Research
Institute for
Symbolic
Computation

LINZ
Johannes Kepler University, A-4040 Linz, Austria (Europe)

Publications / Reports

Editors: RISC-LINZ faculty

(B. Buchberger, A. Leitsch, F. Lichtenberger, P. Paule,
H. Rolletschek, F. Winkler, H. Zassenhaus)

Applications of Gröbner Bases: Solution of Algebraic Equations and Decomposition of Radicals

M. Kalkbrener

Diploma Thesis

RISC-LINZ Series no. 87-30.0

Sponsored by:

Applications of Gröbner Bases: Solution of Algebraic Equations and Decomposition of Radicals

Diplomarbeit

zur Erlangung des akademischen Grades
"Diplom-Ingenieur"
in der Studienrichtung
"Technische Mathematik"

eingereicht von

Michael Kalkbrener

September 1987

Angefertigt am Institut für Mathematik
Technisch-Naturwissenschaftliche Fakultät
Johannes Kepler Universität Linz
Eingereicht bei o.Univ.-Prof. Dr. Bruno Buchberger

Abstract

In this paper we use Gröbner bases mainly for the exact solution of systems of algebraic equations and questions about the solvability of such systems. In particular, we give an explicit description of an algorithm for finding all solutions of a system of algebraic equations which is solvable and has finitely many solutions. This algorithm is an improved version of a method which was deviced by B. Buchberger. By a theorem proven in this paper, gcd-computations occuring in Buchberger's method can be avoided in our algorithm. Furthermore, some other properties of Gröbner bases of zero-dimensional ideals are proved, which lead to further refined versions of this algorithm.

We give a structure theorem for reduced Gröbner bases of zero-dimensional prime ideals and present an algorithm that decomposes the radical of a zero-dimensional ideal that is given by its reduced Gröbner basis into the intersection of prime ideals. The reduced Gröbner bases of these prime ideals are the output of this algorithm. This method reduces the problem of finding all solutions of a system of algebraic equations to an easier problem. In addition, it is shown how this algorithm can be used for deciding membership in the radical of a given zero-dimensional polynomial ideal and for solving the primary decomposition problem for zero-dimensional polynomial ideals.

Contents

Chapter 1

Introduction

For many years G. Hermann's algorithm for deciding the ideal membership problem was the only algorithmic method in polynomial ideal theory (see [8]). However, her work does not give solution to the "simplification problem modulo an ideal" (i.e. the problem of finding unique representatives in the residue classes modulo the ideal) and to the problem of effectively computing in the residue class ring modulo an ideal.

In 1964 Hironaka defined the notion of a standard basis for an ideal in a regular local ring (see [9]). One year later in his Ph.D.thesis B. Buchberger independently introduced the concept of Gröbner bases, which is basically identical to Hironaka's definition of a standard basis. However, in contrast to Hironaka, Buchberger presented an algorithm for constructing the bases. Buchberger's Ph.D.thesis is accessible in [3].

The method of Gröbner bases, as its central objective, solves the simplification problem for polynomial ideals and, on this basis, gives easy solutions to a large number of other algorithmic problems including Hermann's original membership problem. Only about eleven years ago the computer algebra community has become aware of the concept of Gröbner bases and since that time this method has been refined, generalized, applied and analysed in a number of papers.

In the present paper we use Gröbner bases mainly for the exact solution of systems of algebraic equations and questions about the solvability of such systems. In particular, we deal with the following problems:

Problem 1

Given: *F, a finite set of polynomials in the indeterminates $x_1, \ldots, x_n$ over a field K.*

Decide: *whether*

F is unsolvable,
F is solvable and has finitely many solutions, or
F is solvable and has infinitely many solutions.

(A solution of F is an element b of $\bar{K}^n$ such that

$$f(b) = 0 \text{ for all } f \in F,$$

where $\bar{K}$ is the algebraic closure of K.)

Problem 2

Given: *F, a finite set of polynomials in the indeterminates $x_1, \ldots, x_n$ over a field K such that F is solvable and has finitely many solutions.*

Find: *all solutions of the system F.*

A decision method for Problem 1 is given in [3], see also [6].

A first algorithm for reducing the multivariate Problem 2 to a univariate one by using Gröbner bases appears in [3]. W. Trinks shows that the i-th elimination ideal of a Gröbner basis G with respect to the purely lexicographical ordering is generated by the polynomials in G that depend only on the variables $x_1, \ldots, x_i$ (see [14]). Therefore, every reduced Gröbner basis $\{G_{1,1}, G_{2,1}, \ldots, G_{2,car_2}, \ldots, G_{n,1}, \ldots, G_{n,car_n}\}$ of a zero-dimensional ideal in $K[x_1, \ldots, x_n]$ has the form

$$\begin{array}{rcl} G_{1,1} & \in & K[x_1], \\ G_{2,1} & \in & K[x_1, x_2], \\ \ldots & & \ldots \\ G_{2,car_2} & \in & K[x_1, x_2], \\ \ldots & & \ldots \\ G_{n,1} & \in & K[x_1, \ldots, x_n], \\ \ldots & & \ldots \\ G_{n,car_n} & \in & K[x_1, \ldots, x_n], \end{array}$$

where $car_2, \ldots, car_n \in N_+$.

In [6] an algorithm is presented, which makes use of this structure. Method 6.10 in [6] finds a solution $(b_1, \ldots, b_i, c)$ of the $i+1$-th elimination ideal by adjoining a zero c of the polynomial

$$gcd(G_{i+1,1}(b_1, \ldots, b_i, x_{i+1}), \ldots, G_{i+1,car_{i+1}}(b_1, \ldots, b_i, x_{i+1}))$$

to the solution $(b_1, \ldots, b_i)$ of the i-th elimination ideal.

One of the main results in this paper is a theorem which says that there exists a $d \in \bar{K}$ and an $r \in \{1, \ldots, car_{i+1}\}$ such that

$$d \cdot G_{i+1,r}(b_1, \ldots, b_i, x_{i+1}) = gcd(G_{i+1,1}(b_1, \ldots, b_i, x_{i+1}), \ldots, G_{i+1,car_{i+1}}(b_1, \ldots, b_i, x_{i+1}))$$

and that the polynomial $G_{i+1,r}$ can be easily found by a test for zero in an extension field of K. Therefore, this theorem leads to an improved version of Method 6.10, in which the gcd-computation is avoided. Furthermore, we show that every solution of one of the elimination ideals can be continued.

The most time-consuming subalgorithm in our improved version is the algorithm that continues every partial solution $(b_1 \ldots, b_i)$ by computing the zeros of the corresponding $G_{i+1,r}$. Therefore, we investigate the problem whether it is possible to decompose such a $G_{i+1,r}$ by using properties of the structure of reduced Gröbner bases. We show that it is often possible to find non-constant polynomials $f_1, \ldots, f_s$ such that

$$G_{i+1,r} = f_1 \cdot \ldots \cdot f_s \text{ and } s \geq 2.$$

In this case we can compute the zeros of $G_{i+1,r}$ by computing the zeros of the polynomials $f_1, \ldots, f_s$. As the degrees of $f_1, \ldots, f_s$ are smaller than the degree of $G_{i+1,r}$, this strategy might lead to a speed-up.

Furthermore, we present a method for solving Problem 2, which has the advantage that a subalgorithm for finding the zeros of a univariate polynomial over K and not over an extension field of K is required. Roughly, this is achieved by multiplication of appropriate univariate polynomials over an extension field of K. The result of this multiplication is a univariate polynomial over K.

We give a structure theorem for reduced Gröbner bases of zero-dimensional prime ideals and present an algorithm that decomposes the radical of a zero-dimensional ideal, which is given by its reduced Gröbner basis, into the intersection of prime ideals. The reduced Gröbner bases of these prime ideals are the output of the algorithm. This method reduces Problem 2 to an easier problem. In addition, the following question can be answered too:

Problem 3

Given: *$f_1, \ldots, f_m, g$, polynomials in the indeterminates $x_1, \ldots, x_n$ over a field K. Furthermore, we assume that $\{f_1, \ldots, f_m\}$ is solvable and has finitely many solutions.*

Decide: *whether*

$$f_1(b) = \ldots = f_m(b) = 0 \textit{ implies } g(b) = 0 \textit{ for all } n\textit{-tuples } b \textit{ in } \bar{K}^n,$$

or in other words, whether

g is contained in the radical of the ideal generated by $\{f_1, \ldots, f_m\}$.

Another method for deciding membership in a radical is due to Rabinowitsch and can be found in [15].

Our algorithm for decomposing a radical can also be used for solving Problem 4, the primary decomposition problem for zero-dimensional polynomial ideals (see, for instance, [13]):

Problem 4

Given: *I, a zero-dimensional ideal in the polynomial ring in the indeterminates $x_1, \ldots, x_n$ over a field K.*

Find: *$Q_1, \ldots, Q_r$, primary ideals such that*

$$I = Q_1 \cap \ldots \cap Q_r$$

is a reduced primary decomposition of I.

In Chapter 2 we give the necessary definitions for working with multivariate polynomial rings and exactly specify the problems we want to solve in the present paper. In Chapter 3 the definition of a Gröbner basis and the algorithm for constructing reduced Gröbner bases are given. Furthermore, we review how Gröbner bases can be used for solving Problem 1 and Problem 2. In Chapter 4 we show that every solution of one of the elimination ideals can be continued. In Chapter 5 we prove some new properties of reduced Gröbner bases of zero-dimensional ideals and present different versions of Buchberger's Method 6.10 for solving systems of algebraic equations. In Chapter 6 an algorithm for decomposing the radical of a zero-dimensional ideal into the intersection of prime ideals is given. Furthermore, we apply this algorithm to Problem 2, Problem 3, and Problem 4.

Chapter 2

Definitions and Problems

2.1 A Model for Multivariate Polynomial Rings

In this section we review a suitable model for the ring of polynomials over a field K in n indeterminates (see [4]).

If we think, for example, of polynomials in the polynomial ring over the rational numbers Q in two indeterminates, we usually think of expressions of the form

$$3xy^2 + 5x - 1 \text{ or}$$
$$y^3x - 2y + 3xy + 4.$$

Note that several of these expressions may denote the same polynomials. For instance,

$$3xy^2 + 5x - 1,$$
$$-1 + 5x + 3xy^2, \text{ and}$$
$$0x^2 + 3xy^2 + 5x - 1$$

are expressions denoting the same polynomial $xy^2 + 5x - 1 + 2xy^2$. If one wanted to think of the polynomial ring over Q in two indeterminates to be a set of expressions of the above kind, one had to norm these expressions by some rules (for instance,

1. *combine equal terms*

2. *omit terms with zero coefficient*

3. *use a fixed order of terms)* .

One should carefully distinguish between the two meanings of the sign + in expressions like

$$(5x^2 + 3y) + (2xy + 1),$$

where the first and the third + are separators between terms and the second + is a symbol for addition of two polynomials. Otherwise, by the suggestive notations above, one is easily mislead to draw incorrect conclusions in reduction arguments for polynomials. In order to make the subsequent discussions unambiguous we adopt the following model of the set of polynomials in n indeterminates over a field K.

Throughout the paper K denotes an arbitrary field, $\bar{K}$ the algebraic closure of K, and n an element of $N \setminus \{0,1\}$. ($N \ldots$ set of natural numbers including zero, $N_+ := N \setminus \{0\}$).

The following typed variables will be used:

$m \ldots$	an element in $\{1,\ldots,n\}$
$l \ldots$	an element in $\{2,\ldots,n\}$
$r,s,t,u \ldots$	elements in N
$d,e \ldots$	elements in $\bar{K}$
$L \ldots$	a field with $K \subseteq L \subseteq \bar{K}$

For $k,k' \in N^m$, $k+k'$ is the componentwise sum of k and k'.

We write $f(j_1,\ldots,j_n)$ instead of $f((j_1,\ldots,j_n))$, where $f \in \bar{K}[x_1,\ldots,x_n]$ and $j \in N^n$. Furthermore, (i,i') denotes $(i_1,\ldots,i_r,i'_1,\ldots,i'_s) \in N^{r+s}$, where $i \in N^r$ and $i' \in N^s$.

The polynomial ring in n indeterminates over the field L is the structure $(L[x_1,\ldots,x_n],+,\cdot)$, where

$$L[x_1,\ldots,x_n] := \{\, f : N^n \to L \mid \{\, i \mid i \in N^n,\ f(i) \neq 0 \,\} \text{ is finite} \}$$

and for $f,g \in L[x_1,\ldots,x_n]$ and $i \in N^n$

$$\begin{aligned} (f+g)(i) &:= f(i)+g(i) \\ (f\cdot g)(i) &:= \sum_{\substack{j \in N^n,\\ k \in N^n \\ j+k=i}} f(j)\cdot g(k) \end{aligned}$$

Furthermore,

$$C(f) := \{\, i \mid i \in N^n \text{ and } f(i) \neq 0 \,\}.$$

Note that in this definition the "indeterminates" $x_1,\ldots,x_n$ do not play any logical role. They are only "syntactical sugar".

In this model polynomials in $L[x_1,\ldots,x_n]$ are functions from N^n to L. In examples, however, we will use the usual notation of polynomials as arithmetical expressions involving indeterminates. For instance, the polynomial $g \in Q[x_1,x_2]$ with

$$g(0,0) = -1,\ g(1,0) = 5,\ g(1,2) = 3, \text{ and } g(i_1,i_2) = 0 \text{ otherwise,}$$

might be written in the form $3xy^2 + 5x - 1$ in the examples.

If we replace x by $\sqrt{2}$ in this polynomial we get the polynomial

$$(3\cdot\sqrt{2})x^0y^2 + (5\cdot\sqrt{2} - 1)x^0y^0.$$

In this paper we want to conceive this polynomial as a special *bivariate* polynomial. In the formal model this replacement operation is defined as follows:

Let $f \in \bar{K}[x_1, \ldots, x_n]$ and $b \in \bar{K}^m$.
Then the polynomial $\overline{f(b)}$ is an element of $\bar{K}[x_1, \ldots, x_n]$ such that

$$\begin{array}{llll} \overline{f(b)}: & N^n & \rightarrow & \bar{K} \\ & j & \mapsto & 0 \quad \text{if there exists an } r \in \{1, \ldots, m\} \text{ with } j_r \neq 0 \\ & j & \mapsto & \sum_{i \in N^m} f(i, (j_{m+1}, \ldots, j_n)) \cdot b^i \quad \text{otherwise,} \\ & & & \text{where } b^i := \prod_{r=1}^{m} b_r^{i_r}. \end{array}$$

(Note that there are only finitely many $i \in N^n$ with $f(i) \neq 0$.)

We write $\overline{f(b_1, \ldots, b_m)}$ instead of $\overline{f((b_1, \ldots, b_m))}$.

For the above g,

$\overline{g(\sqrt{2})}$ is $(3 \cdot \sqrt{2})x^0y^2 + (5 \cdot \sqrt{2} - 1)x^0y^0$ and
$\overline{g(\sqrt{2}, 0)}$ is $(5 \cdot \sqrt{2} - 1)x^0y^0$

in the usual notation.

Before we prove a few basic properties of the introduced model we make the following convention:

Convention: To avoid confusion we denote $0 \in \bar{K}^m$ and $0 \in N^m$, the neutral elements with respect to $+$ in $\bar{K}^m$ and in N^m, by 0_m, $0 \in \bar{K}[x_1, \ldots, x_n]$, the neutral element with respect to $+$ in $\bar{K}[x_1, \ldots, x_n]$, by 0_p, and reserve 0 as symbol for the integer zero and the zero in $\bar{K}$.

Lemma 1 *Let $f, g \in \bar{K}[x_1, \ldots, x_n]$ and $b \in \bar{K}^m$.*
Then

$$\overline{(f+g)(b)} = \overline{f(b)} + \overline{g(b)} \text{ and } \overline{(f \cdot g)(b)} = \overline{f(b)} \cdot \overline{g(b)}.$$

Proof: Let $i \in N^m$ and $j \in N^{n-m}$.

Case $i \neq 0_m$:

$$\overline{(f+g)(b)}(i,j) = 0 = \overline{f(b)}(i,j) + \overline{g(b)}(i,j) = (\overline{f(b)} + \overline{g(b)})(i,j).$$

$$\overline{(f \cdot g)(b)}(i,j) = 0 = \sum_{\substack{i', i'' \in N^m, \\ j', j'' \in N^{n-m} \\ (i',j')+(i'',j'')=(i,j)}} \overline{f(b)}(i',j') \cdot \overline{g(b)}(i'',j'') = (\overline{f(b)} \cdot \overline{g(b)})(i,j).$$

Case $i = 0_m$:

$$\overline{(f+g)(b)}(0_m, j) = \sum_{k\in N^m} (f+g)(k,j)\cdot b^k =$$

$$= \sum_{k\in N^m} f(k,j)\cdot b^k + \sum_{k\in N^m} g(k,j)\cdot b^k = \overline{f(b)}(0_m,j) + \overline{g(b)}(0_m,j).$$

$$\overline{(f\cdot g)(b)}(0_m, j) = \sum_{k\in N^m} (f\cdot g)(k,j)\cdot b^k =$$

$$= \sum_{k\in N^m} \sum_{\substack{k',k''\in N^m,\\ j',j''\in N^{n-m}\\ (k',j')+(k'',j'')=(k,j)}} f(k',j')\cdot g(k'',j'')\cdot b^k =$$

$$= \sum_{\substack{j',j''\in N^{n-m}\\ j'+j''=j}} \sum_{k\in N^m} \sum_{\substack{k',k''\in N^m,\\ k'+k''=k}} f(k',j')\cdot g(k'',j'')\cdot b^k =$$

$$= \sum_{\substack{j',j''\in N^{n-m}\\ j'+j''=j}} \sum_{k',k''\in N^m} f(k',j')\cdot g(k'',j'')\cdot b^{k'+k''} =$$

$$= \sum_{\substack{j',j''\in N^{n-m}\\ j'+j''=j}} (\sum_{k'\in N^m} f(k',j')\cdot b^{k'})\cdot(\sum_{k''\in N^m} g(k'',j'')\cdot b^{k''}) =$$

$$= \sum_{\substack{j',j''\in N^{n-m}\\ j'+j''=j}} \overline{f(b)}(0_m,j')\cdot\overline{g(b)}(0_m,j'') = (\overline{f(b)}\cdot\overline{g(b)})(0_m,j). \quad \bullet$$

Lemma 2 *Let* $f \in \bar{K}[x_1,\ldots,x_n]$, $r \in \{1,\ldots,l-1\}$, $b \in \bar{K}^r$, *and* $c \in \bar{K}^{l-r}$. *Then*

$$\overline{f(b,c)} = \overline{\overline{f(b)}(0_r,c)}.$$

Proof: Let $j \in N^{n-l}$.

$$\overline{\overline{f(b)}(0_r,c)}(0_l,j) = \sum_{i\in N^l} \overline{f(b)}(i,j)\cdot(0_r,c)^i = \sum_{i'\in N^{l-r}} \overline{f(b)}(0_r,i',j)\cdot c^{i'} =$$

$$\sum_{i'\in N^{l-r}} \sum_{i''\in N^r} f(i'',i',j)\cdot b^{i''}\cdot c^{i'} = \overline{f(b,c)}(0_l,j)$$

Let $i \in N^l \setminus \{0_l\}$.

$$\overline{f(b,c)}(i,j) = 0 = \overline{\overline{f(b)}(0_r,c)}(i,j).$$

Thus, $\overline{f(b,c)} = \overline{\overline{f(b)}(0_r,c)}$. $\bullet$

2.2 Definitions and Theorems

In this section we give further definitions and state some well-known theorems.

Definition 1 Let $\{r_1, \ldots, r_s\} \subseteq \{1, \ldots, n\}$. Obviously,

$\{ h \mid h \in L[x_1, \ldots, x_n]$ and $i_t = 0$ for all $i \in C(h)$ and all $t \in \{1, \ldots, n\} \backslash \{r_1, \ldots, r_s\} \}$

is a subring of $L[x_1, \ldots, x_n]$. It is called *the polynomial ring in the indeterminates* $x_{r_1}, \ldots, x_{r_s}$ *over the field* L, abbreviated $L[x_{r_1}, \ldots, x_{r_s}]$.

Let J be an ideal in $L[x_1, \ldots, x_m]$ and $s \in \{1, \ldots, m\}$. We call the ideal

$$J \cap L[x_1, \ldots, x_s]$$

the *s-th elimination ideal of* J, abbreviated $J_{/x_s}$.

Let $f_1, f_2 \in L[x_1, \ldots, x_m]$.
We write

$$f_1 \equiv_J f_2$$

for f_1 *is congruent to* f_2 *modulo* J (i.e. $f_1 - f_2 \in J$).

Let $f \in \bar{K}[x_1, \ldots, x_n] \setminus \{0_p\}$. We denote

$$\max\{ r \mid \text{there exists an } i \in C(f) \text{ such that } i_m = r \}$$

by $deg(f, m)$. Furthermore,

$$deg(0_p, m) = -1. \quad \bullet$$

Example 1 Let $f := xy^2 - y^2 - x^3y + y + 2 \in Q[x, y]$.

Sometimes it is necessary to consider f as a univariate polynomial in y and to write it in the form

$$(x - 1)y^2 + (-x^3 + 1)y + 2.$$

We denote the coefficient of y^r in f by $f_{(.,(r))}$. In this example:

$$\begin{array}{lcl} f_{(.,(2))} & := & x - 1, \\ f_{(.,(1))} & := & -x^3 + 1, \text{ and} \\ f_{(.,(0))} & := & 2. \end{array}$$

As the degree of f in y is 2, $f_{(.,(2))}$ is called the leading coefficient of f. $\bullet$

We give a formal definition of $f_{(.i)}$ and the leading coefficient of f:

Definition 2 Let $f \in \bar{K}[x_1, \ldots, x_n]$ and $i \in N^m$.

$$\begin{array}{llll} f_{(.,i)} : & N^n & \rightarrow & \bar{K} \\ & j & \mapsto & 0 & \text{if } (j_{n-m+1}, \ldots, j_n) \neq 0_m \\ & j & \mapsto & f(j_1, \ldots, j_{n-m}, i_1, \ldots, i_m) & \text{otherwise.} \end{array}$$

Let g be a non-constant polynomial in $\bar{K}[x_1, \ldots, x_n]$ and $j \in N^{n-s'+1}$ such that

$$j_1 = deg(g, s') \text{ and } j_2 = \ldots = j_{n-s'+1} = 0,$$

where

$$s' := max\{\, m \mid deg(g, m) > 0 \,\}.$$

The polynomial $g_{(.,j)}$ is called *the leading coefficient of* g, abbreviated $lc(g)$.

Let $F = \{f_1, \ldots, f_r\}$ be a finite subset of $L[x_1, \ldots, x_m]$. By $Ideal_{L,m}(F)$ we denote the ideal in $L[x_1, \ldots, x_m]$ generated by F (i.e. the set

$$\{\, f_1 \cdot g_1 + \ldots + f_r \cdot g_r \mid g_s \in L[x_1, \ldots, x_m],\ f_s \in F\ (s = 1, \ldots, r) \,\}).$$

Let J be an ideal in $L[x_1, \ldots, x_m]$. The set

$$V(J) := \{\, b \mid b \in \bar{K}^m \text{ and } \overline{f(b)} = 0_p \text{ for all } f \in J \,\}$$

is called *the variety of* J. •

By Hilbert's basis theorem, we can choose a finite subset $H = \{h_1, \ldots, h_r\}$ of $L[x_1, \ldots, x_m]$ such that $Ideal_{L,m}(H) = J$. Let $g \in J$ and $b \in \bar{K}^m$ with

$$\overline{h_1(b)} = \ldots = \overline{h_r(b)} = 0_p.$$

As there exist $q_1, \ldots, q_r \in L[x_1, \ldots, x_m]$ with

$$g = h_1 \cdot q_1 + \ldots + h_r \cdot q_r,$$

we have

$$\overline{g(b)} = 0_p.$$

Thus, the common zeros of $h_1, \ldots, h_r$ are exactly the elements of the variety of the ideal generated by $\{h_1, \ldots, h_r\}$.

Definition 3 An element b of $V(J)$ is a *generic zero of ideal* J iff

for all $f \in L[x_1, \ldots, x_m]$: $\overline{f(b)} = 0_p$ *implies* $f \in J$.

An ideal P in $L[x_1, \ldots, x_m]$ is *prime* iff it satisfies the following condition:

Given $f, g \in L[x_1, \ldots, x_m]$, $f \cdot g \in P$, *and* $f \notin P$, *then* $g \in P$.

An ideal Q in $L[x_1, \ldots, x_m]$ is *primary* iff it satisfies the following condition:

Given $f, g \in L[x_1, \ldots, x_m]$, $f \cdot g \in Q$, *and* $f \notin Q$, *then* $g^r \in Q$ *for some* $r \in N_+$.

A prime ideal P in $L[x_1, \ldots, x_m]$ is called *zero-dimensional* iff

there exists an element b *in* $V(P)$ *such that* b *is a generic zero of* P. •

Theorem 1 *Let P be a prime ideal in $L[x_1, \ldots, x_m]$.*
Then $V(P)$ is non-empty and finite iff P is zero-dimensional.

Proof: see [15], *section 129, p. 162.* and [6] *Method 6.9.*

Theorem 2 *Let P be a zero-dimensional prime ideal in $L[x_1, \ldots, x_m]$.*
Then every $b \in V(P)$ is a generic zero of P.

Proof: see [15], *section 129, p. 162.*

Definition 4 Let J be an ideal in $L[x_1, \ldots, x_m]$. We denote the set

$$\sqrt{J} := \{ f \mid f \in L[x_1, \ldots, x_m] \text{ and there exists an } r \in N_+ \text{ with } f^r \in J \}$$

by *radical of ideal J.* •

Theorem 3 *Let Q be a primary ideal in $L[x_1, \ldots, x_m]$.*
Then $\sqrt{Q}$ is a prime ideal and $V(Q) = V(\sqrt{Q})$.

Proof: see [15], *section 117, p. 129*, and [15], *section 131, p. 167.*

Definition 5 When ideal J in $L[x_1, \ldots, x_m]$ is written as a finite intersection of primary ideals in $L[x_1, \ldots, x_m]$, say

$$J = Q_1 \cap \ldots \cap Q_r,$$

we call this a *primary decomposition of J.* A primary decomposition such that $\sqrt{Q_1}, \ldots, \sqrt{Q_r}$ are distinct and J cannot be expressed as an intersection of a proper subfamily of the primary ideals $\{Q_1, \ldots, Q_r\}$ is said to be *reduced.* •

Theorem 4 *Let J be an ideal in $L[x_1, \ldots, x_m]$.*
Then there exists a reduced primary decomposition of J.

Proof: see [15], *section 118, p. 136*, or [11], *chapter 6, p. 235.*

Theorem 5 *Let $J = Q_1 \cap \ldots \cap Q_r = Q'_1 \cap \ldots \cap Q'_s$ be reduced primary decompositions of J.*
Then $r = s$ and $\{\sqrt{Q_1}, \ldots, \sqrt{Q_r}\} = \{\sqrt{Q'_1}, \ldots, \sqrt{Q'_s}\}$.

Proof: see [15], *section 119, p. 137*, or [11], *chapter 6, p. 234.*

Definition 6 If a prime ideal P is an element of the uniquely determined set $\{\sqrt{Q_1}, \ldots, \sqrt{Q_r}\}$ in Theorem 5, then we say that P is *associated* with J.

An ideal J in $L[x_1, \ldots, x_m]$ is called *zero-dimensional* iff

$$\textit{every prime ideal } P \textit{ that is associated with } J \textit{ is zero} - \textit{dimensional.} \;\; \bullet$$

Theorem 6 *Let J be an ideal in $L[x_1, \ldots, x_m]$.*
Then $V(J) = \emptyset$ implies $J{=}L[x_1, \ldots, x_m]$.

Proof: see [15], *section 130, p. 164.*

Theorem 6 is a special case of Hilbert's Nullstellensatz. As we consider only zeros in $\bar{K}^m$, we state this theorem only for zero-dimensional ideals.

Theorem 7 (Hilbert's Nullstellensatz) *Let J be a zero-dimensional ideal in $L[x_1, \ldots, x_m]$ and $f \in L[x_1, \ldots, x_m]$ such that $\overline{f(b)} = 0_p$ for all $b \in V(J)$.*
Then there exists an $r \in N_+$ such that $f^r \in J$.

Proof: see [15], *section 130, p. 164*, or [11], *chapter 10, p. 375.*

An easy consequence of Theorem 7 is the following theorem:

Theorem 8 *Let J be a zero-dimensional ideal in $L[x_1, \ldots, x_m]$ and $f \in L[x_1, \ldots, x_m]$.*
Then $f \in \sqrt{J}$ iff $\overline{f(b)} = 0_p$ for all $b \in V(J)$.

From the fact that $J = J_1 \cap J_2$ implies $V(J) = V(J_1) \cup V(J_2)$ for all ideals J, J_1, and J_2 in $L[x_1, \ldots, x_m]$, from Theorem 1, Theorem 3, and Theorem 6 we obtain the following result:

Theorem 9 *An ideal J in $L[x_1, \ldots, x_m]$ is zero-dimensional iff V(J) is non-empty and finite.*

2.3 Problems

In this paper we are concerned with the following problems:

Problem 1

Given: *F, a finite subset of* $K[x_1, \ldots, x_n]$.

Decide: *whether*

$$\begin{gathered} V(I) \text{ is empty, or} \\ V(I) \text{ is non-empty and finite, or} \\ V(I) \text{ is infinite,} \end{gathered}$$

where $I := Ideal_{K,n}(F)$.

Problem 2

Given: *F, a finite subset of* $K[x_1, \ldots, x_n]$ *such that I is zero-dimensional, where* $I := Ideal_{K,n}(F)$.

Find: *V(I).*

The algorithm that is given in chapter 6 reduces Problem 2 to an easier problem. In addition, it can also be used for solving Problem 3 and Problem 4:

Problem 3

Given: *g, a polynomial in* $K[x_1, \ldots, x_n]$ *and*

F, a finite subset of $K[x_1, \ldots, x_n]$ *such that I is zero-dimensional, where* $I := Ideal_{K,n}(F)$.

Decide: *whether*

$$\overline{g(b)} = 0_p \text{ for all } b \in V(I),$$

or in other words, whether

$$g \in \sqrt{I}.$$

Problem 4

Given: *F, a finite subset of* $K[x_1, \ldots, x_n]$ *such that I is zero-dimensional, where* $I := Ideal_{K,n}(F)$.

Find: $H_1, \ldots, H_r$*, finite subsets of* $K[x_1, \ldots, x_n]$ *such that*

$$I = Ideal_{K,n}(H_1) \cap \ldots \cap Ideal_{K,n}(H_r)$$

is a reduced primary decomposition of I.

Let us consider the following example:

Example 2 Given $F := \{f_1, f_2, f_3\} \subseteq Q[x, y]$, where

$$\begin{aligned} f_1 &:= x^2y - y + x^2 - 1, \\ f_2 &:= xy + x - 1, \\ f_3 &:= xy^3 + y^3 + y + 2, \end{aligned}$$

and $G := \{g_1, g_2\} \subseteq Q[x, y]$, where

$$\begin{aligned} g_1 &:= x + 1, \\ g_2 &:= y + 2. \end{aligned}$$

Both sets are generating sets for the same ideal I. Note that the solution of each of the given problems does not depend on a specific generating set. Therefore, we could choose F or G as generating set for the ideal I. Intuitively, G would be the right choice in this example. •

This idea, the idea of looking for a "favourable" generating set for a given ideal, leads us to the concept of Gröbner bases.

Chapter 3

Gröbner Bases

In this chapter we give the definition of a Gröbner basis, an algorithm for constructing one, and describe how a Gröbner basis can be used to solve Prob'em 1 and Problem 2 (see [6]).

3.1 Definition of Gröbner Bases

Definition 7 The polynomial $v \in K[x_1, \ldots, x_n]$ is called a power product iff

there exists an $i \in N^n$ *such that* $v(i) = 1$ *and* $v(j) = 0$ *for all* $j \in N^n \setminus \{i\}$.

We denote the set of all power products in $K[x_1, \ldots, x_n]$ by $K\langle x_1, \ldots, x_n \rangle$. •

Convention:
We will use v, w as typed variables in $K\langle x_1, \ldots, x_n \rangle$.

Definition 8 Before one can define the notion of Gröbner bases the notion of "reduction" must be introduced. For this it is necessary to fix a total ordering of the power products. In this paper we use the "purely lexicographical ordering" and denote it by $\ll$:

$v \ll w$ iff

there exists an m *such that*

$$deg(v, m) < deg(w, m) \text{ and } deg(v, r) = deg(w, r)$$

for all $r \in \{m + 1, \ldots, n\}$.

With respect to $\ll$, we use the following notation:

Let $f \in \bar{K}[x_1, \ldots, x_n]$, $i \in N^n$, and v such that $v(i) = 1$.
We call *f(i) the coefficient of v in f*, abbreviated $coeff(f, v)$.

Let us assume that $f \neq 0_p$. *The leading power product of* f, abbreviated $lpp(f)$, is the maximal power product (with respect to $\ll$) occuring with non-zero coefficient in f (i.e.

$$lpp(f) := \max\{\, v \mid coeff(f,v) \neq 0 \,\}).$$

We denote

$$coeff(f, lpp(f))$$

by $hcoeff(f)$, *the head-coefficient of* f. (Note that it is not possible to denote $coeff(f, lpp(f))$ by *leading coefficient of* f as in [6], because we have already introduced this notion in Chapter 2).

Let F be a finite subset of $K[x_1, \ldots, x_n]$, $g, h \in K[x_1, \ldots, x_n]$, and $d \in K$. We say that *g reduces to h modulo F*, abbreviated $g \rightarrow_F h$, iff

there exist $f \in F$, $e \in K$, and w such that $g \hookrightarrow_{f,e,w}$ and $h = g - e \cdot w \cdot f$.

We say that *g is reducible using h, d, v*, abbreviated $g \hookrightarrow_{h,d,v}$, iff

$coeff(g, v \cdot lpp(h)) \neq 0$ and $d = coeff(g, v \cdot lpp(h))/hcoeff(h)$. •

Hence, roughly, g reduces to h modulo F iff a monomial in g can be deleted by the subtraction of an appropriate multiple $e \cdot w \cdot f$ of a polynomial f in F yielding h. Thus, the reduction may be viewed as one step in a generalized division.

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

$$\begin{aligned} f_1 &:= 3x^2y + 2xy + y + 9x^2 + 5x - 3, \\ f_2 &:= 2x^3y - xy - y + 6x^3 - 2x^2 - 3x + 3, \\ f_3 &:= x^3y + x^2y + 3x^3 + 2x^2. \end{aligned}$$

The polynomials f_1, f_2, f_3 are ordered according to $\ll$. The leading power products are x^2y, x^3y, and x^3y, respectively, and the head-coefficients are 3, 2, and 1. Consider

$$g := 5y^2 + 2x^2y + (5/2)xy + (3/2)y + 8x^2 + (3/2)x - 9/2.$$

Modulo F, g reduces, for example, to

$$h := 5y^2 + (7/6)xy + (5/6)y + 2x^2 - (11/6)x - 5/2.$$

Namely,

$$g \hookrightarrow_{f,e,w} \textit{for } f := f_1,\ e := 2/3,\ w := 1, \text{ because}$$

$$\begin{aligned} coeff(g, 1 \cdot x^2y) &= 2 \neq 0, \\ e &= coeff(g, 1 \cdot x^2y)/hcoeff(f_1), \text{ and} \\ h &= g - (2/3) \cdot 1 \cdot f_1. \ \bullet \end{aligned}$$

Definition 9 Let F be a finite subset of $K[x_1, \ldots, x_n]$ and $f, h \in K[x_1, \ldots, x_n]$.
We say that h is in *normal form* (or *reduced form) modulo* F iff

$$\textit{there is no } h' \in K[x_1, \ldots, x_n] \textit{ such that } h \rightarrow_F h'.$$

We say that h is a *normal form of f modulo F* iff

$$\begin{gathered}\textit{there is a sequence of reductions}\\ f = g_0 \rightarrow_F g_1 \rightarrow_F g_2 \rightarrow_F \ldots \rightarrow_F g_m = h\\ \textit{and } h \textit{ is in normal form modulo } F.\end{gathered}$$

An algorithm S is called a *normal form algorithm* (or *simplifier*) iff

S(F,g) is a normal form of g modulo F for all finite subsets F of $K[x_1, \ldots, x_n]$ *and for all* $g \in K[x_1, \ldots, x_n]$. •

Lemma 3 *The following algorithm is a normal form algorithm:*

Algorithm 1 (h:=NormalForm(F,g)):

input: g, a polynomial in $K[x_1, \ldots, x_n]$, and
F, a finite subset of $K[x_1, \ldots, x_n]$.

output: h, a polynomial in $K[x_1, \ldots, x_n]$ such that h is a normal form of g modulo F.

```
$h := g$
while there exist $f \in F$, $e \in K$, and $w$ such that $g \hookrightarrow_{f,e,w}$ do
    choose $f, e, w$ such that $h \hookrightarrow_{f,e,w}$ and
                    $w \cdot lpp(f)$ is maximal (w.r.t. $\ll$)
    $h := h - e \cdot w \cdot f$
```

The correctness of this algorithm should be clear. For the correctness, the selection of the maximal product $w \cdot lpp(f)$ is not mandatory. However, this choice is of crucial importance for efficiency. The termination of the algorithm is guaranteed by the following lemma:

Lemma 4 *[4]: Let F be a finite subset of $K[x_1, \ldots, x_n]$.
Then $\rightarrow_F$ is a noetherian relation (i.e. there is no infinite sequence*

$$g_0 \rightarrow_F g_1 \rightarrow_F g_2 \rightarrow_F \ldots).$$

Example 4 The polynomial h in the Example 2 is in normal form modulo F: no power product occuring in h is a multiple of the leading power product of one of the polynomials in F. Thus, no reduction is possible. Another example:

$$x^3y \rightarrow_{f_1} -(2/3)x^2y - (1/3)xy - 3x^3 - (5/3)x^2 + x \; =: \; g_1.$$

g_1 can be further reduced:

$$g_1 \; \rightarrow_{f_1} \; (1/9)xy + (2/9)y - 3x^3 + (1/3)x^2 + (19/9)x - 2/3 \; =: \; g_1'.$$

The polynomial g_1' is in normal form modulo F. Therefore, g_1' is a normal form of x^3y modulo F. Actually, g_1' may be the result of applying the algorithm "NormalForm" to x^3y (depending on how the instruction "choose $f \in F$, such that ..." in the algorithm is implemented). In this example, a second reduction is possible:

$$x^3y \rightarrow_{f_2} (1/2)xy + (1/2)y - 3x^3 + x^2 + (3/2)x - 3/2 \; =: \; g_2.$$

g_2 is already in normal form modulo F. •

From the example one sees that, in general, it is possible that, modulo F, g_1 and g_2 are normal forms of a polynomial g, but $g_1 \neq g_2$. Those sets F, for which such a situation does not occur, play the crucial role for this approach to an algorithmic solution of problems in polynomial ideal theory:

Definition 10 [2],[3] Let F be a finite subset of $K[x_1, \ldots, x_n]$.
F is called a *Gröbner basis* or *Gröbner set* iff it satisfies the following condition:

Given $g, h_1, h_2 \in K[x_1, \ldots, x_n]$ and h_1 and h_2 are normal forms of g modulo F, then $h_1 = h_2$. •

Gröbner bases can be equivalently defined in many different ways. One of the well-known equivalences is the following:

Theorem 10 *(Characterization Theorem for Gröbner Bases):*
Let S be a normal form algorithm. The following properties are equivalent:

(GB1) F is a Gröbner basis.
(GB2) For all $f, g \in F$: $f \equiv_I g$ iff $S(F, f) = S(F, g)$,
where $I := Ideal_{K,n}(F)$.

3.2 Algorithmic Construction of Gröbner Bases

Before we give the algorithmic applications of Gröbner bases we show how it may be decided whether a given set F is a Gröbner basis and how Gröbner bases may be constructed. For this the notion of an "S-polynomial" is fundamental:

Definition 11 Let $f_1, f_2 \in K[x_1, \ldots, x_n]$.
The *S-polynomial corresponding to f_1 and f_2* is

$SPol(f_1, f_2) \; := \; v_1 \cdot f_1 - (d_1/d_2) \cdot v_2 \cdot f_2$,
where $d_r \; = \; hcoeff(f_r)$ and
$lpp(f_r) \cdot v_r \; = \;$ *the least common multiple of* $lpp(f_1)$, $lpp(f_2)$ $\;(r = 1, 2)$.

Example 5 For f_1 and f_2 as in Example 2, the $SPol(f_1, f_2)$ is

$$2x^2y + (5/2)xy + (3/2)y + 8x^2 + (3/2)x - 9/2. \quad \bullet$$

Note that the least common multiple of $lpp(f_1)$ and $lpp(f_2)$ is the minimal power product that is reducible both modulo f_1 and modulo f_2. The algorithmic criterion for Gröbner bases is formulated in the following theorem, which forms the core of the method (both for the construction of Gröbner bases and for the applications):

Theorem 11 *(Algorithmic Characterization of Gröbner bases)[2],[3]:*
Let F be a finite subset of $K[x_1, \ldots, x_n]$ and S an arbitrary normal form algorithm. The following properties are equivalent:

(GB1) *F is a Gröbner basis.*
(GB3) *For all $f_1, f_2 \in F$: $S(F, SPol(f_1, f_2)) = 0_p$.*

$(GB3)$, indeed, is a decision algorithm for the property "F is a Gröbner basis": one only has to consider the finitely many pairs f_1, f_2 of polynomials in F, compute the corresponding S-polynomials and see whether they reduce to zero by application of the normal form algorithm S. In addition, Theorem 11 is the basis for (a first and primitive version of) an algorithm for computing a Gröbner basis. For more advanced versions we refer to [4] and [6].

Algorithm 2

input: F, a finite subset of $K[x_1, \ldots, x_n]$.

output: G, a finite subset of $K[x_1, \ldots, x_n]$ such that $Ideal_{K,n}(F) = Ideal_{K,n}(G)$ and G is a Gröbner basis.

```
$G := F$
$B := \{ \{f_1, f_2\} \mid f_1, f_2 \in G,\ f_1 \neq f_2 \}$
while $B \neq \emptyset$ do
    $\{f_1, f_2\}$:= a pair in $B$
    $B := B \setminus \{ \{f_1, f_2\} \}$
    $h := SPol(f_1, f_2)$
    $h' := NormalForm(G, h)$
    if $h' \neq 0_p$
    then
        $B := B \cup \{ \{g, h'\} \mid g \in G \}$
        $G := G \cup \{h'\}$
```

The partial correctness of this algorithm, essentially, relies on Theorem 11. The termination can be shown in two ways, see [3], [1].

Definition 12 A finite subset F of $K[x_1, \ldots, x_n]$ is said to be a *reduced Gröbner basis* iff

F is a Gröbner basis and
for all $f \in F$: f is in normal form modulo $F \setminus \{f\}$ and hcoeff(f)=1. •

Theorem 12 *(Uniqueness of reduced Gröbner bases):*
Let F and F' be finite subsets of $K[x_1, \ldots, x_n]$.
If $Ideal_{K,n}(F) = Ideal_{K,n}(F')$ and F and F' are both reduced Gröbner bases then $F = F'$.

Proof: see [5].

Let GB be the function that associates with every finite subset F of $K[x_1, \ldots, x_n]$ a finite subset G of $K[x_1, \ldots, x_n]$ such that $Ideal_{K,n}(F) = Ideal_{K,n}(G)$ and G is a reduced Gröbner basis.

The main result, which summarizes the basic algorithmic knowledge about Gröbner bases, is the following theorem:

Theorem 13 *GB is an algorithmic function that satisfies for all finite subsets F,F' of $K[x_1, \ldots, x_n]$:*

(SGB1) $Ideal_{K,n}(F) = Ideal_{K,n}(GB(F))$,
(SGB2) if $Ideal_{K,n}(F) = Ideal_{K,n}(F')$ then $GB(F) = GB(F')$,
(SGB3) GB(F) is a reduced Gröbner basis.

Proof: see [3].

3.3 Application: Solvability and Exact Solution of Systems of Algebraic Equations

In this section it is shown how the algorithm for constructing Gröbner bases may be used for the exact solution of systems of algebraic equations and questions about the solvability of such systems. The significance of Gröbner bases for problems in this category stems from the fact that, for Gröbner bases, the explicit construction of all the elimination ideals is extremely simple.

Theorem 14 *Let G be a Gröbner basis in $K[x_1,\ldots,x_n]$. Then*

$$Ideal_{K,n}(G) \cap K[x_1,\ldots,x_m] = Ideal_{K,m}(G \cap K[x_1,\ldots,x_m]).$$

Proof: see [14].

This theorem shows that the m-th elimination ideal of G is generated by just those polynomials in G that are elements of $K[x_1,\ldots,x_m]$.

The following two theorems are criterions that allow to decide whether the set of all solutions of a system of algebraic equations is empty, finite, or infinite.

Theorem 15 *Let F be a finite subset of $K[x_1,\ldots,x_n]$. Then*

$$V(Ideal(F)) = \emptyset \;\; iff \;\; 1 \in GB(F).$$

Proof: see [6].

Theorem 16 *Let F be a finite subset of $K[x_1,\ldots,x_n]$. Then*

$$V(Ideal(F)) \; is \; finite$$

$$iff$$

$$for \; every \; m: \; there \; exists \; a \; polynomial \; f \; in \; GB(F) \; such \; that \; lpp(f) \in K[x_m].$$

Proof: see [6].

Therefore, we can decide whether $V(Ideal(F))$ is empty, non-empty and finite, or infinite for a finite set $F \subseteq K[x_1,\ldots,x_n]$ by computing $GB(F)$ and applying Theorem 15 and Theorem 16.

Example 6 Given $F_1, F_2, F_3 \subseteq Q[x,y]$, where

$$\begin{aligned} F_1 \;\; := \;\; & \{x^2y - y + x^2 - 1, \\ & xy + x - 1, \\ & xy^3 + y^3 + y + 2\}, \end{aligned}$$

$$
\begin{aligned}
F_2 \;&:=\; \{xy^2 - y^2 + x - 1,\\
&\qquad x^3 + x^2,\\
&\qquad y^2 - y\},
\end{aligned}
$$

$$
\begin{aligned}
F_3 \;&:=\; \{xy^2 - y^2 - x + 1,\\
&\qquad xy^2 - y,\\
&\qquad x^3 - x^2 - x + 1\}.
\end{aligned}
$$

We want to solve Problem 1 for each of these sets. First of all, we have to compute their reduced Gröbner bases:

$$
\begin{aligned}
GB(F_1) \;&:=\; \{x + 1,\\
&\qquad y + 2\},
\end{aligned}
$$

$$
GB(F_2) \;:=\; \{1\},
$$

$$
\begin{aligned}
GB(F_3) \;&:=\; \{x^2 - 1,\\
&\qquad xy - y - x + 1\}.
\end{aligned}
$$

The variaty of the ideal generated by F_1 is non-empty and finite, because $GB(F_1)$ does not contain the polynomial 1 and x and y appear as leading power products in $GB(F_1)$.

As the polynomial 1 is an element of $GB(F_2)$, the system F_2 is unsolvable.

The polynomials in F_3 have infinitely many common zeros, because no power product of the form y^r ocurrs among the leading power products. •

Definition 13 Let G be the reduced Gröbner basis of a zero-dimensional ideal in $K[x_1, \ldots, x_n]$.

Let $G_{m,1}, \ldots, G_{m,car_m}$ be the polynomials in G that belong to $K[x_1, \ldots, x_m]$ but not to $K[x_1, \ldots, x_{m-1}]$. We suppose the order chosen in such a way that

$$r < s \textit{ implies } lpp(G_{m,r}) \ll lpp(G_{m,s}) \textit{ for all } r, s \in \{1, \ldots, car_m\}. \;\bullet$$

Based on Theorem 14 the following algorithm gives a solution to Problem 2 (see [6], Method 6.10):

Algorithm 3

input: F, a finite subset of $K[x_1, \ldots, x_n]$ such that I is a zero-dimensional ideal in $K[x_1, \ldots, x_n]$, where $I := Ideal_{K,n}(F)$.

output: X_n, a finite subset of $\bar{K}^n$ such that $X_n = V(I)$.

```
$G:=GB(F)$
```

Comment: The polynomials in G, then, have their variables "separated" in the precise sense of Theorem 14 (G is "triangularized"). G contains exactly one polynomial of $K[x_1]$ (actually, it is the polynomial in $Ideal_{K,n}(G) \cap K[x_1]$ with smallest degree). According to our definition we denote it by $G_{1,1}$.

The successive elimination can, then, be carried out by the following process:

```
$X_1 := \{ c \mid c \in \bar{K}^1$ and $\overline{G_{1,1}(c)} = 0_p \}$
for $r := 1$ to $n-1$ do
    $X_{r+1} := \emptyset$
    for all $b \in X_r$ do
        $H := \{ \overline{G_{r+1,s}(b)} \mid s \in \{1, \ldots, car_{r+1}\} \}$
        $q :=$ greatest common divisor of the polynomials in $H$
        $X_{r+1} := X_{r+1} \cup \{ (b,c) \mid c \in \bar{K}^1$ and $\overline{q(0_r, c)} = 0_p \}$
```

Note that for $q \in \bar{K}[x_{r+1}]$,

$$\overline{q(0_r, c)} = 0_p$$

iff

there exists an $a \in \bar{K}^r$ with $\overline{q(a,c)} = 0_p$

iff

$\overline{q(a,c)} = 0_p$ for every $a \in \bar{K}^r$.

Example 7 We consider $F \subseteq Q[x,y]$, where

$$\begin{aligned} F \;:=\; \{&x^3 - x^2 + x - 1, \\ &xy - y - x^2 + x, \\ &y^2 - x^2\}. \end{aligned}$$

F already is a reduced Gröbner basis. As 1 is not in F and x^3 and y^2 appear as leading power products in F, the system F is solvable and has finitely many solutions. We compute these solutions by using Algorithm 3.

We set

$G := F.$

According to our definition we denote

$$\begin{gathered} x^3 - x^2 + x - 1 \text{ by } G_{1,1}, \\ xy - y - x^2 + x \text{ by } G_{2,1}, \text{ and} \\ y^2 - x^2 \text{ by } G_{2,2}. \end{gathered}$$

Now we have to compute the zeros of the univariate polynomial $G_{1,1}$.

$X_1 := \{(i), (-i), (1)\}.$

We set

$r := 1,$
$X_2 := \emptyset,$

choose the element (i) of the set X_1, and perform the following operations:

```
for $(i)$ do,
$H := \{iy - y + 1 + i, y^2 + 1\},$
$q := y - i,$
$X_2 := \{(i, i)\}.$
```

The elements $(-i)$ and (1) of the set X_1 are continued in the same way and we finally get a set X_2 that contains all the solutions.

$X_2 := \{(i, i), (-i, -i), (1, 1), (1, -1)\}.$

Note that in this example none of the q is 1, i.e. the corresponding partial solution $b \in \bar{K}^r$ can be continued. In the next chapter we prove that this is always possible.

Chapter 4

Continuing Zeros of Elimination Ideals

Let Q be a zero-dimensional primary ideal in $K[x_1, \ldots, x_n]$. Our first goal in this chapter is to prove the following result, which we will make use of in chapter 5:

For all $b, c \in V(Q_{/x_{l-1}})$ and for all $f \in K[x_1, \ldots, x_n]$:

$$deg(\overline{f(b)}, l) = deg(\overline{f(c)}, l).$$

A relatively easy consequence of this lemma is that

(1) *for every common zero* $(b_1, \ldots, b_{l-1})$ *of the polynomials in* $Q_{/x_{l-1}}$ *there exists a* $c \in \bar{K}^{n-l+1}$ *such that* $(b_1, \ldots, b_{l-1}, c_1, \ldots, c_{n-l+1})$ *is a common zero of the polynomials in* Q.

By using Noether's decomposition theorem we show that **(1)** holds for every zero-dimensional ideal. A different proof of this result can be found in [7].

Lemma 5 *Let* Q *be a primary ideal in* $K[x_1, \ldots, x_n]$.
Then $Q_{/x_m}$ *is a primary ideal in* $K[x_1, \ldots, x_m]$ *and* $\sqrt{Q_{/x_m}} = \sqrt{Q}_{/x_m}$.

Proof: Let $f, g \in K[x_1, \ldots, x_m]$ such that $f \cdot g \in Q_{/x_m}$ and $f \notin Q_{/x_m}$.
Thus, $f \cdot g \in Q$ and $f \notin Q$. As Q is a primary ideal,

$$\text{there exists an } r \in N_+ \text{ such that } g^r \in Q.$$

From $g \in K[x_1, \ldots, x_m]$ it follows that

$$g^r \in Q_{/x_m}.$$

Thus, $Q_{/x_m}$ is a primary ideal in $K[x_1, \ldots, x_m]$.

Let $f \in K[x_1, \ldots, x_n]$.

$$f \in \sqrt{Q_{/x_m}}$$

iff

there exists an $r \in N_+$ with $f^r \in Q_{/x_m}$

iff

$f \in K[x_1, \dots, x_m]$ and there exists an $r \in N_+$ with $f^r \in Q_{/x_m}$

iff

$f \in K[x_1, \dots, x_m]$ and there exists an $r \in N_+$ with $f^r \in Q$

iff

$$f \in \sqrt{Q}_{/x_m}. \bullet$$

Lemma 6 *Let P be a zero-dimensional prime ideal in $K[x_1, \dots, x_n]$. Then $P_{/x_m}$ is a zero-dimensional prime ideal in $K[x_1, \dots, x_m]$.*

Proof: It can be shown by the same arguments as in Lemma 5 that $P_{/x_m}$ is a prime ideal in $K[x_1, \dots, x_m]$.

Let $f \in P_{/x_m}$, $g \in K[x_1, \dots, x_m]$, $b \in \bar{K}^m$, and $c \in \bar{K}^{n-m}$ such that (b,c) is a generic zero of P.

As $f \in K[x_1, \dots, x_m]$,

$$\overline{f(b)} = \overline{f(b,c)} = 0_p.$$

Therefore, $b \in V(P_{/x_m})$.

We assume that $\overline{g(b)} = 0_p$. Thus,

$$\overline{g(b,c)} = 0_p.$$

Hence, g is an element of P. From $g \in K[x_1, \dots, x_m]$ we obtain

$$g \in P_{/x_m}.$$

Therefore, b is a generic zero of $P_{/x_m}$ and $P_{/x_m}$ is zero-dimensional. $\bullet$

Lemma 7 *Let $f \in K[x_1, \dots, x_n]$ and $b \in \bar{K}^{l-1}$. Then $\overline{f(b)} = g$, where*

$$\begin{array}{llll} g: & N^n & \rightarrow & \bar{K} \\ & j & \mapsto & 0 \qquad\qquad \textit{if } (j_1, \dots, j_{l-1}) \neq 0_{l-1} \\ & j & \mapsto & \overline{f_{(.,k)}(b)}(0_n) \quad \textit{otherwise,} \\ & & & \qquad\qquad\quad \textit{where } k \in N_{n-l+1} \textit{ and } (0_{l-1}, k) = j. \end{array}$$

Proof: Let $i \in N^{n-l+1}$.

$$\overline{f(b)}(0_{l-1}, i) = \sum_{k \in N^{l-1}} f(k, i) \cdot b^k =$$

$$= \sum_{k \in N^{l-1}} f_{(.,i)}(k, 0_{n-l+1}) \cdot b^k = \overline{f_{(.,i)}(b)}(0_n) = g(0_{l-1}, i).$$

Let $j \in N^{l-1} \setminus \{0_{l-1}\}$.

$$\overline{f(b)}(j, i) = 0 = g(j, i).$$

Thus,

$$\overline{f(b)} = g. \quad \bullet$$

Lemma 8 *Let Q be a zero-dimensional primary ideal in $K[x_1, \ldots, x_n]$, $b, c \in V(Q_{/x_{l-1}})$, and $f \in K[x_1, \ldots, x_n]$.*

Then

$$deg(\overline{f(b)}, l) = deg(\overline{f(c)}, l).$$

Proof: From Theorem 3 and the fact that Q is zero-dimensional we know that $\sqrt{Q}$ is a zero-dimensional prime ideal in $K[x_1, \ldots, x_n]$. By Lemma 6, $\sqrt{Q}_{/x_{l-1}}$ is a zero-dimensional prime ideal in $K[x_1, \ldots, x_{l-1}]$. From Lemma 5 we obtain

$$\sqrt{Q}_{/x_{l-1}} = \sqrt{Q_{/x_{l-1}}}.$$

Thus, by Theorem 2 and Theorem 3, b and c are generic zeros of $\sqrt{Q_{/x_{l-1}}}$.

We show that $C(\overline{f(b)}) = C(\overline{f(c)})$:

Let $k \in C(\overline{f(b)})$. By the definition of $\overline{f(b)}$, there exists a $j \in N^{n-l+1}$ such that $k = (0_{l-1}, j)$. By Lemma 7,

$$\overline{f_{(.,j)}(b)}(0_n) = \overline{f(b)}(0_{l-1}, j) = \overline{f(b)}(k) \neq 0.$$

Thus,

$$\overline{f_{(.,j)}(b)} \neq 0_p.$$

As b and c are generic zeros of $\sqrt{Q_{/x_{l-1}}}$ and $f_{(.,j)} \in K[x_1, \ldots, x_{l-1}]$, it follows that

$$\overline{f_{(.,j)}(c)} \neq 0_p.$$

From $C(\overline{f_{(.,j)}(c)}) \subseteq \{0_n\}$ and Lemma 7 we obtain

$$\overline{f(c)}(k) = (\overline{f_{(.,j)}(c)})(0_n) \neq 0.$$

Thus,

$$C(\overline{f(b)}) \subseteq C(\overline{f(c)}).$$

As we can show by the same arguments that

$$C(\overline{f(c)}) \subseteq C(\overline{f(b)}),$$

it follows that

$$C(\overline{f(b)}) = C(\overline{f(c)}).$$

Thus, by definition,

$$deg(\overline{f(b)}, l) = deg(\overline{f(c)}, l). \bullet$$

Definition 14 Let J be an ideal in $K[x_1, \ldots, x_l]$, $b \in \bar{K}^{l-1}$, $f, g \in J$ and $q \in K(b)[x_l]$. We can choose an $h \in K[x_1, \ldots, x_l]$ such that $\overline{h(b)} = q$. As, by Lemma 1,

$$\overline{f(b)} + \overline{g(b)} = \overline{(f+g)(b)} \text{ and } q \cdot \overline{f(b)} = \overline{h(b)} \cdot \overline{f(b)} = \overline{(h \cdot f)(b)},$$

the set

$$\{\, \overline{h(b)} \mid h \in J \,\}$$

is an ideal in $K(b)[x_l]$. We denote it by $\overline{J(b)}$.

Obviously, $K(b)[x_l]$ is isomorphic to the univariate polynomial ring over $K(b)$. Therefore, $K(b)[x_l]$ is a principal ideal domain. Thus, there exists a uniquely determined polynomial q in $\overline{J(b)}$ such that

$$\overline{J(b)} \textit{ is generated by } \{q\} \textit{ and } hcoeff(q) = 1.$$

We denote it by $gcd(J, b)$. $\bullet$

Lemma 9 *Let $\{f_1, \ldots, f_r\}$ be a finite subset of $K[x_1, \ldots, x_l]$ and $b \in \bar{K}^{l-1}$.*

Then

$$gcd(\{\overline{f_1(b)}, \ldots, \overline{f_r(b)}\}) = gcd(J, b),$$

where $J := Ideal_{K,l}(\{f_1, \ldots, f_r\})$.

Proof: Let $g \in J$.

As there exist $h_1, \ldots, h_r \in K[x_1, \ldots, x_l]$ such that

$$g = h_1 \cdot f_1 + \ldots + h_r \cdot f_r,$$

$$\overline{g(b)} = \overline{h_1(b)} \cdot \overline{f_1(b)} + \ldots + \overline{h_r(b)} \cdot \overline{f_r(b)}.$$

Thus,

$$\{\overline{f_1(b)}, \ldots, \overline{f_r(b)}\} \text{ generates } \overline{J(b)}.$$

Therefore,

$$gcd(J, b) \text{ divides } gcd(\{\overline{f_1(b)}, \ldots, \overline{f_r(b)}\}) \text{ and vice versa.}$$

From

$$hcoeff(gcd(J,b)) = 1 = hcoeff(gcd(\{\overline{f_1(b)},\dots,\overline{f_r(b)}\}))$$

we obtain

$$gcd(\{\overline{f_1(b)},\dots,\overline{f_r(b)}\}) = gcd(J,b). \;\bullet$$

Now we have made all the preparations that are needed for proving that zeros of elimination ideals of zero-dimensional primary ideals can be continued.

Lemma 10 *Let Q be a zero-dimensional primary ideal in $K[x_1,\dots,x_n]$ and $b \in V(Q_{/x_{l-1}})$.*
Then there exists a $c \in \bar{K}^{n-l+1}$ such that $(b,c) \in V(Q)$.

Proof: Let $b' \in \bar{K}^{l-1}$, $c' \in \bar{K}^{n-l+1}$ such that $(b',c') \in V(Q)$.
Obviously,

$$b' \in V(Q_{/x_{l-1}}).$$

We choose $h \in Q_{/x_l}$ such that $\overline{h(b)} = gcd(Q_{/x_l}, b)$. By Lemma 2,

$$\overline{\overline{h(b')}(0_{l-1},c')} = \overline{h(b',c')} = 0_p.$$

Let us assume that $deg(\overline{h(b')},l) = 0$.
As $\overline{h(b')} \in K(b')[x_l]$,

$$deg(\overline{h(b')},m) = 0 \text{ for every } m.$$

Thus, $\overline{h(b')}$ is a constant polynomial and

$$\overline{h(b')} = \overline{\overline{h(b')}((0_{l-1},c'))} = 0_p.$$

On the other hand,

$$deg(0_p,m) = -1 \text{ for every } m$$

and therefore

$$0_p \neq \overline{h(b')}.$$

Contradiction.

Hence, by Lemma 8,

$$deg(\overline{h(b)},l) = deg(\overline{h(b')},l) \neq 0.$$

Thus, there exists a $c \in \bar{K}^{n-l+1}$ such that $\overline{\overline{h(b)}(0_{l-1},c)} = 0_p$. From $h \in K[x_1,\dots,x_l]$ and from Lemma 2 we obtain

$$\overline{h(b_1,\dots,b_{l-1},c_1)} = 0_p.$$

By the definition of $gcd(Q_{/x_l}, b)$,

$$(b_1, \ldots, b_{l-1}, c_1) \in V(Q_{/x_l}).$$

If $l = n$, the proof is finished.

Otherwise, we can choose a $c_2 \in \bar{K}$ with

$$(b_1, \ldots, b_{l-1}, c_1, c_2) \in V(Q_{/x_{l+1}}).$$

Proceeding in this way, we get $(c_1, \ldots, c_{n-l+1}) \in \bar{K}^{n-l+1}$ with

$$(b_1, \ldots, b_{l-1}, c_1, \ldots, c_{n-l+1}) \in V(Q)$$

after $n - l + 1$ steps. •

It remains to show that the restriction to primary ideals is not necessary. We will do this in Theorem 17. In the proof of the theorem the following lemma is required:

Lemma 11 *Let I be an ideal in $K[x_1, \ldots, x_n]$ and $I = Q_1 \cap \ldots \cap Q_r$ a primary decomposition of I.*

Then $I_{/x_m} = Q_{1/x_m} \cap \ldots \cap Q_{r/x_m}$ is a primary decomposition of $I_{/x_m}$.

Proof: Let $f \in K[x_1, \ldots, x_n]$.

$$f \in I_{/x_m}$$

iff

$$f \in I \text{ and } f \in K[x_1, \ldots, x_m]$$

iff

$$f \in Q_s \text{ for every } s \in \{1, \ldots, r\} \text{ and } f \in K[x_1, \ldots, x_m]$$

iff

$$f \in Q_{s/x_m} \text{ for every } s \in \{1, \ldots, r\}$$

iff

$$f \in Q_{1/x_m} \cap \ldots \cap Q_{r/x_m}.$$

By Lemma 5, Q_{s/x_m} is a primary ideal for every $s \in \{1, \ldots, r\}$. •

Theorem 17 *Let I be a zero-dimensional ideal in $K[x_1, \ldots, x_n]$ and $b \in V(I_{/x_{l-1}})$.*

Then there exists a $c \in \bar{K}^{n-l+1}$ such that $(b, c) \in V(I)$.

Proof: Let $I = Q_1 \cap \ldots \cap Q_r$ be a primary decomposition of I.

By Lemma 11,

$$I_{/x_{l-1}} = Q_{1/x_{l-1}} \cap \ldots \cap Q_{r/x_{l-1}}$$

is a primary decomposition of $I_{/x_{l-1}}$. Hence, there exists an $s \in \{1, \ldots, r\}$ with

$$b \in V(Q_{s/x_{l-1}}).$$

As Q_s is a zero-dimensional primary ideal, we can apply Lemma 10 and obtain that there exists a $c \in \bar{K}^{n-l+1}$ such that

$$(b, c) \in V(Q_s).$$

Thus,

$$(b, c) \in V(I). \quad \bullet$$

At the end of the previous chapter we have asserted that every partial solution $(b_1, \ldots, b_r)$ computed by Algorithm 3 can be continued. Now we are in the position to verify this assertion:

By Theorem 14, $(b_1, \ldots, b_r)$ is an element of the r-th elimination ideal. From Theorem 17 we know that in this case there exists a $(c_1, \ldots, c_{n-r})$ in $\bar{K}^{n-r}$ such that $(b_1, \ldots, b_r, c_1, \ldots, c_{n-r})$ is a zero of the given system.

Chapter 5

Algorithms for Solving Systems of Algebraic Equations

In Algorithm 3 a subalgorithm is required that computes the greatest common divisor of a finite set of univariate "intermediate" polynomials over an extension field of K. In the first section of this chapter we prove a theorem that leads to an improved version of Algorithm 3. Namely, it turns out that the greatest common divisor of the univariate "intermediate" polynomials is one of the polynomials. In our method, as an auxiliary operation, a test for zero in an extension field of K is needed. We present this algorithm in section 2. In section 3 and section 4 further algorithms for solving Problem 2 are given.

5.1 Some Properties of Reduced Gröbner Bases of Zero-Dimensional Ideals

Definition 15 Let I be a zero-dimensional ideal in $K[x_1, \ldots, x_n]$, G the reduced Gröbner basis in $K[x_1, \ldots, x_n]$ such that $Ideal_{K,n}(G) = I$, and $b \in V(I_{/x_{l-1}})$.

Then min_b denotes the minimum of the set

$$\{\, r \mid r \in \{1, \ldots, car_l\} \text{ and } \overline{lc(G_{l,r})(b)} \neq 0_p \,\}. \quad \bullet$$

Is min_b always well-defined, or in other words, is the set

$$\{\, r \mid r \in \{1, \ldots, car_l\} \text{ and } \overline{lc(G_{l,r})(b)} \neq 0_p \,\}.$$

always non-empty?

By Theorem 9, Theorem 15, and Theorem 16, there exists a non-constant polynomial f in G such that

$$lpp(f) \in K[x_l].$$

Hence, there exists a

$$j \in \{\, j \mid j \in N^n \setminus \{0_n\} \text{ and } j_r = 0 \text{ for } r \in \{1, \ldots, l-1, l+1, \ldots, n\} \,\}$$

such that

$$lpp(f)(j) = 1.$$

From

$$lc(f) = f_{(.,j')}, \text{ where } (0_{l-1}, j') = j,$$
$$f_{(.,j')}(0_n) = f(0_{l-1}, j') = coeff(f, lpp(f)) = hcoeff(f) = 1, \text{ and}$$
$$f_{(.,j')}(i) = 0 \text{ for all } i \in N^n \setminus \{0_n\}$$

we obtain

$$lc(f) = 1.$$

As G is reduced and $lpp(f) \in K[x_l]$,

$$deg(g, l) < deg(f, l) \text{ for all } g \in G \setminus \{f\}$$
$$\text{and } f \in K[x_1, \ldots, x_l].$$

Therefore,

$$f = G_{l,car_l}.$$

Hence,

$$lc(G_{l,car_l}) = 1$$

and car_l is always an element of

$$\{\, r \mid r \in \{1, \ldots, car_l\} \text{ and } \overline{lc(G_{l,r})(b)} \neq 0_p \,\}.$$

Theorem 20, which we prove at the end of this section, says that if G is a reduced Gröbner basis of a zero-dimensional ideal in $K[x_1, \ldots, x_n]$ and b is an element of $\bar{K}^{l-1}$ such that b is a zero of

$$\begin{array}{rcl} G_{1,1} & \in & K[x_1], \\ G_{2,1} & \in & K[x_1, x_2], \\ \ldots & & \ldots \\ G_{2,car_2} & \in & K[x_1, x_2], \\ \ldots & & \ldots \\ G_{l-1,1} & \in & K[x_1, \ldots, x_{l-1}], \\ \ldots & & \ldots \\ G_{l-1,car_{l-1}} & \in & K[x_1, \ldots, x_{l-1}], \end{array}$$

then there exists a d and an element of

$$\{G_{l,1}, \ldots, G_{l,car_l}\} \subseteq K[x_1, \ldots, x_l],$$

namely G_{l,min_b}, such that

$$d \cdot \overline{G_{l,min_b}(b)} = gcd(\{\overline{G_{l,1}(b)}, \ldots, \overline{G_{l,car_l}(b)}\}).$$

For proving this we first show a stronger result for reduced Gröbner bases of zero-dimensional primary ideals:

Theorem 18 *Let Q be a zero-dimensional primary ideal in $K[x_1, \ldots, x_n]$ and G the reduced Gröbner basis in $K[x_1, \ldots, x_n]$ such that $Ideal_{K,n}(G) = Q$. Then*

$$\overline{G_{l,1}(b)} = \ldots = \overline{G_{l,car_l-1}(b)} = 0_p \qquad (5.1)$$

for all $b \in V(Q_{/x_{l-1}})$.

Proof:

We first show that (5.1) holds for some $b \in V(Q_{/x_{l-1}})$:

We assume, to the contrary, that

$$\begin{gathered}\text{for every } b \in V(Q_{/x_{l-1}})\\ \text{there exists an } r \in \{1, \ldots, car_l - 1\} \text{ with } \overline{G_{l,r}(b)} \neq 0_p.\end{gathered} \qquad (5.2)$$

In this proof we denote $(G \cap K[x_1, \ldots, x_l]) \setminus \{G_{l,car_l}\}$ by F.
Let $f_1, f_2 \in F$.
From the fact that

$$deg(f_s, l) = deg(lpp(f_s), l) \quad (s = 1, 2)$$

and the definition of the S-polynomial we obtain

$$deg(SPol(f_1, f_2), l) \leq \max\{deg(f_1, l), deg(f_2, l)\} < deg(G_{l,car_l}, l).$$

Thus, $SPol(f_1, f_2)$ reduces to zero modulo F. By Theorem 11,

$$F \textit{ is a Gröbner basis.} \qquad (5.3)$$

Obviously,

$$F \textit{ is reduced.} \qquad (5.4)$$

Let $(c_1, \ldots, c_l) \in V(Ideal_{K,l}(F))$. Then

$$\overline{f(c_1, \ldots, c_{l-1})} = 0_p \text{ for every } f \in G \cap K[x_1, \ldots, x_{l-1}].$$

So, by Theorem 14,

$$(c_1, \ldots, c_{l-1}) \in V(Q_{/x_{l-1}}).$$

From assumption (5.2) we know that there exists an $r \in \{1, \ldots, car_l - 1\}$ with

$$\overline{G_{l,r}(c_1, \ldots, c_{l-1})} \neq 0_p.$$

Thus, there exist only finitely many $a \in \bar{K}^1$ such that

$$\overline{\overline{G_{l,r}(c_1, \ldots, c_{l-1})}(0_{l-1}, a)} = 0_p.$$

Therefore, by Lemma 2,

$$\{\, a \mid a \in \bar{K}^1 \text{ and } ((c_1, \ldots, c_{l-1}), a) \in V(Ideal_{K,l}(F)) \,\} \text{ is finite.}$$

By Theorem 17,

$$V(Q_{/x_{l-1}}) \text{ is finite }.$$

Hence,

$$V(Ideal_{K,l}(F)) \textit{ is finite.} \tag{5.5}$$

Thus, by (5.3), (5.4), and (5.5), F is a reduced Gröbner basis and $V(Ideal_{K,l}(F))$ is finite.

On the other hand, there exists no polynomial f in $G \setminus \{G_{l,car_l}\}$ such that

$$lpp(f) \in K[x_l].$$

Hence, there exists no polynomial f in F such that

$$lpp(f) \in K[x_l].$$

This is a contradiction to Theorem 16.

Thus, in contrast to assumption (5.2), there exists a $b' \in V(Q_{/x_{l-1}})$ with

$$\overline{G_{l,1}(b')} = \ldots = \overline{G_{l,car_l-1}(b')} = 0_p.$$

By Lemma 8,

$$\overline{G_{l,1}(b)} = \ldots = \overline{G_{l,car_l-1}(b)} = 0_p$$

for all $b \in V(Q_{/x_{l-1}})$. •

Corollary 1 is an easy consequence of the previous theorem.

Corollary 1 *Let Q be a zero-dimensionsal primary ideal in $K[x_1, \ldots, x_n]$. Then there exists an $f \in Q_{/x_l}$ such that*

$$gcd(Q_{/x_l}, b) = \overline{f(b)} \textit{ for all } b \in V(Q_{/x_{l-1}}) \textit{ and } lc(f) = 1.$$

Proof: Let G be the reduced Gröbner basis in $K[x_1, \ldots, x_n]$ such that

$$Ideal_{K,n}(G) = Q.$$

We have proven that

$$lc(G_{l,car_l}) = 1.$$

Furthermore, by Theorem 14, Theorem 18, and Lemma 9,

$$gcd(Q_{/x_l}, b) = \overline{G_{l,car_l}(b)} \text{ for all } b \in V(Q_{/x_{l-1}}). \quad \bullet$$

A generalization of Corollary 1 is the next theorem.

Theorem 19 *Let I be a zero-dimensional ideal in $K[x_1,\ldots,x_n]$ and $b \in V(I_{/x_{l-1}})$. Then there exists an $f \in I_{/x_l}$ such that*

$$gcd(I_{/x_l}, b) = \overline{f(b)} \text{ and } \overline{lc(f)(b)} \neq 0_p.$$

Before we give a proof of Theorem 19 we show the following two lemmas, which are required in the proof of the theorem.

Lemma 12 *Let $f \in K[x_1,\ldots,x_n] \setminus K[x_1]$ and $b \in \bar{K}^{r-1}$, where*

$$r := \max\{\, m \mid deg(f,m) > 0 \,\}.$$

Then

$$\overline{lc(f)(b)} \neq 0_p \quad iff \quad deg(f,r) = deg(\overline{f(b)}, r).$$

Proof: Let $i \in N^{n-r+1}$ such that $i_1 = deg(f,r)$ and $i_2 = \ldots = i_{n-r+1}$. Thus,

$$lc(f) = f_{(.,i)}.$$

From $C(\overline{f_{(.,i)}(b)}) \subseteq \{0_n\}$ and Lemma 7 we obtain

$$\overline{f_{(.,i)}(b)} \neq 0_p$$

$$\text{iff}$$

$$\overline{f_{(.,i)}(b)}(0_n) \neq 0$$

$$\text{iff}$$

$$\overline{f(b)}(0_{r-1}, i) \neq 0$$

$$\text{iff}$$

$$(0_{r-1}, i) \in C(\overline{f(b)}).$$

As $deg(\overline{f(b)}, r) \leq deg(f,r)$,

$$(0_{r-1}, i) \in C(\overline{f(b)})$$

$$\text{iff}$$

$$deg(\overline{f(b)}, r) = deg(f,r). \quad \bullet$$

Lemma 13 *Let J be a zero-dimensionsal ideal in $K[x_1,\ldots,x_m]$ and*

$$J = Q_1 \cap \ldots \cap Q_r$$

a reduced primary decomposition of J. Then

$$V(Q_s) \cap V(Q_{s'}) = \emptyset \text{ for } s \neq s'.$$

Proof: We assume that there exists a

$$b \in V(Q_s) \cap V(Q_{s'}) \text{ for some } s, s' \in \{1, \ldots, r\}.$$

As, by Theorem 3, $V(Q_s) = V(\sqrt{Q_s})$ and $V(Q_{s'}) = V(\sqrt{Q_{s'}})$,

$$b \in V(\sqrt{Q_s}) \cap V(\sqrt{Q_{s'}}).$$

As $\sqrt{Q_s}$ and $\sqrt{Q_{s'}}$ are zero-dimensional, b is a generic zero of $\sqrt{Q_s}$ and $\sqrt{Q_{s'}}$.

Let $f \in K[x_1, \ldots, x_m]$. From

$$f \in \sqrt{Q_s}$$

$$\text{iff}$$

$$\overline{f(b)} = 0_p$$

$$\text{iff}$$

$$f \in \sqrt{Q_{s'}}$$

we obtain

$$\sqrt{Q_s} = \sqrt{Q_{s'}}.$$

Hence,

$$s = s',$$

because we assumed the primary decomposition to be reduced. •

Proof of Theorem 19:

Let $Q_1, \ldots, Q_r$ be zero-dimensional primary ideals in $K[x_1, \ldots, x_n]$ such that $I_{/x_l} = Q_{1/x_l} \cap \ldots \cap Q_{r/x_l}$ is a reduced primary decomposition of $I_{/x_l}$.

We can show by the same arguments as in Lemma 11 that

$$I_{/x_{l-1}} = Q_{1/x_{l-1}} \cap \ldots \cap Q_{r/x_{l-1}}.$$

Thus,

$$V(I_{/x_{l-1}}) = V(Q_{1/x_{l-1}}) \cup \ldots \cup V(Q_{r/x_{l-1}}).$$

Without loss of generality, we assume that the primary ideals $Q_1, \ldots, Q_r$ are ordered in such a way that there exists an $s \in \{1, \ldots, r\}$ with

$$b \in V(Q_{1/x_{l-1}}), \ldots, b \in V(Q_{s/x_{l-1}}), b \notin V(Q_{s+1/x_{l-1}}), \ldots, b \notin V(Q_{r/x_{l-1}}).$$

We define $h_t \in Q_{1/x_l} \cap \ldots \cap Q_{t/x_l}$ such that

$$\overline{h_t(b)} = gcd(Q_{1/x_l} \cap \ldots \cap Q_{t/x_l}, b) \textit{ and } lc(h_t) = 1 \textit{ for every } t \in \{1, \ldots, s\}.$$

By Corollary 1, there exists an $f \in Q_{1/x_l}$ with

$$lc(f) = 1 \text{ and } \overline{f(b)} = gcd(Q_{1/x_l}, b).$$

Set $h_1 := f$.

We assume that $t \in \{1, \ldots, s-1\}$ and that h_t is already defined.

Let $f \in Q_{t+1/x_l}$ such that

$$lc(f) = 1 \text{ and } \overline{f(b)} = gcd(Q_{t+1/x_l}, b).$$

Set $h_{t+1} := h_t \cdot f$.

From

$$gcd(Q_{1/x_l} \cap \ldots \cap Q_{t+1/x_l}, b) \in \overline{(Q_{1/x_l} \cap \ldots \cap Q_{t/x_l})(b)} \text{ and}$$

$$gcd(Q_{1/x_l} \cap \ldots \cap Q_{t+1/x_l}, b) \in \overline{Q_{t+1/x_l}(b)}$$

we obtain

$$\overline{h_t(b)} \text{ divides } gcd(Q_{1/x_l} \cap \ldots \cap Q_{t+1/x_l}, b) \text{ and}$$

$$\overline{f(b)} \text{ divides } gcd(Q_{1/x_l} \cap \ldots \cap Q_{t+1/x_l}, b).$$

Assume that there exists a $g \in K(b)[x_l]$ such that $deg(g, l) > 0$ and g divides $\overline{h_t(b)}$ and $\overline{f(b)}$.

Let $c \in \bar{K}^l$ such that $c_1 = \ldots = c_{l-1} = 0$ and $\overline{g(c)} = 0_p$. Thus,

$$\overline{\overline{h_t(b)}(c)} = \overline{\overline{f(b)}(c)} = 0_p.$$

From the fact that $\overline{h_t(b)}$ divides every element of $\overline{(Q_{1/x_l} \cap \ldots \cap Q_{t/x_l})(b)}$ and that $\overline{f(b)}$ divides every element of $\overline{Q_{t+1/x_l}(b)}$ and from Lemma 2 we obtain

$$(b_1, \ldots, b_{l-1}, c_l) \in V(Q_{1/x_l} \cap \ldots \cap Q_{t/x_l}) \cap V(Q_{t+1/x_l}).$$

As

$$V(Q_{1/x_l}) \cup \ldots \cup V(Q_{t/x_l}) = V(Q_{1/x_l} \cap \ldots \cap Q_{t/x_l}),$$

we have a contradiction to Lemma 13.

Therefore, $\overline{h_t(b)}$ and $\overline{f(b)}$ are relatively prime. Thus,

$$\overline{h_{t+1}(b)} \text{ divides } gcd(Q_{1/x_l} \cap \ldots \cap Q_{t+1/x_l}, b).$$

As $\overline{h_{t+1}(b)} \in \overline{(Q_{1/x_l} \cap \ldots \cap Q_{t+1/x_l})(b)}$ and $lc(h_{t+1}) = 1$, it follows

$$\overline{h_{t+1}(b)} = gcd(Q_{1/x_l} \cap \ldots \cap Q_{t+1/x_l}, b).$$

We define $q \in K[x_1, \dots, x_l]$ such that there exists an e with

$$e \cdot \overline{q(b)} = gcd(I_{/x_l}, b) \text{ and } deg(q, l) = deg(\overline{q(b)}, l).$$

We choose a $p_t \in Q_{t/x_{l-1}}$ for every $t \in \{s+1, \dots, r\}$ such that

$$\overline{p_t(b)} \neq 0_p.$$

This is always possible, because $b \notin V(Q_{t/x_{l-1}})$ for all $t \in \{s+1, \dots, r\}$.

Set $q := p_{s+1} \cdot \ldots \cdot p_r \cdot h_s$.

Obviously, $q \in I_{/x_l}$. As

$$\overline{q(b)} = \overline{p_{s+1}(b)} \cdot \ldots \cdot \overline{p_r(b)} \cdot gcd(Q_{1/x_l} \cap \ldots \cap Q_{s/x_l}, b),$$

$(\overline{p_{s+1}(b)} \cdot \ldots \cdot \overline{p_r(b)})(j) = 0$ for all $j \in N^n \setminus \{0_n\}$, and $\overline{p_{s+1}(b)} \cdot \ldots \cdot \overline{p_r(b)} \neq 0_p$, we know that

$$\overline{q(b)} \text{ divides } gcd(Q_{1/x_l} \cap \ldots \cap Q_{s/x_l}, b).$$

From $lc(h_s) = 1$ and Lemma 12 we obtain

$$deg(q, l) = deg(h_s, l) = deg(\overline{h_s(b)}, l) = deg(\overline{q(b)}, l).$$

As $I_{/x_l}$ is a subset of $Q_{1/x_l} \cap \ldots \cap Q_{s/x_l}$,

$$gcd(Q_{1/x_l} \cap \ldots \cap Q_{s/x_l}, b) \text{ divides } gcd(I_{/x_l}, b).$$

Thus,

$$\overline{q(b)} \text{ divides } gcd(I_{/x_l}, b) \text{ and } q \in I_{/x_l}.$$

Hence, there exists an e such that

$$e \cdot \overline{q(b)} = gcd(I_{/x_l}, b).$$

Altogether,

$$\overline{e \cdot q(b)} = gcd(I_{/x_l}, b) \text{ and } deg(e \cdot q, l) = deg(\overline{e \cdot q(b)}, l).$$

As $e \cdot q \in K[x_1, \dots, x_l] \setminus K[x_1, \dots, x_{l-1}]$, we can apply Lemma 12 and obtain

$$\overline{lc(e \cdot q)(b)} \neq 0_p. \quad \bullet$$

By means of Theorem 19 it is relatively easy to prove one of the main results of this paper:

Theorem 20 *Let I be a zero-dimensional ideal in $K[x_1, \ldots, x_n]$, G the reduced Gröbner basis in $K[x_1, \ldots, x_n]$ such that $Ideal_{K,n}(G) = I$, and $b \in V(I_{/x_{l-1}})$.*

Then there exists a d such that

$$d \cdot \overline{G_{l,min_b}(b)} = gcd(\{\overline{G_{l,1}(b)}, \ldots, \overline{G_{l,car_l}(b)}\}).$$

Proof: Let $q \in I_{/x_l}$ such that

$$gcd(I_{/x_l}, b) = \overline{q(b)} \text{ and } \overline{lc(q)(b)} \neq 0_p.$$

We know that

$$\overline{g(b)} = 0_p \text{ for all } g \in G \cap K[x_1, \ldots, x_{l-1}],$$
$$\overline{q(b)} \neq 0_p, \text{ and}$$
$$q \text{ reduces to zero modulo } G.$$

Thus, there exists an $f \in G \cap K[x_1, \ldots, x_l] \setminus K[x_1, \ldots, x_{l-1}]$ such that

$$\overline{f(b)} \neq 0_p \text{ and } deg(f, l) \leq deg(q, l).$$

Therefore, by Lemma 12,

$$deg(\overline{f(b)}, l) \leq deg(f, l) \leq deg(q, l) = deg(\overline{q(b)}, l).$$

As $\overline{q(b)}$ divides $\overline{f(b)}$, there exists an e such that

$$e \cdot \overline{f(b)} = gcd(I_{/x_l}, b).$$

From Lemma 12 and

$$deg(\overline{f(b)}, l) = deg(\overline{q(b)}, l) = deg(q, l) \geq deg(f, l).$$

we obtain

$$\overline{lc(f)(b)} \neq 0_p.$$

Thus,

$$deg(\overline{G_{l,min_b}(b)}, l) \leq deg(G_{l,min_b}, l) \leq deg(f, l) = deg(\overline{f(b)}, l).$$

On the other hand, $\overline{f(b)}$ divides $\overline{G_{l,min_b}(b)}$. Hence, there exists a d such that

$$d \cdot \overline{G_{l,min_b}(b)} = gcd(I_{/x_l}, b).$$

From Lemma 9 and from Theorem 14,

$$d \cdot \overline{G_{l,min_b}(b)} = gcd(\{\overline{G_{l,1}(b)}, \ldots, \overline{G_{l,car_l}(b)}\}). \bullet$$

5.2 An Improved Version of Algorithm 3

In this section we give a first near-at-hand application of Theorem 20.

First of all, let us write down Algorithm 3 again.

Algorithm 3

input: F, a finite subset of $K[x_1, \ldots, x_n]$ such that I is a zero-dimensional ideal in $K[x_1, \ldots, x_n]$, where $I := Ideal_{K,n}(F)$.

output: X_n, a finite subset of $\bar{K}^n$ such that $X_n = V(I)$.

```
$G := GB(F)$
$X_1 := \{ c \mid c \in \bar{K}^1$ and $\overline{G_{1,1}(c)} = 0_p \}$
$for\ r := 1\ to\ n-1\ do$
    $X_{r+1} := \emptyset$
    $for\ all\ b \in X_r\ do$
        $H := \{ \overline{G_{r+1,s}(b)} \mid s \in \{1, \ldots, car_{r+1}\} \}$
        $q := gcd(H)$
        $X_{r+1} := X_{r+1} \cup \{ (b, c) \mid c \in \bar{K}^1$ and $\overline{q(0_r, c)} = 0_p \}$
```

For continuing a partial solution $b \in \bar{K}^r$ it is necessary to compute

```
$H := \{ \overline{G_{r+1,s}(b)} \mid s \in \{1, \ldots, car_{r+1}\} \}$,
$q$:=gcd(H),
```

and to find the zeros of q. From Theorem 20 we know that there exists a d such that

$$d \cdot \overline{G_{r+1,min_b}(b)} = gcd(H).$$

Therefore, we replace the instructions

```
$H := \{ \overline{G_{r+1,s}(b)} \mid s \in \{1, \ldots, car_{r+1}\} \}$
$q := gcd(H)$
```

in Algorithm 3 by the instruction

```
$q := \overline{G_{r+1,min_b}(b)}$
```

and obtain the following algorithm:

Algorithm 4

input: F, a finite subset of $K[x_1, \dots, x_n]$ such that I is a zero-dimensional ideal in $K[x_1, \dots, x_n]$, where $I := Ideal_{K,n}(F)$.

output: X_n, a finite subset of $\bar{K}^n$ such that $X_n = V(I)$.

```
$G := GB(F)$
$X_1 := \{ c \mid c \in \bar{K}^1$ and $\overline{G_{1,1}(c)} = 0_p \}$
$for\ r := 1\ to\ n-1\ do$
        $X_{r+1} := \emptyset$
        $for\ all\ b \in X_r\ do$
                $q := \overline{G_{r+1,min_b}(b)}$
                $X_{r+1} := X_{r+1} \cup \{ (b,c) \mid c \in \bar{K}^1$ and $\overline{q(0_r, c)} = 0_p \}$
```

Note that for computing min_b, where $b \in V(I_{/x_{r-1}})$, one has to check only whether

$$\begin{array}{rcl} \overline{lc(G_{r,1})(b)} & = & 0_p, \\ \overline{lc(G_{r,2})(b)} & = & 0_p, \\ \dots & . & . \end{array}$$

till the first s is found such that

$$\overline{lc(G_{r,s})(b)} \neq 0_p.$$

Example 8 By using Algorithm 4 we compute the common zeros of the polynomials in the set F that we have defined in Example 7.

Again we set

$$G := F,$$

denote

$$x^3 - x^2 + x - 1 \ by\ G_{1,1},$$
$$xy - y - x^2 + x \ by\ G_{2,1}, \text{ and}$$
$$y^2 - x^2 \ by\ G_{2,2},$$

and compute

$$X_1 := \{(i), (-i), (1)\}.$$

We set

$$r := 1,$$
$$X_2 := \emptyset,$$

and choose $(i) \in X_1$.

for (i) do.

Now it is not necessary to form a set of univariate polynomials over an extension field of Q and to compute the greatest common divisor of the polynomials in this set. We compute $min_{(i)}$ instead. In this case,

$$min_{(i)} = 1,$$

because if we replace x by i in $x-1$, which is the leading coefficent of $G_{2,1}$, we obtain $i-1 \neq 0$. Thus,

$$q := iy - y + 1 + i.$$

As i is the only zero of q,

$$X_2 := \{(i,i)\}.$$

The elements $(-i)$ and (1) of the set X_1 are continued in the same way and we finally obtain a set X_2 that contains all the solutions.

$$X_2 := \{(i,i),(-i,-i),(1,1),(1,-1)\}.$$

Now we define two functions, called $squarefree$ and $normed$, which are required in the following algorithms.

Definition 16 Let $f, h_1, \ldots, h_r \in \bar{K}[x_1, \ldots, x_n]$ such that

$$\begin{gathered} h_t \text{ is irreducible in } \bar{K}[x_1, \ldots, x_n], \\ hcoeff(h_t) = 1 \text{ for every } t \in \{1, \ldots, r\}, \\ \text{and } f = d \cdot \prod_{t \in \{1,\ldots,r\}} h_t^{s_t}, \text{ where } s_1, \ldots, s_r \in N_+. \end{gathered}$$

Then

$$\begin{aligned} squarefree(f) &:= d \cdot \prod_{t \in \{1,\ldots,r\}} h_t \text{ and} \\ normed(f) &:= (1/hcoeff(f)) \cdot f. \bullet \end{aligned}$$

Note that if K is a finite field or a field of characteristic zero and f is an element of $K[x_1, \ldots, x_n]$ then $squarefree(f)$ is an element of $K[x_1, \ldots, x_n]$.

5.3 Decomposing a Polynomial before Computing its Zeros

In Algorithm 3 and Algorithm 4 a partial solution is continued by computing the zeros of the corresponding q. In this section we investigate the problem whether it is possible to decompose such a q by using properties of the structure of reduced Gröbner bases. If we succeed in finding non-constant polynomials $f_1, \dots, f_s$ such that

$$q = f_1 \cdot \dots \cdot f_s \text{ and } s \geq 2,$$

we can compute the zeros of q by computing the zeros of the polynomials $f_1, \dots, f_s$. As the degrees of $f_1, \dots, f_s$ are smaller than the degree of q, this strategy might lead to a speed-up.

In Algorithm 4 the polynomial q that corresponds to a partial solution $(b_1, \dots, b_r)$ has the form

$$\overline{G_{r+1,min_b}(b)}.$$

Let $c \in \bar{K}^1$ such that

$$\overline{G_{r+1,min_b}(b,c)} = 0_p.$$

From the definition of $min_{(b,c)}$ we know that not only

$$\overline{G_{r+1,min_b}(b,c)} = 0_p$$

but also

$$\overline{lc(G_{r+2,1})(b,c)} = \dots = \overline{lc(G_{r+2,min_{(b,c)}-1})(b,c)} = 0_p.$$

Therefore,

$$deg(g, r+1) > 0,$$

where

$$g := gcd(\{\overline{G_{r+1,min_b}(b)}, \overline{lc(G_{r+2,1})(b)}, \dots, \overline{lc(G_{r+2,min_{(b,c)}-1})(b)}\}).$$

If we are lucky and

$$deg(g, r+1) < deg(\overline{G_{r+1,min_b}(b)}, r+1),$$

we have found two non-constant polynomials, namely g and $\overline{G_{r+1,min_b}(b)}/g$, such that

$$\overline{G_{r+1,min_b}(b)} = g \cdot (\overline{G_{r+1,min_b}(b)}/g).$$

In this case we can compute the zeros of $\overline{G_{r+1,min_b}(b)}$ by computing the zeros of g and $\overline{G_{r+1,min_b}(b)}/g$.

Example 9 We consider the reduced Gröbner basis G of a zero-dimensional ideal I in $Q[x, y, z]$, where

$$\begin{aligned} G_{1,1} &:= x^3 - x^2 + x - 1, \\ G_{2,1} &:= xy - y - x^2 + x, \\ G_{2,2} &:= y^2 - x^2, \\ G_{3,1} &:= yz - xz, \\ G_{3,2} &:= z^2 + x^2 z. \end{aligned}$$

Note that (1) is a partial solution of the first elimination ideal and that $min_{(1)} = 2$. As the greatest common divisor of $G_{2,2}(1, y)$ and the leading coefficient of $G_{3,1}(1, y, z)$ is $y - 1$, we divide $G_{2,2}(1, y)$ by $y - 1$ and obtain $y + 1$. Thus, we have found a non-trivial decomposition of $G_{2,min_{(1)}}(1, y)$. •

The following algorithm, which is based on this idea, forms the core of a method for solving Problem 2, which we will present afterwards.

Algorithm 5

input: G, a reduced Gröbner basis such that I is a zero-dimensional ideal, where $I := Ideal_{K,n}(G)$ and $n > 2$,

b, an element of $V(I_{/x_r})$, where $r \in \{1, \ldots, n-2\}$.

output: $X_1, \ldots, X_{car_{r+2}}$, finite subsets of $\bar{K}^{r+1}$ such that

$$X_s = \{\, (b, c) \mid c \in \bar{K}^1,\ (b, c) \in V(I_{/x_{r+1}}), \text{ and } min_{(b,c)} = s \,\}$$

for every $s \in \{1, \ldots, car_{r+2}\}$.

```
$f_1 := squarefree(\overline{G_{r+1,min_b}(b)})$
$for\ s := 1\ to\ car_{r+2}\ do$
    $q := gcd(\{f_s, \overline{lc(G_{r+2,s})(b)}\})$
    $g := f_s/q$
    $X_s := \{\, (b, c) \mid c \in \bar{K}^1 \text{ and } \overline{g(0_r, c)} = 0_p \,\}$
    $f_{s+1} := q$
```

Proof of Correctness

First of all, we want to show that

$$f_s = gcd(\{squarefree(\overline{G_{r+1,min_b}(b)}), \overline{lc(G_{r+2,1})(b)}, \ldots, \overline{lc(G_{r+2,s-1})(b)}\}) \qquad (5.6)$$

$$for\ every\ s \in \{1, \ldots, car_{r+2}\}.$$

If $s = 1$, (5.6) is obviously true.

Now we assume that $s \in \{2, \ldots, car_{r+2}\}$ and (5.6) is true for $s - 1$.

As $f_s = gcd(\{f_{s-1}, \overline{lc(G_{r+2,s-1})(b)}\})$

(5.6) is true for s.

Let $s \in \{1, \ldots, car_{r+2}\}$ and $c \in \bar{K}^1$.

$$(b, c) \in X_s$$

iff

$$\overline{g(0_r, c)} = 0_p, \text{ where}$$

$$\begin{aligned} g &:= f_s/q \text{ and} \\ q &:= gcd(\{f_s, \overline{lc(G_{r+2,s})(b)}\}). \end{aligned}$$

As f_s divides $squarefree(\overline{G_{r+1,min_b}(b)})$,

$$squarefree(f_s) = f_s.$$

Thus,

$$\overline{g(0_r, c)} = 0_p$$

iff

$$\overline{f_s(0_r, c)} = 0_p \text{ and } \overline{q(0_r, c)} \neq 0_p.$$

By (5.6) and Lemma 2,

$$\overline{f_s(0_r, c)} = 0_p \text{ and } \overline{q(0_r, c)} \neq 0_p$$

iff

$$\overline{G_{r+1,min_b}(b, c)} = \overline{lc(G_{r+2,1})(b, c)} = \ldots = \overline{lc(G_{r+2,s-1})(b, c)} = 0_p,$$

$$\text{and } \overline{lc(G_{r+2,s})(b, c)} \neq 0_p.$$

iff

$$(b, c) \in \{\, (b, a) \mid a \in \bar{K}^1,\ (b, a) \in V(I_{/x_{r+1}}), \text{ and } min_{(b,a)} = s \,\}. \ \bullet$$

Example 10 We take the reduced Gröbner bases G that we have already defined in Example 9 and (1) as input for Algorithm 5.

If we replace x by 1 in $x-1$, the leading coefficient of $G_{2,1}$, we obtain $1-1=0$. Thus,

$$min_{(1)} = 2.$$

As $G_{2,2}$ is squarefree already,

$$f_1 := y^2 - 1.$$

We set

$$s := 1.$$

The polynomial $y-1$ is the greatest common divisor of the polynomials y^2-1 and $y-1$, the leading coefficient of $G_{3,1}(1,y,z)$.

$$\begin{aligned} &q := y-1, \\ &g := y^2-1/y-1 = y+1, \\ &X_1 := \{(1,-1)\}, \\ &f_2 := y-1, \\ &s := 2. \end{aligned}$$

The polynomial 1 is the greatest common divisor of the polynomials $y-1$ and 1, the leading coefficient of $G_{3,2}(1,y,z)$.

$$\begin{aligned} &q := 1, \\ &g := y-1, \\ &X_2 := \{(1,1)\}, \\ &f_3 := 1. \end{aligned}$$

Note that we have decomposed the polynomial $G_{2,2}(1,y)$ into its factors $y-1$ and $y+1$ and that we have computed the zeros of $G_{2,2}(1,y)$ by computing the zeros of $y-1$ and $y+1$. •

Slightly different versions of Algorithm 5 form the core of the following algorithm, which solves Problem 2:

Algorithm 6

input: F, a finite subset of $K[x_1, \ldots, x_n]$ such that I is a zero-dimensional ideal in $K[x_1, \ldots, x_n]$, where $I := Ideal_{K,n}(F)$.

output: X_n, a finite subset of $\bar{K}^n$ such that $X_n = V(I)$.

```
$G := GB(F)$
$f := squarefree(G_{1,1})$
$for\ s := 1\ to\ car_2\ do$
        $q := gcd(\{f, lc(G_{2,s})\})$
        $g := f/q$
        $X_{1,s} := \{\, c \mid c \in \bar{K}^1$ and $\overline{g(c)} = 0_p \,\}$
        $f := q$
$for\ r := 1\ to\ n-2\ do$
        $for\ s := 1\ to\ car_{r+2}\ do$
                $X_{r+1,s} := \emptyset$
        $for\ t := 1\ to\ car_{r+1}\ do$
                $for\ all\ b \in X_{r,t}\ do$
                        $f := squarefree(\overline{G_{r+1,t}(b)})$
                        $for\ s := 1\ to\ car_{r+2}\ do$
                                $q := gcd(\{f, \overline{lc(G_{r+2,s})(b)}\})$
                                $g := f/q$
                                $X_{r+1,s} := X_{r+1,s} \cup \{\, (b,c) \mid c \in \bar{K}^1$ and
                                                                        $\overline{g(0_r, c)} = 0_p \,\}$
                                $f := q$
$X_n := \emptyset$
$for\ t := 1\ to\ car_n\ do$
        $for\ all\ b \in X_{n-1,t}\ do$
                $X_n := X_n \cup \{\, (b,c) \mid c \in \bar{K}^1$ and $\overline{G_{n,t}(b,c)} = 0_p \,\}$
```

Proof of Correctness

By the arguments that we have used for proving the correctness of Algorithm 5 we can show that the algorithm

```
$f := squarefree(G_{1,1})$
$for\ s := 1\ to\ car_2\ do$
        $q := gcd(\{f, lc(G_{2,s})\})$
        $g := f/q$
        $X_{1,s} := \{\, c \mid c \in \bar{K}^1$ and $\overline{g(c)} = 0_p \,\}$
        $f := q$
```

meets the specification

input: G, a reduced Gröbner basis such that I is a zero-dimensional ideal, where $I := Ideal_{K,n}(G)$.

output: $X_{1,1}, \ldots, X_{1,car_2}$, finite subsets of $\bar{K}^1$ such that

$$X_{1,s} = \{\, c \mid c \in V(I_{/x_1}) \text{ and } min_c = s \,\}$$

for every $s \in \{1, \ldots, car_2\}$.

Now we prove that the second part of Algorithm 6, the algorithm

```
for $r := 1$ to $n - 2$ do
    for $s := 1$ to $car_{r+2}$ do
        $X_{r+1,s} := \emptyset$
    for $t := 1$ to $car_{r+1}$ do
        for all $b \in X_{r,t}$ do
            $f := squarefree(\overline{G_{r+1,t}(b)})$
            for $s := 1$ to $car_{r+2}$ do
                $q := gcd(\{f, \overline{lc(G_{r+2,s})(b)}\})$
                $g := f/q$
                $X_{r+1,s} := X_{r+1,s} \cup \{\, (b,c) \mid c \in \bar{K}^1$ and
                                                  $\overline{g(0_r, c)} = 0_p \,\}$
                $f := q$
```

satisfies the specification

input: G, a reduced Gröbner basis such that I is a zero-dimensional ideal, where $I := Ideal_{K,n}(G)$, and

$X_{1,1}, \ldots, X_{1,car_2}$, finite subsets of $\bar{K}^1$ such that

$$X_{1,s} = \{\, c \mid c \in V(I_{/x_1}) \text{ and } min_c = s \,\}$$

for every $s \in \{1, \ldots, car_2\}$.

output: $X_{n-1,1}, \ldots, X_{n-1,car_n}$, finite subsets of $\bar{K}^{n-1}$ such that

$$X_{n-1,s} = \{\, c \mid c \in V(I_{/x_{n-1}}) \text{ and } min_c = s \,\}$$

for every $s \in \{1, \ldots, car_n\}$.

Let $r \in \{1, \ldots, n-2\}$.

We assume that

$$X_{r,s} = \{ c \mid c \in V(I_{/x_r}) \text{ and } min_c = s \}$$

for every $s \in \{1,\ldots,car_{r+1}\}$ and *show that*

$$X_{r+1,s} = \{ c \mid c \in V(I_{/x_{r+1}}) \text{ and } min_c = s \}$$

for every $s \in \{1,\ldots,car_{r+2}\}$.

Let $s \in \{1,\ldots,car_{r+2}\}$.

At the beginning of the loop

```
for $t := 1$ to $car_{r+1}$ do
    for all $b \in X_{r,t}$ do
        $f := squarefree(\overline{G_{r+1,t}(b)})$
        for $s := 1$ to $car_{r+2}$ do
            $q := gcd(\{f, \overline{lc(G_{r+2,s})(b)}\})$
            $g := f/q$
            $X_{r+1,s} := X_{r+1,s} \cup \{ (b,c) \mid c \in \bar{K}^1 \text{ and } \overline{g(0_r, c)} = 0_p \}$
            $f := q$
```

$X_{r+1,s}$ is empty.

Let $t \in \{1,\ldots,car_{r+1}\}$.

From the specification of Algorithm 5 we know that after the t-th pass of the loop

$$X_{r+1,s} = \bigcup_{u\in\{1,\ldots,t\}} \bigcup_{b\in X_{r,u}} \{ (b,c) \mid c \in \bar{K}^1,\ (b,c) \in V(I_{/x_{r+1}}),\ \text{and } min_{(b,c)} = s \}.$$

Thus, after termination

$$X_{r+1,s} = \bigcup_{u\in\{1,\ldots,car_{r+1}\}} \bigcup_{b\in X_{r,u}} \{ (b,c) \mid c \in \bar{K}^1,\ (b,c) \in V(I_{/x_{r+1}}),\ \text{and } min_{(b,c)} = s \} =$$

$$= \{ a \mid a \in V(I_{/x_{r+1}}) \text{ and } min_a = s \}.$$

It remains to show that the third part of Algorithm 6, the algorithm

```
$X_n := \emptyset$
for $t := 1$ to $car_n$ do
    for all $b \in X_{n-1,t}$ do
        $X_n := X_n \cup \{ (b,c) \mid c \in \bar{K}^1 \text{ and } \overline{G_{n,t}(b,c)} = 0_p \}$
```

meets the specification

input: G, a reduced Gröbner basis such that I is a zero-dimensional ideal, where $I := Ideal_{K,n}(G)$.

$X_{n-1,1}, \ldots, X_{n-1,car_n}$, finite subsets of $\bar{K}^{n-1}$ such that

$$X_{n-1,s} = \{ c \mid c \in V(I_{/x_{n-1}}) \text{ and } min_c = s \}$$

for every $s \in \{1, \ldots, car_n\}$.

output: X_n, a finite subset of $\bar{K}^n$ such that

$$X_n = V(I).$$

Let $t \in \{1, \ldots, car_n\}$. After the t-th pass of the for-loop

$$X_n = \bigcup_{u \in \{1,\ldots,t\}} \bigcup_{b \in X_{n-1,u}} \{ (b,c) \mid c \in \bar{K}^1 \text{ and } \overline{G_{n,u}(b,c)} = 0_p \}.$$

As $min_b = u$ for every $u \in \{1, \ldots, t\}$ and every $b \in X_{n-1,u}$, we can apply Theorem 20 and obtain

$$\bigcup_{u \in \{1,\ldots,t\}} \bigcup_{b \in X_{n-1,u}} \{ (b,c) \mid c \in \bar{K}^1 \text{ and } \overline{G_{n,u}(b,c)} = 0_p \} =$$

$$= \bigcup_{u \in \{1,\ldots,t\}} \bigcup_{b \in X_{n-1,u}} \{ (b,c) \mid c \in \bar{K}^1 \text{ and } (b,c) \in V(I) \}.$$

Thus, after termination

$$X_n = V(I). \bullet$$

Example 11 We consider $F \subseteq Q[x,y,z]$, where

$$\begin{aligned} F \; := \; & \{x^3 - x^2 + x - 1, \\ & xy - y - x^2 + x, \\ & y^2 - x^2, \\ & yz - xz, \\ & z^2 + x^2 z\}. \end{aligned}$$

By using Algorithm 6 we compute all the solutions of the system F, which we have already defined in Example 9.

F already is a reduced Gröbner basis of a zero-dimensional ideal in $Q[x,y,z]$. We set

$$G := F$$

and denote

$$x^3 - x^2 + x - 1 \; by \; G_{1,1},$$
$$xy - y - x^2 + x \; by \; G_{2,1},$$
$$y^2 - x^2 \; by \; G_{2,2},$$
$$yz - xz \; by \; G_{3,1},$$
$$z^2 + x^2 z \; by \; G_{3,2}.$$

As $G_{1,1}$ is squarefree,

$f := x^3 - x^2 + x - 1.$

We set

$s := 1.$

The polynomial $x - 1$ is the greatest common divisor of $x^3 - x^2 + x - 1$ and $x - 1$, the leading coefficient of $G_{2,1}$.

$q := x - 1,$
$g := x^3 - x^2 + x - 1/x - 1 = x^2 + 1.$

The zeros of g are i and $-i$.

$X_{1,1} := \{(i), (-i)\},$
$f := x - 1,$
$s := 2.$

The polynomial 1 is the greatest common divisor of $x - 1$ and 1, the leading coefficient of $G_{2,2}$.

$q := 1,$
$g := x - 1,$
$X_{1,2} := \{(1)\},$
$f := 1.$

Note that we have decomposed the polynomial $x^3 - x^2 + x - 1$ into its factors $x - 1$ and $x^2 + 1$ and that we have computed the zeros of $x^3 - x^2 + x - 1$ by computing the zeros of $x - 1$ and $x^2 + 1$. Now we set

$r := 1,$
$s := 1,$
$X_{2,1} := \emptyset,$
$s := 2,$
$X_{2,2} := \emptyset,$
$t := 1,$

and choose $(i) \in X_{1,1}$.

for (i) do.

The polynomial that we obtain by replacing x by i in $G_{2,1}$ is squarefree already.

$$f := iy - y + 1 + i,$$
$$s := 1.$$

The polynomial $y - i$ is the greatest common divisor of $iy - y + 1 + i$ and $y - i$, the leading coefficient of $G_{3,1}(i, y, z)$.

$$q := y - i,$$
$$g := iy - y + 1 + i/y - i = i - 1.$$

As g has no zeros, $X_{2,1}$ remains empty.

$$X_{2,1} := \emptyset,$$
$$f := y - i,$$
$$s := 2.$$

The polynomial 1 is the greatest common divisor of $y - i$ and 1, the leading coefficient of $G_{3,2}(i, y, z)$.

$$q := 1,$$
$$g := y - i,$$
$$X_{2,2} := \{(i, i)\},$$
$$f := 1.$$

Now we perform the same operations for $(-i) \in X_{1,1}$ and $(1) \in X_{1,2}$ and obtain sets $X_{2,1}$ and $X_{2,2}$.

$$X_{2,1} := \{(1, -1)\},$$
$$X_{2,2} := \{(i, i), (-i, -i), (1, 1)\}.$$

The set $X_{2,1} \cup X_{2,2}$ contains all the zeros of the second elimination ideal. To get the common zeros of the polynomials in F, we have to continue every element of $X_{2,1} \cup X_{2,2}$. We set

$$X_3 := \emptyset,$$
$$t := 1,$$

and take $(1, -1)$, the only element of $X_{2,1}$.

for $(1, -1)$ do.

As 0 is the only zero of $G_{3,1}(1, -1, z) := -2z$,

$$X_3 := \{(1, -1, 0)\}.$$

Finally, this process yields a set X_3 that contains all the solutions.

$$X_3 := \{(1, 1, -1), (1, 1, 0), (1 -1, 0), (i, i, 0), (i, i, 1), (-i, -i, 0), (-i, -i, 1)\}.$$

The following theorem, which can also be found in [12], immediately leads to a slightly different version of Algorithm 6.

Theorem 21 *Let G be a reduced Gröbner basis in $K[x_1, x_2]$ such that $Ideal_{K,2}(G)$ is zero-dimensional. Then*

$$\begin{array}{rcl} lc(G_{2,car_2}) & divides & lc(G_{2,car_2-1}), \\ lc(G_{2,car_2-1}) & divides & lc(G_{2,car_2-2}), \\ \dots & \dots & \dots \\ lc(G_{2,2}) & divides & lc(G_{2,1}), and \\ lc(G_{2,1}) & divides & G_{1,1}. \end{array}$$

Let us consider the first part of Algorithm 6:

```
$G := GB(F)$
$f := squarefree(G_{1,1})$
$for\ s := 1\ to\ car_2\ do$
        $q := gcd(\{f, lc(G_{2,s})\})$
        $g := f/q$
        $X_{1,s} := \{\, c \mid c \in \bar{K}^1$ and $\overline{g(c)} = 0_p \,\}$
        $f := q$
```

During the first pass of the loop

$$gcd(\{squarefree(G_{1,1}), lc(G_{2,1})\})$$

is assigned to q. During the second pass of the loop

$$gcd(\{squarefree(G_{1,1}), lc(G_{2,1}), lc(G_{2,2})\})$$

is assigned to q ...

As Theorem 21 shows that

$$gcd(\{squarefree(G_{1,1}), lc(G_{2,1}), \dots, lc(G_{2,s})\}) = squarefree(lc(G_{2,s}))$$

for every $s \in \{1, \dots, car_2\}$, we replace the instruction

$$q := gcd(\{f, lc(G_{2,s})\})$$

by the instruction

$$q := squarefree(lc(G_{2,s}))$$

and obtain a new version of Algorithm 6:

Algorithm 6'

input: F, a finite subset of $K[x_1, \ldots, x_n]$ such that I is a zero-dimensional ideal in $K[x_1, \ldots, x_n]$, where $I := Ideal_{K,n}(F)$.

output: X_n, a finite subset of $\bar{K}^n$ such that $X_n = V(I)$.

```
$G := GB(F)$
$f := squarefree(G_{1,1})$
$for\ s := 1\ to\ car_2\ do$
    $q := squarefree(lc(G_{2,s}))$
    $g := f/q$
    $X_{1,s} := \{\, c \mid c \in \bar{K}^1$ and $\overline{g(c)} = 0_p \,\}$
    $f := q$
$for\ r := 1\ to\ n-2\ do$
    $for\ s := 1\ to\ car_{r+2}\ do$
        $X_{r+1,s} := \emptyset$
    $for\ t := 1\ to\ car_{r+1}\ do$
        $for\ all\ b \in X_{r,t}\ do$
            $f := squarefree(\overline{G_{r+1,t}(b)})$
            $for\ s := 1\ to\ car_{r+2}\ do$
                $q := gcd(\{f, \overline{lc(G_{r+2,s})(b)}\})$
                $g := f/q$
                $X_{r+1,s} := X_{r+1,s} \cup \{\, (b,c) \mid c \in \bar{K}^1$ and
                                                  $\overline{g(0_r, c)} = 0_p \,\}$
                $f := q$
$X_n := \emptyset$
$for\ t := 1\ to\ car_n\ do$
    $for\ all\ b \in X_{n-1,t}\ do$
        $X_n := X_n \cup \{\, (b,c) \mid c \in \bar{K}^1$ and $\overline{G_{n,t}(b,c)} = 0_p \,\}$
```

Before we give a proof of Theorem 21 we show the following two lemmas, which are required in the proof of the theorem.

Lemma 14 *Let $f, g \in K[x_1, \ldots, x_m] \setminus \{0_p\}$.*
Then $deg(f \cdot g, m) = deg(f, m) + deg(g, m)$.

Proof: Let $i, j \in N^n$ such that $lpp(f)(i) = 1$ and $lpp(g)(j) = 1$. Then

$$lpp(f \cdot g)(i + j) = (lpp(f) \cdot lpp(g))(i + j) = (lpp(f)(i)) \cdot (lpp(g)(j)) = 1.$$

Therefore,

$$deg(f \cdot g, m) = deg(lpp(f \cdot g), m) = (i + j)_m = i_m + j_m =$$

$$deg(lpp(f), m) + deg(lpp(g), m) = deg(f, m) + deg(g, m). \bullet$$

Lemma 15 *Let f, g be non-constant polynomials in $K[x_1, \ldots, x_n]$ and $r \geq s$, where*

$$\begin{aligned} r &:= \max\{\, m \mid deg(f,m) > 0 \,\}, \\ s &:= \max\{\, m \mid deg(g,m) > 0 \,\}. \end{aligned}$$

Then

$$\begin{array}{ll} (1) & r > s \textit{ implies } lc(f \cdot g) = lc(f) \cdot g, \\ (2) & r = s \textit{ implies } lc(f \cdot g) = lc(f) \cdot lc(g), \\ (3) & r = s,\ deg(f,r) = deg(g,s), \textit{ and } lc(f) + lc(g) \neq 0_p \textit{ implies} \\ & lc(f+g) = lc(f) + lc(g) \textit{ and } deg(f+g,r) = deg(f,r). \end{array}$$

Proof: Let $k \in N^{n-r+1}$ such that

$$k_1 = deg(f,r),\ k_2 = \ldots = k_{n-r+1} = 0$$

and $k' \in N^{n-s+1}$ such that

$$k'_1 = deg(g,s),\ k'_2 = \ldots = k'_{n-s+1} = 0.$$

Thus,

$$lc(f) = f_{(.,k)} \textit{ and } lc(g) = g_{(.,k')}.$$

Case $r > s$:

Then

$$r = \max\{\, m \mid deg(f \cdot g, m) > 0 \,\}.$$

By Lemma 14,

$$deg(f \cdot g, r) = deg(f, r).$$

Therefore,

$$lc(f \cdot g) = (f \cdot g)_{(.,k)}.$$

Let $i \in N^{r-1}$. Then

$$lc(f \cdot g)(i, 0_{n-r+1}) = (f \cdot g)(i, k).$$

As $g \in K[x_1, \ldots, x_{r-1}]$,

$$(f \cdot g)(i,k) = \sum_{j+j'=i} f(j,k) \cdot g(j', 0_{n-r+1}) =$$

$$= \sum_{j+j'=i} f_{(.,k)}(j, 0_{n-r+1}) \cdot g(j', 0_{n-r+1}) = \sum_{j+j'=i} lc(f)(j, 0_{n-r+1}) \cdot g(j', 0_{n-r+1}) =$$

$$= (lc(f) \cdot g)(i, 0_{n-r+1}).$$

Let $j \in N^{n-r+1} \setminus \{0_{n-r+1}\}$. From

$$lc(f) \cdot g \in K[x_1, \ldots, x_{r-1}] \text{ and } lc(f \cdot g) \in K[x_1, \ldots, x_{r-1}]$$

it follows

$$(lc(f) \cdot g)(i,j) = 0 = (lc(f \cdot g))(i,j).$$

Thus,

$$lc(f \cdot g) = lc(f) \cdot g.$$

Case r=s:

From

$$f \cdot g \in K[x_1, \ldots, x_r] \setminus K[x_1, \ldots, x_{r-1}] \text{ and } deg(f \cdot g, r) = deg(f, r) + deg(g, r)$$

we obtain

$$lc(f \cdot g) = (f \cdot g)_{(.,k'')}, \text{ where } k'' := k + k'.$$

Let $i \in N^{r-1}$. Then

$$lc(f \cdot g)(i, 0_{n-r+1}) = (f \cdot g)(i, k'') = \sum_{j+j'=i} f(j,k) \cdot g(j', k') =$$

$$\sum_{j+j'=i} lc(f)(j, 0_{n-r+1}) \cdot lc(g)(j', 0_{n-r+1}) = (lc(f) \cdot lc(g))(i, 0_{n-r+1}).$$

Let $j \in N^{n-r+1} \setminus \{0_{n-r+1}\}$. From

$$(lc(f) \cdot lc(g))(i,j) = 0 = (lc(f \cdot g))(i,j)$$

we obtain

$$lc(f \cdot g) = lc(f) \cdot lc(g).$$

Now we assume that $r = s$, $deg(f,r) = deg(g,s)$, and $lc(f) + lc(g) \neq 0_p$. Therefore,

$$lc(f) = f_{(.,k)} \text{ and } lc(g) = g_{(.,k)}.$$

Let $i \in N^{r-1}$ such that $(lc(f) + lc(g))(i, 0_{n-r+1}) \neq 0$. Then

$$(f+g)(i,k) = f(i,k) + g(i,k) =$$

$$= lc(f)(i, 0_{n-r+1}) + lc(g)(i, 0_{n-r+1}) = (lc(f) + lc(g))(i, 0_{n-r+1}) \neq 0.$$

Thus,

$$r \leq \max\{\, m \mid deg(f+g, m) > 0 \,\} \text{ and } deg(f+g, r) \geq k_1 = deg(f, r).$$

On the other hand,

$$f + g \in K[x_1, \ldots, x_r] \text{ and } deg(f+g, r) \leq \max(\{deg(f,r), deg(g,r)\}) = deg(f,r).$$

Therefore,

$$r = \max\{\, m \mid deg(f+g, m) > 0 \,\} \text{ and } deg(f+g, r) = deg(f, r).$$

Hence,

$$lc(f+g) = (f+g)_{(.,k)} = f_{(.,k)} + g_{(.,k)} = lc(f) + lc(g). \bullet$$

Now we prove Theorem 21.

Proof of Theorem 21:

We assume that there exists an $r \in \{1, \ldots, car_2 - 1\}$ such that $lc(G_{2,r+1})$ does not divide $lc(G_{2,r})$.

Let $h := SPol(G_{2,r+1}, G_{2,r})$. As

$$deg(lpp(G_{2,r}), 2) < deg(lpp(G_{2,r+1}), 2) \text{ and}$$

$$deg(lpp(G_{2,r}), 1) > deg(lpp(G_{2,r+1}), 1),$$

there exist v, w and d such that

$$h = w \cdot G_{2,r+1} - d \cdot v \cdot G_{2,r},$$

$$w \in K[x_1], \text{ and } v \in K[x_2].$$

By Lemma 15,

$$lc(w \cdot G_{2,r+1}) = w \cdot lc(G_{2,r+1}) \text{ and}$$

$$lc(d \cdot v \cdot G_{2,r}) = lc(d \cdot v) \cdot lc(G_{2,r}) = d \cdot lc(G_{2,r}).$$

Therefore,

$$lc(G_{2,r+1}) \text{ divides } lc(w \cdot G_{2,r+1}) \text{ and}$$

$$lc(G_{2,r+1}) \text{ does not divide } lc(d \cdot v \cdot G_{2,r}).$$

Thus,

$$lc(w \cdot G_{2,r+1}) \neq lc(d \cdot v \cdot G_{2,r}).$$

As

$$deg(w \cdot G_{2,r+1}, 2) = deg(d \cdot v \cdot G_{2,r}, 2) \neq 0,$$

we can apply Lemma 15 and obtain

$$deg(G_{2,r+1}, 2) = deg(w \cdot G_{2,r+1}, 2) = deg(h, 2) \text{ and}$$

$$lc(h) = lc(w \cdot G_{2,r+1}) - lc(d \cdot v \cdot G_{2,r}).$$

Therefore,

$$lc(G_{2,r+1}) \text{ does not divide } lc(h).$$

Let h' denote the polynomial that we obtain by reducing h to normal form modulo $\{G_{2,r+1}\}$. As $deg(h, 2) = deg(G_{2,r+1}, 2)$, there exists a $q \in K[x_1]$ such that

$$h' = h - q \cdot G_{2,r+1}.$$

Thus,

$$0 \neq deg(h, 2) = deg(G_{2,r+1}, 2) = deg(q \cdot G_{2,r+1}, 2).$$

Furthermore,

$$lc(h) - lc(q \cdot G_{2,r+1}) \neq 0_p,$$

because

$$lc(q \cdot G_{2,r+1}) = q \cdot lc(G_{2,r+1})$$

and $lc(G_{2,r+1})$ does not divide $lc(h)$.

Therefore, by Lemma 15,

$$deg(lpp(h'), 2) = deg(h', 2) = deg(q \cdot G_{2,r+1}, 2) = deg(G_{2,r+1}, 2) = deg(lpp(G_{2,r+1}), 2).$$

From the fact that h' is in normal form modulo $\{G_{2,r+1}\}$ it follows that

$$deg(lpp(h'), 1) < deg(lpp(G_{2,r+1}), 1).$$

As h' is reducible to zero, there exists an $f \in G$ with

$$deg(lpp(f), s) \leq deg(lpp(h'), s) \quad (s = 1, 2).$$

Therefore,

$$deg(lpp(f), s) \leq deg(lpp(G_{2,r+1}), s) \quad (s = 1, 2).$$

Hence, G is not reduced. Contradiction.

Therefore,

$$lc(G_{2,r+1}) \text{ divides } lc(G_{2,r}) \text{ for all } r \in \{1, \ldots, car_2 - 1\}.$$

We can show by the same arguments that

$$G_{1,1} \text{ divides } lc(G_{2,1}). \quad \bullet$$

5.4 Avoiding the Computation of Zeros of Polynomials with Coefficients in an Extension Field of K

Each of the algorithms that we have presented so far in this chapter requires a subalgorithm that computes the zeros of a univariate polynomial over an extension field of K. In this section we concentrate on the question how this time-consuming subalgorithm can be avoided.

Example 12 We consider $G := \{G_{1,1}, G_{2,1}, G_{2,2}\} \subseteq Q[x, y]$, where

$$\begin{aligned} G_{1,1} &:= x^3 - x^2 + x - 1, \\ G_{2,1} &:= x^2y + y + x^2 + 1, \\ G_{2,2} &:= y^3 + xy^2 - y^2 - xy. \end{aligned}$$

G is the reduced Gröbner basis of a zero-dimensional ideal. If we solve the system G by using Algorithm 4 we have to compute the zeros $i, -i, 1$ of $G_{1,1}$ first. In the next step the zeros of each of the polynomials

$$\begin{aligned} G_{2,2}(i,y) &:= y^3 + iy^2 - y^2 - iy, \\ G_{2,2}(-i,y) &:= y^3 - iy^2 - y^2 + iy, \\ G_{2,1}(1,y) &:= 2y + 2 \end{aligned}$$

have to be computed, because

$$min_{(i)} = min_{(-i)} = 2 \text{ and } min_{(1)} = 1.$$

Therefore, a subalgorithm is required that finds the zeros of a univariate polynomial over an extension field of Q.

We want to show that there exists an alternative method to continue (i) and $(-i)$ without using this subalgorithm. Instead of solving the equation

$$G_{2,2}(i,y) = 0$$

and the equation

$$G_{2,2}(-i,y) = 0$$

we solve the equation

$$h(y) = 0, \text{ where}$$

$$h := normed(squarefree(G_{2,2}(i,y) \cdot G_{2,2}(-i,y))).$$

As

$$h = y^4 - y^3 + y^2 - y,$$

h is an element of $Q[y]$. Therefore, a subalgorithm is required that finds the zeros of a univariate polynomial over Q.

The solutions of

$$h(y) = 0$$

are $1, 0, i$ and $-i$. We know from the definition of h that every zero of $G_{2,2}(i,y)$ or $G_{2,2}(-i,y)$ is a zero of h. Hence, we only have to check for every element b of $\{1, 0, i, -i,\}$ whether b satisfies

$$G_{2,2}(i,b) = 0 \text{ or } G_{2,2}(-i,b) = 0$$

to obtain the zeros of $G_{2,2}(i,y)$ or $G_{2,2}(-i,y)$. In this example $1, 0, -i$ are the solutions of

$$G_{2,2}(i,y) = 0$$

and $1, 0, i$ are the solutions of

$$G_{2,2}(-i,y) = 0. \quad \bullet$$

Now the question arises which polynomials shall be multiplied together in general to obtain a polynomial whose coefficients are in K. The answer is given in Theorem 22.

Before we present this theorem we define the so-called minimal polynomials, which are needed in the proof.

Definition 17 Let J be an ideal in $K[x_1, \ldots, x_m]$ and $r \in \{1, \ldots, m\}$.

As $K[x_r]$ is a principal ideal domain, there exists a uniquely determined polynomial $q \in K[x_r]$ such that

the ideal generated by $\{q\}$ in $K[x_r]$ is $J \cap K[x_r]$ and $hcoeff(q) = 1$.

This polynomial is called *minimal polynomial of J in x_r*, abbreviated $minpol(J, r)$.

Theorem 22 *Let G be the reduced Gröbner basis of a zero-dimensional ideal I in $K[x_1, \ldots, x_n]$ and J a zero-dimensional ideal in $K[x_1, \ldots, x_{l-1}]$ such that*

$$V(J) \subseteq V(I_{/x_{l-1}}).$$

Furthermore, we assume that the field K is a finite field or a field of characteristic zero.

Then

$$normed(squarefree(\prod_{b \in V(J)} \overline{G_{l,min_b}(b)})) \in K[x_l].$$

Proof: In this proof we denote

$$normed(squarefree(\prod_{b \in V(J)} \overline{G_{l,min_b}(b)}))$$

by g. Let

$$J' := Ideal_{K,l}(F \cup \{\, G_{l,min_b} \mid b \in V(J)\,\}),$$

where F is a finite subset of $K[x_1, \ldots, x_{l-1}]$ such that $Ideal_{K,l-1}(F) = J$.

We want to show that for all $c \in \bar{K}^1$:

$$\overline{g(0_{l-1}, c)} = 0_p$$

iff

$$\overline{h(0_{l-1}, c)} = 0_p,$$

where $h := squarefree(minpol(J', l))$.

Let $c \in \bar{K}^1$ such that $\overline{g(0_{l-1}, c)} = 0_p$. Thus, there exists a $b \in V(J)$ with $\overline{G_{l,min_b}(b, c)} = 0_p$. By Theorem 20,

$$(b, c) \in V(J').$$

Hence,

$$\overline{h(0_{l-1},c)} = \overline{h(b,c)} = 0_p.$$

Now let $c \in \bar{K}^1$ such that $\overline{h(0_{l-1},c)} = 0_p$. As

$$V(J') \subseteq \{\, (b_1,\ldots,b_{l-1},d) \mid b \in V(J) \text{ and } \overline{G_{l,min_b}(b_1,\ldots,b_{l-1},d)} = 0_p \,\},$$

$$V(J') \text{ is finite.}$$

Therefore, we can show by the same arguments that we used for proving Theorem 17 that there exists a $b \in \bar{K}^{l-1}$ such that $(b,c) \in V(J')$. Thus,

$$b \in V(J) \text{ and } \overline{G_{l,min_b}(b,c)} = 0_p.$$

Hence,

$$\overline{g(0_{l-1},c)} = 0_p.$$

Altogether,

$$\overline{h(0_{l-1},c)} = 0_p$$
$$\text{iff}$$
$$\overline{g(0_{l-1},c)} = 0_p$$

for all $c \in \bar{K}^1$. Besides,

$$h = squarefree(h),\ g = squarefree(g),$$

$$hcoeff(h) = 1, \text{ and } hcoeff(g) = 1.$$

Therefore,

$$h = g.$$

As K is a finite field or a field of characteristic zero and $minpol(J',l) \in K[x_l]$,

$$h \in K[x_l].$$

Thus,

$$g \in K[x_l]. \bullet$$

Definition 18 Let G be a reduced Gröbner basis in $K[x_1,\ldots,x_n]$ such that the ideal I generated by G is zero-dimensional.

We want to investigate for which subset M of $V(I_{/x_{l-1}})$ there exists an ideal J in $K[x_1,\ldots,x_{l-1}]$ such that $V(J) = M$.

Let $r \in \{1,\ldots,n-1\}$. The set

$$\{\, i \mid i \in N^r \text{ and } i_s \leq car_{s+1} \text{ for all } s \in \{1,\ldots,r\} \,\}$$

is denoted by Tup_r.

Let $i \in Tup_r$. The set

$$\{\, b \mid b \in V(I_{/x_r}) \text{ and } min_{(b_1,\ldots,b_s)} = i_s \text{ for all } s \in \{1,\ldots,r\} \,\}$$

is denoted by CZ_i. $\bullet$

Example 13 Let $G := \{G_{1,1}, G_{2,1}, G_{2,2}, G_{3,1}, G_{3,2}\} \subseteq Q[x, y, z]$, where

$$\begin{aligned} G_{1,1} &:= x^3 - x^2 + x - 1, \\ G_{2,1} &:= xy - y - x^2 + x, \\ G_{2,2} &:= y^2 - x^2, \\ G_{3,1} &:= yz - xz, \\ G_{3,2} &:= z^2 + x^2 z. \end{aligned}$$

G is the reduced Gröbner basis of a zero-dimensional ideal I in $Q[x, y, z]$. According to the above definition,

$$\begin{aligned} Tup_1 &:= \{(1), (2)\}, \\ Tup_2 &:= \{(1,1), (1,2), (2,1), (2,2)\}. \end{aligned}$$

From

$$V(I_{/x_1}) = \{(1), (i), (-i)\},$$

$$min_{(i)} = min_{(-i)} = 1, \text{ and } min_{(1)} = 2$$

we obtain

$$\begin{aligned} CZ_{(1)} &:= \{(i), (-i)\}, \\ CZ_{(2)} &:= \{(1)\}. \end{aligned}$$

From

$$V(I_{/x_2}) = \{(1,1), (1,-1), (i,i), (-i,-i)\},$$

$$min_{(1,-1)} = 1, \text{ and } min_{(1,1)} = min_{(i,i)} = min_{(-i,-i)} = 2$$

we obtain

$$\begin{aligned} CZ_{(1,1)} &:= \emptyset, \\ CZ_{(1,2)} &:= \{(i,i), (-i,-i)\}, \\ CZ_{(2,1)} &:= \{(1,-1)\}, \\ CZ_{(2,2)} &:= \{(1,1)\}. \bullet \end{aligned}$$

Theorem 23 *Let G be a reduced Gröbner basis in $K[x_1, \ldots, x_n]$ such that the ideal I generated by G in $K[x_1, \ldots, x_n]$ is zero-dimensional, $r \in \{1, \ldots, n-1\}$, and $i \in Tup_r$.*

Then there exists an ideal J in $K[x_1, \ldots, x_r]$ such that

$$V(J) = CZ_i.$$

Proof: If $CZ_i = \emptyset$ then

$$CZ_i = \emptyset = V(K[x_1, \ldots, x_r]).$$

So let us assume that CZ_i is not empty.

Let $I_{/x_r} = Q_1 \cap \ldots \cap Q_s$ be a reduced primary decomposition of $I_{/x_r}$. Without loss of generality, we assume that the primary ideals $Q_1, \ldots, Q_s$ are ordered in such a way that there exists an $s' \in \{1, \ldots, s\}$ with

$$V(Q_1) \cap CZ_i \neq \emptyset, \ldots, V(Q_{s'}) \cap CZ_i \neq \emptyset,$$

$$V(Q_{s'+1}) \cap CZ_i = \emptyset, \ldots, V(Q_s) \cap CZ_i = \emptyset.$$

Obviously,

$$CZ_i \subseteq V(Q_1) \cup \ldots \cup V(Q_{s'}) = V(Q_1 \cap \ldots \cap Q_{s'}).$$

Let $c \in V(Q_1 \cap \ldots \cap Q_{s'})$.

Then there exists a $t \in \{1, \ldots, s'\}$ such that $c \in V(Q_t)$. We choose $c' \in V(Q_t) \cap CZ_i$.

Let $u \in \{1, \ldots, r\}$

As $(c_1, \ldots, c_u)$ and $(c_1', \ldots, c_u')$ are generic zeros of $\sqrt{Q_{t/x_u}}$,

$$\overline{f(c_1, \ldots, c_u)} = 0_p$$

$$\text{iff}$$

$$f \in \sqrt{Q_{t/x_u}}$$

$$\text{iff}$$

$$\overline{f(c_1', \ldots, c_u')} = 0_p$$

for all $f \in K[x_1, \ldots, x_u]$. Hence,

$$\overline{lc(G_{u+1,u'})(c_1, \ldots, c_u)} = \overline{lc(G_{u+1,u'})(c_1', \ldots, c_u')} = 0_p$$

for all $u' \in \{1, \ldots, min_{(c_1', \ldots, c_u')} - 1\}$. From

$$\overline{lc(G_{u+1,min_{(c_1', \ldots, c_u')}})(c_1', \ldots, c_u')} \neq 0_p$$

we obtain

$$\overline{lc(G_{u+1,min_{(c_1', \ldots, c_u')}})(c_1, \ldots, c_u)} \neq 0_p.$$

Thus,

$$min_{(c_1, \ldots, c_u)} = min_{(c_1', \ldots, c_u')} = i_u.$$

Therefore,

$$c \in CZ_i.$$

Altogether,

$$CZ_i = V(Q_1 \cap \ldots \cap Q_{s'}). \quad \bullet$$

Let $r \in \{1, \ldots, n-1\}$, $i \in Tup_r$, and G a reduced Gröbner basis such that the ideal I generated by G in $K[x_1, \ldots, x_n]$ is zero-dimensional.

From Theorem 22 and Theorem 23 we know that

$$normed(squarefree(\prod_{b \in CZ_i} \overline{G_{r+1,i_r}(b)}))$$

is an element of $K[x_{r+1}]$. Therefore, we can compute the set

$$ZWT_{(i_1,\ldots,i_r,1)} := \{\, (b,c) \mid b \in CZ_{(i_1,\ldots,i_r)},\ c \in \bar{K}^1, \text{ and } (b,c) \in V(I_{/x_{r+1}}) \,\}$$

by the following procedure, which requires a subalgorithm for finding the zeros of a univariate polynomial over K and not over an extension field of K.

```
if $CZ_{(i_1,\ldots,i_r)} = \emptyset$
then
        $h := 1$, where $1 \in K[x_1, \ldots, x_n]$
else
        $h := normed(squarefree(h'))$, where
                        $h' := \prod_{b \in CZ_{(i_1,\ldots,i_r)}} \overline{G_{r+1,i_r}(b)}$
$Con_{(i_1,\ldots,i_r)} := \{\, c \mid c \in \bar{K}^1$ and $\overline{h(0_r, c)} = 0_p \,\}$
$ZWT_{(i_1,\ldots,i_r,1)} := \{\, (b,c) \mid b \in CZ_{(i_1,\ldots,i_r)}, c \in Con_{(i_1,\ldots,i_r)}$, and
                                                $\overline{G_{r+1,i_r}(b,c)} = 0_p \,\}$
```

If $r < n-1$ we can obtain $CZ_{(i_1,\ldots,i_r,1)}, \ldots, CZ_{(i_1,\ldots,i_r,car_{r+2})}$ in the following way:

```
for $t := 1$ to $car_{r+2}$ do
        $CZ_{(i_1,\ldots,i_r,t)} := \{\, b \mid b \in ZWT_{(i_1,\ldots,i_r,t)}$ and $\overline{lc(G_{r+2,t})(b)} \neq 0_p \,\}$
        $ZWT_{(i_1,\ldots,i_r,t+1)} := ZWT_{(i_1,\ldots,i_r,t)} \setminus CZ_{(i_1,\ldots,i_r,t)}$
```

The sets $CZ_{(1)}, \ldots, CZ_{(car_2)}$ can be computed by a procedure that we have already used in Algorithm 6':

```
$f := squarefree(G_{1,1})$
for $s := 1$ to $car_2$ do
        $q := squarefree(lc(G_{2,s}))$
        $g := f/q$
        $CZ_{(s)} := \{\, c \mid c \in \bar{K}^1$ and $\overline{g(c)} = 0_p \,\}$
        $f := q$
```

Altogether, we obtain the following algorithm:

Algorithm 7

input: F, a finite subset of $K[x_1,\ldots,x_n]$ such that I is a zero-dimensional ideal in $K[x_1,\ldots,x_n]$, where $I := Ideal_{K,n}(F)$.

output: X, a finite subset of $\bar{K}^n$ such that $X = V(I)$.

```
$X := \emptyset$
$G := GB(F)$
$f := squarefree(G_{1,1})$
$for\ s := 1\ to\ car_2\ do$
    $q := squarefree(lc(G_{2,s}))$
    $g := f/q$
    $CZ_{(s)} := \{\, c \mid c \in \bar{K}^1$ and $\overline{g(c)} = 0_p \,\}$
    $f := q$
$for\ r := 1\ to\ n-1\ do$
    $for\ all\ (i_1,\ldots,i_r) \in Tup_r\ do$
        $if\ CZ_{(i_1,\ldots,i_r)} = \emptyset$
        $then$
            $h := 1$, where $1 \in K[x_1,\ldots,x_n]$
        $else$
            $h := normed(squarefree(h'))$, where
              $h' := \prod_{b \in CZ_{(i_1,\ldots,i_r)}} \overline{G_{r+1,i_r}(b)}$
        $Con_{(i_1,\ldots,i_r)} := \{\, c \mid c \in \bar{K}^1$ and $\overline{h(0_r,c)} = 0_p \,\}$
        $ZWT_{(i_1,\ldots,i_r,1)} := \{\, (b,c) \mid b \in CZ_{(i_1,\ldots,i_r)},\ c \in Con_{(i_1,\ldots,i_r)},$
                                                  and $\overline{G_{r+1,i_r}(b,c)} = 0_p \,\}$
        $if\ r = n-1$
        $then$
            $X := X \cup ZWT_{(i_1,\ldots,i_r,1)}$
        $else$
            $for\ t := 1\ to\ car_{r+2}\ do$
                $CZ_{(i_1,\ldots,i_r,t)} := \{\, b \mid b \in ZWT_{(i_1,\ldots,i_r,t)}$ and
                                                  $\overline{lc(G_{r+2,t})(b)} \neq 0_p \,\}$
                $ZWT_{(i_1,\ldots,i_r,t+1)} := ZWT_{(i_1,\ldots,i_r,t)} \setminus CZ_{(i_1,\ldots,i_r,t)}$
```

Example 14 Given $F \subseteq Q[x,y,z]$, where

$$\begin{aligned} F \ := \ & \{x^4 - x^3 + x^2 - x, \\ & z - 1, \\ & x^2y + y + x^2 + 1, \\ & y^3 + xy^2 - y^2 - xy, \\ & -x^3y - xy - x^4 - x^2\}, \end{aligned}$$

We want to find all the solutions of this system by means of Algorithm 7.

We set

$X := \emptyset,$
$G := GB(F).$

The reduced Gröbner basis G of the ideal generated by F is the set $\{G_{1,1}, G_{2,1}, G_{2,2}, G_{3,1}\}$, where

$$\begin{aligned} G_{1,1} &:= x^3 - x^2 + x - 1, \\ G_{2,1} &:= x^2y + y + x^2 + 1, \\ G_{2,2} &:= y^3 + xy^2 - y^2 - xy, \\ G_{3,1} &:= z - 1. \end{aligned}$$

As $G_{1,1}$ is squarefree,

$f := x^3 - x^2 + x - 1.$

We set

$s := 1.$

The polynomial $x^2 + 1$ is the squarefree form of the leading coefficient of $G_{2,1}$. Therefore,

$q := x^2 + 1,$
$g := x^3 - x^2 + x - 1/x^2 + 1 = x - 1,$
$CZ_{(1)} := \{(1)\},$
$f := x^2 + 1,$
$s := 2.$

The polynomial 1 is the squarefree form of the leading coefficient of $G_{2,2}$. Therefore,

$q := 1,$
$g := x^2 + 1,$
$CZ_{(2)} := \{(i), (-i)\},$
$f := 1.$

Now we set

$r := 1$

and choose $(2) \in Tup_1$.

for (2) do.

As $CZ_{(2)} = \{(i), (-i)\}$,

$$\begin{aligned}&h := normed(squarefree((y^3+iy^2-y^2-iy)\cdot(y^3-iy^2-y^2+iy))) = \\ &\quad = y^4-y^3+y^2-y, \\ &Con_{(2)} := \{(1),(0),(i),(-i)\}, \\ &ZWT_{(2,1)} := \{(i,1),(i,0),(i,-i),(-i,1)(-i,0)(-i,i)\}.\end{aligned}$$

Note that we have found the zeros of the polynomials $G_{2,2}(-i,y)$ and $G_{2,2}(i,y)$ in $Q(i)[y]$ by computing the set of zeros $Con_{(2)}$ of $y^4-y^3+y^2-y \in Q[y]$ and by testing whether an element of $Con_{(2)}$ is a zero of $G_{2,2}(i,y)$ or $G_{2,2}(-i,y)$.

As $r \neq 2$, we set

$$t := 1.$$

As there is only one polynomial in $G \cap Q[x,y,z] \setminus Q[x,y]$,

$$CZ_{(2,1)} = ZWT_{(2,1)}.$$

$$\begin{aligned}&CZ_{(2,1)} := \{(i,1),(i,0),(i,-i),(-i,1)(-i,0)(-i,i)\}, \\ &ZWT_{(2,2)} := \emptyset.\end{aligned}$$

Now we take (1), the other element of Tup_1, continue as before, and obtain

$$CZ_{(1,1)} := \{(1,-1)\}.$$

The set $CZ_{(1,1)} \cup CZ_{(2,1)}$ contains all the zeros of the second elimination ideal. To continue each of these zeros, we set

$$r := 2$$

and choose $(1,1) \in Tup_2$.

for $(1,1)$ do.

As $CZ_{(1,1)} = \{(1,-1)\}$,

$$\begin{aligned}&h := normed(squarefree((z-1)) = z-1, \\ &Con_{(1,1)} := \{(1)\}, \\ &ZWT_{(1,1,1)} := \{(1,-1,1)\}.\end{aligned}$$

As $r = 2$,

$$X := \{(1,-1,1)\}.$$

We do the same for $(2,1)$, the other element of Tup_2, and we finally obtain a set X that contains all the solutions.

$$X := \{(1,-1,1),(i,1,1),(i,0,1),(i,-i,1),(-i,1,1)(-i,0,1)(-i,i,1)\}. \quad \bullet$$

It is a near-at-hand problem for future research to decide whether it is possible to design an algorithm which is based on the results given in this section and on the decomposition idea of the previous section.

Chapter 6

Computing the Associated Ideals

In section 3 of this chapter it is shown how the Problems 2-4 can be solved by means of an algorithm that meets the following specification:

input: G, a reduced Gröbner basis such that I is a zero-dimensional ideal, where $I := Ideal_{K,n}(G)$.

output: X_n, such that $X_n = \{(f_1{}^1, \ldots, f_n{}^1), \ldots, (f_1{}^r, \ldots, f_n{}^r)\}$ and $\{f_1{}^s, \ldots, f_n{}^s\}$ is the reduced Gröbner basis of a prime ideal P_s that is associated with I for every $s \in \{1, \ldots, r\}$. Furthermore, if P' is a prime ideal associated with I then there exists an $s \in \{1, \ldots, r\}$ such that $\{f_1{}^s, \ldots, f_n{}^s\}$ is the reduced Gröbner basis of P'.

This algorithm is given in section 2. Its correctness is mainly based on the following theorem.

6.1 A Structure Theorem for Reduced Gröbner Bases of Zero-Dimensional Prime Ideals

Theorem 24 *The set $G \subseteq K[x_1, \ldots, x_n]$ is a reduced Gröbner basis of a zero-dimensional prime ideal in $K[x_1, \ldots, x_n]$*

iff

G satisfies the following three conditions:

1. *For every m there exists just one polynomial $f_m \in G$ that belongs to $K[x_1, \ldots, x_m]$ but not to $K[x_1, \ldots, x_{m-1}]$.*
2. *Let $b \in \bar{K}^{l-1}$ with*

$$\overline{f_1(b_1)} = \ldots = \overline{f_{l-1}(b_1, \ldots, b_{l-1})} = 0_p.$$

Then $\overline{f_l(b_1, \ldots, b_{l-1})}$ is irreducible in $K(b)[x_l]$. Furthermore, f_1 is irreducible in $K[x_1]$.

3. $lc(f_m) = 1$ and f_m is in normal form modulo $G \setminus \{f_m\}$ for every m.

Proof: Let G be the reduced Gröbner basis of a zero-dimensional prime ideal in $K[x_1, \ldots, x_n]$. From Theorem 16 and the fact that G is reduced we know that there exists just one polynomial f_1 in $G \cap K[x_1]$. Obviously, f_1 is irreducible.

By Theorem 16, there exist polynomials $G_{l,1}, \ldots, G_{l,car_l}$ in G which belong to $K[x_1, \ldots, x_l]$ but not to $K[x_1, \ldots, x_{l-1}]$.

Let us assume that car_l is greater than 1.

From Theorem 18 we obtain

$$\overline{G_{l,1}(b)} = 0_p \text{ for all } b \in V(Ideal_{K,n}(G) \cap K[x_1, \ldots, x_{l-1}]).$$

Thus,

$$\overline{lc(G_{l,1})(b)} = 0_p \text{ for all } b \in V(Ideal_{K,n}(G) \cap K[x_1, \ldots, x_{l-1}]).$$

As, by Lemma 6,

$Ideal_{K,n}(G) \cap K[x_1, \ldots, x_{l-1}]$ is a zero-dimensional prime ideal in $K[x_1, \ldots, x_{l-1}]$,

it follows from Theorem 2 that

$$\text{every } b \in Ideal_{K,n}(G) \cap K[x_1, \ldots, x_{l-1}]$$
$$\text{is a generic zero of } Ideal_{K,n}(G) \cap K[x_1, \ldots, x_{l-1}].$$

Thus,

$$lc(G_{l,1}) \in Ideal_{K,n}(G) \cap K[x_1, \ldots, x_{l-1}].$$

Let $h_1, h_2 \in G \cap K[x_1, \ldots, x_{l-1}]$.

As $SPol(h_1, h_2)$ reduces to zero modulo G and $SPol(h_1, h_2) \in K[x_1, \ldots, x_{l-1}]$,

$$SPol(h_1, h_2) \text{ reduces to zero modulo } G \cap K[x_1, \ldots, x_{l-1}].$$

Therefore,

$$G \cap K[x_1, \ldots, x_{l-1}] \text{ is a reduced Gröbner basis.}$$

By Theorem 14,

$G \cap K[x_1, \ldots, x_{l-1}]$ is the reduced Gröbner basis of $Ideal_{K,n}(G) \cap K[x_1, \ldots, x_{l-1}]$.

Hence,

$$lc(G_{l,1}) \text{ reduces to zero modulo } G \cap K[x_1, \ldots, x_{l-1}].$$

Therefore,

$$G_{l,1} \text{ is reducible modulo } G.$$

Contradiction.

Thus, condition 1 is satisfied.

Now let $b \in \bar{K}^{l-1}$ with

$$\overline{f_1(b_1)} = \ldots = \overline{f_{l-1}(b_1, \ldots, b_{l-1})} = 0_p.$$

We assume that $\overline{f_l(b_1,\ldots,b_{l-1})}$ is reducible in $K(b)[x_l]$.

Therefore, we can choose a $g \in K[x_1,\ldots,x_l]$ such that $\overline{g(b_1,\ldots,b_{l-1})}$ is an irreducible factor of $\overline{f_l(b_1,\ldots,b_{l-1})}$.

Let $b' \in \bar{K}^1$ such that $(0_{l-1},b')$ is a zero of $\overline{g(b)}$. Then, by Lemma 2,

$$(b,b') \text{ is an element of the variety of } Ideal_{K,l}(\{f_1,\ldots,f_l\}).$$

As $Ideal_{K,l}(\{f_1,\ldots,f_l\})$ is a zero-dimensional prime ideal in $K[x_1,\ldots,x_l]$,

$$(b,b') \text{ is a generic zero of } Ideal_{K,l}(\{f_1,\ldots,f_l\}).$$

Thus,

$$g \in Ideal_{K,l}(\{f_1,\ldots,f_l\}).$$

On the other hand,

$$g \text{ does not reduce to zero modulo } \{f_1,\ldots,f_l\},$$

although $\{f_1,\ldots,f_l\}$ is a Gröbner basis of $Ideal_{K,l}(\{f_1,\ldots,f_l\})$.

Contradiction.

Thus, condition 2 is satisfied.

By Theorem 16,

$$lc(f_m) = 1 \text{ for all } m.$$

Obviously, f_m is in normal form modulo $G \setminus \{f_m\}$.

Now we want to show the other direction

and assume that G satisfies the conditions 1-3.

First of all, we prove that G is a reduced Gröbner basis.

Let $r,s \in \{1,\ldots,n\}$ with $r < s$. Then

$$SPol(f_s,f_r) = lpp(f_r)\cdot f_s - 1\cdot lpp(f_s)\cdot f_r.$$

Therefore, we can write $SPol(f_s,f_r)$ in the following form:

$$SPol(f_s,f_r) = (-f_r + lpp(f_r))\cdot lpp(f_s) + (f_s - lpp(f_s))\cdot lpp(f_r).$$

Note that

$$deg(f_s - lpp(f_s),s) < deg(lpp(f_s),s).$$

Hence, $SPol(f_s,f_r)$ reduces to a polynomial g modulo $\{f_s\}$ with $deg(g,s) < deg(f_s,s)$. Thus,

$$g = (-f_r + lpp(f_r))\cdot lpp(f_s) + (f_s - lpp(f_s))\cdot lpp(f_r) + (f_r - lpp(f_r))\cdot f_s =$$

$$f_r \cdot (f_s - lpp(f_s)).$$

Obviously, g reduces to zero modulo $\{f_r\}$. Therefore, G is a reduced Gröbner basis.

Let P denote $Ideal_{K,n}(\{f_1, \ldots, f_n\})$ and P' be a prime ideal in $K[x_1, \ldots, x_n]$ with $P \subseteq P'$.

By Theorem 9, Theorem 15, and Theorem 16,

$$P \text{ is zero-dimensional.}$$

Thus,

$$P' \text{ is zero-dimensional.}$$

As $\{f'_1, \ldots, f'_n\}$, the reduced Gröbner basis of P', satisfies the conditions 1-3, we can demand that

$$f'_m \in K[x_1, \ldots, x_m] \setminus K[x_1, \ldots, x_{m-1}] \text{ for all } m.$$

Now let us assume that $\{\, m \mid f_m \neq f'_m \,\}$ is not empty.

Let $s := \min\{\, m \mid f_m \neq f'_m \,\}$.

As $f_1 \in P'$,

$$f_1 \text{ reduces to zero modulo } \{f'_1\}.$$

Furthermore,

$$f_1 \text{ and } f'_1 \text{ are irreducible in } K[x_1] \text{ and}$$
$$lc(f_1) = lc(f'_1) = 1.$$

Thus,

$$f_1 = f'_1 \text{ and } s > 1.$$

Obviously,

$$Ideal_{K,s-1}(\{f_1, \ldots, f_{s-1}\}) = Ideal_{K,s-1}(\{f'_1, \ldots, f'_{s-1}\}).$$

We denote this ideal by J. Because of $f_s \in P'$ there exist $g_1, \ldots, g_s \in K[x_1, \ldots, x_s]$ with

$$f_s = g_1 \cdot f'_1 + \ldots + g_s \cdot f'_s.$$

Let $b \in \bar{K}^{s-1}$ with $\overline{f'_1(b_1)} = \ldots = \overline{f'_{s-1}(b_1, \ldots, b_{s-1})} = 0_p$. Then

$$\overline{f_s(b_1, \ldots, b_{s-1})} = \overline{g_s(b_1, \ldots, b_{s-1})} \cdot \overline{f'_s(b_1, \ldots, b_{s-1})}.$$

From the irreducibility of $\overline{f_s(b_1, \ldots, b_{s-1})}$ and from the fact that $lc(f_s) = lc(f'_s) = 1$ we obtain

$$\overline{g_s(b_1, \ldots, b_{s-1})} = 1.$$

Thus,

$$\overline{f_s(b_1, \ldots, b_{s-1})} = \overline{f'_s(b_1, \ldots, b_{s-1})}.$$

Let $i \in N^{n-s+1}$. By Lemma 7,

$$\overline{f_{s(.,i)}(b)}(0_n) = \overline{f_s(b)}(0_{s-1}, i) = \overline{f'_s(b)}(0_{s-1}, i) = \overline{f'_{s(.,i)}(b)}(0_n).$$

From $C(\overline{f_{s(.,i)}(b)}) \subseteq \{0_n\}$ and $C(\overline{f'_{s(.,i)}(b)}) \subseteq \{0_n\}$ we obtain

$$\overline{f_{s(.,i)}(b)} = \overline{f'_{s(.,i)}(b)}.$$

As b is a generic zero of J,

$$f_{s(.,i)} - f'_{s(.,i)} \in J.$$

Therefore,

$$f_{s(.,i)} \equiv_J f'_{s(.,i)}.$$

As f_s and f'_s are reduced modulo $\{f_1, \ldots, f_{s-1}\}$,

$$f_{s(.,i)} \text{ and } f'_{s(.,i)} \text{ are in normal form modulo } \{f_1, \ldots, f_{s-1}\}.$$

Thus,

$$f_{s(.,i)} = f'_{s(.,i)}.$$

Let $j \in N^{s-1}$. Then

$$f_s(j, i) = f_{s(.,i)}(j, 0_{n-s+1}) = f'_{s(.,i)}(j, 0_{n-s+1}) = f'_s(j, i).$$

Therefore,

$$f_s = f'_s.$$

Contradiction.

Thus,

$$\{f_1, \ldots, f_n\} = \{f'_1, \ldots, f'_n\} \text{ and}$$
$$\{f_1, \ldots, f_n\} \text{ is the reduced Gröbner basis of } P'. \bullet$$

6.2 An Algorithm for Computing the Associated Ideals

Before we are able to present the algorithm we have to do a few preparations.

Example 15 Let

$$\begin{aligned} f &:= -x^2y + xy + x, \\ g &:= x^2 + 1, \end{aligned}$$

and J the ideal in $Q[x]$ generated by $\{g\}$. Obviously, $\{g\}$ is the reduced Gröbner basis of J. Let us consider f as a univariate polynomial in y. We write it in the form

$$(-x^2 + x)y + x.$$

If we replace $(-x^2 + x)$ by $\langle -x^2 + x\rangle_J$ and x by $\langle x\rangle_J$, where $\langle -x^2 + x\rangle_J$ (respectively $\langle x\rangle_J$) denotes the congruence class of $-x^2 + x$ (respectively x) modulo J, we obtain the polynomial

$$f^{\downarrow J} := \langle -x^2 + x\rangle_J \cdot y + \langle x\rangle_J$$

in $Q[x]/_J[y]$.

By the Characterisation Theorem of Gröbner Bases, every congruence class C in $Q[x]/_J$ contains an element q such that q is the normal form of p modulo $\{g\}$ for every $p \in C$. In this example $x + 1$ is the normal form of every polynomial in $\langle -x^2 + x\rangle_J$ and x is the normal form of every polynomial in $\langle x\rangle_J$. If we replace $\langle -x^2 + x\rangle_J$ by $x + 1$ and $\langle x\rangle_J$ by x in $f^{\downarrow J}$, we get the polynomial

$$(f^{\downarrow J})^{\uparrow J} := xy + y + x$$

in $Q[x, y]$. Note that

$$f \neq (f^{\downarrow J})^{\uparrow J}.$$

We will prove that this cannot happen if f is reduced modulo $\{g\}$. On the other hand, if $h \in Q[x]/_J[y]$ then

$$h = (h^{\uparrow J})^{\downarrow J}$$

holds in any case. •

Now we give a formal definition of $h^{\uparrow J}$ and $f^{\downarrow J}$.

Definition 19 Let $r \in \{1, \ldots, n-1\}$, $g \in K[x_1, \ldots, x_r]$, and G the reduced Gröbner basis of an ideal J in $K[x_1, \ldots, x_r]$.

The *congruence class of g modulo J* (i.e. the set

$$\{\, g' \mid g' \in K[x_1, \ldots, x_r] \text{ and } g \equiv_J g' \,\})$$

is denoted by $\langle g\rangle_J$.

Let $f \in K[x_1, \ldots, x_n]$.

The polynomial $f^{\downarrow J} \in K[x_1, \ldots, x_r]/_J[x_{r+1}, \ldots, x_n]$ is defined as follows:

$$\begin{array}{llll} f^{\downarrow J} : & N^n & \to & K[x_1, \ldots, x_r]/_J \\ & j & \mapsto & \langle 0_p\rangle_J \qquad\qquad \text{if } (j_1, \ldots, j_r) \neq 0_r \\ & j & \mapsto & \langle f_{(.,k)}\rangle_J \qquad\quad \text{otherwise,} \\ & & & \qquad\qquad\qquad \text{where } k \in N^{n-r} \text{ such that } (0_r, k) = j. \end{array}$$

Let $C \in K[x_1, \ldots, x_r]/_J$.

The Characterisation Theorem for Gröbner Bases shows that there exists a polynomial q in C such that q is the normal form of p modulo G for all $p \in C$. This polynomial is called *the representant of C*, abbreviated $rep(C)$.

Let $h \in K[x_1, \ldots, x_r]/_J[x_{r+1}, \ldots, x_n]$.

The polynomial $h^{\uparrow J} \in K[x_1, \ldots, x_n]$ is defined as follows:

$$\begin{array}{llll} h^{\uparrow J} : & N^n & \to & K \\ & j & \mapsto & rep(h(0_r, k'))(k, 0_{n-r}), \\ & & & \qquad \text{where } k \in N^r \text{ and } k' \in N^{n-r} \text{ such that } (k, k') = j. \end{array}$$ •

Lemma 16 *Let $r \in \{1,\ldots,n-1\}$, G the reduced Gröbner basis of an ideal J in $K[x_1,\ldots,x_r]$, $f \in K[x_1,\ldots,x_n]$, and $h \in K[x_1,\ldots,x_r]/_J[x_{r+1},\ldots,x_n]$. Then*

(1) $h{=}(h^{\uparrow J})^{\downarrow J}$,

(2) if f is reduced modulo G then $f{=}(f^{\downarrow J})^{\uparrow J}$.

Proof: Let $i \in N^r$ and $j \in N^{n-r}$.

If $i \neq 0_r$ then

$$(h^{\uparrow J})^{\downarrow J}(i,j) = \langle 0_p \rangle_J = h(i,j),$$

because $h \in K[x_1,\ldots,x_r]/_J[x_{r+1},\ldots,x_n]$.

If $i = 0_r$ then

$$(h^{\uparrow J})^{\downarrow J}(i,j) = \langle h^{\uparrow J}{}_{(.,j)} \rangle_J.$$

Let $k \in N^r$ and $k' \in N^{n-r} \setminus \{0_{n-r}\}$.

From

$$h^{\uparrow J}{}_{(.,j)}(k,k') = 0 = rep(h(0_r,j))(k,k') \text{ and}$$

$$h^{\uparrow J}{}_{(.,j)}(k,0_{n-r}) = h^{\uparrow J}(k,j) = rep(h(0_r,j))(k,0_{n-r})$$

we obtain

$$h^{\uparrow J}{}_{(.,j)} = rep(h(0_r,j)).$$

Thus,

$$\langle h^{\uparrow J}{}_{(.,j)} \rangle_J = \langle rep(h(0_r,j)) \rangle_J.$$

As $\langle rep(C) \rangle_J = C$ for all $C \in K[x_1,\ldots,x_r]/_J$,

$$\langle rep(h(0_r,j)) \rangle_J = h(0_r,j) = h(i,j).$$

Therefore, *(1)* is proven.

Let $i \in N^r$ and $j \in N^{n-r}$.

$$(f^{\downarrow J})^{\uparrow J}(i,j) = rep(f^{\downarrow J}(0_r,j))(i,0_{n-r}) = rep(\langle f_{(.,j)} \rangle_J)(i,0_{n-r}).$$

As f is in normal form modulo G,

$$rep(\langle f_{(.,j)} \rangle_J) = f_{(.,j)}.$$

Thus,

$$rep(\langle f_{(.,j)} \rangle_J)(i,0_{n-r}) = f_{(.,j)}(i,0_{n-r}) = f(i,j). \;\bullet$$

Let $r \in \{1,\ldots,n-1\}$, P a zero-dimensional prime ideal in $K[x_1,\ldots,x_n]$, and $b \in V(P_{/x_r})$.

As there exists an isomorphism h from $K[x_1,\ldots,x_r]/_{P_{/x_r}}[x_{r+1},\ldots,x_n]$ to $K(b)[x_{r+1},\ldots,x_n]$ with $h(f^{\downarrow P_{/x_r}}) = \overline{f(b)}$ for every $f \in K[x_1,\ldots,x_n]$, we can restate the Structure Theorem of the previous section.

Theorem 25 *The set $G \subseteq K[x_1, \ldots, x_n]$ is a reduced Gröbner basis of a zero-dimensional prime ideal in $K[x_1, \ldots, x_n]$*

iff

G satisfies the following three conditions:

1. *For every m there exists just one polynomial $f_m \in G$ that belongs to $K[x_1, \ldots, x_m]$ but not to $K[x_1, \ldots, x_{m-1}]$.*
2. *The polynomial $f_l{}^{\downarrow Ideal_{K,l-1}(\{f_1,\ldots,f_{l-1}\})}$ is irreducible in $K[x_1, \ldots, x_{l-1}]/_{Ideal_{K,l-1}(\{f_1, \ldots, f_{l-1}\})}[x_l]$ for every l. Furthermore, f_1 is irreducible in $K[x_1]$.*
3. *$lc(f_m) = 1$ and f_m is in normal form modulo $G \setminus \{f_m\}$ for every m.*

The correctness of Algorithm 8 mainly relies on this result, for which a different proof can be found in [10].

Algorithm 8

input: G, a reduced Gröbner basis such that I is a zero-dimensional ideal, where $I := Ideal_{K,n}(G)$.

output: X_n, such that $X_n = \{(f_1{}^1, \ldots, f_n{}^1), \ldots, (f_1{}^r, \ldots, f_n{}^r)\}$ and $\{f_1{}^s, \ldots, f_n{}^s\}$ is the reduced Gröbner basis of a prime ideal P_s that is associated with I for every $s \in \{1, \ldots, r\}$. Furthermore, if P' is a prime ideal associated with I then there exists an $s \in \{1, \ldots, r\}$ such that $\{f_1{}^s, \ldots, f_n{}^s\}$ is the reduced Gröbner basis of P'.

```
$X_1 := \{\, (f) \mid f$ is an irreducible factor of $G_{1,1}$ in $K[x_1]$ and $lc(f) = 1\,\}$
$for\ r := 1\ to\ n-1\ do$
    $X_{r+1} := \emptyset$
    $for\ all\ (f_1, \ldots, f_r) \in X_r\ do$
        $min_{(f_1,\ldots,f_r)} := \min\{\, s \mid s \in \{1, \ldots, car_{r+1}\}$ and $lc(G_{r+1,s})$ does
                              not reduce to zero modulo $\{f_1, \ldots, f_r\}\,\}$
        $h := G_{r+1, min_{(f_1,\ldots,f_r)}}$
        $IF_{(f_1,\ldots,f_r)} := \{\, f \mid f$ is an irreducible factor of $h^{\downarrow J}$ in
                              $K[x_1, \ldots, x_r]/_J[x_{r+1}]$ and $lc(f) = 1\,\}$,
                              where $J := Ideal_{K,r}(\{f_1, \ldots, f_r\})$.
        $X_{r+1} := X_{r+1} \cup \{\, (f_1, \ldots, f_r, f^{\uparrow J}) \mid f \in IF_{(f_1,\ldots,f_r)}\,\}$
```

Proof of Correctness

We want to show for every m that

(1) *for every $(f_1, \ldots, f_m) \in X_m$:*

$\{f_1, \ldots, f_m\}$ is the reduced Gröbner basis of a zero-dimensional prime ideal in $K[x_1, \ldots, x_m]$ that is associated with $I_{/x_m}$,

(2) *for every prime ideal P' in $K[x_1, \ldots, x_m]$ that is associated with $I_{/x_m}$:*
there exists an element $(f_1, \ldots, f_m)$ in X_m such that $\{f_1, \ldots, f_m\}$ is the reduced Gröbner basis of P'.

If $m = 1$ then (1) and (2) are obviously satisfied.

We assume that $m < n$ and (1) and (2) holds for m.

Let $(f_1, \ldots, f_{m+1}) \in X_{m+1}$ and $f \in IF_{(f_1,\ldots,f_m)}$ such that $f^{\uparrow J} = f_{m+1}$, where $J := Ideal_{K,m}(\{f_1, \ldots, f_m\})$ and $IF_{(f_1,\ldots,f_m)}$ is defined as in Algorithm 8.
As f is irreducible in $K[x_1, \ldots, x_m]_{/J}[x_{m+1}]$,

$$f_{m+1} \in K[x_1, \ldots, x_{m+1}] \setminus K[x_1, \ldots, x_m]. \tag{6.1}$$

By Lemma 16,

$$f = {f_{m+1}}^{\downarrow J}.$$

Thus,

$${f_{m+1}}^{\downarrow J} \textit{ is irreducible in } K[x_1, \ldots, x_m]_{/J}[x_{m+1}]. \tag{6.2}$$

Next, we want to prove that

$$lc(f_{m+1}) = 1.$$

Let $k \in N^{n-m}$ such that

$$f_{(.,k)} = lc(f).$$

From

$$\max\{\, r \mid r \in \{1, \ldots, n\} \text{ and } deg(f, r) > 0 \,\} = m + 1 =$$
$$= \max\{\, r \mid r \in \{1, \ldots, n\} \text{ and } deg(f_{m+1}, r) > 0 \,\}$$

and

$$deg(f, m+1) = deg(f_{m+1}, m+1)$$

we obtain

$$f_{m+1(.,k)} = lc(f_{m+1}).$$

Let $i \in N^m$.
As $lc(f_{m+1}) \in K[x_1, \ldots, x_m]$, $rep((lc(f))(0_n)) \in K[x_1, \ldots, x_m]$, and

$$(lc(f_{m+1}))(i, 0_{n-m}) = f_{m+1(.,k)}(i, 0_{n-m}) = f_{m+1}(i, k) = f^{\uparrow J}(i, k) =$$

$$= rep(f(0_m, k))(i, 0_{n-m}) = rep(f_{(.,k)}(0_n))(i, 0_{n-m}) = rep((lc(f))(0_n))(i, 0_{n-m}).$$

it follows that

$$1 = rep(\langle 1 \rangle_J) = rep((lc(f))(0_n)) = lc(f_{m+1}). \tag{6.3}$$

As $f_{m+1} = f^{\uparrow J}$,

$$f_{m+1} \textit{ is reduced modulo } \{f_1, \ldots, f_m\}. \tag{6.4}$$

Thus, by (6.1), (6.2), (6.3), (6.4), and Theorem 25, $\{f_1, \ldots, f_{m+1}\}$ is the reduced Gröbner basis of a zero-dimensional prime ideal P in $K[x_1, \ldots, x_{m+1}]$.

Now we want to prove that P is associated with $I_{/x_{m+1}}$.

As $I_{/x_{m+1}}$ is zero-dimensional, it suffices to show that

$$I_{/x_{m+1}} \subseteq P.$$

Let $b \in V(P_{/x_m})$.

As b is a generic zero of the prime ideal $P_{/x_m}$,

$$\overline{f(b)} = 0_p \text{ iff } f \text{ reduces to zero modulo } \{f_1, \ldots, f_m\}$$

for all $f \in K[x_1, \ldots, x_m]$. Thus,

$$min_b = min_{(f_1, \ldots, f_m)},$$

where $min_{(f_1, \ldots, f_m)}$ is defined as in Algorithm 8.

Let $g \in I_{/x_{m+1}}$.

By Theorem 20,

$$h^{\downarrow P_{/x_m}} \text{ divides } g^{\downarrow P_{/x_m}},$$

where $h := G_{m+1, min_{(f_1, \ldots, f_m)}}$.

As ${f_{m+1}}^{\downarrow P_{/x_m}}$ divides $h^{\downarrow P_{/x_m}}$, there exist $q_1, q_2 \in K[x_1, \ldots, x_{m+1}]$ such that

$$g = q_1 \cdot f_{m+1} + q_2 \text{ and } q_2 \in P_{/x_m}.$$

Thus,

$$g \in P.$$

It remains to show that (2) *holds for $m + 1$.*

Let P' be a prime ideal in $K[x_1, \ldots, x_{m+1}]$ associated with $I_{/x_{m+1}}$.

By Theorem 25, the reduced Gröbner basis of P' consists of $m + 1$ polynomials $f_1, \ldots, f_{m+1}$ such that

$$f_s \in K[x_1, \ldots, x_s] \setminus K[x_1, \ldots, x_{s-1}] \text{ for every } s \in \{1, \ldots, m+1\}.$$

By Lemma 6, $P'_{/x_m}$ is a prime ideal in $K[x_1, \ldots, x_m]$. As P' is associated with $I_{/x_{m+1}}$, $P'_{/x_m}$ is associated with $I_{/x_m}$. Thus,

$$(f_1, \ldots, f_m) \in X_m,$$

because $\{f_1, \ldots, f_m\}$ is the reduced Gröbner basis of $P'_{/x_m}$.

Let $h := G_{m+1,min_{(f_1,\dots,f_m)}}$.
As $h \in Ideal_{K,m+1}(\{f_1,\cdots,f_{m+1}\})$,

$$f_{m+1}{}^{\downarrow P'_{/x_m}} \text{ divides } h^{\downarrow P'_{/x_m}}.$$

By Theorem 25,

$$f_{m+1}{}^{\downarrow P'_{/x_m}} \text{ is irreducible in } K[x_1,\dots,x_m]/_{P'_{/x_m}}[x_{m+1}]$$

$$\text{and } lc(f_{m+1}) = 1.$$

Therefore,

$$lc(f_{m+1}{}^{\downarrow P'_{/x_m}}) = 1.$$

Thus,

$$f_{m+1}{}^{\downarrow P'_{/x_m}} \in IF_{(f_1,\dots,f_m)} \text{ and}$$

$$(f_1,\dots,f_m,(f_{m+1}{}^{\downarrow P'_{/x_m}})^{\uparrow P'_{/x_m}}) \in X_{m+1}.$$

As f_{m+1} is reduced modulo $\{f_1,\dots,f_m\}$, by Lemma 16,

$$f_{m+1} = (f_{m+1}{}^{\downarrow P'_{/x_m}})^{\uparrow P'_{/x_m}}. \quad \bullet$$

Example 16 We take the reduced Gröbner basis $G := \{G_{1,1}, G_{2,1}, G_{2,2}\} \subseteq Q[x,y]$, where

$$\begin{aligned} G_{1,1} &:= x^3 - x^2 - 2x + 2, \\ G_{2,1} &:= xy - y - x^2 + x, \\ G_{2,2} &:= y^3 - xy^2 + y - x \end{aligned}$$

as input for Algorithm 8.

The polynomials $x^2 - 2$ and $x - 1$ are the normed and irreducible factors of $x^3 - x^2 - 2x + 2$.

$X_1 := \{(x^2 - 2), (x - 1)\}$.

We set

$r := 1$,
$X_2 := \emptyset$,

and choose $(x^2 - 2) \in X_1$.

for $(x^2 - 2)$ do.

As $x - 1$, the leading coefficient of $G_{2,1}$, does not reduce to zero modulo $\{x^2 - 2\}$,

$min_{(x^2-2)} := 1,$
$h := xy - y - x^2 + x.$

The polynomial $\langle 1\rangle_J \cdot y + \langle -x\rangle_J$ is the only normed and irreducible factor of the polynomial $\langle x-1\rangle_J \cdot y + \langle -x^2 + x\rangle_J$, where J is the ideal in $Q[x]$ generated by $\{x^2-2\}$.

$IF_{(x^2-2)} := \{\langle 1\rangle_J \cdot y + \langle -x\rangle_J\}.$

As 1 is the representant of $\langle 1\rangle_J$ and $-x$ is the representant of $\langle -x\rangle_J$,

$X_2 := \{(x^2-2, y-x)\}.$

Now we take $(x-1)$, the other element of X_1.

for $(x-1)$ do.

As $x-1$, the leading coefficient of the polynomial $G_{2,1}$, reduces to zero modulo $\{x-1\}$,

$min_{(x-1)} := 2,$
$h := y^3 - xy^2 + y - x.$

The polynomials $y + \langle -x\rangle_J$ and $y^2 + \langle 1\rangle_J$ are the normed and irreducible factors of $y^3 + \langle -x\rangle_J \cdot y^2 + y + \langle -x\rangle_J$, where J is the ideal in $Q[x]$ generated by $\{x-1\}$.

$IF_{(x-1)} := \{y + \langle -x\rangle_J, y^2 + \langle 1\rangle_J\}.$

As -1 is the representant of $\langle -x\rangle_J$ and 1 is the representant of $\langle 1\rangle_J$,

$X_2 := \{(x^2-2, y-x), (x-1, y-1), (x-1, y^2+1)\}.$

Thus,

$$\{x^2-2, y-x\},$$
$$\{x-1, y-1\},$$
$$\{x-1, y^2+1\}$$

are the reduced Gröbner bases of the prime ideals P_1, P_2, P_3 that are associated with the ideal generated by G. •

6.3 Applications

Why are we interested in the associated ideals $P_1, \ldots, P_r$ of a given zero-dimensional ideal I?

One reason is that, by Theorem 3,

$$V(I) = V(P_1) \cup \ldots \cup V(P_r).$$

Thus, we can solve Problem 2 in the following way:

Given: *F, a finite subset of $K[x_1, \ldots, x_n]$ such that I is zero-dimensional, where $I := Ideal_{K,n}(F)$.*

Find: *V(I).*

Method:

We compute $G := GB(F)$.

Instead of solving the system G, we compute $G_1, \ldots, G_r$, the reduced Gröbner bases of the ideals $P_1, \ldots, P_r$ that are associated with I.

By solving the systems $G_1, \ldots, G_r$ we obtain the solutions of the system F.

This method derives advantage from the fact that, in general, it is much easier to solve the systems $G_1, \ldots, G_r$ than to solve the system G.

Example 17 We consider the reduced Gröbner basis $G := \{G_{1,1}, G_{2,1}, G_{2,2}\} \subseteq Q[x, y]$ again, where

$$\begin{aligned} G_{1,1} &:= x^3 - x^2 - 2x + 2, \\ G_{2,1} &:= xy - y - x^2 + x, \\ G_{2,2} &:= y^3 - xy^2 + y - x, \end{aligned}$$

which we have already used in the previous example. We have shown that

$$\begin{gathered} \{x^2 - 2, y - x\}, \\ \{x - 1, y - 1\}, \\ \{x - 1, y^2 + 1\}. \end{gathered}$$

are the reduced Gröbner bases of the ideals that are associated with the ideal generated by G. Intuitively, it seems to be easier to solve each of the systems

$$\begin{array}{rclcrclcrcl} x^2 - 2 &=& 0 & \quad & x - 1 &=& 0 & \quad & x - 1 &=& 0 \\ y - x &=& 0 & & y - 1 &=& 0 & & y^2 + 1 &=& 0 \end{array}$$

than to solve the system

$$\begin{aligned} x^3 - x^2 - 2x + 2 &= 0 \\ xy - y - x^2 + x &= 0 \\ y^3 - xy^2 + y - x &= 0. \quad \bullet \end{aligned}$$

Theorem 26 immediately leads to another application of Algorithm 8.

Theorem 26 *Let I be a zero-dimensional ideal in $K[x_1, \ldots, x_n]$ and $P_1, \ldots, P_r$ the prime ideals that are associated with I. Then*

$$\sqrt{I} = P_1 \cap \ldots \cap P_r.$$

Proof: Let $f \in K[x_1, \ldots, x_n]$.

By Hilbert's Nullstellensatz,

$$f \in \sqrt{I}$$

$$\text{iff}$$

$$\overline{f(b)} = 0_p \text{ for all } b \in V(I).$$

By Theorem 3,

$$V(I) = V(P_1) \cup \ldots \cup V(P_r).$$

Thus,

$$\overline{f(b)} = 0_p \text{ for all } b \in V(I).$$

$$\text{iff}$$

$$\overline{f(b)} = 0_p \text{ for all } b \in V(P_1) \cup \ldots \cup V(P_r).$$

Let $s \in \{1, \ldots, r\}$ and $b \in V(P_s)$.

As b is a generic zero of P_s,

$$\overline{f(b)} = 0_p \text{ implies } f \in P_s.$$

Therefore,

$$\overline{f(b)} = 0_p \text{ for all } b \in V(P_1) \cup \ldots \cup V(P_r)$$

$$\text{iff}$$

$$f \in P_1 \cap \ldots \cap P_r. \quad \bullet$$

Thus, we can solve Problem 3 in the following way:

Given: *g, a polynomial in* $K[x_1, \ldots, x_n]$, *and*

F, a finite subset of $K[x_1, \ldots, x_n]$ *such that I is zero-dimensional, where* $I := Ideal_{K,n}(F)$.

Decide: *whether*

$$\overline{g(b)} = 0_p \textit{ for all } b \in V(I),$$

or in other words, whether

$$g \in \sqrt{I}.$$

Method:

We compute $G := GB(F)$.

By using Algorithm 8 we compute $G_1, \ldots, G_r$, the reduced Gröbner bases of the ideals $P_1, \ldots, P_r$ that are associated with $Ideal_{K,n}(G)$.

We reduce g to its normal forms g_s modulo G_s for every $s \in \{1, \ldots, r\}$.

$$\text{The polynomial } g \text{ is an element of } \sqrt{I}$$

$$\text{iff}$$

$$g_s = 0_p \text{ for every } s \in \{1, \ldots, r\}.$$

Example 18 We consider the reduced Gröbner basis $G := \{G_{1,1}, G_{2,1}, G_{2,2}\} \subseteq Q[x,y]$ and $f, g \in Q[x,y]$, where

$$\begin{aligned} f &:= -2xy + 2y + x^4 - x^3, \\ g &:= y^2 - xy - y + x, \\ G_{1,1} &:= x^3 - x^2 - 2x + 2, \\ G_{2,1} &:= xy - y - x^2 + x, \\ G_{2,2} &:= y^3 - xy^2 + y - x. \end{aligned}$$

We have shown that

$$\begin{gathered} \{x^2 - 2, y - x\}, \\ \{x - 1, y - 1\}, \\ \{x - 1, y^2 + 1\} \end{gathered}$$

are the reduced Gröbner bases of the ideals that are associated with the ideal generated by G. As f reduces to zero modulo each of these Gröbner bases, f is an element of the radical of the ideal generated by G.

On the contrary, $-2y$ is the normal form of g modulo $\{x - 1, y^2 + 1\}$. Therefore, g is not in the radical of the ideal generated by G. •

Problem 3 can also be solved by adapting Rabinowitsch's method of proving Hilbert's Nullstellensatz.

Finally, we want to mention a last application.

It is well-known that there exist algorithms that satisfy the following specification (see, for example, [13]):

input: $F, G_1, \ldots, G_r$, finite subsets of $K[x_1, \ldots, x_n]$ such that $Ideal_{K,n}(F)$ is zero-dimensional and $Ideal_{K,n}(G_1), \ldots, Ideal_{K,n}(G_r)$ are the prime ideals that are associated with $Ideal_{K,n}(F)$.

output: $H_1, \ldots, H_r$, finite subsets of $K[x_1, \ldots, x_n]$ such that

$$Ideal_{K,n}(F) = Ideal_{K,n}(H_1) \cap \ldots \cap Ideal_{K,n}(H_r)$$

is a reduced primary decomposition of $Ideal_{K,n}(F)$.

Thus, we can solve Problem 4 in the following way:

Given: *F, a finite subset of $K[x_1, \ldots, x_n]$ such that I is zero-dimensional, where $I := Ideal_{K,n}(F)$.*

Find: *$H_1, \ldots, H_r$, finite subsets of $K[x_1, \ldots, x_n]$ such that*

$$I = Ideal_{K,n}(H_1) \cap \ldots \cap Ideal_{K,n}(H_r)$$

is a reduced primary decomposition of I.

Method:

We compute $G := GB(F)$.

By means of Algorithm 8 we compute $G_1, \ldots, G_r$, the reduced Gröbner bases of the ideals $P_1, \ldots, P_r$ that are associated with $Ideal_{K,n}(G)$.

We use the sets $F, G_1, \ldots, G_r$ as input for an algorithm that meets the above specification and obtain finite subsets $H_1, \ldots, H_r$ of $K[x_1, \ldots, x_n]$ such that

$$I = Ideal_{K,n}(H_1) \cap \ldots \cap Ideal_{K,n}(H_r)$$

is a reduced primary decomposition of I.

Index

Bibliography

[1] G. M. Bergman: *The Diamond Lemma for Ring Theory*, Advances in Math., vol. 29, 178-218 (1978)

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

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

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

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

[6] 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. 184-232 (1985)

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

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

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

[10] A. Kandri-Rody: *Effective Methods in the Theory of Polynomial Ideals*, Ph.D. Thesis, Rensselaer Polytechnic Institute, Troy, New York (1984)

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

[12] D. Lazard: *Ideal Bases and Primary Decomposition: Case of Two Variables*, J. of Symbolic Computation 1, 261-270 (1985)

[13] R. Schrader: *Zur konstruktiven Idealtheorie*, Diploma Thesis, Univ. Karlsruhe (FRG) (1976)

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

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