A Generalized Euclidean Algorithm for Geometry Theorem Proving

Michael Kalkbrener*
Mathematical Sciences Institute
Cornell University
Ithaca, NY 14850, USA

Abstract

In the first part of this paper we present an algorithm that computes an unmixed-dimensional decomposition of a 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 given by regular chains. No factorization is needed.

In the second part this algorithm is applied to geometry theorem proving. We show that it can be used for deciding whether geometry statements are generically true or whether they are true under given nondegeneracy conditions. If a geometry statement is generically true, the simplest nondegeneracy condition with respect to a lexicographical degree ordering can be constructed by means of our algorithm.

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 [Rit50]. Since every irreducible variety is uniquely determined by one of its generic points (see [vdW67], 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 the first part of 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.

*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 United States Army Research Office through the Army Center of Excellence for Symbolic Methods in Algorithmic Mathematics (ACSyAM), Mathematical Sciences Institute of Cornell University, Contract DAAL03-91-C-0027.

We have introduced the concept of regular chains in our Ph.D. thesis [Kal91]. It has been independently defined in [YZ91]. Regular chains are a generalization of Ritt's irreducible ascending sets (see [Rit50]). 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 [Wu86] a modified version of Ritt's decomposition algorithm is presented. Recently Gao and Chou proved that the coarse form decomposition algorithm in [Wu86], which does not use polynomial factorization either, computes unmixed-dimensional decompositions of varieties [GC91].

Regular chains are also similar to triangular sets, a concept introduced by D. Lazard. In [Laz92] 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 [Laz91]. Furthermore, the definition of triangular sets given in [Laz92] is strengthened in [Laz91] 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 [Laz91], 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 [DDD85] and implemented in Scratchpad under the name **D5** (see [DD88]).

In this paper we present our decomposition algorithm without proving its termination and correctness. These proofs can be found in our Ph.D. thesis [Kal91] and in [Kal93].

In the second part of this paper we apply our method to geometry theorem proving. In the late 70's and early 80's the work of Wu Wen-tsun [Wu78], [Wu84] has renewed the interest in this area. Based on Ritt's characteristic sets he has developed an algorithm for a certain class of geometry problems. Intuitively speaking, this class consists of those problems that can be translated into algebraic equations over a field. Wu's approach and its variations have been experimented by many researchers including Wu himself [Wu78], [Wu84], Chou [Cho88], Chou and Gao [CG90], Ko and Hussain [KH85], Kapur and Wan [KW90] and Wang [Wan95].

Another important algorithm for geometry theorem proving is Buchberger's Gröbner bases algorithm [Buc65], [Buc85]. Chou and Schelter [CS86], Kapur [Kap86] and Kutzler and Stifter [KS86] independently demonstrated its usefulness in this area.

In most of the recent research in geometry theorem proving, two different but related formulations for geometry statements have been considered. In the first formulation the objective is to decide whether the conclusion follows from the hypotheses generically. If so, degenerate cases must be ruled out. In the second formulation nondegeneracy conditions are specified as part of the geometry statement. The objective is to decide whether the statement is valid without adding any other conditions.

There are two different but related approaches for considering the above two formulations of geometry statements [KW90]. The direct approach, originally in Wu's paper, consists of two parts. The hypotheses are first brought in some standard form which is used for deciding whether the conclusion is valid or not (see, for instance, [Wu84], [Cho88], [CG90], [CS86], [Ko88], [KS86]). In the refutational approach ([Kap86], [KW90], [Cho88], [CS86]) the conclusion c is negated using Rabinowitsch's trick and the inconsistency (or unsatisfiability) of the negated conclusion and the hypothesis is decided.

Since both formulations can be tackled with the direct and the refutational approach, there exist four different methods. In this paper we show that our algorithm can be used for all four approaches.

We prove that when a variety is represented by a regular chain it can be easily decided whether a polynomial vanishes on this variety. This result is the key to the direct approach. The refutational approach is based on a complete characterization of possible nondegeneracy conditions proved in this paper. We also use this result for constructing the simplest nondegeneracy conditions with respect to a lexicographical degree ordering. An algorithm for finding simplest nondegeneracy conditions with respect to various criteria is given in [Win90].

In Section 2 we introduce the concept of regular chains and state more formally the decomposition problem we are concerned with. In Section 3 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 4 we give an algorithmic solution based on this gcd algorithm for the decomposition problem stated in Section 2. In Section 5 we apply our algorithm to geometry theorem proving and show that it can be used for all four different approaches. In Section 6 an algorithm for constructing simplest nondegeneracy conditions is presented. In Section 7 we illustrate the methods in Section 5 and 6 by means of Apollonios' Circle Theorem and Simpson's Theorem.

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 the variety V 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 [vdW67], p.160). It is well-known (see, for instance, [vdW67], p.161) that a variety is irreducible (over K) iff it has a generic point (over K). A subset X of $\{x_1, \ldots, x_n\}$ is independent modulo a variety V if there does not exist a non-zero polynomial in $K[X]$ that vanishes on V. 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 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 given polynomials. In addition to this common method we use a different representation in this paper, which is a generalization of a concept in [Rit50]. 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 $K[x_1, \ldots, x_n]$ 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 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 $Rep_n(R)$.

Example 2 Let R_3 and R_4 be defined as in the previous example. 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 ([Rit50], [Wu84]). 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 [Laz91] in order to make every polynomial in a triangular set monic, primitive and squarefree in a rather technical sense.

2.3 The Problem

In the next two sections we present an algorithm that solves the following problem:

Given: $F = \{f_1, \ldots, f_k\}$, a finite 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 [Kal91] and [Kal93] it is shown how the dimension of an ideal can be computed and systems of algebraic equations can be solved. Furthermore, we prove in Lemma 1 in this paper that radical membership can be decided. This property plays an important role in the application of our method in geometry theorem proving.

3 Computing Modulo Regular Chains

Before we can present an algorithmic solution of the above problem, 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 [DDD85] and implemented in Scratchpad under the name **D5** (see [DD88]). By means of the following example we illustrate the basic idea behind this method.

Example 3 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

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

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:

common$_n$ (R, g): 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

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

separate$_n$ (R, g): 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 Having **common** and **separate** at hand the following problem can be solved easily:

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?

First we have to check whether a_2^{-1} exists for every (a_1, a_2, a_3) in $RZ_3(R)$:

By computing **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 **common**$_3(R, x_1^2 + x_3x_2^2)$ respectively **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,

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

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

In Example 3 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 **ggcd**$_n$ (= generalized greatest common divisor) that satisfies the following specification.

ggcd$_n$ (R, F): 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 $Rep_n(R_i) \cap V(F)$.

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$_n$ (R, g): 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$_n$ (R, g): 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
$O := \{(R, 0)\}$

Example 5 Let us compute the gcd of $x_2^2 + x_1$ and $x_1x_2 + x_1^2$ modulo $x_1^4 - x_1^3$, i.e. let us compute

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

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,

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

4 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.
We will construct for every natural number n an algorithm named $\mathbf{solve}_n$ that satisfies the following specification.

$\mathbf{solve}_n$ (R, F): 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

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

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

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

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

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

Theorem 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 6 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 $\mathbf{solve}_2(\{x_1^4 + x_1^3\}, \{x_2^2 + x_1, x_1x_2 + x_1^2\})$:

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

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

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

$O := \{\{x_1, x_2^2 + x_1\}, \{x_1 + 1, x_1x_2 + x_1^2\}\}$.

Hence,

$$V_2(\{x_2^2 + x_1, x_1x_2 + x_1^2\}) \;=\; Rep_2(\{x_1, x_2^2 + x_1\}) \cup Rep_2(\{x_1 + 1, x_1x_2 + x_1^2\}). \quad \square$$

5 Regular Chains and Geometry Theorem Proving

5.1 Formulations of the problem

In the following sections let $h_1, \ldots, h_m$ and c be polynomials in $K[x_1, \ldots, x_n]$ and let V denote the variety $V_n(\{h_1, \ldots, h_m\})$. The h_i's and c are obtained by translating the hypotheses and conclusion of a geometrical statement into algebraic equations. During this translation process a set $X \subset \{x_1, \ldots, x_n\}$ of independent variables modulo V can be identified. We assume without loss of generality that $X = \{x_1, \ldots, x_t\}$. Let $V = V_1 \cup \ldots \cup V_r$ be a decomposition into irreducible varieties. We assume that the varieties $V_1, \ldots, V_r$ are ordered in such a way that there exists an $s \in \{1, \ldots, r\}$ such that X is independent modulo V_i for $i \in \{1, \ldots, s\}$ and not independent modulo V_j for $j \in \{s+1, \ldots, r\}$. Let

$$V_{hyp} := \bigcup_{i=1}^{s} V_i \quad \text{and} \quad V_{dege} := \bigcup_{j=s+1}^{r} V_j.$$

In most of the recent research in geometry theorem proving, two different but related formulations for geometry statements have been considered [Cho90].

Formulation 1: Decide whether

$$(\exists d \in K[x_1, \ldots, x_t] - \{0\})(\forall a \in \bar{K}^n)\ [h_1(a) = \ldots = h_m(a) = 0 \wedge d(a) \neq 0 \ \Rightarrow\ c(a) = 0]. \tag{1}$$

If so, find such a nondegeneracy condition d.

Obviously, such a polynomial exists iff c vanishes on V_{hyp}. It can be found by choosing an arbitrary non-zero element in $K[x_1, \ldots, x_t]$ that vanishes on V_{dege}. If c vanishes on V_{hyp}, we say the statement (1) is generally true. If c does not vanish on any irreducible component of V_{hyp}, it is generally false. Otherwise the conclusion is valid on not all but some nondegeneracy components, and the statement needs further investigations. In [YZ91] regular chains and resultants are used for determining the number of components on which c vanishes. Formulation 1 has been used, for instance, in [Cho88], [CS86], [KS86], [Win90].

Formulation 2: In this formulation a nondegeneracy condition $d \in K[x_1, \ldots, x_t]$ is explicitly given. Then the aim is to decide whether the statement

$$(\forall a \in \bar{K}^n)\ [h_1(a) = \ldots = h_m(a) = 0 \wedge d(a) \neq 0 \ \Rightarrow\ c(a) = 0] \tag{2}$$

is true without adding any further conditions (see [Cho88], [CG90], [CS86] [KW90], [Kap86], [Kap88], [Ko88]).

Sometimes it seems natural to use a finite set $\{d_1, \ldots, d_i\}$ of nondegeneracy conditions, replacing $d(a) \neq 0$ by $d_1(a) \neq 0 \wedge \ldots \wedge d_i(a) \neq 0$, thus getting a modified problem. However, since $d_1(a) \neq 0 \wedge \ldots \wedge d_i(a) \neq 0$ iff $(d_1 \cdot d_2 \cdots d_i)(a) \neq 0$ for every $a \in \bar{K}^t$, one nondegeneracy condition is sufficient from a theoretical point of view. For simplicity we will deal with one nondegeneracy condition only.

There are two different but related approaches for considering the above two formulations of geometry statements [KW90]. The direct approach, originally in Wu's paper, consists of two parts. The hypotheses are first brought in some standard form which is used for deciding whether the conclusion is valid or not (see, for instance, [Wu84], [Cho88], [CG90], [CS86], [Ko88], [KH85], [KS86]). In the refutational approach ([Kap86], [KW90], [Cho88], [CS86]) the conclusion c is negated using Rabinowitsch's trick and the inconsistency (or unsatisfiability) of the negated conclusion and the hypotheses is decided.

Since both formulations can be tackled with the direct and the refutational approach there exist four different methods. It is our aim in this section to show that our algorithm can be used for all four approaches.

5.2 Methods

When a variety is given by a regular chain we can decide whether a polynomial completely vanishes on this variety (radical membership problem) respectively does not vanish on any of the irreducible components of the variety.

Lemma 1 *Let $f \in K[x_1, \ldots, x_n]$ and R a regular chain in $K[x_1, \ldots, x_n]$. Then*
a) *f vanishes on $Rep_n(R)$ iff* $\mathbf{separate}_n(R, f) = \emptyset$,
b) *f does not vanish on U for any $U \in AIV_n(R)$ iff* $\mathbf{common}_n(R, f) = \emptyset$.

Proof:

$$\begin{gathered} f \text{ vanishes on } Rep_n(R) \\ \text{iff} \\ f \text{ vanishes on every } U \in AIV_n(R) \\ \text{iff} \\ f(a) = 0 \text{ for every } a \in RZ_n(R) \\ \text{iff} \\ \mathbf{separate}_n(R, f) = \emptyset. \end{gathered}$$

$$\begin{gathered} f \text{ does not vanish on } U \text{ for any } U \in AIV_n(R) \\ \text{iff} \\ f(a) \neq 0 \text{ for every } a \in RZ_n(R) \\ \text{iff} \\ \mathbf{common}_n(R, f) = \emptyset. \quad \square \end{gathered}$$

This lemma leads to the following direct approach to proving geometry statements in formulation 1.

Theorem 2 *Let $\{R_1, \ldots, R_l\} := \mathbf{solve}_n(\emptyset, \{h_1, \ldots, h_m\})$. We assume that the regular chains $R_1, \ldots, R_l$ are ordered in such a way that there exists a $k \in \{1, \ldots, l\}$ such that $R_i \cap K[x_1, \ldots, x_t] = \emptyset$ for $i \in \{1, \ldots, k\}$ and there exists at least one polynomial d_j in $R_j \cap K[x_1, \ldots, x_t]$ for $j \in \{k+1, \ldots, l\}$. Then*

statement (1) is generally false iff $\mathbf{common}_n(R_i, c) = \emptyset$ *for every* $i \in \{1, \ldots, k\}$,
statement (1) is generally true iff $\mathbf{separate}_n(R_i, c) = \emptyset$ *for every* $i \in \{1, \ldots, k\}$.

In the second case the product $d_{k+1} \cdot d_{k+2} \cdots d_l$ is a nondegeneracy condition.

Proof: It is clear from $V = Rep_n(R_1) \cup \ldots \cup Rep_n(R_l)$ and the definition of representation by regular chains that

$$V_{hyp} = \bigcup_{i=1}^{k} Rep_n(R_i) \quad \text{and} \quad V_{dege} = \bigcup_{j=k+1}^{l} Rep_n(R_j).$$

Therefore, by the previous lemma,

statement (1) is generally false iff $\mathbf{common}_n(R_i, c) = \emptyset$ for every $i \in \{1, \ldots, k\}$,
statement (1) is generally true iff $\mathbf{separate}_n(R_i, c) = \emptyset$ for every $i \in \{1, \ldots, k\}$.

Let $a \in \bar{K}^n$. Then $h_1(a) = \ldots = h_m(a) = 0$ and $(d_{k+1} \cdot d_{k+2} \cdots d_l)(a) \neq 0$ imply that a is in the variety V_{hyp}. Therefore, if (1) is generally true then $d_{k+1} \cdot d_{k+2} \cdots d_l$ is a nondegeneracy condition. $\square$

The refutational approach to proving geometry statements in formulation 1 is based on the following result on the set of nondegeneracy conditions.
Let $D \subseteq K[x_1, \ldots, x_t]$ be the set of nondegeneracy conditions, i.e. $d \in D$ iff

$$(\forall a \in \bar{K}^n)\ [h_1(a) = \ldots = h_m(a) = 0 \wedge d(a) \neq 0 \ \Rightarrow\ c(a) = 0].$$

Let F be a subset of $K[x_1, \ldots, x_n]$. Then $Rad_n(F)$ denotes the radical of the ideal generated by F in $K[x_1, \ldots, x_n]$.

Lemma 2 a) $D = Rad_{n+1}(\{h_1, \ldots, h_m, cx_{n+1} - 1\}) \cap K[x_1, \ldots, x_t]$.
b) *Let* $\{R_1, \ldots, R_l\} := \mathbf{solve}_{n+1}(\emptyset, \{h_1, \ldots, h_m, cx_{n+1} - 1\})$. *Then*

$$D = \{d \in K[x_1, \ldots, x_t] \mid d \textit{ vanishes on } \bigcup_{i=1}^{l} Rep_{n+1}(R_i)\}.$$

Proof: a) Let $a = (a_1, \ldots, a_n) \in \bar{K}^n$. Obviously,

$$\begin{gathered}(\exists a_{n+1} \in \bar{K})\ (a_1, \ldots, a_n, a_{n+1}) \in V_{n+1}(\{h_1, \ldots, h_m, cx_{n+1} - 1\}) \\ \text{iff} \\ h_1(a) = \ldots = h_m(a) = 0 \wedge c(a) \neq 0.\end{gathered}$$

Let $d \in K[x_1, \ldots, x_t]$. Then

$$\begin{gathered}d \in D \\ \text{iff} \\ (\forall a \in \bar{K}^n)\ [h_1(a) = \ldots = h_m(a) = 0 \wedge d(a) \neq 0 \ \Rightarrow\ c(a) = 0] \\ \text{iff} \\ (\forall a \in \bar{K}^n)\ [h_1(a) = \ldots = h_m(a) = 0 \wedge c(a) \neq 0 \ \Rightarrow\ d(a) = 0] \\ \text{iff} \\ d \text{ vanishes on } V_{n+1}(\{h_1, \ldots, h_m, cx_{n+1} - 1\}) \\ \text{iff} \\ d \in Rad_{n+1}(\{h_1, \ldots, h_m, cx_{n+1} - 1\}).\end{gathered}$$

Now **b)** follows from **a)** and Theorem 1. □

In [Win90] syzygies are used for characterizing the set of nondegeneracy conditions.
Theorem 3 is an easy consequence of the previous lemma.

Theorem 3 *Let* $\{R_1, \ldots, R_l\} := \mathbf{solve}_{n+1}(\emptyset, \{h_1, \ldots, h_m, cx_{n+1} - 1\})$. *Then*

statement (1) is generally true
iff
there exists at least one polynomial d_j *in* $R_j \cap K[x_1, \ldots, x_t]$ *for every* $j \in \{1, \ldots, l\}$.

In this case the product $d_1 \cdot d_2 \cdots d_l$ *is a nondegeneracy condition.*

Proof: By the previous lemma,

$$\begin{gathered}\text{statement (1) is generally true}\\ \text{iff}\\ \text{there exists at least one non-zero polynomial in } D\\ \text{iff}\\ \text{there exists at least one polynomial } d_j \text{ in } R_j \cap K[x_1,\ldots,x_t] \text{ for every } j \in \{1,\ldots,l\}.\end{gathered}$$

It follows from Lemma 2(b) that the product $d_1 \cdot d_2 \cdots d_l$ is a nondegeneracy condition, because it vanishes on $\bigcup_{i=1}^{l} Rep_{n+1}(R_i)$. $\square$

In the next section we will use the fact that a polynomial $d \in K[x_1,\ldots,x_t]$ is in D iff it vanishes on $\bigcup_{i=1}^{l} Rep_{n+1}(R_i)$ to obtain simplest nondegeneracy conditions. But first, we want to show how our algorithm can be used for proving geometry statements in formulation 2.

Theorem 4 *Let d be the nondegeneracy condition in statement (2) and $\{R_1,\ldots,R_l\} :=$ $\mathbf{solve}_{n+1}(\emptyset, \{h_1,\ldots,h_m, dx_{n+1}-1\})$. Then*

$$\textit{statement (2) is true} \quad \textit{iff} \quad \mathbf{separate}_{n+1}(R_i, c) = \emptyset \quad \textit{for every } i \in \{1,\ldots,l\}.$$

Proof: Let $a = (a_1,\ldots,a_n) \in \bar{K}^n$. Obviously,

$$\begin{gathered}(\exists a_{n+1} \in \bar{K})\ (a_1,\ldots,a_n,a_{n+1}) \in V_{n+1}(\{h_1,\ldots,h_m,dx_{n+1}-1\})\\ \text{iff}\\ h_1(a) = \ldots = h_m(a) = 0 \ \wedge\ d(a) \neq 0.\end{gathered}$$

Therefore, by Theorem 1 and Lemma 1,

$$\begin{gathered}\text{statement (2) is true}\\ \text{iff}\\ (\forall a \in \bar{K}^n)\ [h_1(a) = \ldots = h_m(a) = 0 \ \wedge\ d(a) \neq 0 \ \Rightarrow\ c(a) = 0]\\ \text{iff}\\ c \text{ vanishes on } V_{n+1}(\{h_1,\ldots,h_m,dx_{n+1}-1\})\\ \text{iff}\\ c \text{ vanishes on } Rep_{n+1}(R_i) \text{ for every } i \in \{1,\ldots,l\}\\ \text{iff}\\ \mathbf{separate}_{n+1}(R_i,c) = \emptyset \text{ for every } i \in \{1,\ldots,l\}. \ \square\end{gathered}$$

Theorem 5 *Let d be the nondegeneracy condition in statement (2).*

$$\textit{Statement (2) is true} \quad \textit{iff} \quad \mathbf{solve}_{n+2}(\emptyset, \{h_1,\ldots,h_m,dx_{n+1}-1,cx_{n+2}-1\}) = \emptyset.$$

Proof: It has been shown in [Kap86] that statement (2) is true iff 1 is in the ideal generated by the set $\{h_1,\ldots,h_m,dx_{n+1}-1,cx_{n+2}-1\}$ in $K[x_1,\ldots,x_{n+2}]$. This is equivalent to

$$\mathbf{solve}_{n+2}(\emptyset, \{h_1,\ldots,h_m,dx_{n+1}-1,cx_{n+2}-1\}) = \emptyset. \ \square$$

6 Computing simplest nondegeneracy conditions

We define the following relation on $K[x_1, \ldots, x_t]$. Let $f, g \in K[x_1, \ldots, x_t]$. Then $f \prec g$ if there exists an $i \in \{1, \ldots, t\}$ such that $deg_i(f) < deg_i(g)$ and $deg_j(f) = deg_j(g)$ for every $j \in \{i+1, \ldots, t\}$.

We assume that statement (1) is generally true. It is our aim in this section to construct a nondegeneracy condition $d \in D - \{0\}$ which is minimal in $D - \{0\}$ with respect to the relation $\prec$.

Let f be a non-constant polynomial in $K[x_1, \ldots, x_t]$. Then $squarefree(f)$ denotes the squarefree form of f, $class(f)$ denotes the greatest element $i \in \{1, \ldots, t\}$ such that $deg_i(f) > 0$ and $primpart(f)$ denotes the primitive part of f with respect to x_i. Let $R = \{f_1, f_2, \ldots, f_k\}$ be a non-empty regular chain in $K[x_1, \ldots, x_t]$ with the polynomials $f_1, \ldots, f_k$ ordered in such a way that $class(f_i) < class(f_j)$ if $i < j$. We denote f_1 by $first(R)$.

Let $\{R_1, \ldots, R_l\} := \mathbf{solve}_{n+1}(\emptyset, \{h_1, \ldots, h_m, cx_{n+1} - 1\})$. We assume that $R_1, \ldots, R_l$ are ordered in such a way that $class(first(R_i)) \geq class(first(R_j))$ for $i < j$. We define

$$\begin{array}{lcll} d_1 & := & squarefree(primpart(first(R_1))), & \\ d_i & := & squarefree(d_{i-1} \cdot \prod_{j=1}^{k_i} primpart(first(R'_{ji}))), & (i = 2, \ldots, l) \end{array}$$

where $\{R'_{1i}, \ldots, R'_{k_i i}\} := \mathbf{separate}_{n+1}(R_i, d_{i-1})$.

Theorem 6 *The polynomial d_l is a minimal nondegeneracy condition with respect to $\prec$. Two minimal nondegeneracy conditions are identical except for a multiplicative constant.*

Proof: For every $i \in \{1, \ldots, l\}$ let D_i be the set of those non-zero polynomials in $K[x_1, \ldots, x_t]$ that vanish on the variety $Rep_{n+1}(R_1) \cup \ldots \cup Rep_{n+1}(R_i)$. We will show the following result by induction:

The polynomial d_i is in D_i for every $i \in \{1, \ldots, l\}$. Let d be a polynomial in D_i with $deg_j(d) = deg_j(d_i)$ for every $j > class(first(R_i))$. Then d_i divides d. Furthermore, d_i is minimal in D_i with respect to $\prec$.

Induction basis: $i = 1$. In this case the statement follows from the definition of $Rep_{n+1}(R_1)$.

Induction step: $i \in \{2, \ldots, l\}$. For proving that $d_i \in D_i$ it suffices to prove that d_i vanishes on $Rep_{n+1}(R_i)$. Let $a \in RZ_{n+1}(R_i)$. If there exists a $j \in \{1, \ldots, k_i\}$ such that $a \in RZ_{n+1}(R'_{ji})$ then a is a zero of $primpart(first(R'_{ji}))$. Otherwise, by specification of **separate**, $d_{i-1}(a) = 0$. In both cases a is a zero of d_i. Therefore, d_i vanishes on $Rep_{n+1}(R_i)$.

Let d be a polynomial in D_i with $deg_j(d) = deg_j(d_i)$ for every $j > class(first(R_i))$. By definition of d_i, $deg_j(d_i) = deg_j(d_{i-1})$ for every $j > class(first(R_i))$. Hence,

$$deg_j(d) = deg_j(d_{i-1}) \text{ for every } j > class(first(R_i)). \tag{3}$$

From $class(first(R_{i-1})) \geq class(first(R_i))$ we obtain $deg_j(d) = deg_j(d_{i-1})$ for every $j > class(first(R_{i-1}))$. Since $d \in D_{i-1}$ it follows from the induction hypothesis that

$$d_{i-1} \text{ divides } d. \tag{4}$$

Let $j \in \{1, \ldots, k_i\}$ and $f := d/d_{i-1}$. It follows from (3) that

$$class(f) \leq class(first(R_i)) = class(first(R'_{ji})). \tag{5}$$

For every $a \in RZ_{n+1}(R'_{ji})$ we have $f(a) = 0$, because $d(a) = 0$ and $d_{i-1}(a) \neq 0$. By (5) and the definition of $RZ_{n+1}(R'_{ji})$, f is divided by $squarefree(primpart(first(R'_{ji})))$. Therefore, d_i divides d, because of (4) and because d_i is squarefree.

Let d be an arbitrary polynomial in D_i. Let us assume that $d \prec d_i$. If there exists a $u > class(first(R_i))$ with $deg_u(d) < deg_u(d_i)$ and $deg_j(d) = deg_j(d_i)$ for every $j \in \{u+1, \ldots, t\}$ then $d \prec d_{i-1}$, because $deg_j(d_i) = deg_j(d_{i-1})$ for every $j > class(first(R_i))$. Since d is in D_{i-1}, this is a contradiction to the induction hypothesis. Hence $deg_j(d) = deg_j(d_i)$ for every $j > class(first(R_i))$. In this case we already proved that d_i divides d. This is a contradiction to $d \prec d_i$. This completes the induction.

Now it follows from Lemma 2(b) that d_l is a minimal nondegeneracy condition. If d is another minimal nondegeneracy condition then $deg_j(d) = deg_j(d_l)$ for every $j > class(first(R_i))$. Therefore, d_l divides d. Since d is minimal with respect to $\prec$, d_l and d are identical except for a multiplicative constant. □

Since all the minimal elements in D with respect to $\prec$ are identical except for multiplicative constants, it is justified to call each of these minimal elements the simplest nondegeneracy condition with respect to $\prec$.

7 Examples

Recently we have implemented the algorithm **solve** in the computer algebra system MAPLE V. The following two examples have been computed by means of our present implementation.

Apollonios' Circle Theorem: *The altitude pedal of the hypotenuse of a right-angled triangle and the midpoints of the three sides of the triangle lie on a circle.*

We use the algebraic formulation given in [Buc87]. We have 8 hypotheses polynomials $h_1, \ldots, h_8 \in Q[x_1, x_2, \ldots, x_{10}]$:

$$\begin{aligned}
h_1 &:= 2x_3 - x_1, & h_5 &:= (x_7 - x_3)^2 + x_8^2 - (x_7 - x_4)^2 - (x_8 - x_5)^2,\\
h_2 &:= 2x_4 - x_1, & h_6 &:= (x_7 - x_3)^2 + x_8^2 - (x_8 - x_6)^2 - x_7^2,\\
h_3 &:= 2x_5 - x_2, & h_7 &:= (x_9 - x_1)x_2 + x_1x_{10},\\
h_4 &:= 2x_6 - x_2, & h_8 &:= -x_1x_9 + x_2x_{10}.
\end{aligned}$$

The conclusion is

$$c := (x_7 - x_3)^2 + x_8^2 - (x_7 - x_9)^2 - (x_8 - x_{10})^2.$$

The set of independent variables is $\{x_1, x_2\}$.
We apply all four methods in Section 5 to Apollonios' Circle Theorem.

Formulation 1, direct approach: We have to compute $\mathbf{solve}_{10}(\emptyset, \{h_1, \ldots, h_8\})$. The output set contains 4 regular chains in $Q[x_1, \ldots, x_{10}]$:

$$\begin{aligned}
R_1 &:= \{\, x_1x_{10} + x_2x_9 - x_2x_1, \quad -x_1^2x_9 - x_2^2x_9 + x_2^2x_1, \quad 4x_8 - x_2, \quad -4x_7 + x_1, \\
&\qquad 2x_6 - x_2, \quad 2x_5 - x_2, \quad 2x_4 - x_1, \quad 2x_3 - x_1 \,\}, \\
R_2 &:= \{\, x_{10}, \quad x_9, \quad 4x_8 - x_2, \quad 2x_6 - x_2, \quad 2x_5 - x_2, \quad x_4, \quad x_3, \quad x_1 \,\}, \\
R_3 &:= \{\, x_{10}, \quad x_9, \quad -4x_7 + x_1, \quad x_6, \quad x_5, \quad 2x_4 - x_1, \quad 2x_3 - x_1, \quad x_2 \,\}, \\
R_4 &:= \{\, x_6, \quad x_5, \quad x_4, \quad x_3, \quad x_2, \quad x_1 \,\}.
\end{aligned}$$

Only R_1 does not contain an element in $Q[x_1, x_2]$. By Theorem 2, we can check whether the Apollonios' Circle Theorem is generally true by computing $\mathbf{separate}_{10}(R_1, c)$. Since the output set is empty, Apollonios' Circle Theorem is generally true. The polynomial x_1x_2 is a nondegeneracy condition, because x_1 is in R_2 and R_4 and x_2 is in R_3.

Formulation 1, refutational approach: We have to compute $\mathbf{solve}_{11}(\emptyset, \{h_1, \ldots, h_8, cx_{11} - 1\})$. The output set contains the regular chain $R := R_4 \cup \{cx_{11} - 1\}$ in $Q[x_1, \ldots, x_{11}]$ only. Since $R \cap Q[x_1, x_2] = \{x_1, x_2\}$ we obtain from Theorem 3 that Apollonios' Circle Theorem is generally true. Lemma 2 states that the set of nondegeneracy conditions is the prime ideal generated by $\{x_1, x_2\}$. Hence, x_1 and x_2 are both nondegeneracy conditions. Obviously, x_1 is the simplest nondegeneracy condition with respect to the relation $\prec$ in Section 6.

Formulation 2, direct approach: Using the minimal nondegeneracy condition x_1 we have to compute $\mathbf{solve}_{11}(\emptyset, \{h_1, \ldots, h_8, x_1x_{11} - 1\})$. The output set contains two regular chains $R_1 \cup \{x_1x_{11} - 1\}$ and $R_3 \cup \{x_1x_{11} - 1\}$ in $Q[x_1, \ldots, x_{11}]$. Since $\mathbf{separate}_{11}(R_1 \cup \{x_1x_{11} - 1\}, c) = \emptyset$ and $\mathbf{separate}_{11}(R_3 \cup \{x_1x_{11} - 1\}, c) = \emptyset$, Apollonios' Circle Theorem is true (see Theorem 4).

Formulation 2, refutational approach: Using the minimal nondegeneracy condition x_1 we compute $\mathbf{solve}_{12}(\emptyset, \{h_1, \ldots, h_8, x_1x_{11} - 1, cx_{12} - 1\})$. The output set is empty. Therefore, we obtain from Theorem 5 that Apollonios' Circle Theorem is true. □

Simson's Theorem: *The pedal points of the altitudes drawn from an arbitrary point on a triangle's circumscribed circle to the three sides are collinear.*

We use the algebraic formulation given in [Cho90]. We have 9 hypotheses polynomials $h_1, \ldots, h_9 \in Q[x_1, x_2, \ldots, x_{13}]$:

$$\begin{aligned}
h_1 &:= 2x_1x_4 - x_1^2, & h_2 &:= 2x_2x_5 + 2x_3x_4 - x_3^2 - x_2^2, \\
h_3 &:= x_7^2 - 2x_4x_7 + x_6^2 - 2x_5x_6, & h_4 &:= x_2x_9 - (x_3 - x_1)x_8 - x_1x_2, \\
h_5 &:= (x_3 - x_1)x_9 + x_2x_8 - (x_3 - x_1)x_7 - x_2x_6, & h_6 &:= x_2x_{11} - x_3x_{10}, \\
h_7 &:= x_3x_{11} + x_2x_{10} - x_3x_7 - x_2x_6, & h_8 &:= x_1x_{12}, \\
h_9 &:= x_1x_{13} - x_1x_7.
\end{aligned}$$

The conclusion is

$$c := (x_{10} - x_8)x_{13} - (x_{11} - x_9)x_{12} + x_8x_{11} - x_9x_{10}.$$

The set of independent variables is $\{x_1, x_2, x_3\}$.

We want to prove that Simson's Theorem is generally true and to compute the simplest nondegeneracy condition with respect to the relation $\prec$ in Section 6. We use the refutational approach to formulation 1 and compute $\mathbf{solve}_{14}(\emptyset, \{h_1, \ldots, h_9, cx_{14} - 1\})$. It turns out that all regular chains in the output set have at least one element in $Q[x_1, x_2, x_3]$. Therefore, it follows from Theorem 3 that Simson's Theorem is generally true. Applying the algorithm in Section 6, we obtain

$$(x_3^2 + x_2^2) \cdot (x_3^2 + x_2^2 + x_1^2 - 2x_1x_3)$$

as the simplest nondegeneracy condition. In [Cho90] the nondegeneracy condition

$$(x_3^2 + x_2^2) \cdot (x_3^2 + x_2^2 + x_1^2 - 2x_1x_3) \cdot x_1x_2 \cdot x_1^2$$

is given. In fact, a more careful analysis of the many regular chains in the output set of $\mathbf{solve}_{14}(\emptyset, \{h_1, \ldots, h_9, cx_{14} - 1\})$ shows that the ideal of nondegeneracy conditions D is generated by $(x_3^2 + x_2^2) \cdot (x_3^2 + x_2^2 + x_1^2 - 2x_1x_3)$. This can be proved using Lemma 2(b) and the following easy result:

Lemma 3 *Let R be a regular chain in $K[x_1, \ldots, x_t]$ and $f \in K[x_1, \ldots, x_t]$. Then*
a) *$V_t(\{primpart(f)\}) = Rep_t(\{f\})$ and*
b) *$Rep_t(R) \subseteq Rep_t(\{f\})$ iff $\mathbf{separate}_t(R, primpart(f)) = \emptyset$.* □

We intend to make a practical comparison between our method and the characteristic sets and Gröbner bases methods in the future.

No complexity analysis of our algorithm has been made. We think that such an analysis and a comparison with the complexity results on computing characteristic sets [GM90], Gröbner bases [DFGS89] and equidimensional decompositions of varieties [GH90] is a challenging problem for future research.

References

[Buc65] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* PhD thesis, Univ. Innsbruck, Dept. of Math., Innsbruck, Austria, 1965.

[Buc85] B. Buchberger. Gröbner bases: An algorithmic method in polynomial ideal theory. In N.K. Bose, editor, *Multidimensional Systems Theory*, pages 184–232. D. Reidel Publishing Company, Dordrecht-Boston-Lancaster, 1985.

[Buc87] B. Buchberger. Applications of Gröbner bases in non-linear computational geometry. In *Proc. Workshop on Scientific Software*, pages 59–88, IMA, Minneapolis, USA, 1987.

[CG90] S.C. Chou and X.S. Gao. Ritt-Wu's decomposition algorithm and geometry theorem proving. In *Proc. CADE-10*, pages 202–220, Kaiserslautern, Germany, 1990.

[Cho88] S.C. Chou. *Mechanical Geometry Theorem Proving*. D. Reidel Publ. Comp., Dordrecht, 1988.

[Cho90] S.C. Chou. Automated reasoning in geometries using the characteristic set method and Gröbner basis method. In *Proc. ISSAC'90*, pages 255–260, Tokyo, Japan, 1990.

[CS86] S.C. Chou and W.F. Schelter. Proving geometry theorems with rewrite rules. *J. Automated Reasoning*, 2:253–273, 1986.

[DD88] C. Dicrescenzo and D. Duval. Algebraic extensions and algebraic closure in Scratchpad II. In *Proc. ISSAC'88*, pages 440–446, Rome, Italy, 1988. Springer LNCS 358.

[DDD85] J. Della Dora, C. Dicrescenzo, and D. Duval. About a new method for computing in algebraic number fields. In *Proc. EUROCAL'85*, pages 289–290, Linz, Austria, 1985. Springer LNCS 204.

[DFGS89] A. Dickenstein, N. Fitchas, M. Giusti, and C. Sessa. The membership problem for unmixed polynomial ideals is solvable in subexponential time. In *Proc. AAECC-7*, pages 73–94, Toulouse, France, 1989.

[GC91] X.S. Gao and S.C. Chou. On the dimension of an arbitrary ascending chain. *Chinese Bull. of Sci. (to appear)*, 1991.

[GH90] M. Giusti and J. Heintz. Algorithmes – disons rapides – pour la décomposition d'une variété algébrique en composantes irréductibles et éq uidimentionnelles. In *Proc. MEGA'90*, pages 169–194, Livorno, Italy, 1990. Birkhäuser, Progress in Mathematics 94.

[GM90] G. Gallo and B. Mishra. Efficient algorithms and bounds for Wu-Ritt characteristic sets. In *Proc. MEGA'90*, pages 119–142, Livorno, Italy, 1990. Birkhäuser, Progress in Mathematics 94.

[Kal91] M. Kalkbrener. *Three contributions to elimination theory*. PhD thesis, Research Institute for Symbolic Computation, Univ. of Linz, Austria, 1991.

[Kal93] M. Kalkbrener. A generalized Euclidean algorithm for computing triangular representations of algebraic varieties. *J. Symb. Comp.*, 15:143–167, 1993.

[Kap86] D. Kapur. Geometry theorem proving using Hilbert's Nullstellensatz. In *Proc. SYMSAC'86*, pages 202–208, Waterloo, Canada, 1986.

[Kap88] D. Kapur. A refutational approach to geometry theorem proving. *Artificial Intelligence*, 37:61–94, 1988.

[KH85] H.P. Ko and M.A. Hussain. A study of Wu's method – a method to prove certain theorems in elementary geometry. In *Proc. of 1985 Congressus Numerantium*, 1985.

[Ko88] H.P. Ko. Geometry theorem proving by decomposition of quasi-algebraic sets: An application of the Ritt-Wu principle. *Artificial Intelligence*, 37:95–122, 1988.

[KS86] B. Kutzler and S. Stifter. Automated geometry theorem proving using Buchberger's algorithm. In *Proc. SYMSAC'86*, pages 209–214, Waterloo, Canada, 1986.

[KW90] D. Kapur and H.K. Wan. Refutational proofs of geometry theorems via characteristic set computation. In *Proc. ISSAC'90*, pages 277–284, Tokyo, Japan, 1990. ACM Press.

[Laz91] D. Lazard. A new method for solving algebraic systems of positive dimension. *Discrete Applied Math.*, 33:147–160, 1991.

[Laz92] D. Lazard. Solving zero-dimensional algebraic systems. *J. Symb. Comp.*, 13(2):117–132, 1992.

[Rit50] J.F. Ritt. *Differential Algebra*, volume 33 of *Colloquium Publications*. AMS, New York, 1950.

[vdW67] B.L. van der Waerden. *Algebra II (in German)*. Springer, Berlin Heidelberg New York, 5. edition, 1967.

[Wan95] D. Wang. Elimination procedures for mechanical theorem proving in geometries. *Annals of Math. and Artificial Intelligence*, 13:1–24, 1995.

[Win90] F. Winkler. Gröbner bases in geometry theorem proving and simplest degeneracy conditions. *Mathematica Pannonica*, 1:15–32, 1990.

[Wu78] W. Wu. On the decision problem and the mechanization of theorem proving in elementary geometry. *Scientia Sinica*, 21:157–179, 1978.

[Wu84] W. Wu. Basic principles of mechanical theorem proving in elementary geometries. *J. Sys. Sci. and Math. Scis*, 4:207–235, 1984.

[Wu86] W. Wu. On zeros of algebraic equations – an application of Ritt principle. *Kexue Tongbao*, 31(1):1–5, 1986.

[YZ91] L. Yang and J. Zhang. Searching dependency between algebraic equations: an algorithm applied to automated reasoning. Technical Report IC/91/6, International Atomic Energy Agency, Miramare, Trieste, 1991.