A Generalized Euclidean Algorithm for Computing Triangular Representations of Algebraic Varieties

MICHAEL KALKBRENER[†]

Research Institute for Symbolic Computation, Univ. Linz, Austria

We present an algorithm that computes an unmixed-dimensional decomposition of an arbitrary algebraic variety V. Each V_i in the decomposition $V = V_1 \cup \ldots \cup V_m$ is given by a finite set of polynomials which represents the generic points of the irreducible components of V_i. The basic operation in our algorithm is the computation of greatest common divisors of univariate polynomials over extension fields. No factorization is needed.

Some of the main problems in polynomial ideal theory can be solved by means of our algorithm: we show how the dimension of an ideal can be computed, systems of algebraic equations can be solved, and radical membership can be decided.

Our algorithm has been implemented in the computer algebra system MAPLE. Timings on well-known examples from computer algebra literature are given.

1. Introduction

Algebraic varieties are usually represented as sets of common zeros of finitely many polynomials. In addition to this common method we use a different representation in this paper, which is a generalization of a concept in Ritt (1950). Since every irreducible variety is uniquely determined by one of its generic points (see van der Waerden (1967), p.160 and p.161) we represent varieties by representing the generic points of their irreducible components. These generic points are given by certain finite sets of polynomials, so-called regular chains.

In this paper we present an algorithm that computes an unmixed-dimensional decomposition of an arbitrary variety V given as the set of common zeros of finitely many multivariate polynomials over a field. Every unmixed-dimensional variety V_i in the decomposition $V = V_1 \cup \ldots \cup V_m$ is given by a regular chain which represents the generic points of the irreducible components of V_i.

We have introduced the concept of regular chains in our Ph.D. thesis (Kalkbrener, 1991). It has been independently defined in Yang & Zhang (1991). Regular chains are a

[†] A large part of this work has been done during our stay at FUJITSU's International Institute for Advanced Study of Social Information Science in Numazu, Japan. This work has been supported by the Austrian Fonds zur Förderung der wissenschaftlichen Forschung, project no. P6763, the Austrian Ministry of Science, project ESPRIT BRA 3125 "MEDLAR", and the U.S. Army Research Office through the ACSyAM branch of the Mathematical Sciences Institute of Cornell University, Contract DAAL03-91-C-0027.

generalization of Ritt's irreducible ascending sets (see Ritt, 1950). The main difference between these two concepts is that no irreducibility condition is imposed on regular chains. Therefore, regular chains represent unmixed-dimensional varieties instead of irreducible varieties, and no factorization is required to compute them.

In Wu (1986) a modified version of Ritt's decomposition algorithm is presented. Recently Gao and Chou proved that the coarse form decomposition algorithm in Wu (1986), which does not use polynomial factorization either, computes unmixed-dimensional decompositions of varieties (Gao & Chou, 1991).

Regular chains are also similar to triangular sets, a concept introduced by D. Lazard. In Lazard (1992) triangular sets are used for solving zero-dimensional systems of algebraic equations. Without giving a correctness proof, D. Lazard generalized this algorithm to systems of arbitrary dimension in Lazard (1991). Furthermore, the definition of triangular sets given in Lazard (1992) is strengthened in Lazard (1991) in order to guarantee that different triangular sets represent different varieties. Regular chains do not have this "canonical representation" property. Compared to the definition of triangular sets given in Lazard (1991), the definition of regular chains is simpler and more general. Our whole algorithm has a rather simple structure and is easy to implement. Recently, an implementation has been done in MAPLE V.

The basic operation in our algorithm is the computation of greatest common divisors of univariate polynomials over extension fields given by regular chains. Our strategy for computing in these extension fields is similar to the one for computing in algebraic extension fields suggested in Della Dora et al. (1985) and implemented in Scratchpad under the name **D5** (see Dicrescenzo & Duval, 1988).

In Section 2 we introduce the concept of regular chains and state more formally the problem we are concerned with. In Section 3 we show that if a variety is represented by regular chains then it is easy to determine its dimension, to compute the generic points of its irreducible components, and to decide radical membership. In Section 4 algorithms are developed for computing in extension fields given by regular chains. In particular, we present an algorithm for computing the greatest common divisor of univariate polynomials over extension fields given by regular chains. In Section 5 we give an algorithmic solution based on this gcd algorithm for the problem stated in Section 2. In Section 6 timings on well-known examples from computer algebra literature are presented. The termination and correctness of every algorithm presented in this paper are proved in Section 7 or Section 8.

2. Definitions

2.1. BASIC DEFINITIONS

Throughout the paper let K be a field and $\bar{K}$ an algebraically closed field which has infinite transcendence degree over K (a so-called universal domain).

Let F be a subset of $K[x_1, \ldots, x_n]$. If F is a finite set then we denote the number of elements in F by $|F|$. $V_n(F)$ denotes the variety of F in $\bar{K}^n$, i.e. the set

$$\{a \in \bar{K}^n \mid f(a) = 0 \text{ for every } f \in F\}.$$

A variety in $\bar{K}^n$ is any subset of $\bar{K}^n$ which is the variety of some subset of $K[x_1, \ldots, x_n]$. An element a of a variety V in $\bar{K}^n$ is a generic point of V (over K) if for every $f \in$

$K[x_1, \ldots, x_n]$:

$$f(a) = 0 \quad \text{implies} \quad f(b) = 0 \ \text{ for every } b \in V.$$

If $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ are two generic points of V then there exists a K-isomorphism h of the extension field $K(a_1, \ldots, a_n)$ onto the extension field $K(b_1, \ldots, b_n)$ such that $h(a_i) = b_i$ for every $i \in \{1, \ldots, n\}$ (see van der Waerden (1967), p.160). It is well-known (see, for instance, van der Waerden (1967), p.159 and p.161) that every element of $\bar{K}^n$ is a generic point of an irreducible variety and that a variety is irreducible if and only if it has a generic point. The dimension of V is denoted by $dim(V)$. Let

$$f = \sum_{i=0}^{d} q_i(x_1, \ldots, x_{n-1}) x_n^i$$

be a polynomial in $K[x_1, \ldots, x_n]$ with $q_d \neq 0$. The polynomial q_d is called the leading coefficient of f with respect to x_n, abbreviated $lc_n(f)$. The degree of f in x_n is denoted by $deg_n(f)$. Furthermore, we define $deg_n(0) := -1$. For non-zero $f_1, f_2 \in K[x_1, \ldots, x_n]$ the pseudoremainder and pseudoquotient with respect to x_n are denoted by $prem_n(f_1, f_2)$ and $pquo_n(f_1, f_2)$. The monic gcd of the polynomials in F is denoted by $gcd(F)$ for every finite subset F of $K[x_1, \ldots, x_n]$ with $F \neq \{0\}$. Furthermore, we define $gcd(\{0\}) := 0$.

If there is no danger of confusion we sometimes drop the subscript.

2.2. REGULAR CHAINS

Varieties are usually represented as sets of common zeros of finitely many polynomials. In addition to this common method we use a different representation in this paper, which is a generalization of a concept in Ritt (1950). Since every irreducible variety in $\bar{K}^n$ is uniquely determined by one of its generic points we represent varieties by representing the generic points of their irreducible components. These generic points are given by certain subsets of $K[x_1, \ldots, x_n]$, so-called regular chains in $K[x_1, \ldots, x_n]$. The set of generic points in $\bar{K}^n$ given by a regular chain R is called the set of regular zeros of R. Every set of regular zeros of a regular chain R contains all generic points of a finite number of irreducible varieties $V_1, \ldots, V_r$. The variety $V_1 \cup \ldots \cup V_r$ is said to be represented by R.

We now give a formal inductive definition of regular chains and regular zeros of regular chains:

Let n be 0. The empty set is the only regular chain in K and the set $\bar{K}^0$ which contains the empty list only is called the set of regular zeros of $\emptyset$, abbreviated $RZ_0(\emptyset)$.

Let n be a natural number. A subset R of the polynomial ring $K[x_1, \ldots, x_n]$ is a regular chain in $K[x_1, \ldots, x_n]$ if

(1) $R \cap K[x_1, \ldots, x_{n-1}]$ is a regular chain in $K[x_1, \ldots, x_{n-1}]$,
(2) $R - K[x_1, \ldots, x_{n-1}]$ has at most one element, and
(3) if there exists an f in $R - K[x_1, \ldots, x_{n-1}]$ then $lc_n(f)(a_1, \ldots, a_{n-1}) \neq 0$ for every element $(a_1, \ldots, a_{n-1})$ of the set of regular zeros of $R \cap K[x_1, \ldots, x_{n-1}]$.

Let R be a regular chain in $K[x_1, \ldots, x_n]$ and RZ the set of regular zeros of $R \cap K[x_1, \ldots, x_{n-1}]$. If $R \subseteq K[x_1, \ldots, x_{n-1}]$ then the set

$$\{(a_1, \ldots, a_n) \mid (a_1, \ldots, a_{n-1}) \in RZ,\ a_n \in \bar{K} \text{ is transcendental over } K(a_1, \ldots, a_{n-1})\}$$

is called the set of regular zeros of R. If there exists an $f \in R - K[x_1, \ldots, x_{n-1}]$ then

$$\{(a_1, \ldots, a_n) \mid (a_1, \ldots, a_{n-1}) \in RZ,\ a_n \in \bar{K},\ \text{and}\ f(a_1, \ldots, a_n) = 0\}$$

is called the set of regular zeros of R. The set of regular zeros of R is denoted by $RZ_n(R)$. It is clear from the definition that $RZ_n(R)$ is not empty for every regular chain R in $K[x_1, \ldots, x_n]$.

EXAMPLE 2.1. Let Q denote the rational numbers and let

$$\begin{array}{lcl} R_1 & := & \{x_2^2 - x_1^2,\ x_3,\ x_3 + 1\}, \\ R_2 & := & \{x_2^2 - x_1^2,\ (x_2 - x_1)x_3\}, \\ R_3 & := & \{x_2^2 - x_1^2,\ x_3 - x_1\}, \\ R_4 & := & \{x_2^2 - x_1^2,\ x_2(x_3 - x_1)\}. \end{array}$$

R_1 is not a regular chain in $Q[x_1, x_2, x_3]$ because two of the elements are in $Q[x_1, x_2, x_3] - Q[x_1, x_2]$. Obviously, $\{x_2^2 - x_1^2\}$ is a regular chain in $Q[x_1, x_2]$ and $RZ_2(\{x_2^2 - x_1^2\})$ is the set

$$\{(a, a) \mid a \in \bar{Q}\ \text{transcendental over}\ Q\} \cup \{(a, -a) \mid a \in \bar{Q}\ \text{transcendental over}\ Q\}.$$

Since $lc_3((x_2 - x_1)x_3)(a, a) = 0$ for (a, a) in $RZ_2(\{x_2^2 - x_1^2\})$, R_2 is not a regular chain. R_3 and R_4 are regular chains and $RZ_3(R_3)$ and $RZ_3(R_4)$ are the set

$$\{(a, a, a) \mid a \in \bar{Q}\ \text{transcendental over}\ Q\} \cup \{(a, -a, a) \mid a \in \bar{Q}\ \text{transcendental over}\ Q\}.$$

Note that $(0, 0, a)$ is a common zero of the polynomials in R_4, but it is not in $RZ_3(R_4)$. □

Let n be a natural number. If R is a regular chain in $K[x_1, \ldots, x_n]$ then the set

$$\{V \mid V\ \text{is an irreducible variety in}\ \bar{K}^n\ \text{with a generic point in}\ RZ_n(R)\}$$

is called the set of irreducible varieties associated with R, abbreviated $AIV_n(R)$. Note that $AIV_n(\emptyset) = \{\bar{K}^n\}$. Therefore, we define $AIV_0(\emptyset) := \{\bar{K}^0\}$. For every non-negative integer n and every regular chain R in $K[x_1, \ldots, x_n]$ the variety

$$\bigcup_{V \in AIV_n(R)} V$$

is said to be represented by R and is denoted by $Rep_n(R)$. Note that every generic point of a variety $V \in AIV_n(R)$ is in $RZ_n(R)$.

EXAMPLE 2.2. Let R_3 and R_4 be defined as in Example 2.1. Obviously, $AIV_3(R_3)$ and $AIV_3(R_4)$ contain the two irreducible varieties $V(\{x_2 + x_1,\ x_3 - x_1\})$ and $V(\{x_2 - x_1,\ x_3 - x_1\})$. Hence, R_3 and R_4 represent the variety $V(\{x_2^2 - x_1^2,\ x_3 - x_1\})$. □

Regular chains can be considered as a generalization of Ritt's irreducible ascending sets (Ritt, 1950; Wu, 1984). Every irreducible ascending set in $K[x_1, \ldots, x_n]$ represents exactly one irreducible variety in $\bar{K}^n$. Since we have dropped the condition of irreducibility, a finite number of irreducible varieties is given by a regular chain. This is also true for triangular sets. Instead of the Condition 3 in our definition of regular chains, five other conditions are imposed on triangular sets in Lazard (1991) in order to make every polynomial in a triangular set monic, primitive and squarefree in a rather technical sense.

2.3. THE PROBLEM

In this paper we are concerned with the development of an algorithm that solves the following problem:

Given: $F = \{f_1, \ldots, f_k\}$, a finite, non-empty subset of $K[x_1, \ldots, x_n]$.
Find: $M = \{R_1, \ldots, R_l\}$, a (possibly empty) set of regular chains in $K[x_1, \ldots, x_n]$ such that

$$V_n(F) = \bigcup_{i=1}^{l} Rep_n(R_i).$$

Some of the main problems in polynomial ideal theory can be easily solved if we are able to represent arbitrary varieties by means of regular chains. In the following section we show how the dimension of an ideal can be computed, systems of algebraic equations can be solved, and radical membership can be decided. Several other algorithms for solving these problems have been developed and implemented during the last years. Many of them are based on Gröbner bases (Buchberger, 1965; 1985) or characteristic set computations (Ritt, 1950). See, for instance, Kredel & Weispfenning (1988), Wu (1986), Gao & Chou (1991) for computing dimensions of ideals, Buchberger (1985), Wu (1986) for solving systems of algebraic equations and Kapur (1986), Ritt (1950) for deciding radical membership.

3. Properties of Regular Chains

In this section let $F = \{f_1, \ldots, f_k\}$ be a finite subset of $K[x_1, \ldots, x_n]$ and $M = \{R_1, \ldots, R_l\}$ a (possibly empty) set of regular chains in $K[x_1, \ldots, x_n]$ such that

$$V_n(F) = \bigcup_{i=1}^{l} Rep_n(R_i).$$

Note that

$$\bigcup_{i=1}^{l} Rep_n(R_i) = \emptyset \quad \text{iff} \quad M = \emptyset. \tag{3.1}$$

3.1. COMPUTING THE DIMENSION OF AN IDEAL

THEOREM 3.1. *Let R be a regular chain in $K[x_1, \ldots, x_n]$. Then $Rep_n(R)$ is unmixed-dimensional and*

$$dim(Rep_n(R)) = n - |R|.$$

PROOF. By definition,

$$Rep_n(R) = \bigcup_{V \in AIV_n(R)} V.$$

Let $V \in AIV_n(R)$ and $(a_1, \ldots, a_n) \in RZ_n(R)$ a generic point of V. By definition

of $RZ_n(R)$, the transcendence degree of $K(a_1, \ldots, a_n)$ is $n - |R|$. Hence, $Rep_n(R)$ is unmixed-dimensional and

$$dim(Rep_n(R)) = n - |R|. \quad \square$$

We obtain from (3.1) and the previous theorem that

$$dim(V(F)) = -1 \quad \text{iff} \quad M = \emptyset, \tag{3.2}$$

$$dim(V(F)) = n - min(|R_1|, \ldots, |R_l|) \quad \text{iff} \quad M \neq \emptyset. \tag{3.3}$$

Since the ideal I generated by F has the same dimension as $V(F)$ we can use (3.2) and (3.3) for determining the dimension of I as well.

3.2. SOLVING SYSTEMS OF ALGEBRAIC EQUATIONS

First of all, we can decide whether the system

$$f_1 = 0, \ldots, f_k = 0 \tag{3.4}$$

has no, finitely many, or infinitely many solutions: it is an easy consequence of (3.2) and (3.3) that

system (3.4) has no solutions	iff	$M = \emptyset$,
(3.4) has finitely many solutions	iff	$M \neq \emptyset$ and $\|R_i\| = n$ for every $i \in \{1, \ldots, l\}$,
(3.4) has infinitely many solutions	iff	there exists an $R \in M$ with $\|R\| < n$.

By definition,

$$V_n(F) = \bigcup_{i=1}^{l} Rep_n(R_i)$$

and for every $i \in \{1, \ldots, l\}$ $RZ_n(R_i)$ is the subset of $Rep_n(R_i)$ that contains those elements that are generic points of one of the irreducible varieties associated with R_i. We know from (van der Waerden (1967), p.162) that if $Rep_n(R_i)$ has only finitely many elements then

$$Rep_n(R_i) = RZ_n(R_i).$$

Each of the sets $RZ_n(R_1), \ldots, RZ_n(R_l)$ can be computed by "successive substitution".

EXAMPLE 3.1. We consider the following system of algebraic equations due to Arnborg and Davenport:

$$f_1 := x_1 + x_2 + x_3 + x_4, \qquad f_2 := x_1x_2 + x_2x_3 + x_3x_4 + x_4x_1,$$
$$f_3 := x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_1 + x_4x_1x_2, \quad f_4 := x_1x_2x_3x_4 - 1.$$

Using the algorithm **solve** in Section 5 we can represent every variety by a finite number of regular chains. In this example the variety $V_4(\{f_1, f_2, f_3, f_4\})$ can be represented by a single regular chain:

$$V_4(\{f_1, f_2, f_3, f_4\}) = Rep_4(R), \quad \text{where } R := \{\, x_1^2x_2^2 - 1,\ x_3 + x_1,\ x_4 + x_2 \,\}.$$

Since R contains 3 elements, the variety is unmixed one-dimensional. The polynomial

$x_1^2x_2^2 - 1$ can be factored into $x_1x_2 - 1$ and $x_1x_2 + 1$. Therefore, $RZ_2(\{x_1^2x_2^2 - 1\})$ is the set

$$\{(a, 1/a) \mid a \in \bar{Q} \text{ transcendental over } Q\} \cup \{(a, -1/a) \mid a \in \bar{Q} \text{ transcendental over } Q\}.$$

In this example we easily obtain by successive substitution that

$$\begin{aligned} RZ_4(R) \quad = \quad & \{(a, 1/a, -a, -1/a) \mid a \in \bar{Q} \text{ transcendental over } Q\} \cup \\ & \{(a, -1/a, -a, 1/a) \mid a \in \bar{Q} \text{ transcendental over } Q\}. \end{aligned}$$ □

3.3. DECIDING RADICAL MEMBERSHIP

In the following section we develop an algorithm called $\mathbf{separate}_n$ that satisfies the following specification:

Input: R, a regular chain in $K[x_1, \ldots, x_n]$,
g, a polynomial in $K[x_1, \ldots, x_n]$.
Output: O, a set of regular chains in $K[x_1, \ldots, x_n]$ such that

$$\{a \in RZ_n(R) \mid g(a) \neq 0\} = \bigcup_{R' \in O} RZ_n(R').$$

By means of $\mathbf{separate}_n$ we can easily decide radical membership. Let J be the radical of the ideal generated by F and g a polynomial in $K[x_1, \ldots, x_n]$. Obviously,

g is an element of J
iff
g vanishes on $V(F)$
iff
for every $i \in \{1, \ldots, l\}$ $\mathbf{separate}_n(R_i, g) = \emptyset$.

4. Computing Modulo Regular Chains

Before we can present an algorithmic solution of the problem in Subsection 2.3, we have to develop algorithms for computing in extension fields given by regular chains. Our strategy for computing in these extension fields is similar to the one for computing in algebraic extension fields suggested in Della Dora et al. (1985) and implemented in Scratchpad under the name **D5** (see Dicrescenzo & Duval, 1988). By means of the following example we illustrate the basic idea behind this method.

EXAMPLE 4.1. Let us assume that we want to decide for every zero a of the polynomial $x^6 - 10x^4 + 31x^2 - 30$ whether $a^2 - 3 = 0$.

One possible strategy is to decompose $x^6 - 10x^4 + 31x^2 - 30$ into its irreducible factors $x^2 - 2$, $x^2 - 3$, $x^2 - 5$ and to decide this question for each of the extension fields $Q[x]_{/x^2-2}$, $Q[x]_{/x^2-3}$, $Q[x]_{/x^2-5}$ separately.

Obviously, factorization can be replaced by gcd computations in this example: since

$$\begin{gathered} gcd(x^6 - 10x^4 + 31x^2 - 30, x^2 - 3) = x^2 - 3, \\ x^6 - 10x^4 + 31x^2 - 30 = (x^2 - 3)(x^4 - 7x^2 + 10), \\ \text{and } x^4 - 7x^2 + 10 \text{ and } x^2 - 3 \text{ are relatively prime} \end{gathered}$$

we know that

$$\begin{array}{lll} a^2-3=0 & \text{iff} & a \text{ is a zero of } x^2-3, \\ a^2-3\neq 0 & \text{iff} & a \text{ is a zero of } x^4-7x^2+10. \ \square \end{array}$$

For using this "splitting on demand"-strategy we need for every natural number n two algorithms called $\mathbf{common}_n$ and $\mathbf{separate}_n$ that satisfy the following specifications:

$\mathbf{common}_n$ (in: R, g; out: O)

Input: R, a regular chain in $K[x_1,\ldots,x_n]$,
g, a polynomial in $K[x_1,\ldots,x_n]$.
Output: O, a set of regular chains in $K[x_1,\ldots,x_n]$ such that

$$\{a \in RZ_n(R) \mid g(a)=0\} = \bigcup_{R'\in O} RZ_n(R').$$

$\mathbf{separate}_n$ (in: R, g; out: O)

Input: R, a regular chain in $K[x_1,\ldots,x_n]$,
g, a polynomial in $K[x_1,\ldots,x_n]$.
Output: O, a set of regular chains in $K[x_1,\ldots,x_n]$ such that

$$\{a \in RZ_n(R) \mid g(a)\neq 0\} = \bigcup_{R'\in O} RZ_n(R').$$

EXAMPLE 4.2. Let R be the regular chain $\{x_2^2+x_1^2, x_3^2-x_1x_3-x_3+x_1\}$ in $Q[x_1,x_2,x_3]$. For which (a_1,a_2,a_3) in $RZ_3(R)$ is $a_1^2a_2^{-2}+a_3$ equal to 0?

This problem can be easily solved by means of **common** and **separate**. First we check whether a_2^{-1} exists for every (a_1,a_2,a_3) in $RZ_3(R)$: by computing $\mathbf{common}_3(R,x_2)$ we obtain as output the empty set. Therefore, $a_2\neq 0$ and a_2^{-1} exists for every $(a_1,a_2,a_3)\in RZ_3(R)$. By computing $\mathbf{common}_3(R,x_1^2+x_3x_2^2)$ respectively $\mathbf{separate}_3(R,x_1^2+x_3x_2^2)$ we obtain as output set $\{x_2^2+x_1^2, x_1^2+x_3x_2^2\}$ respectively $\{x_2^2+x_1^2, x_2^2x_3-x_2^2x_1-x_2^2-x_1^2\}$. Therefore,

$$\begin{array}{lll} a_1^2a_2^{-2}+a_3=0 & \text{iff} & (a_1,a_2,a_3) \text{ is an element of } RZ_3(R'), \\ a_1^2a_2^{-2}+a_3\neq 0 & \text{iff} & (a_1,a_2,a_3) \text{ is an element of } RZ_3(R''), \end{array}$$

where $R' := \{x_2^2+x_1^2, x_1^2+x_3x_2^2\}$ and $R'' := \{x_2^2+x_1^2, x_2^2x_3-x_2^2x_1-x_2^2-x_1^2\}$. $\square$

In Example 4.1 we have found two factors of the polynomial $x^6-10x^4+31x^2-30$ by a gcd computation. A general gcd algorithm also is the core of **common** and **separate** and plays a crucial role in the algorithm in the next section which solves the problem stated in Subsection 2.3.

We define for every natural number n an algorithm named $\mathbf{ggcd}_n$ (= generalized greatest common divisor) that satisfies the following specification.

ggcd$_n$(in: R, F; out: O)

Input: R, a regular chain in $K[x_1, \ldots, x_{n-1}]$,
F, a finite, non-empty subset of $K[x_1, \ldots, x_n]$.
Output: O, where $O = \{(R_1, g_1), \ldots, (R_l, g_l)\}$ and $R_1, \ldots, R_l$ are regular chains in $K[x_1, \ldots, x_{n-1}]$ and $g_1, \ldots, g_l$ are polynomials in $K[x_1, \ldots, x_n]$ with

(1) $RZ_{n-1}(R) = RZ_{n-1}(R_1) \cup \ldots \cup RZ_{n-1}(R_l)$,
(2) for every $i \in \{1, \ldots, l\}$ and every $a = (a_1, \ldots, a_{n-1}) \in RZ(R_i)$:
   (a) if $g_i \neq 0$ then $lc(g_i)(a) \neq 0$,
   (b) $g_i(a, x_n)$ is the gcd of the polynomials in $\{f(a, x_n) \mid f \in F\}$ (up to a multiplicative constant),
(3) for every $i \in \{1, \ldots, l\}$:
   g_i vanishes on $Rep_n(R_i) \cap V_n(F)$.

We will do the construction of these algorithms by induction.

Induction basis: Construction of **ggcd**$_1$.

Obviously, the simple algorithm

$O := \{(\emptyset, gcd(F))\}$

satisfies the above specification.

Induction step: Construction of **ggcd**$_{n+1}$.

By means of **ggcd**$_n$ we construct the algorithms **common**$_n$ and **separate**$_n$ first.

common$_n$ (in: R, g; out: O)

Input: R, a regular chain in $K[x_1, \ldots, x_n]$,
g, a polynomial in $K[x_1, \ldots, x_n]$.
Output: O, a set of regular chains in $K[x_1, \ldots, x_n]$ such that

$$\{a \in RZ_n(R) \mid g(a) = 0\} = \bigcup_{R' \in O} RZ_n(R').$$

$\{(S_1, g_1), \ldots, (S_r, g_r)\} :=$ **ggcd**$_n(R \cap K[x_1, \ldots, x_{n-1}], R - K[x_1, \ldots, x_{n-1}] \cup \{g\})$
if $R - K[x_1, \ldots, x_{n-1}] = \emptyset$
then
  $O := \{S_j \mid j \in \{1, \ldots, r\}$ and $g_j = 0\}$
else
  $O := \{S_j \cup \{g_j\} \mid j \in \{1, \ldots, r\}$ and $g_j \notin K[x_1, \ldots, x_{n-1}]\}$

separate$_n$ (in: R, g; out: O)

Input: R, a regular chain in $K[x_1, \ldots, x_n]$,
g, a polynomial in $K[x_1, \ldots, x_n]$.
Output: O, a set of regular chains in $K[x_1, \ldots, x_n]$ such that

$$\{a \in RZ_n(R) \mid g(a) \neq 0\} = \bigcup_{R' \in O} RZ_n(R').$$

$\{(S_1, g_1), \ldots, (S_r, g_r)\} := \mathbf{ggcd}_n(R \cap K[x_1, \ldots, x_{n-1}], R - K[x_1, \ldots, x_{n-1}] \cup \{g\})$
if $R - K[x_1, \ldots, x_{n-1}] = \emptyset$
then
$O := \{S_j \mid j \in \{1, \ldots, r\} \text{ and } g_j \neq 0\}$
else
$f :=$ the only element in $R - K[x_1, \ldots, x_{n-1}]$
$J := \{j \in \{1, \ldots, r\} \mid g_j \notin K[x_1, \ldots, x_{n-1}] \text{ and } deg_n(g_j) < deg_n(f)\}$
$O := \{S_j \cup \{f\} \mid j \in \{1, \ldots, r\} \text{ and } g_j \in K[x_1, \ldots, x_{n-1}]\} \cup$
$\bigcup_{j \in J} \mathbf{separate}_n(S_j \cup \{pquo(f, g_j)\}, g)$

Now we are in the position to define $\mathbf{ggcd}_{n+1}$:

if $|F - \{0\}| \geq 2$ **or** there exists a non-zero $g \in F$ and an $a \in RZ_n(R)$ such that
$lc_{n+1}(g)(a) = 0$
then
$f :=$ a non-zero element in F with minimal degree in x_{n+1}
$F' := F - \{f\}$
$M' := \mathbf{common}_n(R, lc_{n+1}(f))$
$M'' := \mathbf{separate}_n(R, lc_{n+1}(f))$
$f' := f - lc(f) \cdot x_{n+1}^{deg_{n+1}(f)}$
$F'' := \{prem_{n+1}(g, f) \mid g \in F'\}$
$O := \bigcup_{S' \in M'} \mathbf{ggcd}_{n+1}(S', F' \cup \{f'\}) \cup \bigcup_{S'' \in M''} \mathbf{ggcd}_{n+1}(S'', F'' \cup \{f\})$
else
if there exists a non-zero $f \in F$
then
$O := \{(R, f)\}$
else
$O := \{(R, 0)\}$

The termination and correctness of the algorithms presented in this section is proved in Section 7.

Example 4.3. Let us compute the gcd of $x_2^2 + x_1$ and $x_1 x_2 + x_1^2$ modulo $x_1^4 - x_1^3$, i.e. let us compute

$$\mathbf{ggcd}_2(\{x_1^4 - x_1^3\}, \{x_2^2 + x_1, x_1 x_2 + x_1^2\}).$$

First we want to divide $x_2^2 + x_1$ by $x_1x_2 + x_1^2$. Since the leading coefficient of $x_1x_2 + x_1^2$ is x_1 and

$$\mathbf{common}_1(\{x_1^4 - x_1^3\}, x_1) = \{\{x_1\}\} \text{ and } \mathbf{separate}_1(\{x_1^4 - x_1^3\}, x_1) = \{\{x_1 - 1\}\}$$

we split the computation into two independent parts: We compute

$$\mathbf{ggcd}_2(\{x_1\}, \{x_2^2 + x_1, x_1^2\}),$$

where x_1^2 has been obtained by computing $(x_1x_2 + x_1^2) - lc_2(x_1x_2 + x_1^2) \cdot x_2$, and we compute

$$\mathbf{ggcd}_2(\{x_1 - 1\}, \{x_1x_2 + x_1^2, x_1^4 + x_1^3\}),$$

where $x_1^4 + x_1^3$ is the pseudoremainder of $x_2^2 + x_1$ and $x_1x_2 + x_1^2$.

Computation of $\mathbf{ggcd}_2(\{x_1\}, \{x_2^2 + x_1, x_1^2\})$:

From

$$lc_2(x_1^2) = x_1^2, \ \mathbf{common}_1(\{x_1\}, x_1^2) = \{\{x_1\}\}, \text{ and } \mathbf{separate}_1(\{x_1\}, x_1^2) = \emptyset$$

we obtain

$$\mathbf{ggcd}_2(\{x_1\}, \{x_2^2 + x_1, x_1^2\}) = \mathbf{ggcd}_2(\{x_1\}, \{x_2^2 + x_1, 0\}).$$

Since the leading coefficient of $x_2^2 + x_1$ does not vanish if x_1 is replaced by 0, which is the only element in $RZ_1(\{x_1\})$,

$$\mathbf{ggcd}_2(\{x_1\}, \{x_2^2 + x_1, 0\}) = \{(\{x_1\}, x_2^2 + x_1)\}.$$

Computation of $\mathbf{ggcd}_2(\{x_1 - 1\}, \{x_1x_2 + x_1^2, x_1^4 + x_1^3\})$:

From

$$lc_2(x_1^4 + x_1^3) = x_1^4 + x_1^3, \ \mathbf{common}_1(\{x_1 - 1\}, x_1^4 + x_1^3) = \emptyset,$$

$$\mathbf{separate}_1(\{x_1 - 1\}, x_1^4 + x_1^3) = \{\{x_1 - 1\}\}$$

and the fact that the pseudoremainder of $x_1x_2 + x_1^2$ and $x_1^4 + x_1^3$ with respect to x_2 is 0 we obtain

$$\mathbf{ggcd}_2(\{x_1 - 1\}, \{x_1x_2 + x_1^2, x_1^4 + x_1^3\}) = \mathbf{ggcd}_2(\{x_1 - 1\}, \{x_1^4 + x_1^3, 0\}).$$

Since $lc_2(x_1^4 + x_1^3)$ does not vanish if x_1 is replaced by 1, which is the only element in $RZ_1(\{x_1 - 1\})$,

$$\mathbf{ggcd}_2(\{x_1 - 1\}, \{x_1^4 + x_1^3, 0\}) = \{(\{x_1 - 1\}, x_1^4 + x_1^3)\}.$$

Altogether,

$$\mathbf{ggcd}_2(\{x_1^4 - x_1^3\}, \{x_2^2 + x_1, x_1x_2 + x_1^2\}) = \{(\{x_1\}, x_2^2 + x_1), (\{x_1 - 1\}, x_1^4 + x_1^3)\}. \ \square$$

5. Computing Regular Chains

The objective of this section is to show how the algorithm **ggcd** can be used for solving the problem stated in Subsection 2.3.

Let n be a non-negative integer. We define a partial ordering on the elements of $\bar{K}^n$.

Let $a := (a_1, \ldots, a_n)$ and $b := (b_1, \ldots, b_n)$ be elements of $\bar{K}^n$. Then a is smaller than b, written $a \prec b$, if there exists an $i \in \{1, \ldots, n\}$ such that for every $j \in \{1, \ldots, i-1\}$

$$K(a_1, \ldots, a_j) \text{ and } K(b_1, \ldots, b_j) \text{ have the same transcendence degree (over } K)$$
$$\text{and } K(a_1, \ldots, a_i) \text{ has a smaller transcendence degree than } K(b_1, \ldots, b_i).$$

(Strictly speaking, not $\prec$ but the relation $\preceq$ is a partial ordering, where $a \preceq b$ if $a \prec b$ or $a = b$.) If neither $a \prec b$ nor $b \prec a$ then a and b are similar, denoted by $a \sim b$.

Obviously, the following lemma holds.

LEMMA 5.1. *Let R be a regular chain in $K[x_1, \ldots, x_n]$ and $a, b \in RZ_n(R)$. Then*

$$a \sim b.$$

Because of this result we can define the following two relations on regular chains. Let R and S be two regular chains in $K[x_1, \ldots, x_n]$, $a \in RZ_n(R)$, and $b \in RZ_n(S)$. Then

$$R \prec S \quad \text{iff} \quad a \prec b$$

and

$$R \sim S \quad \text{iff} \quad a \sim b.$$

Another obvious result is stated in Lemma 5.2.

LEMMA 5.2. *There do not exist infinitely many regular chains $R_1, R_2, \ldots$ in $K[x_1, \ldots, x_n]$ such that*

$$R_1 \succ R_2 \succ \ldots$$

We will construct for every natural number n an algorithm named $\mathbf{solve}_n$ that satisfies the following specification.

$\mathbf{solve}_n$ (in: R, F; out: O)

Input: R, a regular chain in $K[x_1, \ldots, x_{n-1}]$,
F, a non-empty, finite subset of $K[x_1, \ldots, x_n]$.
Output: O, a set of regular chains in $K[x_1, \ldots, x_n]$ such that

(1) for every $R' \in O$, every $a \in RZ_{n-1}(R' \cap K[x_1, \ldots, x_{n-1}])$ and every $b \in RZ_{n-1}(R)$:
$a \in RZ_{n-1}(R)$ or $a \prec b$,
(2)

$$Rep_n(R) \cap V_n(F) \subseteq \bigcup_{R' \in O} Rep_n(R') \subseteq V_n(F).$$

Again we will do the construction of these algorithms by induction.

Induction basis: Construction of $\mathbf{solve}_1$.

Obviously, the simple algorithm

if $gcd(F) = 1$
then
$O := \emptyset$
else
$O := \{\{gcd(F)\} - \{0\}\}$

satisfies the above specification.

Induction step: Construction of $\mathbf{solve}_n$, where $n > 1$.

$\{(S_1, g_1), \ldots, (S_l, g_l)\} := \mathbf{ggcd}_n(R, F)$
$J := \{i \in \{1, \ldots, l\} \mid g_i \neq 0\}$
$M := \bigcup_{j \in J} \mathbf{solve}_{n-1}(S_j \cap K[x_1, \ldots, x_{n-2}], S_j - K[x_1, \ldots, x_{n-2}] \cup \{lc_n(g_j)\})$
$O := \{S_i \mid i \in \{1, \ldots, l\},\ i \notin J\} \cup$
$\{S_j \cup \{g_j\} \mid j \in J,\ g_j \notin K[x_1, \ldots, x_{n-1}]\} \cup$
$\bigcup_{S \in M} \mathbf{solve}_n(S, F)$

The termination and correctness of this algorithm is proved in Section 8.

The following theorem states the solution of the problem we are concerned with.

THEOREM 5.1. *Let F be a non-empty, finite subset of $K[x_1, \ldots, x_n]$ and $\{R_1, \ldots, R_l\} := \mathbf{solve}_n(\emptyset, F)$. Then*

$$V_n(F) = \bigcup_{i=1}^{l} Rep_n(R_i).$$

PROOF. Since $Rep_n(\emptyset) = \bar{K}^n$, we obtain from the specification of $\mathbf{solve}_n$ that

$$V_n(F) = \bar{K}^n \cap V_n(F) \subseteq \bigcup_{i=1}^{l} Rep_n(R_i) \subseteq V_n(F). \quad \square$$

EXAMPLE 5.1. As an easy application of **solve** we compute a representation by regular chains of the variety $V_2(\{x_2^2 + x_1, x_1x_2 + x_1^2\})$.

Computation of $\mathbf{solve}_2(\emptyset, \{x_2^2 + x_1, x_1x_2 + x_1^2\})$:

$\{(S_1, g_1)\} := \mathbf{ggcd}_2(\emptyset, \{x_2^2 + x_1, x_1x_2 + x_1^2\}) = \{(\emptyset, x_1^4 + x_1^3)\}$,
$J := \{1\}$,
$M := \mathbf{solve}_1(\emptyset, \{x_1^4 + x_1^3\}) = \{\{x_1^4 + x_1^3\}\}$,
$O := \mathbf{solve}_2(\{x_1^4 + x_1^3\}, \{x_2^2 + x_1, x_1x_2 + x_1^2\})$.

Computation of $\mathbf{solve}_2(\{x_1^4 + x_1^3\}, \{x_2^2 + x_1, x_1x_2 + x_1^2\})$:

$\{(S_1, g_1), (S_2, g_2)\} := \mathbf{ggcd}_2(\{x_1^4 + x_1^3\}, \{x_2^2 + x_1, x_1x_2 + x_1^2\}) =$
$\{(\{x_1\}, x_2^2 + x_1), (\{x_1 + 1\}, x_1x_2 + x_1^2)\}$,

$J := \{1, 2\}$,

$M := \mathbf{solve}_1(\emptyset, \{x_1, 1\}) \cup \mathbf{solve}_1(\emptyset, \{x_1 + 1, x_1\}) = \emptyset$,

$O := \{\{x_1, x_2^2 + x_1\}, \{x_1 + 1, x_1 x_2 + x_1^2\}\}$.

Hence,

$$V_2(\{x_2^2 + x_1, x_1 x_2 + x_1^2\}) = Rep_2(\{x_1, x_2^2 + x_1\}) \cup Rep_2(\{x_1 + 1, x_1 x_2 + x_1^2\}). \quad \square$$

6. Examples and Computing Times

We have implemented **solve** in MAPLE V and have applied this algorithm to the following systems of algebraic equations that can be found in Böge et al. (1986) or Czapor & Geddes (1986).

(1) Trinks' system: 6 equations, 6 variables (see Böge et al., 1986) with
   (a) ordering $w > p > z > t > s > b$ (see Problem 1(a) in Czapor (1989) or Problem 1 in Czapor & Geddes (1986)),
   (b) ordering $w > b > p > z > s > t$ (see Problem 1(b) in Czapor (1989)),
   (c) ordering $b > t > s > w > p > z$ (see Problem 1(c) in Czapor (1989)).

(2) Katsura's system: 5 equations, 5 variables (see Böge et al., 1986) with
   (a) ordering $u_4 > u_2 > u_0 > u_3 > u_1$ (see Problem 2(a) in Czapor (1989)),
   (b) ordering $u_4 > u_0 > u_3 > u_2 > u_1$ (see Problem 2(b) in Czapor (1989) or Problem 4(b) in Czapor & Geddes (1986)).

(3) Rose's system: 3 equations, 3 variables (see Böge et al., 1986) with ordering $u_4 > u_3 > a_{46}$ (see Problem 3 in Czapor (1989)).

(4) Problem 2 in Czapor & Geddes (1986): 3 equations, 3 variables with ordering $x > y > z$.

(5) Fee's system: 4 equations, 5 variables (see Czapor & Geddes, 1986) with
   (a) substitution $b = 2$ and ordering $q > c > p > d$ (see Problem 5(a) in Czapor & Geddes (1986)),
   (b) ordering $q > c > p > d$ and parameter b (see Problem 5(b) in Czapor & Geddes (1986)),
   (c) ordering $c > d > q > b > p$ (see Problem 4 in Czapor (1989)).

(6) Problem 7 in Czapor & Geddes (1986): 2 equations, 2 variables, 9 parameters with ordering $x > y$.

(7) Problem 9 in Czapor & Geddes (1986): 3 equations, 3 variables, 9 parameters with
   (a) substitution $d = e = f = 0$ and ordering $x > y > z$ (see Problem 9(a) in Czapor & Geddes (1986)),
   (b) substitution $a = b = c = g = h = k = 1$ and ordering $x > y > z$ (see Problem 9(b) in Czapor & Geddes (1986)),
   (c) 9 free parameters and ordering $x > y > z$.

All computations have been done on a Sun Sparcstation 2. The computing times are given in seconds. We have compared **solve** with the Gröbner bases implementation **gbasis** in MAPLE V. The times in parentheses are the computing times of **gbasis** with respect to the lexicographical ordering.

Computing times of **solve**

	1(**a**)	**1**(**b**)	**1**(**c**)	**2**(**a**)	**2**(**b**)	**3**	**4**
solve :	26	615	10843	194	> 20000	301	10
gbasis :	(7)	(178)	(1070)	(90)	(1597)	(16550)	(10)

	5(**a**)	**5**(**b**)	**5**(**c**)	**6**	**7**(**a**)	**7**(**b**)	**7**(**c**)
solve :	3077	> 20000	> 20000	12	7	12	96
gbasis :	($\star$)	(> 20000)	(> 20000)	(20)	(30)	(7335)	(> 20000)

$\star$ error message from **gbasis**: degree of one of the intermediate polynomials too large.

Compared with the Gröbner bases implementation in MAPLE the current implementation of **solve** performs rather well in examples with at most three variables. In the case of more variables it seems to be extremely sensitive to the ordering of variables. In some of the examples very large intermediate polynomials have been computed. This seems to be the main reason for the bad performance in some of the examples with more than three variables. We intend to investigate the practical applicability of **solve** more carefully. In particular, a comparison with the algorithms of Ritt, Wu and Lazard seems to be interesting.

No complexity analysis of **solve** and its subalgorithms has been made. We think that such an analysis and a comparison with the complexity results in Giusti & Heintz (1990) is a challenging problem for future research.

7. Proofs of Termination and Correctness of the Algorithms in Section 4

Let n be a natural number and let us assume that $\mathbf{ggcd}_n$ terminates and satisfies its specification. Under this assumption we have to prove termination and correctness of $\mathbf{common}_n$, $\mathbf{separate}_n$, and $\mathbf{ggcd}_{n+1}$.

Proof of termination and correctness of $\mathbf{common}_n$*:*

Let R and g satisfy the input specification. Termination readily follows from the termination of $\mathbf{ggcd}_n$. By the specification of $\mathbf{ggcd}_n$ and the definition of the output set O, every element of O is a regular chain in $K[x_1, \ldots, x_n]$. Let $a = (a_1, \ldots, a_n)$ be an element of $\bar{K}^n$.

Case: $R - K[x_1, \ldots, x_{n-1}] = \emptyset$.

$$
\begin{gathered}
a \in \bigcup_{R' \in O} RZ_n(R') \\
\text{iff} \\
\text{there exists a } j \in \{1, \ldots, r\} \text{ with } g_j = 0 \text{ and } a \in RZ_n(S_j) \\
\text{iff} \\
\text{there exists a } j \in \{1, \ldots, r\} \text{ with } g_j(a_1, \ldots, a_{n-1}, x_n) = 0, \\
(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(S_j), \text{and } a_n \text{ is transcendental over } K(a_1, \ldots, a_{n-1}) \\
\text{iff} \\
\text{there exists a } j \in \{1, \ldots, r\} \text{ with } (a_1, \ldots, a_{n-1}) \in RZ_{n-1}(S_j), \\
a_n \text{ is transcendental over } K(a_1, \ldots, a_{n-1}), \text{ and } g(a_1, \ldots, a_{n-1}, x_n) = 0 \\
\text{iff} \\
(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(R \cap K[x_1, \ldots, x_{n-1}]), \\
a_n \text{ is transcendental over } K(a_1, \ldots, a_{n-1}), \text{ and } g(a) = 0 \\
\text{iff} \\
a \in RZ_n(R) \text{ and } g(a) = 0.
\end{gathered}
$$

Case: $R - K[x_1, \ldots, x_{n-1}] \neq \emptyset$.

Let us denote the element of $R - K[x_1, \ldots, x_{n-1}]$ by f.

$$
\begin{gathered}
a \in \bigcup_{R' \in O} RZ_n(R') \\
\text{iff} \\
\text{there exists a } j \in \{1, \ldots, r\} \text{ with } g_j \notin K[x_1, \ldots, x_{n-1}] \text{ and } a \in RZ_n(S_j \cup \{g_j\}) \\
\text{iff} \\
\text{there exists a } j \in \{1, \ldots, r\} \text{ with } g_j \notin K[x_1, \ldots, x_{n-1}], \\
(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(S_j), \text{and } g_j(a) = 0 \\
\text{iff} \\
(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(R \cap K[x_1, \ldots, x_{n-1}]) \text{ and } f(a) = g(a) = 0 \\
\text{iff} \\
a \in RZ_n(R) \text{ and } g(a) = 0. \quad \square
\end{gathered}
$$

Proof of termination and correctness of $\mathbf{separate}_n$*:*

Let R and g satisfy the input specification and let $a = (a_1, \ldots, a_n)$ be an element of $\bar{K}^n$.

Case: $R - K[x_1, \ldots, x_{n-1}] = \emptyset$.

In this case termination readily follows from the termination of $\mathbf{ggcd}_n$. By the specification of $\mathbf{ggcd}_n$ and the definition of the output set O, every element of O is a regular chain in $K[x_1, \ldots, x_n]$.

$$
\begin{gathered}
a \in \bigcup_{R' \in O} RZ_n(R') \\
\text{iff} \\
\text{there exists a } j \in \{1, \ldots, r\} \text{ with } g_j \neq 0 \text{ and } a \in RZ_n(S_j) \\
\text{iff} \\
\text{there exists a } j \in \{1, \ldots, r\} \text{ with } g_j \neq 0, (a_1, \ldots, a_{n-1}) \in RZ_{n-1}(S_j), \\
\text{and } a_n \text{ is transcendental over } K(a_1, \ldots, a_{n-1}) \\
\text{iff}
\end{gathered}
$$

$$\begin{gathered}\text{there exists a } j \in \{1,\ldots,r\} \text{ with } g_j(a_1,\ldots,a_{n-1},x_n) \neq 0,\\ (a_1,\ldots,a_{n-1}) \in RZ_{n-1}(S_j), \text{and } a_n \text{ is transcendental over } K(a_1,\ldots,a_{n-1})\\ \text{iff}\\ \text{there exists a } j \in \{1,\ldots,r\} \text{ with } (a_1,\ldots,a_{n-1}) \in RZ_{n-1}(S_j),\\ a_n \text{ is transcendental over } K(a_1,\ldots,a_{n-1}), \text{ and } g(a_1,\ldots,a_{n-1},x_n) \neq 0\\ \text{iff}\\ (a_1,\ldots,a_{n-1}) \in RZ_{n-1}(R \cap K[x_1,\ldots,x_{n-1}]),\\ a_n \text{ is transcendental over } K(a_1,\ldots,a_{n-1}), \text{ and } g(a) \neq 0\\ \text{iff}\\ a \in RZ_n(R) \text{ and } g(a) \neq 0.\end{gathered}$$

Case: $R - K[x_1,\ldots,x_{n-1}] \neq \emptyset$.

We will prove termination and correctness by induction on the degree of the only element f in $R - K[x_1,\ldots,x_{n-1}]$.

Induction basis: $deg_n(f) = 1$.

As there does not exist a $j \in \{1,\ldots,r\}$ with $0 < deg_n(g_j) < deg_n(f) = 1$ we know that $J = \emptyset$. Thus, $\mathbf{separate}_n$ terminates. Obviously, every element of O is a regular chain in $K[x_1,\ldots,x_n]$. Since $deg_n(f) = 1$,

$$\begin{gathered}a \in \textstyle\bigcup_{R' \in O} RZ_n(R')\\ \text{iff}\\ \text{there exists a } j \in \{1,\ldots,r\} \text{ with } g_j \in K[x_1,\ldots,x_{n-1}] \text{ and } a \in RZ_n(S_j \cup \{f\})\\ \text{iff}\\ \text{there exists a } j \in \{1,\ldots,r\} \text{ with } g_j \in K[x_1,\ldots,x_{n-1}],\\ (a_1,\ldots,a_{n-1}) \in RZ_{n-1}(S_j), f(a) = 0, \text{ and } f(a_1,\ldots,a_{n-1},x_n) \neq 0\\ \text{iff}\\ \text{there exists a } j \in \{1,\ldots,r\} \text{ with } g_j(a_1,\ldots,a_{n-1},x_n) \in \bar{K} - \{0\},\\ (a_1,\ldots,a_{n-1}) \in RZ_{n-1}(S_j), f(a) = 0, \text{ and } f(a_1,\ldots,a_{n-1},x_n) \neq 0\\ \text{iff}\\ \text{there exists a } j \in \{1,\ldots,r\} \text{ with } g_j(a) \neq 0, (a_1,\ldots,a_{n-1}) \in RZ_{n-1}(S_j),\\ f(a) = 0, \text{ and } f(a_1,\ldots,a_{n-1},x_n) \neq 0\\ \text{iff}\\ (a_1,\ldots,a_{n-1}) \in RZ_{n-1}(R \cap K[x_1,\ldots,x_{n-1}]),\\ f(a) = 0, \ f(a_1,\ldots,a_{n-1},x_n) \neq 0, \text{ and } g(a) \neq 0\\ \text{iff}\\ a \in RZ_n(R) \text{ and } g(a) \neq 0.\end{gathered}$$

Induction step: $deg_n(f) > 1$.

Obviously, $\mathbf{separate}_n$ terminates with input R and g if it terminates for every $j \in J$ with input $S_j \cup \{pquo(f,g_j)\}$ and g. Let $j \in J$ and q_j be the pseudoquotient of f and g_j. First we will show that $S_j \cup \{q_j\}$ is a regular chain in $K[x_1,\ldots,x_n]$. By specification of $\mathbf{ggcd}_n$, S_j is a regular chain in $K[x_1,\ldots,x_{n-1}]$. As $deg_n(g_j) < deg_n(f)$ and $deg_n(g_j) + deg_n(q_j) = deg_n(f)$,

$$q_j \notin K[x_1,\ldots,x_{n-1}]. \tag{7.1}$$

By definition of pseudodivision,

$$lc_n(q_j) = lc_n(g_j)^d \cdot lc_n(f),$$

where $d := deg_n(f) - deg_n(g_j)$. Therefore, for every $b \in RZ_{n-1}(S_j)$ we obtain from

$lc(g_j)(b) \neq 0$ and $lc(f)(b) \neq 0$ that $lc(q_j)(b) \neq 0$. Thus, $S_j \cup \{q_j\}$ is a regular chain in $K[x_1, \ldots, x_n]$. It follows from the definition of J that $g_j \notin K[x_1, \ldots, x_{n-1}]$ and therefore $deg_n(q_j) < deg_n(f)$. Hence, the termination of $\mathbf{separate}_n$ with input $S_j \cup \{q_j\}$ and g follows from the induction hypothesis. This completes the proof of termination.

We can deduce from the induction hypothesis that every element of the output set O is a regular chain in $K[x_1, \ldots, x_n]$. It remains to show that

$$\{a \in RZ_n(R) \mid g(a) \neq 0\} = \bigcup_{R' \in O} RZ_n(R').$$

$\supseteq$: Let $a \in \bigcup_{R' \in O} RZ_n(R')$. Then there exists

$$\text{a } j \in \{1, \ldots, r\} \text{ with } g_j \in K[x_1, \ldots, x_{n-1}] \text{ and } a \in RZ_n(S_j \cup \{f\}) \text{ or}$$
$$\text{a } j \in J \text{ and an } R_j \in O_j \text{ such that } a \in RZ_n(R_j),$$

where O_j denotes the output set of $\mathbf{separate}_n$ with input $S_j \cup \{pquo(f, g_j)\}$ and g. If there exists a $j \in \{1, \ldots, r\}$ with $g_j \in K[x_1, \ldots, x_{n-1}]$ and $a \in RZ_n(S_j \cup \{f\})$ then $a \in RZ_n(R)$ and $g(a) \neq 0$ can be shown by the same arguments as used in the induction basis. So let us assume that there exists a $j \in J$ and an $R_j \in O_j$ such that $a \in RZ_n(R_j)$. By induction hypothesis,

$$a \in RZ_n(S_j \cup \{pquo(f, g_j)\}) \text{ and } g(a) \neq 0.$$

Since $g_j(a_1, \ldots, a_{n-1}, x_n)$ divides $f(a_1, \ldots, a_{n-1}, x_n)$, $pquo(f, g_j)(a_1, \ldots, a_{n-1}, x_n)$ divides $f(a_1, \ldots, a_{n-1}, x_n)$ and therefore $f(a_1, \ldots, a_n) = 0$. Thus, $a \in RZ_n(R)$.

$\subseteq$: Let $a \in RZ_n(R)$ and $g(a) \neq 0$. Then, by the specification of $\mathbf{ggcd}_n$, there exists a $j \in \{1, \ldots, r\}$ such that $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(S_j)$. If $g_j \in K[x_1, \ldots, x_{n-1}]$ then $S_j \cup \{f\} \in O$ and therefore

$$a \in \bigcup_{R' \in O} RZ_n(R').$$

So let us assume that $g_j \notin K[x_1, \ldots, x_{n-1}]$. Since $g(a) \neq 0$, $f(a) = 0$, and the polynomial $g_j(a_1, \ldots, a_{n-1}, x_n)$ is the gcd of $f(a_1, \ldots, a_{n-1}, x_n)$ and $g(a_1, \ldots, a_{n-1}, x_n)$,

$$g_j(a) \neq 0 \text{ and } deg_n(g_j(a_1, \ldots, a_{n-1}, x_n)) < deg_n(f(a_1, \ldots, a_{n-1}, x_n)).$$

From $lc(g_j)(a_1, \ldots, a_{n-1}) \neq 0$ we obtain $deg_n(g_j) < deg_n(f)$. Hence, $j \in J$. Since $g_j(a_1, \ldots, a_{n-1}, x_n)$ divides $f(a_1, \ldots, a_{n-1}, x_n)$,

$$prem_n(f, g_j)(a_1, \ldots, a_{n-1}, x_n) = 0.$$

Together with $g_j(a) \neq 0$ and $f(a) = 0$ it follows that $pquo(f, g_j)(a) = 0$. Thus, $a \in RZ_n(S_j \cup \{pquo(f, g_j)\})$. From $g(a) \neq 0$ and the induction hypothesis we obtain

$$a \in \bigcup_{R' \in O} RZ_n(R'). \quad \square$$

Proof of termination and correctness of $\mathbf{ggcd}_{n+1}$*:*

Let G be a finite, non-empty subset of $K[x_1, \ldots, x_{n+1}]$. Then

$$sumdeg(G) := \sum_{g \in G} (deg_{n+1}(g) + 1).$$

Let R and F be sets which satisfy the input specification. We will prove termination and correctness by induction on $sumdeg(F)$.

Induction basis: $sumdeg(F) = 0$.

Then $F = \{0\}$ and termination and correctness are obvious.

Induction step: $sumdeg(F) > 0$.

Case: there exists exactly one non-zero $g \in F$ and $lc(g)(a) \neq 0$ for every $a \in RZ_n(R)$.

Again termination and correctness are obvious.

Case: $|F - \{0\}| \geq 2$ or there exists a non-zero $g \in F$ and an $a \in RZ_n(R)$ such that $lc(g)(a) = 0$.

It follows from the termination of $\mathbf{common}_n$ and $\mathbf{separate}_n$ that $\mathbf{ggcd}_{n+1}$ terminates with the input sets R and F if it terminates for every $S' \in M'$ with the input sets S' and $F' \cup \{f'\}$ and for every $S'' \in M''$ with the input sets S'' and $F'' \cup \{f\}$. Let $S' \in M'$. By definition of f',

$$sumdeg(F' \cup \{f'\}) = sumdeg(F') + deg(f') + 1 < sumdeg(F') + deg(f) + 1 = sumdeg(F).$$

By induction hypothesis, $\mathbf{ggcd}_{n+1}$ terminates with input $S', F' \cup \{f'\}$.

Let $S'' \in M''$. By specification of $\mathbf{separate}_n$, $lc(f)(a) \neq 0$ for every $a \in RZ_n(S'')$. Therefore, if $F'' \subseteq \{0\}$ then the termination of $\mathbf{ggcd}_{n+1}$ with input $S'', F'' \cup \{f\}$ is obvious. On the other hand, there exists a $g \in F'$ with $deg(g) \geq deg(f)$. Hence, $sumdeg(F'') < sumdeg(F')$ and therefore

$$sumdeg(F'' \cup \{f\}) < sumdeg(F' \cup \{f\}) = sumdeg(F).$$

By induction hypothesis, $\mathbf{ggcd}_{n+1}$ terminates with input $S'', F'' \cup \{f\}$. This completes the proof of termination.

We obtain from the induction hypothesis and the first case of the induction step that for every element (R', g') of O the set R' is a regular chain in $K[x_1, \ldots, x_n]$, g' is a polynomial in $K[x_1, \ldots, x_{n+1}]$, and condition 2(a) holds.

By the specifications of $\mathbf{common}_n$ and $\mathbf{separate}_n$,

$$RZ_n(R) = \bigcup_{S' \in M'} RZ_n(S') \cup \bigcup_{S'' \in M''} RZ_n(S'').$$

Therefore,

$$RZ_n(R) = \bigcup_{(R', g') \in O} RZ_n(R')$$

follows from the induction hypothesis and the first case of the induction step. Thus, it remains to prove conditions 2(b) and 3.

For the rest of the proof let (R', g') be an element of the output set O and let $a \in RZ_n(R')$.

Case: there exists an $S' \in M'$ with $(R', g') \in \mathbf{ggcd}_{n+1}(S', F' \cup \{f'\})$.

By induction hypothesis, $RZ_n(R') \subseteq RZ_n(S')$. From this and from $lc(f)(b) = 0$ for every $b \in RZ_n(S')$ we obtain $lc(f)(a) = 0$ and therefore $f'(a, x_{n+1}) = f(a, x_{n+1})$. Thus, condition 2(b) follows from the induction hypothesis. Since $lc(f)(a) = 0$, $lc(f)$ vanishes on $Rep_{n+1}(R')$. Therefore, f' vanishes on $Rep_{n+1}(R') \cap V_{n+1}(\{f\})$. By induction hypothesis, g' vanishes on $Rep_{n+1}(R') \cap V_{n+1}(F' \cup \{f'\})$. Hence, g' vanishes on $Rep_{n+1}(R') \cap V_{n+1}(F)$.

Case: there exists an $S'' \in M''$ with $(R', g') \in \mathbf{ggcd}_{n+1}(S'', F'' \cup \{f\})$.

By induction hypothesis and the first case of the induction step, $RZ_n(R') \subseteq RZ_n(S'')$. From this and from $lc(f)(b) \neq 0$ for every $b \in RZ_n(S'')$ we obtain $lc(f)(a) \neq 0$. Therefore, the polynomials in the set $\{h(a, x_{n+1}) \mid h \in F\}$ and the polynomials in the set $\{h(a, x_{n+1}) \mid h \in F'' \cup \{f\}\}$ have the same gcd. Thus, by induction hypothesis and the first case of the induction step, condition 2(b) is satisfied.

From the fact that every polynomial in F'' vanishes on $V_{n+1}(F)$, the induction hypothesis, and the first case of the induction step we can deduce condition 3. □

8. Proof of Termination and Correctness of the Algorithm in Section 5

Let n be a natural number greater than 1. We have to prove termination and correctness of $\mathbf{solve}_n$ under the assumption that $\mathbf{solve}_{n-1}$ terminates and satisfies its specification.

Proof of termination of $\mathbf{solve}_n$*:*

Let R and F satisfy the input specification. We will show that for every $S \in M$

$$S \prec R. \tag{8.1}$$

Let S be an arbitrary element in M. Then there exists a $j \in J$ such that

$$S \in \mathbf{solve}_{n-1}(S_j \cap K[x_1, \ldots, x_{n-2}], S_j - K[x_1, \ldots, x_{n-2}] \cup \{lc(g_j)\}).$$

Let $(a_1, \ldots, a_{n-1}) \in RZ(S)$ and $(b_1, \ldots, b_{n-1}) \in RZ(S_j)$. By specification of $\mathbf{ggcd}_n$,

$$(b_1, \ldots, b_{n-1}) \in RZ(R) \tag{8.2}$$

and by specification of $\mathbf{solve}_{n-1}$,

$$lc(g_j)(a_1, \ldots, a_{n-1}) = 0 \tag{8.3}$$

and

$$(a_1, \ldots, a_{n-2}) \in RZ(S_j \cap K[x_1, \ldots, x_{n-2}]) \text{ or } (a_1, \ldots, a_{n-2}) \prec (b_1, \ldots, b_{n-2}).$$

If $(a_1, \ldots, a_{n-2}) \prec (b_1, \ldots, b_{n-2})$ then, by definition of $\prec$, $(a_1, \ldots, a_{n-1}) \prec (b_1, \ldots, b_{n-1})$ and therefore, together with (8.2), $S \prec R$. Thus, let us assume that

$$(a_1, \ldots, a_{n-2}) \in RZ(S_j \cap K[x_1, \ldots, x_{n-2}]).$$

Case: There exists a polynomial f in $S_j - K[x_1, \ldots, x_{n-2}]$.

By specification of $\mathbf{solve}_{n-1}$, $f(a_1, \ldots, a_{n-1}) = 0$. Hence, $(a_1, \ldots, a_{n-1}) \in RZ(S_j)$ and therefore, by specification of $\mathbf{ggcd}_n$, $lc(g_j)(a_1, \ldots, a_{n-1}) \neq 0$. This is a contradiction to (8.3).

Case: $S_j - K[x_1, \ldots, x_{n-2}] = \emptyset$.

Since $(a_1, \ldots, a_{n-2}) \in RZ_{n-2}(S_j \cap K[x_1, \ldots, x_{n-2}])$,

$$(a_1, \ldots, a_{n-2}, a'_{n-1}) \in RZ_{n-1}(S_j),$$

where a'_{n-1} is transcendental over $K(a_1, \ldots, a_{n-2})$. Thus, $lc(g_j)(a_1, \ldots, a_{n-2}, a'_{n-1}) \neq 0$ and therefore $lc(g_j)(a_1, \ldots, a_{n-2}, x_{n-1}) \neq 0$. From this and (8.3) we obtain that a_{n-1} is algebraic over $K(a_1, \ldots, a_{n-2})$. On the other hand, b_{n-1} is transcendental over $K(b_1, \ldots, b_{n-2})$. We know from $(a_1, \ldots, a_{n-2}) \in RZ_{n-2}(S_j \cap K[x_1, \ldots, x_{n-2}])$ and Lemma

5.1 that $(a_1, \ldots, a_{n-2}) \sim (b_1, \ldots, b_{n-2})$. Thus, we can deduce that $(a_1, \ldots, a_{n-1}) \prec (b_1, \ldots, b_{n-1})$. By (8.2), $S \prec R$. This completes the proof of (8.1).

If $\mathbf{solve}_n$ does not terminate then an infinite sequence of regular chains $R, S, \ldots$ is generated such that $R \succ S \succ \ldots$ This is a contradiction to Lemma 5.2 and therefore $\mathbf{solve}_n$ terminates. □

In Lemma 8.1 a rather obvious property of regular chains is stated, which we need for proving the correctness of $\mathbf{solve}_n$.

LEMMA 8.1. *Let R be a regular chain in $K[x_1, \ldots, x_n]$. Then $(a_1, \ldots, a_n) \in Rep(R)$ implies $(a_1, \ldots, a_{n-1}) \in Rep(R \cap K[x_1, \ldots, x_{n-1}])$.*

PROOF. Let $(a_1, \ldots, a_n) \in Rep(R)$. Then there exists a $(b_1, \ldots, b_n) \in RZ(R)$ such that $(a_1, \ldots, a_n) \in V$, where V is the irreducible variety in $\bar{K}^n$ with $(b_1, \ldots, b_n)$ as generic point. By definition of regular chains, $(b_1, \ldots, b_{n-1})$ is an element of $RZ(R \cap K[x_1, \ldots, x_{n-1}])$. Since $f(b_1, \ldots, b_{n-1}) = 0$ implies $f(a_1, \ldots, a_{n-1}) = 0$ for every $f \in K[x_1, \ldots, x_{n-1}]$, $(a_1, \ldots, a_{n-1})$ is in the irreducible variety in $\bar{K}^{n-1}$ with generic point $(b_1, \ldots, b_{n-1})$. Therefore,

$$(a_1, \ldots, a_{n-1}) \in Rep(R \cap K[x_1, \ldots, x_{n-1}]). \square$$

The next lemma is of crucial importance for the correctness of the algorithm.

LEMMA 8.2. *Let V be an irreducible variety in $\bar{K}^{n-1}$ with $(b_1, \ldots, b_{n-1})$ as generic point, $(a_1, \ldots, a_n) \in \bar{K}^n$ such that $(a_1, \ldots, a_{n-1}) \in V$, and h a polynomial in $K[x_1, \ldots, x_n]$ with*

$$lc(h)(b_1, \ldots, b_{n-1}) \neq 0, \quad lc(h)(a_1, \ldots, a_{n-1}) \neq 0, \quad h(a_1, \ldots, a_n) = 0.$$

Then there exists a $b_n \in \bar{K}$ with

$$h(b_1, \ldots, b_n) = 0 \text{ and } (a_1, \ldots, a_n) \in V',$$

where V' is the irreducible variety in $\bar{K}^n$ with $(b_1, \ldots, b_n)$ as a generic point.

PROOF. As $lc(h)(a_1, \ldots, a_{n-1}) \neq 0$ and $h(a_1, \ldots, a_n) = 0$, $h \notin K[x_1, \ldots, x_{n-1}]$. As $lc(h)(b_1, \ldots, b_{n-1}) \neq 0$ it follows that there exist finitely many distinct zeros $c_1, \ldots, c_k$ of the univariate polynomial $h(b_1, \ldots, b_{n-1}, x_n)$.

Let f be a polynomial in $K[x_1, \ldots, x_n]$ with $f(b_1, \ldots, b_{n-1}, c_i) = 0$ for every $i \in \{1, \ldots, k\}$. Obviously, there exists a natural number l such that $h(b_1, \ldots, b_{n-1}, x_n)$ divides the polynomial $f(b_1, \ldots, b_{n-1}, x_n)^l$.

Let r be the pseudoremainder and q the pseudoquotient of f^l and h with respect to x_n. Obviously, $r(b_1, \ldots, b_{n-1}, x_n) = 0$. As $(a_1, \ldots, a_{n-1}) \in V$, $r(a_1, \ldots, a_{n-1}, x_n) = 0$. From $lc(h)(a_1, \ldots, a_{n-1}) \neq 0$, $h(a_1, \ldots, a_n) = 0$ and $lc(h)^d \cdot f^l = h \cdot q + r$, where $d := max(deg_n(f^l) - deg_n(h) + 1, 0)$, it follows that $f^l(a_1, \ldots, a_n) = 0$. Hence, $f(a_1, \ldots, a_n) = 0$. Thus,

$$(a_1, \ldots, a_n) \in \bigcup_{i=1}^{k} V_i,$$

where V_i is the irreducible variety in $\bar{K}^n$ with $(b_1, \ldots, b_{n-1}, c_i)$ as a generic point. Hence,

there exists a $b_n \in \{c_1, \ldots, c_k\}$ such that $(a_1, \ldots, a_n) \in V'$, where V' is the irreducible variety in $\bar{K}^n$ with $(b_1, \ldots, b_n)$ as a generic point. $\square$

Proof of correctness of $\mathbf{solve}_n$*:*

We will prove correctness by induction on the partial ordering $\prec$ on regular chains. Let R and F satisfy the input specification. Obviously, the regular chain R is minimal with respect to $\prec$ if and only if R represents a zero-dimensional variety.

Induction basis: The dimension of $Rep_{n-1}(R)$ is 0.

From (8.1) in the proof of termination we obtain that $M = \emptyset$. It follows from the specification of $\mathbf{ggcd}_n$ and the definition of the output set O that every element of O is a regular chain in $K[x_1, \ldots, x_n]$.

Let $R' \in O$ and $a \in RZ_{n-1}(R' \cap K[x_1, \ldots, x_{n-1}])$. As $M = \emptyset$ we know that there exists an $i \in \{1, \ldots, l\}$ such that

$$R' \cap K[x_1, \ldots, x_{n-1}] = S_i. \tag{8.4}$$

It readily follows from the specification of $\mathbf{ggcd}_n$ that $a \in RZ_{n-1}(R)$.

It remains to show condition 2. Let $(a_1, \ldots, a_n) \in Rep_n(R) \cap V_n(F)$. By Lemma 8.1, $(a_1, \ldots, a_{n-1})$ is an element of $Rep_{n-1}(R)$. Since $Rep_{n-1}(R)$ is a zero-dimensional variety it follows from (van der Waerden (1967), p.162) that $(a_1, \ldots, a_{n-1})$ is a generic point of one of the irreducible components of $Rep_{n-1}(R)$. Therefore, $(a_1, \ldots, a_{n-1})$ is an element of $RZ(R)$. Hence, by the specification of $\mathbf{ggcd}_n$, there exists an $i \in \{1, \ldots, l\}$ with $(a_1, \ldots, a_{n-1}) \in RZ(S_i)$. Thus, $(a_1, \ldots, a_n) \in Rep_n(S_i)$. Together with $(a_1, \ldots, a_n) \in V(F)$ we obtain $g_i(a_1, \ldots, a_n) = 0$. If $g_i = 0$ then $S_i \in O$. Otherwise, by the specification of $\mathbf{ggcd}_n$, $lc(g_i)(a_1, \ldots, a_{n-1}) \neq 0$ and therefore $g_i \notin K[x_1, \ldots, x_{n-1}]$, $S_i \cup \{g_i\} \in O$ and $(a_1, \ldots, a_n) \in Rep(S_i \cup \{g_i\})$. Altogether,

$$(a_1, \ldots, a_n) \in \bigcup_{R' \in O} Rep(R'). \tag{8.5}$$

Now let $R' \in O$ and $(a_1, \ldots, a_n) \in Rep_n(R')$. It follows from (8.4) that we can choose an $i \in \{1, \ldots, l\}$ with $R' \cap K[x_1, \ldots, x_{n-1}] = S_i$. By Lemma 8.1, $(a_1, \ldots, a_{n-1}) \in Rep(S_i)$. From

$$RZ_{n-1}(R) = RZ_{n-1}(S_1) \cup \ldots \cup RZ_{n-1}(S_l) \text{ and } dim(Rep_{n-1}(R)) = 0$$

we obtain $dim(Rep_{n-1}(S_i)) = 0$. Therefore, it follows from (van der Waerden (1967), p.162) that $(a_1, \ldots, a_{n-1}) \in RZ(S_i)$. If $i \notin J$ then $g_i = 0$. Otherwise, $(a_1, \ldots, a_n) \in Rep(S_i \cup \{g_i\})$. Thus, we obtain in both cases $g_i(a_1, \ldots, a_n) = 0$. Since $g_i(a_1, \ldots, a_{n-1}, x_n)$ is the gcd of the polynomials in $\{f(a_1, \ldots, a_{n-1}, x_n) \mid f \in F\}$,

$$(a_1, \ldots, a_n) \in V(F).$$

Induction step: R is not a minimal regular chain with respect to $\prec$.

It follows from the specification of $\mathbf{ggcd}_n$, the induction hypothesis, and the definition of the output set O that every element of O is a regular chain in $K[x_1, \ldots, x_n]$.

Let $R' \in O$ and $a \in RZ_{n-1}(R' \cap K[x_1, \ldots, x_{n-1}])$. If there exists an $i \in \{1, \ldots, l\}$ such that $R' \cap K[x_1, \ldots, x_{n-1}] = S_i$ then it readily follows from the specification of $\mathbf{ggcd}_n$ that $a \in RZ_{n-1}(R)$. Otherwise, there exists an $S \in M$ such that R' is in the output set of $\mathbf{solve}_n$ with input S and F. Since we have shown in the proof of termination that

$S \prec R$ (see (8.1)), we obtain from the induction hypothesis that $a \in RZ(S)$ or $a \prec b$ for every $b \in RZ(S)$. Therefore, $a \prec c$ for every $c \in RZ(R)$.

It remains to show condition 2. It follows from the specification of $\mathbf{ggcd}_n$ that

$$RZ_n(R) = RZ_n(S_1) \cup \ldots \cup RZ_n(S_l)$$

and therefore

$$Rep_n(R) = Rep_n(S_1) \cup \ldots \cup Rep_n(S_l).$$

Let $(a_1, \ldots, a_n) \in Rep_n(R) \cap V_n(F)$. Then there exists an $i \in \{1, \ldots, l\}$ such that $(a_1, \ldots, a_n) \in Rep(S_i)$. By specification of $\mathbf{ggcd}_n$,

$$g_i(a_1, \ldots, a_n) = 0. \tag{8.6}$$

Case: $g_i = 0$.

Then

$$S_i \in O \text{ and } (a_1, \ldots, a_n) \in \bigcup_{R' \in O} Rep_n(R').$$

Case: $g_i \neq 0$ and $lc(g_i)(a_1, \ldots, a_{n-1}) \neq 0$.

Since $(a_1, \ldots, a_n) \in Rep_n(S_i)$, we obtain from Lemma 8.1 that $(a_1, \ldots, a_{n-1})$ is an element of $Rep_{n-1}(S_i)$. Thus, there exists an irreducible variety V with a $(b_1, \ldots, b_{n-1}) \in RZ_{n-1}(S_i)$ as generic point such that

$$(a_1, \ldots, a_{n-1}) \in V. \tag{8.7}$$

Because of the fact that neither $(a_1, \ldots, a_{n-1})$ nor $(b_1, \ldots, b_{n-1})$ is a zero of $lc_n(g_i)$ and because of (8.6) and (8.7) we obtain from Lemma 8.2 that there exists a zero b_n of $g_i(b_1, \ldots, b_{n-1}, x_n)$ such that $(a_1, \ldots, a_n) \in V'$, where V' is the irreducible variety with $(b_1, \ldots, b_n)$ as generic point. As $(b_1, \ldots, b_{n-1}) \in RZ(S_i)$,

$$(b_1, \ldots, b_n) \in RZ(S_i \cup \{g_i\}).$$

From the fact that $g_i \notin K[x_1, \ldots, x_{n-1}]$ it follows that $S_i \cup \{g_i\} \in O$ and therefore

$$(a_1, \ldots, a_n) \in \bigcup_{R' \in O} Rep_n(R').$$

Case: $g_i \neq 0$ and $lc(g_i)(a_1, \ldots, a_{n-1}) = 0$.

Since $(a_1, \ldots, a_{n-1})$ is an element of $Rep_{n-1}(S_i \cap K[x_1, \ldots, x_{n-2}])$ and an element of $V(S_i - K[x_1, \ldots, x_{n-2}] \cup \{lc_n(g_i)\})$, it follows from the specification of $\mathbf{solve}_{n-1}$ that there exists an $S \in M$ with $(a_1, \ldots, a_{n-1}) \in Rep_{n-1}(S)$ and therefore $(a_1, \ldots, a_n) \in Rep_n(S)$. As $S \prec R$ (see (8.1) in the proof of termination) we obtain from the induction hypothesis that

$$(a_1, \ldots, a_n) \in \bigcup_{\bar{R} \in \bar{O}} Rep_n(\bar{R}),$$

where $\bar{O}$ is the output set of $\mathbf{solve}_n$ with input S and F. By definition of O,

$$(a_1, \ldots, a_n) \in \bigcup_{R' \in O} Rep_n(R').$$

Thus, in every case we have shown that

$$Rep_n(R) \cap V(F) \subseteq \bigcup_{R' \in O} Rep_n(R'). \tag{8.8}$$

Now let $R' \in O$, $(a_1, \ldots, a_n) \in Rep(R')$, and $(b_1, \ldots, b_n) \in RZ(R')$ such that $(a_1, \ldots, a_n) \in V$, where V is the irreducible variety in $\bar{K}^n$ with $(b_1, \ldots, b_n)$ as generic point. If there exists an $S \in M$ such that R' is an element of the output set of $\mathbf{solve}_n$ with input S and F then it follows from the induction hypothesis that

$$(a_1, \ldots, a_n) \in V(F). \tag{8.9}$$

Otherwise, there exists an $i \in \{1, \ldots, l\}$ such that $R' \cap K[x_1, \ldots, x_{n-1}] = S_i$. Hence, $(b_1, \ldots, b_{n-1}) \in RZ(S_i)$ and $g_i(b_1, \ldots, b_n) = 0$. Since $g_i(b_1, \ldots, b_{n-1}, x_n)$ is the gcd of the polynomials in $\{f(b_1, \ldots, b_{n-1}, x_n) \mid f \in F\}$,

$$(b_1, \ldots, b_n) \in V(F).$$

Hence, $(a_1, \ldots, a_n) \in V(F)$. Together with (8.8) and (8.9),

$$Rep_n(R) \cap V_n(F) \subseteq \bigcup_{R' \in O} Rep_n(R') \subseteq V_n(F). \quad \square$$

Acknowledgements

I am indebted to the members of FUJITSU's International Institute for Advanced Study of Social Information Science for organizing a wonderful stay at Numazu, to Shen Wei, who helped me implementing this algorithm, and to Dominique Duval and Daniel Lazard for their helpful comments on an earlier version of this paper.

References

Böge, W., Gebauer, R., Kredel, H. (1986). Some examples for solving systems of algebraic equations by calculating Gröbner Bases. *J. Symbolic Computation* **2**, 83–98.

Buchberger, B. (1965). *An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal (German)*. PhD thesis, Dept. of Mathematics, Univ. Innsbruck, Austria.

Buchberger, B. (1985). Gröbner bases: An algorithmic method in polynomial ideal theory. Chapter 6 in Bose, N.K. (ed.): *Multidimensional Systems Theory*, D. Reidel Publishing Company, Dordrecht-Boston-Lancaster.

Czapor, S.R. (1989). Solving algebraic equations: Combining Buchberger's algorithm with multivariate factorization. *J. Symbolic Computation* **7**, 49–53.

Czapor, S.R., Geddes, K.O. (1986). On implementing Buchberger's algorithm for Gröbner bases. In *Proc. SYMSAC'86*, pp. 233–238, Waterloo, Canada.

Della Dora, J., Dicrescenzo, C., Duval, D. (1985). About a new method for computing in algebraic number fields. In *Proc. EUROCAL'85*, pp. 289–290, Linz, Austria.

Dicrescenzo, C., Duval, D. (1988). Algebraic extensions and algebraic closure in Scratchpad II. In *Proc. ISSAC'88*, pp. 440–446, Rome, Italy.

Gao, X.S., Chou, S.C. (1991). On the dimension of an arbitrary ascending chain. *Chinese Bull. of Sci.*, to appear.

Giusti, M., Heintz, J. (1990). Algorithmes – disons rapides – pour la décomposition d'une variété algébrique en composantes irréductibles et équidimentionnelles. In *Proc. MEGA'90*, pp. 169–194.

Kalkbrener, M. (1991). *Three contributions to elimination theory.* PhD thesis, Research Institute for Symbolic Computation, Univ. Linz, Austria.

Kapur, D. (1986). Geometry theorem proving using Hilbert's Nullstellensatz. In *Proc. SYMSAC'86*, pp. 202–208, Waterloo, Canada.

Kredel, H., Weispfenning, V. (1988). Computing dimension and independent sets for polynomial ideals. *J. Symbolic Computation* **6**, 231–248.

Lazard, D. (1991). A new method for solving algebraic systems of positive dimension. *Discrete Applied Math.* **33**, 147–160.
Lazard, D. (1992). Solving zero-dimensional algebraic systems. *J. Symbolic Computation* **13**, 117–132.
Ritt, J.F. (1950). *Differential Algebra.* AMS Colloquium Publications, New York.
van der Waerden, B.L. (1967). *Algebra II (German).* Springer, Berlin Heidelberg New York, 5. edition.
Wu, W. (1984). Basic principles of mechanical theorem proving in elementary geometries. *J. Sys. Sci. and Math. Scis* **4**, 207–235.
Wu, W. (1986). On zeros of algebraic equations – an application of Ritt principle. *Kexue Tongbao* **31**, 1–5.
Yang, L., Zhang, J. (1991). Searching dependency between algebraic equations: an algorithm applied to automated reasoning. Technical Report IC/91/6, International Atomic Energy Agency, Miramare, Trieste, Italy.