{5} y^{2} + 416\, x^{4} y^{2} - 2924\, x^{3} y^{2} - 1856\, x^{2} y^{2} + 72\, x\, y^{2} - 3136\, y^{2}$$

$$+ 1792\, x^{8} - 11648\, x^{7} + 304\, x^{6} - 11216\, x^{5} - 1252\, x^{4} - 12336\, x^{3} - 1010\, x^{2}$$

$$- 1120\, x,\ 416\, x^{3} y^{2} z^{2} + 416\, x\, y^{2} z^{2} - 256\, x^{7} z^{2} + 1728\, x^{6} z^{2} - 512\, x^{5} z^{2}$$

$$+ 2000\, x^{4} z^{2} - 256\, x^{3} z^{2} + 272\, x^{2} z^{2} - 416\, x^{3} y^{4} z - 416\, x\, y^{4} z + 256\, x^{7} y^{2} z$$

$$- 1728\, x^{6} y^{2} z + 512\, x^{5} y^{2} z - 2208\, x^{4} y^{2} z + 256\, x^{3} y^{2} z - 480\, x^{2} y^{2} z$$

$$+ 1352\, y^{2} z + 128\, x^{8} z - 864\, x^{7} z + 256\, x^{6} z - 1000\, x^{5} z - 704\, x^{4} z$$

$$+ 5620\, x^{3} z - 832\, x^{2} z + 1024\, x\, z - 1456\, x^{4} y^{4} - 1456\, x^{2} y^{4} - 1352\, y^{4}$$

$$+ 896\, x^{5} y^{2} - 6048\, x^{4} y^{2} + 1792\, x^{3} y^{2} - 12824\, x^{2} y^{2} + 1728\, x\, y^{2} - 12532\, x^{3} y^{2}$$

$$+ 832\, x^{2} y^{2} - 6432\, x\, y^{2} + 3584\, x^{9} - 24192\, x^{8} + 7392\, x^{7} - 29512\, x^{6} + 7584\, x^{5}$$

$$- 28638\, x^{4} + 4000\, x^{3} - 4390\, x^{2} + 224\, x,$$

$$- 416\, x\, y^{4} z^{2} + 256\, x^{5} y^{2} z^{2} - 1728\, x^{4} y^{2} z^{2} + 256\, x^{3} y^{2} z^{2} - 272\, x^{2} y^{2} z^{2}$$

$$- 1456\, y^{2} z^{2} + 896\, x^{4} z^{2} - 6048\, x^{3} z^{2} + 896\, x^{2} z^{2} - 952\, x\, z^{2} + 416\, x\, y^{6} z$$

$$- 256\, x^{5} y^{4} z + 1728\, x^{4} y^{4} z - 256\, x^{3} y^{4} z + 480\, x^{2} y^{4} z + 1456\, y^{4} z$$

$$- 128\, x^{6} y^{2} z + 864\, x^{5} y^{2} z - 1024\, x^{4} y^{2} z + 6184\, x^{3} y^{2} z - 1728\, x^{2} y^{2} z$$

$$+ 7156\, x\, y^{2} z + 512\, x^{6} z - 7360\, x^{5} z + 26864\, x^{4} z - 4448\, x^{3} z + 4148\, x^{2} z$$

$$- 490\, z + 1456\, x^{2} y^{6} - 896\, x^{6} y^{4} + 6048\, x^{5} y^{4} - 896\, x^{4} y^{4} + 6776\, x^{3} y^{4}$$

$$+ 832\, x^{2} y^{4} - 380\, x\, y^{4} - 3584\, x^{7} y^{2} + 23680\, x^{6} y^{2} - 32\, x^{5} y^{2} + 2648\, x^{4} y^{2}$$

$$+ 3744\, x^{3} y^{2} - 1566\, x^{2} y^{2} - 224\, x\, y^{2} + 490\, y^{2} - 2048\, x^{7} + 15104\, x^{6} - 10688\, x^{5}$$

$$+ 2672\, x^{4} + 3932\, x^{3} - 1568\, x^{2} + 2989\, x - 764)$$

$$
\begin{aligned}
Q_5 = \; & (1/7280)\,(-6656\,x^{5}y^{2}z^{2} + 44928\,x^{4}y^{2}z^{2} - 13312\,x^{3}y^{2}z^{2} + 8736\,x^{2}y^{2}z^{2} \\
& - 6656\,x\,y^{2}z^{2} + 23296\,x^{6}z^{2} - 157248\,x^{5}z^{2} + 46592\,x^{4}z^{2} - 30576\,x^{3}z^{2} \\
& + 23296\,x^{2}z^{2} + 6656\,x^{6}y^{4}z - 44928\,x^{4}y^{4}z + 13312\,x^{3}y^{4}z - 8736\,x^{2}y^{4}z \\
& + 6656\,x\,y^{4}z + 1040\,y^{4}z - 19968\,x^{6}y^{2}z + 134784\,x^{5}y^{2}z - 38912\,x^{4}y^{2}z \\
& + 19296\,x^{3}y^{2}z - 17280\,x^{2}y^{2}z - 5144\,x\,y^{2}z + 1664\,y^{2}z - 11648\,x^{7}z \\
& + 65312\,x^{6}z + 77120\,x^{5}z - 82816\,x^{4}z + 24704\,x^{3}z - 26612\,x^{2}z + 8320\,x\,z \\
& + 23296\,x^{6}y^{4} - 157248\,x^{5}y^{4} + 46592\,x^{4}y^{4} - 30576\,x^{3}y^{4} + 23296\,x^{2}y^{4} \\
& + 3640\,x\,y^{4} + 11648\,x^{7}y^{2} - 65312\,x^{6}y^{2} - 74880\,x^{5}y^{2} + 67496\,x^{4}y^{2} \\
& - 20224\,x^{3}y^{2} + 10932\,x^{2}y^{2} - 4000\,x\,y^{2} - 1860\,y^{2} - 46592\,x^{9} + 302848\,x^{8} \\
& - 54496\,x^{7} + 291616\,x^{6} - 49016\,x^{5} + 292528\,x^{4} - 41208\,x^{3} + 14224\,x^{2} - 31738\,x \\
& - 10816,\; 6656\,x^{8}z^{2} - 44928\,x^{7}z^{2} + 19968\,x^{6}z^{2} - 53664\,x^{5}z^{2} + 19968\,x^{4}z^{2} \\
& - 8736\,x^{3}z^{2} + 6656\,x^{2}z^{2} - 6656\,x^{8}y^{2}z + 44928\,x^{7}y^{2}z - 19968\,x^{6}y^{2}z \\
& + 53664\,x^{5}y^{2}z - 19968\,x^{4}y^{2}z + 7696\,x^{3}y^{2}z - 6656\,x^{2}y^{2}z - 1040\,x\,y^{2}z \\
& - 3328\,x^{9}z + 22464\,x^{8}z - 11008\,x^{7}z + 33744\,x^{6}z + 7936\,x^{5}z - 133232\,x^{4}z \\
& + 35584\,x^{3}z - 26888\,x^{2}z + 19968\,x\,z - 23296\,x^{9}y^{2} + 157248\,x^{8}y^{2} \\
& - 69888\,x^{7}y^{2} + 187824\,x^{6}y^{2} - 91520\,x^{5}y^{2} + 172952\,x^{4}y^{2} - 66560\,x^{3}y^{2} \\
& + 24752\,x^{2}y^{2} - 21632\,x\,y^{2} - 3380\,y^{2} - 93184\,x^{10} + 628992\,x^{9} - 285376\,x^{8} \\
& + 790608\,x^{7} - 385792\,x^{6} + 753884\,x^{5} - 291520\,x^{4} + 143888\,x^{3} - 103328\,x^{2} \\
& + 4538\,x - 5408,\; -6656\,x^{6}y^{2}z^{2} + 44928\,x^{5}y^{2}z^{2} - 13312\,x^{4}y^{2}z^{2} \\
& + 8736\,x^{3}y^{2}z^{2} - 6656\,x^{2}y^{2}z^{2} - 23296\,x^{5}z^{2} + 157248\,x^{4}z^{2} - 46592\,x^{3}z^{2} \\
& + 30576\,x^{2}z^{2} - 23296\,x\,z^{2} + 6656\,x^{6}y^{4}z - 44928\,x^{5}y^{4}z + 13312\,x^{4}y^{4}z \\
& - 8736\,x^{3}y^{4}z + 6656\,x^{2}y^{4}z + 1040\,x\,y^{4}z + 3328\,x^{7}y^{2}z - 22464\,x^{6}y^{2}z \\
& + 30976\,x^{5}y^{2}z - 168528\,x^{4}y^{2}z + 52608\,x^{3}y^{2}z - 32080\,x^{2}y^{2}z \\
& + 24960\,x\,y^{2}z + 3640\,y^{2}z - 13312\,x^{7}z + 191360\,x^{6}z - 711776\,x^{5}z \\
& + 224064\,x^{4}z - 170728\,x^{3}z + 110912\,x^{2}z - 5264\,x\,z + 5824\,z + 23296\,x^{7}y^{4} \\
& - 157248\,x^{6}y^{4} + 46592\,x^{5}y^{4} - 30576\,x^{4}y^{4} + 23296\,x^{3}y^{4} + 3640\,x^{2}y^{4} \\
& + 93184\,x^{8}y^{2} - 615680\,x^{7}y^{2} + 94016\,x^{6}y^{2} - 78832\,x^{5}y^{2} + 72960\,x^{4}y^{2} \\
& + 18028\,x^{3}y^{2} + 1824\,x^{2}y^{2} - 950\,x\,y^{2} + 53248\,x^{8} - 392704\,x^{7} + 333184\,x^{6} \\
& - 143712\,x^{5} + 58024\,x^{4} - 23968\,x^{3} - 5082\,x^{2} + 5760\,x + 1225)
\end{aligned}
$$

$$
\begin{aligned}
Q_6 = \quad & (1/1456)\,(208\,y^4 z - 128\,x^4 y^2 z + 864\,x^3 y^2 z - 128\,x^2 y^2 z - 592\,x\,y^2 z \\
& + 448\,x^5 z - 3024\,x^4 z + 448\,x^3 z - 476\,x^2 z + 728\,x\,y^4 + 448\,x^3 y^2 \\
& - 2660\,x^2 y^2 + 864\,x\,y^2 - 372\,y^2 - 256\,x^5 + 432\,x^4 - 1700\,x^3 - 1024\,x^2 \\
& - 534\,x, - 208\,x^3 y^2 z - 208\,x\,y^2 z + 128\,x^7 z - 864\,x^6 z + 256\,x^5 z \\
& - 1000\,x^4 z + 128\,x^3 z - 136\,x^2 z - 728\,x^4 y^2 - 728\,x^2 y^2 - 676\,y^2 - 448\,x^6 \\
& + 112\,x^5 - 480\,x^4 - 2766\,x^3 - 32\,x^2 - 512\,x, \\
& 208\,x\,y^4 z - 128\,x^5 y^2 z + 864\,x^4 y^2 z - 128\,x^3 y^2 z + 136\,x^2 y^2 z + 728\,y^2 z \\
& - 448\,x^4 z + 3024\,x^3 z - 448\,x^2 z + 476\,x\,z + 728\,x^2 y^4 + 448\,x^4 y^2 \\
& - 112\,x^3 y^2 + 864\,x^2 y^2 - 190\,x\,y^2 - 256\,x^6 + 3456\,x^5 - 11920\,x^4 + 3568\,x^3 \\
& - 2228\,x^2 + 1568\,x + 246)
\end{aligned}
$$

Let us now deal with the general case where we have t linear inhomogeneous equations. The idea is to solve the first equation and substitute the solution into the second equation. So the number of equations has been reduced by one. Iterating this process, the problem of solving a system of equations can be reduced to the problem of solving a single equation.

Theorem 7: Let $f_{11},\dots,f_{1s}, \dots, f_{t1},\dots,f_{ts}, f_1,\dots,f_t$ be polynomials. Let $\bar{a}=(\bar{a}_1,\dots,\bar{a}_s)^T$ be a polynomial vector and

$$A = \begin{pmatrix} a_{11} & \cdots & a_{m1} \\ \vdots & & \vdots \\ a_{1s} & \cdots & a_{ms} \end{pmatrix}$$

a polynomial matrix such that every solution $z=(z_1,\dots,z_s)^T$ of

$$(*) \qquad \begin{pmatrix} f_{11} & \cdots & f_{1s} \\ \vdots & & \vdots \\ f_{t-1\,1} & \cdots & f_{t-1\,s} \end{pmatrix} \cdot \begin{pmatrix} z_1 \\ \vdots \\ z_s \end{pmatrix} = \begin{pmatrix} f_1 \\ \vdots \\ f_{t-1} \end{pmatrix}$$

is of the form

$$z = \bar{a} + A\cdot(c_1,\dots,c_m)^T$$

for some polynomials $c_1,\dots,c_m$.
Let $\bar{b}=(\bar{b}_1,\dots,\bar{b}_m)^T$ be a polynomial vector and

$$B = \begin{pmatrix} b_{11} & \dots & b_{m1} \\ \vdots & & \vdots \\ b_{1s} & \dots & b_{ms} \end{pmatrix}$$

a polynomial matrix such that every solution $z=(z_1,\dots,z_m)^T$ of

$$(**) \qquad (g_{11} \ \dots \ g_{1s}) \cdot z = g,$$

where $g_i = \Sigma_{j=1}^{0} f_{tj} \cdot a_{ij}$, $i=1,\dots,m$, and $g = f_t - \Sigma_{j=1}^{0} f_{tj} \cdot \bar{a}_j$, is of the form

$$z = \bar{b} + B\cdot(d_1,\dots,d_k)^T$$

for some polynomials $d_1,\dots,d_k$.
Then every solution of

$$(***) \qquad \begin{pmatrix} f_{11} & \dots & f_{1s} \\ \vdots & & \vdots \\ f_{t1} & \dots & f_{ts} \end{pmatrix} \cdot \begin{pmatrix} z_1 \\ \vdots \\ z_s \end{pmatrix} = \begin{pmatrix} f_1 \\ \vdots \\ f_t \end{pmatrix}$$

is of the form

$$z = (\bar{a} + A\cdot\bar{b}) + (A\cdot B)\cdot(e_1,\dots,e_k)^T$$

for some polynomials $e_1,\dots,e_k$.

Proof: Let z be of the form $z = (\bar{a} + A\cdot\bar{b}) + (A\cdot B)\cdot(e_1,\dots,e_k)^T$ for some polynomials $e_1,\dots,e_k$. Then $z = \bar{a} + A\cdot(\bar{b} + B\cdot(e_1,\dots,e_k)^T)$, so z is of the form $\bar{a} + A\cdot(c_1,\dots,c_m)^T$, and therefore z solves the first t-1 equations in (***).
$(f_{t1},\dots,f_{ts})\cdot z = (f_{t1},\dots,f_{ts})\cdot ((\bar{a} + A\cdot\bar{b}) + (A\cdot B)\cdot(e_1,\dots,e_k)^T) =$
$(f_{t1},\dots,f_{ts})\cdot \bar{a} + (f_{t1},\dots,f_{ts})\cdot A\cdot(\bar{b} + B\cdot(e_1,\dots,e_k)^T) =$
$f_t - g + (g_1,\dots,g_m)\cdot (\bar{b} + B\cdot(e_1,\dots,e_k)^T) =$
$f_t - g + g = f_t$.
So z also solves the t-th equation in (***).

On the other hand, let z be a solution of (***). Then z is a solution of (*), and therefore it is of the form

$$z = \bar{a} + A\cdot(c_1,\dots,c_m)^T, \text{ for some polynomials } c_1,\dots,c_m.$$

z is also a solution of the t-th equation in (***), so

$$(f_{t1},\dots,f_{ts})\cdot\bar{a} + (f_{t1},\dots,f_{ts})\cdot A\cdot(c_1,\dots,c_m)^T = f_t$$

and therefore

$$(g_1,\dots,g_m)\cdot(c_1,\dots,c_m)^T = f_t - g.$$

So $(c_1,\dots,c_m)^T$ is a solution of (**), i.e.

$$(c_1,\dots,c_m)^T = \bar{b} + B\cdot(d_1,\dots,d_k)^T, \text{ for some polynomials } d_1,\dots,d_k.$$

Thus,

$$z = \bar{a} + A\cdot(\bar{b} + B\cdot(d_1,\dots,d_k)^T) = (\bar{a} + A\cdot\bar{b}) + (A\cdot B)\cdot(d_1,\dots,d_k)^T. \quad \bullet$$

Based on Theorem 7 one gets the following recursive algorithm for solving (P3):

LinSolve:

input: $f_{11},\dots,f_{1s}, \dots, f_{t1},\dots,f_{ts}, f_1,\dots,f_t$, polynomials,
output: a polynomial vector $\bar{a}=(\bar{a}_1,\dots,\bar{a}_s)^T$, and a polynomial matrix of dimension (s,m) for some m, such that the set of solutions of (P3) is $\{\bar{a} + A\cdot(c_1,\dots,c_m)^T \mid c_1,\dots,c_m \text{ polynomials}\}$
or **unsolvable**.

if $t=0$
then **return** $((0,\dots,0), I_s)$
else $\{$ $(\bar{a}',A') :=$ LinSolve$(f_{11},\dots,f_{1s}, \dots, f_{t-1\,1},\dots,f_{t-1\,s}, f_1,\dots,f_{t-1})$ (if the result is **unsolvable** then return **unsolvable**);
$m :=$ number of columns of A';
$(g_1,\dots,g_m) := (f_{t1},\dots,f_{ts})\cdot A'$;
$g := f_t - (f_{t1},\dots,f_{ts})\cdot\bar{a}'$;
$(\bar{b},B) :=$ LinSolve1$(g_1,\dots,g_m, g)$ (if the result is **unsolvable** then return **unsolvable**);
return $(\bar{a}'+A'\cdot\bar{b}, A'\cdot B)$ $\}$ $\bullet$

Example 5: We want to find the solutions of the system

$$(6) \quad \begin{pmatrix} f_{11} & f_{12} & f_{13} \\ f_{11} & f_{12} & f_{13} \end{pmatrix} \cdot \begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix} = \begin{pmatrix} f_1 \\ f_2 \end{pmatrix}$$

where $f_{11}=x_1x_3-x_2^2$, $f_{12}=x_1x_4-x_2x_3$, $f_{13}=x_2x_4-x_3^2$,
$f_{21}=x_2^2-x_1x_2$, $f_{22}=x_1x_4-x_2x_3$, $f_{23}=x_3x_4-x_1x_4$,
$f_1 = 2x_1x_4 + x_1x_3^3 - x_2^2x_3^2 + 2x_2x_3$,
$f_2 = 2x_1x_4 - 2x_2^4x_3^2 - 2x_1x_2^3x_3^2 - 2x_1^2x_2^2x_3^2 + x_1x_2^2x_3^2 + x_2^2x_3^2 - x_1x_2x_3^2 - 2x_2^5x_3 + 5x_1x_2^4x_3 - 2x_1^2x_2^3x_3 - 2x_2x_3$.

The power products are ordered lexicographically, with $x_4 \gg x_3 \gg x_2 \gg x_1$.

(f_{11}, f_{12}, f_{13}) are already a Gröbner basis. Reducing the S-polynomials of this basis to 0, we get a basis for the solutions of the homogenous equation associated with the first equation in (6) as the columns of the matrix A'.

$$A' = \begin{pmatrix} x_4 & x_2x_4 - x_3^2 & -x_3 \\ -x_3 & 0 & x_2 \\ x_2 & x_2^2 - x_1x_3 & -x_1 \end{pmatrix}$$

The reduction of f_1 to normal form modulo this basis yields 0, and we get the particular solution $\bar{a}' = (x_3^2, 2, 0)^T$ of the first equation in (6).

Substitution of the general solution of the first equation into the second equation of (6) leads to

$$(7) \quad g_1z_1 + g_2z_2 + g_3z_3 = g,$$

where

$g_1 = x_2x_3x_4 - x_1x_3x_4 + x_2^2x_4 - 2x_1x_2x_4 + x_2x_3^2,$

$g_2 = -x_1x_3^2x_4 + x_2^2x_3x_4 + x_1^2x_3x_4 + x_2^3x_4 - 2x_1x_2^2x_4 - x_2^2x_3^2 + x_1x_2x_3^2,$

$g_3 = -x_1x_3x_4 + x_1x_2x_4 + x_1^2x_4 - 2x_2^2x_3 + x_1x_2x_3,$

and $g = x_1x_2^2x_3^3 - 2x_2^4x_3^2 + 2x_1x_2^3x_3^2 - 2x_1^2x_2^2x_3^2 - 2x_2^5x_3 + 5x_1x_2^4x_3 - 2x_1^2x_2^3x_3$.

A Gröbner basis for $ideal(g_1, g_2, g_3)$ is (g_1, g_3, g_4, g_5), where

$g_4 = x_1x_2^2x_4 - x_1^2x_2x_4 - \frac{1}{2}x_1^3x_4 + \frac{1}{2}x_1x_2x_3^2 - x_2^3x_3 + \frac{3}{2}x_1x_2^2x_3 - \frac{1}{2}x_1^2x_2x_3,$

$g_5 = x_1x_2x_3^3 - 2x_2^3x_3^2 + 2x_1x_2^2x_3^2 - 2x_1^2x_2x_3^2 - 2x_2^4x_3 + 5x_1x_2^3x_3 - 2x_1^2x_2^2x_3.$

Compare Example 3. The transformation matrices between the basis (g_1, g_2, g_3) and the Gröbner basis (g_1, g_3, g_4, g_5) are

$$X^T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ \frac{1}{2}x_1 & 0 & -\frac{1}{2}x_1 + \frac{1}{2}x_2 \\ x_1x_3 - x_1x_2 - x_1^2 & 0 & x_2x_3 - x_1x_3 + x_2^2 - 2x_1x_2 \end{pmatrix} \qquad Y^T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ x_2 & x_3 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

The syzygies of (g_1, g_3, g_4, g_5) are the rows $R_1, \ldots, R_6$ of the matrix R, where

$R_1 = (-x_1 , x_1 - x_2 , 2 , 0),$

$R_2 = (x_1x_2\ ,\ \frac{1}{2}x_1^2\ ,\ -x_3-x_2+x_1\ ,\ \frac{1}{2}),$

$R_3 = (x_1x_3^2-2x_2^2x_3-x_1x_2x_3+2x_1x_2^2-2x_1^2x_2-x_1^3\ ,\ -x_1x_3^2-x_1^2x_3\ ,\ 4x_1x_2-2x_2^2\ ,\ -x_4-x_3+x_2-x_1),$

$R_4 = (x_1^2\ ,\ x_2^2-\frac{3}{2}x_1^2\ ,\ x_3-x_2-3x_1\ ,\ -\frac{1}{2}),$

$R_5 = (2x_2^2x_3-x_1x_2x_3\ ,\ x_2x_3^2\ ,\ 0\ ,\ x_4),$

$R_6 = (x_1^2x_3^2-2x_2^3x_3-3x_1^2x_2x_3+\frac{1}{2}x_1^3x_3+x_1x_2^3+2x_1^2x_2^2-\frac{9}{2}x_1^3x_2-\frac{3}{2}x_1^4\ ,\ -\frac{3}{2}x_1^2x_3^2-2x_1^3x_3-\frac{1}{2}x_1^4\ ,\ x_3^3x_2^3-x_1x_2^2+7x_1^2x_2-x_1^3\ ,\ -x_2x_4-\frac{1}{2}x_3^2-\frac{1}{2}x_2x_3-\frac{3}{2}x_1x_3+\frac{1}{2}x_2^2+x_1x_2-2x_1^2).$

Collecting the linearly independent columns of

$$\begin{pmatrix} I_3 - Y^{\mathrm{T}}X^{\mathrm{T}} \\ \hdashline RX^{\mathrm{T}} \end{pmatrix}^{\mathrm{T}}$$

as the columns B_1, B_2 of the matrix B, we get

$B_1 = (-x_2\ ,\ 1\ ,\ -x_3)^{\mathrm{T}},$

$B_2 = (-x_1x_3x_4+x_1x_2x_4+x_1^2x_4-2x_2^2x_3+x_1x_2x_3\ ,\ 0\ ,\ -x_2x_3x_4+x_1x_3x_4-x_2^2x_4+2x_1x_2x_4-x_2x_3^2)^{\mathrm{T}}.$

Collecting the linearly independent columns of $A'\cdot B$ as the columns of the matrix A, the columns of A form a basis for the solutions of the homogeneous system associated with (6).

$$A = \begin{pmatrix} -x_1x_3x_4^2+x_1x_2x_4^2+x_1^2x_4^2+x_2x_3^2x_4-x_1x_3^2x_4-x_2^2x_3x_4-x_1x_2x_3x_4+x_2x_3^2 \\ x_1x_3^2x_4-x_2^2x_3x_4-x_1^2x_3x_4-x_2^3x_4+2x_1x_2^2x_4+x_2^2x_3^2-x_1x_2x_3^2 \\ -x_1^2x_3x_4+2x_1x_2^2x_4-x_1^2x_2x_4+x_1x_2x_3^2-2x_2^3x_3+x_1x_2^2x_3 \end{pmatrix}$$

Reducing g to 0 modulo the Gröbner basis (g_1, g_3, g_4, g_5), we get the particular solution $\bar{b}' = (0,0,0,x_2)^{\mathrm{T}}$ of the equation

$$g_1z_1 + g_3z_3 + g_4z_4 + g_5z_5 = g.$$

So a particular solution of (7) is

$$\bar{b} = (\bar{b}'^{\mathrm{T}}\cdot X^{\mathrm{T}})^{\mathrm{T}} = \begin{pmatrix} x_1x_2x_3-x_1x_2^2-x_1^2x_2 \\ 0 \\ x_2^2x_3-x_1x_2x_3+x_2^3-2x_1x_2^2 \end{pmatrix}.$$

Thus, a particular solution of (6) is

$$\bar{a} = \bar{a}' + A'\cdot\bar{b} = \begin{pmatrix} x_1x_2x_3x_4-x_1x_2^2x_4-x_1^2x_2x_4-x_2^2x_3^2+x_1x_2x_3^2+x_3^2-x_2^3x_3+2x_1x_2^2x_3 \\ -x_1x_2x_3^2+x_2^3x_3+x_1^2x_2x_3+x_2^4-2x_1x_2^3+2 \\ x_1^2x_2x_3-2x_1x_2^3+x_1^2x_2^2 \end{pmatrix}.$$

3.4. Membership in the radical of an ideal

The *radical* of an ideal I, $rad(I)$, consists of all polynomials f such that $f^m \in I$ for some $m \geq 1$. For a polynomial ideal I, the radical of I has a geometric meaning. If $f_1,\ldots,f_s$ generate an ideal I, then $f \in rad(I)$ iff f vanishes on the algebraic curve described by I. The set of points in $\bar{K}^n$ on which all the polynomials of the ideal I vanish is called the *variety* of I.

Theorem 8: Let $f_1,\ldots,f_s$, f be polynomials. $f \in rad(f_1,\ldots,f_s)$ if and only if f vanishes on the variety of $ideal(f_1,\ldots,f_s)$.

Proof: By Hilbert's Nullstellensatz [Lang 84], if f vanishes on the variety of $ideal(f_1,\ldots,f_s) = I$ then $f \in rad(I)$.

On the other hand assume that $f \in rad(I)$. So there is an $m \geq 1$ such that $f^m \in I$. So for every $\bar{x} \in \bar{K}^n$ in the variety of I we have $0 = f^m(\bar{x}) = (f(\bar{x}))^m$, and therefore $f(\bar{x}) = 0$. •

In order to test whether a polynomial f vanishes on the variety of an ideal I, we can adapt Rabinowitsch's method of proving Hilbert's Nullstellensatz.

Theorem 9: Let $f_1,\ldots,f_s$, f be polynomials. f vanishes on the variety of $ideal(f_1,\ldots,f_s) = I$ if and only if $1 \in ideal(f_1,\ldots,f_s,f\cdot z-1)$, where z is a new variable.

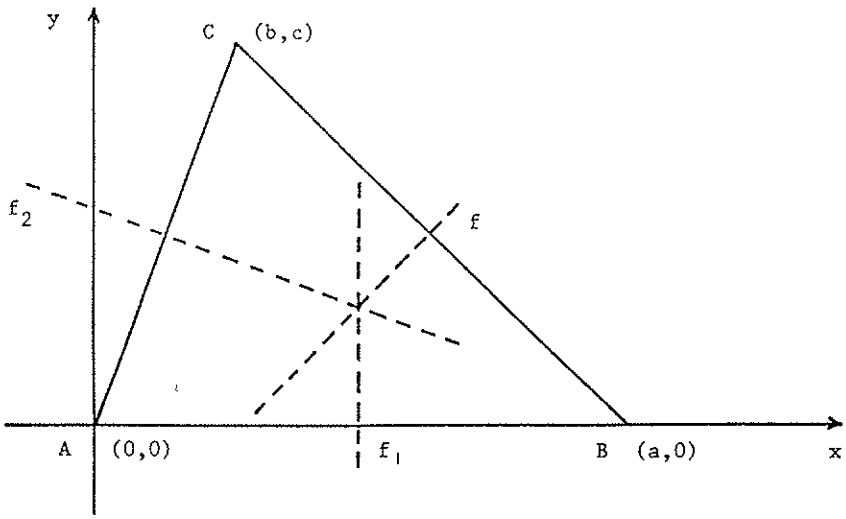
Proof: f vanishes on the variety of I if and only if the system of equations

$$f_1=0, \ldots ,f_s=0, f\cdot z=1$$

has no solution in $\bar{K}^{n+1}$. This is the case if and only if $ideal(f_1,\ldots,f_s,f\cdot z-1)$ is the unit ideal [van der Waerden 67], i.e. I contains 1. •

This geometric interpretation of the radical of an ideal I can be employed for automatizing the solution of a class of geometric problems. In the sequel we present a simple example. For further details the reader is referred to [Chou 84], [Wu 84], [Kutzler/Stifter 86], and [Kapur 86].

Example 6: We want to prove the geometric theorem that for every triangle ABC the lines which are orthogonal to the sides of the triangle and pass through the midpoints of the associated sides have a common point of intersection.



Before we can express this theorem algebraically, we have to place the triangle in a two dimensional coordinate system. Without loss of generality we can assume that A is placed at the origin and that the side AB is parallel to the x-axis. Now a point $(\overline{x},\overline{y})$ lies on the line that is perpendicular to AB and passes through the midpoint of AB if and only if the polynomial

$$f_1(x,y) = x - \tfrac{1}{2}a$$

vanishes on $(\overline{x},\overline{y})$. A point $(\overline{x},\overline{y})$ lies on the line that is perpendicular to AC and passes through the midpoint of AC if and only if the polynomial

$$f_2(x,y) = b(x-\tfrac{1}{2}b) + c(y-\tfrac{1}{2}c)$$

vanishes on $(\overline{x},\overline{y})$. $(\overline{x},\overline{y})$ lies on the line that is perpendicular to BC and passes through the midpoint of BC if and only if the polynomial

$$f(x,y) = (a-b)(x-\tfrac{1}{2}(a+b)) + c(y-\tfrac{1}{2}c)$$

vanishes on $(\overline{x},\overline{y})$. So in order to prove the theorem, we have to prove that f vanishes on the variety of $ideal(f_1,f_2)$, or in other words that $f \in rad(f_1,f_2)$. Computation of a Gröbner basis for $ideal(f_1,f_2,f\cdot z-1)$ yields the basis (1). So f vanishes indeed on the variety of $ideal(f_1,f_2)$, and therefore the theorem holds. •

References

[Buchberger 65] B. Buchberger: *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* Ph.D. dissertation, Univ. Innsbruck (Austria) (1965)

[Buchberger 70] B. Buchberger: Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems, Aequationes Math. 4/3, 374-383 (1970)

[Buchberger 76a] B. Buchberger: A Theoretical Basis for the Reduction of Polynomials to Canonical Forms, *ACM SIGSAM Bull.* **10/3**, 19-29 (1976)

[Buchberger 76b] B. Buchberger: Some Properties of Gröbner-Bases for Polynomial Ideals, *ACM SIGSAM Bull.* **10/4**, 19-24 (1976)

[Buchberger 81] B. Buchberger: H-Bases and Gröbner-Bases for Polynomial Ideals, Techn. Rep. CAMP 81-2.0, Inst. f. Math., Univ. Linz (Austria) (1981)

[Buchberger 83] B. Buchberger: Gröbner Bases: A Method in Symbolic Mathematics, 5th Internat. Conf. on Simulation, Programming and Math. Methods for Solving Physical Problems, Joint Inst. for Nuclear Research, Dubna, USSR (1983)

[Buchberger 85] B. Buchberger: Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory, in *Recent Trends in Multidimensional Systems Theory*, N.K. Bose (ed.), D. Reidel Publ. Comp. (1985)

[Chou 84] S.C. Chou: Proving Elementary Geometry Theorems Using Wu's Algorithm, in *Contemporary Mathematics* **29**, 243-286 (1984)

[Gröbner49] W. Gröbner: Moderne algebraische Geometrie, Springer-Verlag, Wien-Innsbruck, (1949)

[Hermann 26] G. Hermann: Die Frage der endlich vielen Schritte in der Theorie der Polynomideale, *Math. Ann.* **95**, 736-788 (1926)

[Hilbert 1890] D. Hilbert: Über die Theorie der algebraischen Formen, *Math. Ann.* **36**, 473-534 (1890)

[Hironaka 64] H. Hironaka: Resolution of Singularities of an Algebraic Variety over a Field of Characteristic Zero: I, II, *Ann. Math.* **79**, 109-326 (1964)

[Kandri-Rody/Kapur 83] A. Kandri-Rody and D. Kapur: On Relationship between Buchberger's Gröbner Basis Algorithm and the Knuth-Bendix Completion Procedure, Rep. No. 83CRD286, General Electric Research and Development Center, Schenectady, New York (1983)

[Kapur 86] D. Kapur: Geometry Theorem Proving Using Hilbert's Nullstellensatz, Proc. 1986 ACM-SIGSAM Symp. on Symbolic and Algebraic Computation (SYMSAC'86)

[Kutzler/Stifter 86] B. Kutzler and S. Stifter: Automated Geometry Theorem Proving Using Buchberger's Algorithm, Proc. 1986 ACM-SIGSAM Symp. on Symbolic and Algebraic Computation (SYMSAC'86)

[Lang 84] S. Lang: *Algebra*, 2nd ed., Addison-Wesley (1984)

[Llopis 83] R. Llopis de Trias: Canonical Forms for Residue Classes of Polynomial Ideals and Term Rewriting Systems, Techn. Rep., Univ. Aut. de Madrid, Division de Matematicas (1983)

[Macauley 16] F.S. Macauley: Algebraic Theory of Modular Systems, *Cambridge Tracts in Mathematics and Mathematical Physics* **19**, Cambridge Univ. Press (1916)

[Möller/Mora 86] H.M. Möller and F. Mora: New Constructive Methods in Classical Ideal Theory, *J. of Algebra* **100**/1, 138-178 (1986)

[Trinks 78] W. Trinks: Über B. Buchbergers Verfahren, Systeme algebraischer Gleichungen zu lösen, *J. of Number Theory* **10**/4, 475-488 (1978)

[van der Waerden 67] B.L. van der Waerden: *Algebra II*, Springer-Verlag (1967)

[Winkler 84] F. Winkler: *The Church-Rosser Property in Computer Algebra and Special Theorem Proving: An Investigation of Critical-Pair/Completion Algorithms*, Ph.D. dissertation, Univ. Linz (Austria) (1984)

[Winkler/Buchberger 83] F. Winkler and B. Buchberger: A Criterion for Eliminating Unnecessary Reductions in the Knuth-Bendix Algorithm, Proc. Colloquium on Algebra, Combinatorics and Logic in Computer Science, Györ (Hungary) (1983)

[Winkler et al 85] F. Winkler, B. Buchberger, F. Lichtenberger, and H. Rolletschek: An Algorithm for Constructing Canonical Bases of Polynomial Ideals, *ACM Trans. on Math. Software* **11**/1, 66-78 (1985)

[Wu 84] W.T. Wu: Some Recent Advances in Mechanical Theorem Proving of Geometries, in *Contemporary Mathematics* **29**, 235-241 (1984)