Comprehensive Triangular Decomposition

Changbo Chen[1], Oleg Golubitsky[1], François Lemaire[2], Marc Moreno Maza[1], and Wei Pan[1]

[1] University of Western Ontario, London N6A 1M8, Canada
[2] Université de Lille 1, 59655 Villeneuve d'Ascq Cedex, France

Abstract. We introduce the concept of comprehensive triangular decomposition (CTD) for a parametric polynomial system F with coefficients in a field. In broad words, this is a finite partition of the the parameter space into regions, so that within each region the "geometry" (number of irreducible components together with their dimensions and degrees) of the algebraic variety of the specialized system $F(u)$ is the same for all values u of the parameters.

We propose an algorithm for computing the CTD of F. It relies on a procedure for solving the following set theoretical instance of the coprime factorization problem. Given a family of constructible sets $A_1, \ldots, A_s$, compute a family $B_1, \ldots, B_t$ of pairwise disjoint constructible sets, such that for all $1 \leq i \leq s$ the set A_i writes as a union of some of the $B_1, \ldots, B_t$.

We report on an implementation of our algorithm computing CTDs, based on the `RegularChains` library in MAPLE. We provide comparative benchmarks with MAPLE implementations of related methods for solving parametric polynomial systems. Our results illustrate the good performances of our CTD code.

1 Introduction

Solving polynomial systems with parameters has become an increasing need in several applied areas such as robotics, geometric modeling, stability analysis of dynamical systems and others. For a given parametric polynomial system F, the following problems are of interest.

(P1) Compute the values of the parameters for which F has solutions, or has finitely many solutions.
(P2) Compute the solutions of F as functions of the parameters.

These questions have been approached by various techniques including comprehensive Gröbner bases (CGB) [22,23,14,13,17], cylindrical algebraic decomposition (CAD) [4] and triangular decompositions [24,25,6,7,10,9,20,19,26,5]. Methods based on CGB, or more generally Gröbner bases, are powerful tools for solving problems such as (P1), that is, determining the values u of the parameters such that, the specialized system $F(u)$ satisfies a given property. Methods based on CAD or triangular decompositions are naturally well designed for solving Problem (P2).

In this paper, we introduce the concept of *comprehensive triangular decomposition* for a parametric polynomial system with coefficients in a field. This notion plays the role for triangular decompositions that CGB does for Gröbner bases. With this concept

V.G. Ganzha, E.W. Mayr, and E.V. Vorozhtsov (Eds.): CASC 2007, LNCS 4770, pp. 73–101, 2007.

at hand, we show that Problems (P1) and (P2) can be completely answered by means of triangular decompositions.

Let F be a finite set of polynomials with coefficients in a field $\mathbb{K}$, parameters $U = U_1, \ldots, U_d$, and unknowns $X = X_1, \ldots, X_m$, that is, $F \subset \mathbb{K}[U_1, \ldots, U_d, X_1, \ldots, X_m]$. Let $\overline{\mathbb{K}}$ be the algebraic closure of $\mathbb{K}$, and let $\mathbf{V}(F) \subset \overline{\mathbb{K}}^{d+m}$ be the zero set of F . Let also Π_U be the projection from $\overline{\mathbb{K}}^{d+m}$ on the parameter space $\overline{\mathbb{K}}^{d}$. For all $u \in \overline{\mathbb{K}}^{d}$ we define $\mathbf{V}(F(u)) \subseteq \overline{\mathbb{K}}^{m}$ the zero set defined by F after specializing U at u.

Our first contribution is to show how to compute a finite partition $\mathcal{C}$ of $\Pi_U(\mathbf{V}(F))$ and a family of triangular decompositions $(\mathcal{T}_C, C \in \mathcal{C})$ in $\mathbb{K}[U, X]$ such that for each $C \in \mathcal{C}$ and for each parameter value $u \in C$ the triangular decomposition $\mathcal{T}_C$ specializes at u into a triangular decomposition $\mathcal{T}_C(u)$ of $\mathbf{V}(F(u))$ given by regular chains. Moreover, each "cell" $C \in \mathcal{C}$ is a constructible set given by a family of regular systems in $\mathbb{K}[U]$. We call the pair $(\mathcal{T}_C, C \in \mathcal{C})$ a *comprehensive triangular decomposition* of $\mathbf{V}(F)$, see Section 5.

This is a natural definition inspired by that of a comprehensive Gröbner basis [22] introduced by Weispfenning with the additional requirements proposed by Montes in [14]. From each pair $(C, \mathcal{T}_C)$, we can read geometrical information, such as for which parameter values $u \in C$ the set $\mathbf{V}(F(u))$ is finite; we also obtain a "generic" equidimensional decomposition of $\mathbf{V}(F(u))$, for all $u \in C$. The notion of CTD is also related to the border polynomial of a polynomial system in [26] and the minimal discriminant variety of $\mathbf{V}(F)$ as defined in [12] for the case where $\overline{\mathbb{K}}$ is the field of complex numbers.

Example 1. Let $F = \{vxy + ux^2 + x, uy^2 + x^2\}$ be a parametric polynomial system with parameters $u > v$ and unknowns $x > y$. Then a comprehensive triangular decomposition of $\mathbf{V}(F)$ is:

$$\begin{aligned} C_1 = \{u(u^3+v^2) \neq 0\} : &\quad \mathcal{T}_{C_1} = \{T_3, T_4\} \\ C_2 = \{u = 0\} : &\quad \mathcal{T}_{C_2} = \{T_2, T_3\} \\ C_3 = \{u^3 + v^2 = 0, v \neq 0\} : &\quad \mathcal{T}_{C_3} = \{T_1, T_3\} \end{aligned}$$

where

$$\begin{aligned} T_1 &= \{vxy + x - u^2y^2, 2vy + 1, u^3 + v^2\} \\ T_2 &= \{x, u\} \\ T_3 &= \{x, y\} \\ T_4 &= \{vxy + x - u^2y^2, u^3y^2 + v^2y^2 + 2vy + 1\} \end{aligned}$$

Here , C_1, C_2, C_3 is a partition of $\Pi_U(\mathbf{V}(F))$ and $\mathcal{T}_{C_i}$ is a triangular decomposition of $\mathbf{V}(F)$ above C_i, for $i = 1, 2, 3$. For different parameter values u, we can directly read geometrical information, such as the dimension of $\mathbf{V}(F(u))$.

By `RegSer` [19], $\mathbf{V}(F)$ can be decomposed into a set of regular systems:

$$R_1 = \begin{cases} ux + vy + 1 = 0 \\ (u^3 + v^2)y^2 + 2vy + 1 = 0 \\ u(u^3 + v^2) \neq 0 \end{cases}, \quad R_2 = \begin{cases} x = 0 \\ y = 0 \\ u \neq 0 \end{cases},$$

$$R_3 = \begin{cases} x = 0 \\ vy + 1 = 0 \\ u = 0 \\ v \neq 0 \end{cases}, \quad R_4 = \begin{cases} 2ux + 1 = 0 \\ 2vy + 1 = 0 \\ u^3 + v^2 = 0 \\ v \neq 0 \end{cases}, \quad R_5 = \begin{cases} x = 0 \\ u = 0 \end{cases}.$$

For each regular system, one can directly read its dimension when parameters take corresponding values. However, the dimension of the input system could not be obtained immediately, since there is not a partition of the parameter space.

By `DISPGB` [14], one can obtain all the cases over the parameters leading to different reduced Gröbner bases with parameters:

$$\begin{aligned} u(u^3+v^2) \neq 0 &: \{ux+(u^3v+v^3)y^3+(-u^3+v^2)y^2, (u^3+v^2)y^4+2vy^3+y^2\} \\ u(u^3+v^2) = 0, u \neq 0 &: \{ux+2v^2y^2, 2vy^3+y^2\} \\ u = 0, v \neq 0 &: \{x^2, vxy+x\} \\ u = 0, v = 0 &: \{x\} \end{aligned}$$

Here for each parameter value, the input system specializes into a Gröbner basis. Since Gröbner bases do not necessarily have a triangular shape, the dimension may not be read directly either. For example, when $u = 0, v \neq 0$, $\{x^2, vxy + x\}$ is not a triangular set.

In Section 5 we also propose an algorithm for computing the CTD of parametric polynomial system. We rely on an algorithm for computing the difference of the zero sets of two regular systems. Based on the procedures of the TRIADE algorithm [15] and elementary set theoretical considerations, such an algorithm could be developed straightforwardly. We actually tried this and our experimental results (not reported here) shows that this naive approach is very inefficient comparing to the more advanced algorithm presented in Section 3. Indeed, this latter algorithm heavily exploits the structure and properties of regular chains, whereas the former is unable to do so.

This latter procedure, is used to solve the following problem. Given a family of constructible sets, $A_1, \ldots, A_s$ (each of them given by a regular system) compute a family $B_1, \ldots, B_t$ of pairwise disjoint constructible sets, such that for all $1 \leq i \leq s$ the set A_i writes as a union of some the $B_1, \ldots, B_t$. A solution is presented in Section 4. This can be seen as the set theoretical version of the *coprime factorization* problem, see [2,8] for other variants of this problem.

Our second contribution is an implementation report of our algorithm computing CTDs, based on the `RegularChains` library in MAPLE. We provide comparative benchmarks with MAPLE implementations of related methods for solving parametric polynomial systems, namely: *decompositions into regular systems* by Wang [19] and *discussing parametric Gröbner bases* by Montes [14]. We use a large set of well-known test-problems from the literature. Our implementation of the CTD algorithm can solve all problems which can be solved by the other methods. In addition, our CTD code can solve problems which are out of reach of the other two methods, generally due to memory consumption.

2 Preliminaries

In this section we introduce notations and review fundamental results in the theory of regular chains and regular systems [1,3,11,15,19,21].

We shall use some notions from commutative algebra (such as the dimension of an ideal) and refer for instance to [16] for this subject.

2.1 Basic Notations and Definitions

Let $\mathbb{K}[Y] := \mathbb{K}[Y_1, \ldots, Y_n]$ be the polynomial ring over the field $\mathbb{K}$ in variables $Y_1 < \cdots < Y_n$. Let $p \in \mathbb{K}[Y]$ be a non-constant polynomial. The *leading coefficient* and the *degree* of p regarded as a univariate polynomial in Y_i will be denoted by $\mathrm{lc}(p, Y_i)$ and $\deg(p, Y_i)$ respectively. The greatest variable appearing in p is called the *main variable* denoted by $\mathrm{mvar}(p)$. The degree, the leading coefficient, and the leading monomial of p regarding as a univariate polynomial in $\mathrm{mvar}(p)$ are called the *main degree*, the *initial*, and the *rank* of p; they are denoted by $\mathrm{mdeg}(p)$, $\mathrm{init}(p)$ and $\mathrm{rank}(p)$ respectively.

Let $F \subset \mathbb{K}[Y]$ be a finite polynomial set. Denote by $\langle F \rangle$ the ideal it generates in $\mathbb{K}[Y]$ and by $\sqrt{\langle F \rangle}$ the radical of $\langle F \rangle$. Let h be a polynomial in $\mathbb{K}[Y]$, the *saturated ideal* $\langle F \rangle : h^\infty$ of $\langle F \rangle$ w.r.t h, is the set

$$\{q \in \mathbb{K}[Y] \mid \exists m \in \mathbb{N} \text{ s.t. } h^m q \in \langle F \rangle\},$$

which is an ideal in $\mathbb{K}[Y]$.

A polynomial $p \in \mathbb{K}[Y]$ is a *zerodivisor* modulo $\langle F \rangle$ if there exists a polynomial q such that pq is zero modulo $\langle F \rangle$, and q is not zero modulo $\langle F \rangle$. The polynomial is *regular* modulo $\langle F \rangle$ if it is neither zero, nor a zerodivisor modulo $\langle F \rangle$. Denote by $\mathbf{V}(F)$ the *zero set* (or solution set, or algebraic variety) of F in $\overline{\mathbb{K}}^n$. For a subset $W \subset \overline{\mathbb{K}}^n$, denote by $\overline{W}$ its closure in the Zariski topology, that is the intersection of all algebraic varieties $\mathbf{V}(G)$ containing W for all $G \subset \mathbb{K}[Y]$.

Let $T \subset \mathbb{K}[Y]$ be a *triangular set*, that is a set of non-constant polynomials with pairwise distinct main variables. Denote by $\mathrm{mvar}(T)$ the set of main variables of $t \in T$. A variable in Y is called *algebraic* w.r.t. T if it belongs to $\mathrm{mvar}(T)$, otherwise it is called *free* w.r.t. T. For a variable $v \in Y$ we denote by $T_{<v}$ (resp. $T_{>v}$) the subsets of T consisting of the polynomials t with main variable less than (resp. greater than) v. If $v \in \mathrm{mvar}(T)$, we say T_v is defined. Moreover, we denote by T_v the polynomial in T whose main variable is v, by $T_{\leqslant v}$ the set of polynomials in T with main variables less than or equal to v and by $T_{\geqslant v}$ the set of polynomials in T with main variables greater than or equal to v.

Definition 1. *Let* p, $q \in \mathbb{K}[Y]$ *be two nonconstant polynomials. We say* $\mathrm{rank}(p)$ *is smaller than* $\mathrm{rank}(q)$ *w.r.t* Ritt ordering *and we write,* $\mathrm{rank}(p) <_r \mathrm{rank}(q)$ *if one of the following assertions holds:*

- $\mathrm{mvar}(p) < \mathrm{mvar}(q)$,
- $\mathrm{mvar}(p) = \mathrm{mvar}(q)$ *and* $\mathrm{mdeg}(p) < \mathrm{mdeg}(q)$.

Note that the partial order $<_r$ is a well ordering. Let $T \subset \mathbb{K}[Y]$ be a triangular set. Denote by $\mathrm{rank}(T)$ the set of $\mathrm{rank}(p)$ for all $p \in T$. Observe that any two ranks in $\mathrm{rank}(T)$ are comparable by $<_r$. Given another triangular set $S \subset \mathbb{K}[Y]$, with $\mathrm{rank}(S) \neq \mathrm{rank}(T)$, we write $\mathrm{rank}(T) <_r \mathrm{rank}(S)$ whenever the minimal element of the symmetric difference $(\mathrm{rank}(T) \setminus \mathrm{rank}(S)) \cup (\mathrm{rank}(S) \setminus \mathrm{rank}(T))$ belongs to $\mathrm{rank}(T)$. By

$\operatorname{rank}(T) \leqslant_r \operatorname{rank}(S)$, we mean either $\operatorname{rank}(T) < \operatorname{rank}(S)$ or $\operatorname{rank}(T) = \operatorname{rank}(S)$. Note that any sequence of triangular sets, of which ranks strictly decrease w.r.t $<_r$, is finite.

Given a triangular set $T \subset \mathbb{K}[Y]$, denote by h_T be the product of the initials of T (throughout the paper we use this convention and when T consists of a single element g we write it in h_g for short). The *quasi-component* $\mathbf{W}(T)$ of T is $\mathbf{V}(T) \setminus \mathbf{V}(h_T)$, in other words, the points of $\mathbf{V}(T)$ which do not cancel any of the initials of T. We denote by $\operatorname{Sat}(T)$ the *saturated ideal of* T: if T is empty then $\operatorname{Sat}(T)$ is defined as the trivial ideal $\langle 0 \rangle$, otherwise it is the ideal $\langle T \rangle : h_T^{\infty}$.

Let $h \in \mathbb{K}[Y]$ be a polynomial and $F \subset \mathbb{K}[Y]$ a set of polynomials, we write

$$\mathbf{Z}(F, T, h) := (\mathbf{V}(F) \cap \mathbf{W}(T)) \setminus \mathbf{V}(h).$$

When F consists of a single polynomial p, we use $\mathbf{Z}(p, T, h)$ instead of $\mathbf{Z}(\{p\}, T, h)$; when F is empty we just write $\mathbf{Z}(T, h)$. By $\mathbf{Z}(F, T)$, we denote $\mathbf{V}(F) \cap \mathbf{W}(T)$.

Given a family of pairs $\mathbf{S} = \{[T_i, h_i] \mid 1 \leq i \leq e\}$, where $T_i \subset \mathbb{K}[Y]$ is a triangular set and $h_i \in \mathbb{K}[Y]$ is a polynomial. We write

$$\mathbf{Z}(S) := \bigcup_{i=1}^{e} \mathbf{Z}(T_i, h_i).$$

We conclude this section with some well known properties of ideals and triangular sets. For a proper ideal $\mathcal{I}$, we denote by $\dim(\mathbf{V}(\mathcal{I}))$ the dimension of $\mathbf{V}(\mathcal{I})$.

Lemma 1. *Let $\mathcal{I}$ be a proper ideal in $\mathbb{K}[Y]$ and $p \in \mathbb{K}[Y]$ be a polynomial regular w.r.t $\mathcal{I}$. Then, either $\mathbf{V}(\mathcal{I}) \cap \mathbf{V}(p)$ is empty or we have:* $\dim(\mathbf{V}(\mathcal{I}) \cap \mathbf{V}(p)) \leq \dim(\mathbf{V}(\mathcal{I})) - 1$.

Lemma 2. *Let T be a triangular set in $\mathbb{K}[Y]$. Then, we have*

$$\overline{\mathbf{W}(T)} \setminus \mathbf{V}(h_T) = \mathbf{W}(T) \ \text{ and } \ \overline{\mathbf{W}(T)} \setminus \mathbf{W}(T) = \mathbf{V}(h_T) \cap \overline{\mathbf{W}(T)}.$$

PROOF. Since $\mathbf{W}(T) \subseteq \overline{\mathbf{W}(T)}$, we have

$$\mathbf{W}(T) = \mathbf{W}(T) \setminus \mathbf{V}(h_T) \subseteq \overline{\mathbf{W}(T)} \setminus \mathbf{V}(h_T).$$

On the other hand, $\overline{\mathbf{W}(T)} \subseteq \mathbf{V}(T)$ implies

$$\overline{\mathbf{W}(T)} \setminus \mathbf{V}(h_T) \subseteq \mathbf{V}(T) \setminus \mathbf{V}(h_T) = \mathbf{W}(T).$$

This proves the first claim. Observe that we have:

$$\overline{\mathbf{W}(T)} = \left(\overline{\mathbf{W}(T)} \setminus \mathbf{V}(h_T)\right) \cup \left(\overline{\mathbf{W}(T)} \cap \mathbf{V}(h_T)\right).$$

We deduce the second one.

Lemma 3 ([1,3]). *Let T be a triangular set in $\mathbb{K}[Y]$. Then, we have*

$$\mathbf{V}(\operatorname{Sat}(T)) = \overline{\mathbf{W}(T)}.$$

Assume furthermore that $\mathbf{W}(T) \neq \emptyset$ holds. Then $\mathbf{V}(\operatorname{Sat}(T))$ is a nonempty unmixed algebraic set with dimension $n - |T|$. Moreover, if N is the free variables of T, then for every prime ideal $\mathcal{P}$ associated with $\operatorname{Sat}(T)$ *we have*

$$\mathcal{P} \cap \mathbb{K}[N] = \langle 0 \rangle.$$

2.2 Regular Chain and Regular System

Definition 2 (Regular Chain). *A triangular set $T \subset \mathbb{K}[Y]$ is a* regular chain *if one of the following conditions hold:*

- *either T is empty,*
- *or $T \setminus \{T_{\max}\}$ is a regular chain, where $T_{\max}$ is the polynomial in T with maximum rank, and the initial of $T_{\max}$ is regular w.r.t.* $\mathrm{Sat}(T \setminus \{T_{\max}\})$.

It is useful to extend the notion of regular chain as follows.

Definition 3 (Regular System). *A pair $[T, h]$ is a regular system if T is a regular chain, and $h \in \mathbb{K}[Y]$ is regular w.r.t* $\mathrm{Sat}(T)$.

Remark 1. *A regular system in a stronger sense was presented in [19]. For example, consider the polynomial system $[T, h]$ where $T = [Y_1Y_4 - Y_2]$ and $h = Y_2Y_3$. Then $[T, h]$ is still a regular system in our sense but not a regular system in Wang's sense. Also we do not restrict the main variables of polynomials in the inequality part. At least our definition is more convenient for our purpose in dealing with zerodivisors and conceptually clear as well. We also note that in the zerodimensional case (no free variables exist) the notion of regular chain and that of a regular set in [19] are the same, see [1,19] for details.*

There are several equivalent characterizations of a regular chain, see [1]. In this paper, we rely on the notion of *iterated resultant* in order to derive a characterization which can be checked by solving a polynomial system.

Definition 4. *Let $p \in \mathbb{K}[Y]$ be a polynomial and $T \subset \mathbb{K}[Y]$ be a triangular set. The* iterated resultant *of p w.r.t. T, denoted by* $\mathrm{res}(p, T)$*, is defined as follows:*

- *if $p \in \mathbb{K}$ or all variables in p are free w.r.t. T, then* $\mathrm{res}(p, T) = p$,
- *otherwise, if v is the largest variable of p which is algebraic w.r.t. T, then* $\mathrm{res}(p, T) = \mathrm{res}(r, T_{<v})$ *where r is the resultant of p and the polynomial T_v.*

Lemma 4. *Let $p \in \mathbb{K}[Y]$ be a polynomial and $T \subset \mathbb{K}[Y]$ be a zerodimensional regular chain. Then the following statements are equivalent:*

(i) *The iterated resultant* $\mathrm{res}(p, T) \neq 0$.
(ii) *The polynomial p is regular modulo $\langle T \rangle$.*
(iii) *The polynomial p is invertible modulo $\langle T \rangle$.*

PROOF. "$(i) \Rightarrow (ii)$" Let $r := \mathrm{res}(p, T)$. Then there exist polynomials $A_i \in \mathbb{K}[Y]$, $0 \le i \le n$, such that $r = A_0 p + \sum_{i=1}^{n} A_i T_i$. So $r \neq 0$ implies p is invertible modulo $\langle T \rangle$. Therefore, p is regular modulo $\langle T \rangle$.

"$(ii) \Rightarrow (iii)$" If p is regular modulo $\langle T \rangle$, then p is regular modulo $\sqrt{\langle T \rangle}$. Since T is a zerodimensional regular chain, which implies $\mathrm{Sat}(T) = \langle T \rangle$, we know that $\mathbb{K}[Y]/\sqrt{\langle T \rangle}$ is a direct product of fields. Therefore p is invertible modulo $\sqrt{\langle T \rangle}$, which implies p is invertible modulo $\langle T \rangle$.

"$(iii) \Rightarrow (i)$" Assume $\mathrm{res}(p, T) = 0$, then we claim that p and T have at least one common solution, which is a contradiction to (iii).

We prove our claim by induction on $|T|$.

If $|T| = 1$, we have two cases

(1) If all variables in p are free w.r.t. T, then $\mathrm{res}(p, T) = p = 0$. The claim holds.
(2) Otherwise, we have $\mathrm{res}(p, T) = \mathrm{res}(p, T, \mathrm{mvar}(T)) = 0$. Since $\mathrm{init}(T) \neq 0$, the claim holds.

Now we assume that the claim holds for $|T| = n - 1$. If $|T| = n$, let $v := Y_n$. We have two cases

(1) If v does not appear in p, then $\mathrm{res}(p, T) = \mathrm{res}(p, T_{<v})$. By induction hypothesis, there exist $\xi_1, \xi_2, \cdots, \xi_{n-1} \in \overline{\mathbb{K}}$, such that $\xi' = (\xi_1, \xi_2, \cdots, \xi_{n-1})$ is a common solution of p and $T_{<v}$. Since T is a zerodimensional regular chain, h_{T_v} is invertible modulo $\langle T \rangle$ (by "$(ii) \Rightarrow (iii)$"). So $h_{T_v}(\xi') \neq 0$, which implies that there exists a $\xi_n \in \overline{\mathbb{K}}$, such that $\xi := (\xi_1, \xi_2, \cdots, \xi_{n-1}, \xi_n)$ is a solution of T_v. Therefore ξ is a common solution of p and T.
(2) If v appears in p, then $\mathrm{res}(p, T) = \mathrm{res}(\mathrm{res}(p, T_v, v), T_{<v}) = 0$. Similarly to (1), there exists $\xi' = (\xi_1, \xi_2, \cdots, \xi_{n-1})$, such that $\mathrm{res}(p, T_v, v)(\xi') = T_{<v}(\xi') = 0$ and $h_{T_v}(\xi') \neq 0$. So by the specialization property of resultant, $\mathrm{res}(p(\xi'), T_v(\xi'), v) = 0$, which implies that there exists a $\xi_n \in \overline{\mathbb{K}}$, such that $\xi := (\xi_1, \xi_2, \cdots, \xi_{n-1}, \xi_n)$ is a common solution of p and T_v. Therefore ξ is a common solution of p and T.

Theorem 1. *The triangular set T is a regular chain if and only if* $\mathrm{res}(h_T, T) \neq 0$.

PROOF. We start by assuming that T is a zerodimensional regular chain, then the conclusion follows from Lemma 4.

We reduce the general case to the zerodimensional one. First, we introduce a new total ordering $<_T$ on Y defined as follows: if Y_i and Y_j are both in $\mathrm{mvar}(T)$ or both in its complement then $Y_i <_T Y_j$ holds if and only if $Y_i < Y_j$ holds, otherwise $Y_i <_T Y_j$ holds if and only if $Y_j \in \mathrm{mvar}(T)$. Clearly T is also a triangular set w.r.t $<_T$. We observe that h_T, and thus $\mathrm{Sat}(T)$, are unchanged when replacing the variable ordering $<$ by $<_T$. Similarly, it is easy to check that a polynomial $p \in \mathbb{K}[Y]$ reduces to zero by pseudo-division by T w.r.t. $<$ if and only if it reduces to zero by pseudo-division by T w.r.t. $<_T$. Therefore, by applying Theorem 6.1 [1] we deduce that T is a regular chain w.r.t. $<$ if and only if it is a regular chain w.r.t. $<_T$. Similarly, we have $\mathrm{res}(h_T, T) \neq 0$ w.r.t. $<$ if and only if $\mathrm{res}(h_T, T) \neq 0$ w.r.t. $<_T$.

Now we assume that the variables are ordered according to $<_T$. Let N be the set of the variables of Y that do not belong to $\mathrm{mvar}(T)$. The triangular set T is a regular chain in $\mathbb{K}[Y]$ if and only if it is a zerodimensional regular chain when regarded as a triangular set in $\mathbb{K}(N)[Y \setminus N]$ (where $\mathbb{K}(N)$ denotes the field of rational functions with coefficients in $\mathbb{K}$ and variables in N). This is Corollary 3.2 in [3]. Similarly, it is easy to check that $\mathrm{res}(h_T, T) \neq 0$ holds when regarding T in $\mathbb{K}[Y]$ if and only if $\mathrm{res}(h_T, T) \neq 0$ holds when regarding T in $\mathbb{K}(N)[Y \setminus N]$.

Proposition 1. *For every regular system $[T, h]$ we have $\mathbf{Z}(T, h) \neq \emptyset$.*

PROOF. Since T is a regular chain, by Lemma 3 we have $\mathbf{V}(\mathrm{Sat}(T)) \neq \emptyset$. By definition of regular system, the polynomial hh_T is regular w.r.t Sat(T). Hence, by Lemma 1, the set $\mathbf{V}(hh_T) \cap \mathbf{V}(\mathrm{Sat}(T))$ either is empty, or has lower dimension than $\mathbf{V}(\mathrm{Sat}(T))$. Therefore, the set

$$\mathbf{V}(\mathrm{Sat}(T)) \setminus \mathbf{V}(hh_T) = \mathbf{V}(\mathrm{Sat}(T)) \setminus (\mathbf{V}(hh_T) \cap \mathbf{V}(\mathrm{Sat}(T)))$$

is not empty. Finally, by Lemma 2, the set

$$\mathbf{Z}(T,h) = \mathbf{W}(T) \setminus \mathbf{V}(h) = \overline{\mathbf{W}(T)} \setminus \mathbf{V}(hh_T) = \mathbf{V}(\mathrm{Sat}(T)) \setminus \mathbf{V}(hh_T)$$

is not empty.

Notation 1. *For a regular system $R = [T, h]$, we define* rank(R) := rank(T). *For a set $\mathcal{R}$ of regular systems, we define*

$$\mathrm{rank}(\mathcal{R}) := \max\{\mathrm{rank}(T) \mid [T,h] \in \mathcal{R}\}.$$

For a pair of regular systems (L, R), we define rank$((L, R))$:= (rank(L), rank(R)). *For a pair of lists of regular systems, we define*

$$\mathrm{rank}((\mathcal{L}, \mathcal{R})) = (\mathrm{rank}(\mathcal{L}), \mathrm{rank}(\mathcal{R})).$$

For triangular sets $T, T_1, \ldots, T_e$ we write $\mathbf{W}(T) \xrightarrow{D} (\mathbf{W}(T_i), i = 1 \ldots e)$ if one of the following conditions holds:

- *either $e = 1$ and $T = T_1$,*
- *or $e > 1$,* rank$(T_i) <$ rank(T) *for all $i = 1 \ldots e$ and*

$$\mathbf{W}(T) \subseteq \bigcup_{i=1}^{e} \mathbf{W}(T_i) \subseteq \overline{\mathbf{W}(T)}.$$

2.3 Triangular Decompositions

Definition 5. *Given a finite polynomial set $F \subset \mathbb{K}[Y]$, a* triangular decomposition *of $\mathbf{V}(F)$ is a finite family $\mathcal{T}$ of regular chains of $\mathbb{K}[Y]$ such that*

$$\mathbf{V}(F) = \bigcup\nolimits_{T \in \mathcal{T}} \mathbf{W}(T).$$

For a finite polynomial set $F \subset \mathbb{K}[Y]$, the TRIADE algorithm [15] computes a triangular decomposition of $\mathbf{V}(F)$. We list below the specifications of the operations from TRIADE that we use in this paper.

Let p, p_1, p_2 be polynomials, and let T, C, E be regular chains such that $C \cup E$ is a triangular set (but not necessarily a regular chain).

- $\mathbf{Regularize}(p, T)$ returns regular chains $T_1, \ldots, T_e$ such that
  - $\mathbf{W}(T) \xrightarrow{D} (\mathbf{W}(T_i), i = 1 \ldots e)$,
  - for all $1 \leq i \leq e$ the polynomial p is either 0 or regular modulo Sat(T_i).

– For a set of polynomials F, $\mathbf{Triangularize}(F, T)$ returns regular chains $T_1, \ldots, T_e$ such that we have

$$\mathbf{V}(F) \cap \mathbf{W}(T) \subseteq \mathbf{W}(T_1) \cup \cdots \cup \mathbf{W}(T_e) \subseteq \mathbf{V}(F) \cap \overline{\mathbf{W}(T)}.$$

and for $1 \leq i \leq e$ we have $\operatorname{rank}(T_i) < \operatorname{rank}(T)$.

– $\mathbf{Extend}(C \cup E)$ returns a set of regular chains $\{C_i \mid i = 1 \ldots e\}$ such that we have $\mathbf{W}(C \cup E) \xrightarrow{D} (\mathbf{W}(C_i), i = 1 \ldots e)$.

– Assume that p_1 and p_2 are two non-constant polynomials with the same main variable v, which is larger than any variable appearing in T, and assume that the initials of p_1 and p_2 are both regular w.r.t. Sat(T). Then, $\mathbf{GCD}(p_1, p_2, T)$ returns a sequence

$$([g_1, C_1], \ldots, [g_d, C_d], [\emptyset, D_1], \ldots, [\emptyset, D_e]),$$

where g_i are polynomials and C_i, D_i are regular chains such that the following properties hold:

  - $\mathbf{W}(T) \xrightarrow{D} (\mathbf{W}(C_1), \ldots, \mathbf{W}(C_d), \mathbf{W}(D_1), \ldots, \mathbf{W}(D_e))$,
  - $\dim \mathbf{V}(\text{Sat}(C_i)) = \dim \mathbf{V}(\text{Sat}(T))$ and $\dim \mathbf{V}(\text{Sat}(D_j)) < \dim \mathbf{V}(\text{Sat}(T))$, for all $1 \leqslant i \leqslant d$ and $1 \leqslant j \leqslant e$,
  - the leading coefficient of g_i w.r.t. v is regular w.r.t. Sat(C_i),
  - for all $1 \leqslant i \leqslant d$ there exist polynomials u_i and v_i such that we have $g_i = u_i p_1 + v_i p_2 \mod \text{Sat}(C_i)$,
  - if g_i is not constant and its main variable is v, then p_1 and p_2 belong to Sat$(C_i \cup \{g_i\})$.

2.4 Constructible Sets

Definition 6 (Constructible set). *A constructible subset of $\overline{\mathbb{K}}^n$ is any finite union*

$$(A_1 \setminus B_1) \cup \cdots \cup (A_e \setminus B_e)$$

where $A_1, \ldots, A_e, B_1, \ldots, B_e$ are algebraic varieties in $\overline{\mathbb{K}}^n$.

Lemma 5. *Every constructible set can write as a union of zero sets of regular systems.*

PROOF. By the definition of constructible set, we only need to prove that the difference of two algebraic varieties can write as a union of zero sets of regular systems. Let $\mathbf{V}(F), \mathbf{V}(G)$, where $F, G \subset \mathbb{K}[Y]$, be two algebraic varieties in $\overline{\mathbb{K}}^n$. With the $\mathbf{Triangularize}$ operation introduced in last subsection, we write $\mathbf{V}(F)$ as a union of the zero sets of some regular systems

$$\mathbf{V}(F) = \bigcup_{i=1}^{s} \mathbf{W}(T_i) = \bigcup_{i=1}^{s} \mathbf{Z}(T_i, 1).$$

Similarly, we can write $\mathbf{V}(G)$ as

$$\mathbf{V}(G) = \bigcup_{i=1}^{t} \mathbf{Z}(C_i, 1).$$

Then the conclusion follows from the algorithm $\mathbf{DifferenceLR}$ introduced in next section.

3 The Difference Algorithms

In this section, we present an algorithm to compute the set theoretical difference of two constructible sets given by regular systems. As mentioned in the Introduction, a naive approach appears to be very inefficient in practice. Here we contribute a more sophisticated algorithm, which heavily exploits the structure and properties of regular chains.

Two procedures, **Difference** and **DifferenceLR**, are involved in order to achieve this goal. Their specifications and pseudo-codes can be found below. The rest of this section is dedicated to proving the correctness and termination of these algorithms. For the pseudo-code, we use the MAPLE syntax. However, each of the two functions below returns a sequence of values. Individual value or sub-sequences of the returned sequence are thrown to the flow of output by means of an **output** statement. Hence an **output** statement does not cause the termination of the function execution.

Algorithm 1 **Difference**$([T, h], [T', h'])$
Input $[T, h]$, $[T', h']$ two regular systems.
Output Regular systems $\{[T_i, h_i] \mid i = 1 \ldots e\}$ such that

$$\mathbf{Z}(T, h) \setminus \mathbf{Z}(T', h') = \bigcup_{i=1}^{e} \mathbf{Z}(T_i, h_i),$$

and $\operatorname{rank}(T_i) \leqslant_r \operatorname{rank}(T)$.

Algorithm 2 **DifferenceLR**$(\mathcal{L}, \mathcal{R})$
Input $\mathcal{L} := \{[L_i, f_i] \mid i = 1 \ldots r\}$ and $\mathcal{R} := \{[R_j, g_j] \mid j = 1 \ldots s\}$ two lists of regular systems.
Output Regular systems $\mathcal{S} := \{[T_i, h_i] \mid i = 1 \ldots e\}$ such that

$$\left(\bigcup_{i=1}^{r} \mathbf{Z}(L_i, f_i)\right) \setminus \left(\bigcup_{j=1}^{s} \mathbf{Z}(R_j, g_j)\right) = \bigcup_{i=1}^{e} \mathbf{Z}(T_i, h_i),$$

with $\operatorname{rank}(\mathcal{S}) \leqslant_r \operatorname{rank}(\mathcal{L})$.

To prove the termination and correctness of above two algorithms, we present a series of technical lemmas.

Lemma 6. *Let p and h be polynomials and T a regular chain. Assume that $p \notin \operatorname{Sat}(T)$. Then there exists an operation* $\mathbf{Intersect}(p, T, h)$ *returning a set of regular chains* $\{T_1, \ldots, T_e\}$ *such that*

(i) *h is regular w.r.t* $\operatorname{Sat}(T_i)$ *for all i;*
(ii) $\operatorname{rank}(T_i) <_r \operatorname{rank}(T)$*;*
(iii) $\mathbf{Z}(p, T, h) \subseteq \cup_{i=1}^{e} \mathbf{Z}(T_i, h) \subseteq (\mathbf{V}(p) \cap \overline{\mathbf{W}(T)}) \setminus \mathbf{V}(h)$*;*
(iv) *Moreover, if the product of initials h_T of T divides h then*

$$\mathbf{Z}(p, T, h) = \bigcup_{i=1}^{e} \mathbf{Z}(T_i, h).$$

Algorithm 1. Difference$([T,h],[T',h'])$

```
if Sat(T) = Sat(T') then
    output Intersect(h' h_{T'}, T, h h_T)
else
    Let v be the largest variable s.t. Sat(T_{<v}) = Sat(T'_{<v})
    if v ∈ mvar(T') and v ∉ mvar(T) then
        p' ← T'_v
        output [T, hp']
        output DifferenceLR(Intersect(p', T, h h_T), [T', h'])
    else if v ∉ mvar(T') and v ∈ mvar(T) then
        p ← T_v
        output DifferenceLR([T, h], Intersect(p, T', h' h_{T'}))
    else
        p ← T_v
        G ← GCD(T_v, T'_v, T_{<v})
        if |G| = 1 then
            Let (g, C) ∈ G
            if g ∈ K then
                output [T, h]
            else if mvar(g) < v then
                output [T, gh]
                output DifferenceLR(Intersect(g, T, h h_T), [T', h'])
            else if mvar(g) = v then
                if mdeg(g) = mdeg(p) then
                    D'_p ← T'_{<v} ∪ {p} ∪ T'_{>v}
                    output Difference([T, h], [D'_p, h' h_{T'}])
                else if mdeg(g) < mdeg(p) then
                    q ← pquo(p, g, C)
                    D_g ← C ∪ {g} ∪ T_{>v}
                    D_q ← C ∪ {q} ∪ T_{>v}
                    output Difference([D_g, h h_T], [T', h'])
                    output Difference([D_q, h h_T], [T', h'])
                    output DifferenceLR(Intersect(h_g, T, h h_T), [T', h'])
                end if
            end if
        else if |G| ≥ 2 then
            for (g, C) ∈ G do
                if |C| > |T_{<v}| then
                    for E ∈ Extend(C, T_{⩾v}) do
                        for D ∈ Regularize(h h_T, E) do
                            if h h_T ∉ Sat(D) then
                                output Difference([D, h h_T], [T', h'])
                            end if
                        end for
                    end for
                else
                    output Difference([C ∪ T_{⩾v}, h h_T], [T', h'])
                end if
            end for
        end if
    end if
end if
```

Algorithm 2. $\mathbf{DifferenceLR}(L, R)$

if $L = \emptyset$ **then**
  output $\emptyset$
else if $R = \emptyset$ **then**
  output L
else if $|R| = 1$ **then**
  Let $[T', h'] \in R$
  for $[T, h] \in L$ **do**
    output $\mathbf{Difference}([T, h], [T', h'])$
  end for
else
  while $R \neq \emptyset$ **do**
    Let $[T', h'] \in R$, $R \leftarrow R \setminus \{ [T', h'] \}$
    $S \leftarrow \emptyset$
    for $[T, h] \in L$ **do**
      $S \leftarrow S \cup \mathbf{Difference}([T, h], [T', h'])$
    end for
    $L \leftarrow S$
  end while
  output L
end if

PROOF. Let

$$\mathcal{S} = \mathbf{Triangularize}(p, T),$$
$$\mathcal{R} = \bigcup_{C \in \mathcal{S}} \mathbf{Regularize}(h, C).$$

We then have

$$\mathbf{V}(p) \cap \mathbf{W}(T) \ \subseteq \ \bigcup_{R \in \mathcal{R}} \ \subseteq \ \mathbf{V}(p) \cap \overline{\mathbf{W}(T)}.$$

This implies

$$\mathbf{Z}(p, T, h) \subseteq \bigcup_{R \in \mathcal{R},\ h \notin \mathrm{Sat}(R)} \mathbf{Z}(R, h) \subseteq (\mathbf{V}(p) \cap \overline{\mathbf{W}(T)}) \setminus \mathbf{V}(h).$$

Rename the regular chains $\{R \mid R \in \mathcal{R},\ h \notin \mathrm{Sat}(R)\}$ as $\{T_1, \ldots, T_e\}$. By the specification of $\mathbf{Regularize}$ we immediately conclude that (i), (iii) hold. Since $p \notin \mathrm{Sat}(T)$, by the specification of $\mathbf{Triangularize}$, (ii) holds. By Lemma 2, (iv) holds.

Lemma 7. *Let* $[T, h]$ *and* $[T', h']$ *be two regular systems. If* $\mathrm{Sat}(T) = \mathrm{Sat}(T')$*, then* $h' h_{T'}$ *is regular w.r.t* $\mathrm{Sat}(T)$ *and*

$$\mathbf{Z}(T, h) \setminus \mathbf{Z}(T', h') = \mathbf{Z}(h' h_{T'}, T, h h_T).$$

PROOF. Since $\text{Sat}(T) = \text{Sat}(T')$ and $h'h_{T'}$ is regular w.r.t $\text{Sat}(T')$, $h'h_{T'}$ is regular w.r.t $\text{Sat}(T)$. By Lemma 2 and Lemma 3, we have

$$\begin{aligned}\mathbf{Z}(T, hh'h_{T'}) &= \mathbf{W}(T) \setminus \mathbf{V}(hh'h_{T'})\\ &= \overline{\mathbf{W}(T)} \setminus \mathbf{V}(hh'h_T h_{T'})\\ &= \overline{\mathbf{W}(T')} \setminus \mathbf{V}(hh'h_T h_{T'})\\ &= \mathbf{W}(T') \setminus \mathbf{V}(hh'h_T)\\ &= \mathbf{Z}(T', hh'h_T).\end{aligned}$$

Then, we can decompose $\mathbf{Z}(T, h)$ into the disjoint union

$$\mathbf{Z}(T, h) = \mathbf{Z}(T, hh'h_{T'}) \bigsqcup \mathbf{Z}(h'h_{T'}, T, hh_T).$$

Similarly, we have:

$$\mathbf{Z}(T', h') = \mathbf{Z}(T', hh'h_T) \bigsqcup \mathbf{Z}(hh_T, T', h'h_{T'}).$$

The conclusion follows from the fact that

$$\mathbf{Z}(T, hh'h_{T'}) \setminus \mathbf{Z}(T', hh'h_T) = \emptyset \quad \text{and} \quad \mathbf{Z}(h'h_{T'}, T, hh_T) \cap \mathbf{Z}(T', h') = \emptyset.$$

Lemma 8. *Assume that* $\text{Sat}(T_{<v}) = \text{Sat}(T'_{<v})$. *We have*

(i) *If* $p' := T'_v$ *is defined but not* T_v*, then* p' *is regular w.r.t* $\text{Sat}(T)$ *and*

$$\mathbf{Z}(T, h) \setminus \mathbf{Z}(T', h') = \mathbf{Z}(T, hp') \bigsqcup (\mathbf{Z}(p', T, hh_T) \setminus \mathbf{Z}(T', h')) .$$

(ii) *If* $p := T_v$ *is defined but not* T'_v*, then* p *is regular w.r.t* $\text{Sat}(T')$ *and*

$$\mathbf{Z}(T, h) \setminus \mathbf{Z}(T', h') = \mathbf{Z}(T, h) \setminus \mathbf{Z}(p, T', h'h_{T'}).$$

PROOF. (i) As $\text{init}(p')$ is regular w.r.t $\text{Sat}(T'_{<v})$, it is also regular w.r.t $\text{Sat}(T_{<v})$. Since T_v is not defined, we know $v \notin \text{mvar}(T)$. Therefore, p' is also regular w.r.t $\text{Sat}(T)$. On the other hand, we have a disjoint decomposition

$$\mathbf{Z}(T, h) = \mathbf{Z}(T, hp') \bigsqcup \mathbf{Z}(p', T, hh_T).$$

By the definition of p', $\mathbf{Z}(T', h') \subseteq \mathbf{V}(p')$ which implies

$$\mathbf{Z}(T, hp') \bigcap \mathbf{Z}(T', h') = \emptyset.$$

The conclusion follows.

(ii) Similarly, we know p is regular w.r.t $\text{Sat}(T')$. By the disjoint decomposition

$$\mathbf{Z}(T', h') = \mathbf{Z}(T', h'p) \bigsqcup \mathbf{Z}(p, T', h'h_{T'}),$$

and $\mathbf{Z}(T, h) \cap \mathbf{Z}(T', h'p) = \emptyset$, we have

$$\mathbf{Z}(T, h) \setminus \mathbf{Z}(T', h') = \mathbf{Z}(T, h) \setminus \mathbf{Z}(p, T', h'h_{T'}),$$

from which the conclusion follows.

Lemma 9. *Assume that* $\mathrm{Sat}(T_{<v}) = \mathrm{Sat}(T'_{<v})$ *but* $\mathrm{Sat}(T_{\leqslant v}) \neq \mathrm{Sat}(T'_{\leqslant v})$ *and that* v *is algebraic w.r.t both* T *and* T'. *Define*

$$\begin{aligned}
\mathcal{G} &= \mathbf{GCD}(T_v, T'_v, T_{<v});\\
\mathcal{E} &= \bigcup_{(g,C)\in\mathcal{G},\ |C|>|T_{<v}|} \mathbf{Extend}(C, T_{\geqslant v});\\
\mathcal{R} &= \bigcup_{E\in\mathcal{E}} \mathbf{Regularize}(hh_T, E).
\end{aligned}$$

Then we have

(i)

$$\begin{aligned}
&\mathbf{Z}(T,h)\\
&= \left(\bigcup_{R\in\mathcal{R},\ hh_T\notin \mathrm{Sat}(R)} \mathbf{Z}(R, hh_T)\right) \bigcup \left(\bigcup_{(g,C)\in\mathcal{G},\ |C|=|T_{<v}|} \mathbf{Z}(C\cup T_{\geqslant v}, hh_T)\right).
\end{aligned}$$

(ii) $\mathrm{rank}(R)\ <_r \mathrm{rank}(T)$, *for all* $R \in \mathcal{R}$.
(iii) *Assume that* $|C| = |T_{<v}|$. *Then*
$(iii.a)$ $C \cup T_{\geqslant v}$ *is a regular chain and* hh_T *is regular w.r.t it.*
$(iii.b)$ *If* $|\mathcal{G}| > 1$, *then* $\mathrm{rank}(C \cup T_{\geqslant v}) <_r \mathrm{rank}(T)$.

PROOF. By the specification of $\mathbf{GCD}$ we have

$$\mathbf{W}(T_{<v}) \subseteq \bigcup_{(g,C)\in\mathcal{G}} \mathbf{W}(C) \subseteq \overline{\mathbf{W}(T_{<v})}.$$

That is,

$$\mathbf{W}(T_{<v}) \xrightarrow{D} (\mathbf{W}(C), (g,C) \in \mathcal{G}).$$

From the specification of $\mathbf{Extend}$ we have: for each $(g,C) \in \mathcal{G}$ such that $|C| > |T_{<v}|$,

$$\mathbf{W}(C\cup T_{\geqslant v}) \xrightarrow{D} (\mathbf{W}(E), E \in \mathbf{Extend}(C\cup\ T_{\geqslant v})).$$

From the specification of $\mathbf{Regularize}$, we have for all $(g,C) \in \mathcal{G}$ such that $|C| > |T_{<v}|$ and all $E \in \mathbf{Extend}(C \cup T_{\geqslant v})$,

$$\mathbf{W}(E) \xrightarrow{D} (\mathbf{W}(R),\ R \in \mathbf{Regularize}(hh_T, E)).$$

Therefore, by applying the Lifting Theorem [15] we have:

$$\begin{aligned}
\mathbf{W}(T) &= \mathbf{W}(T_{<v}\cup T_{\geqslant v})\\
&\subseteq \left(\bigcup_{R\in\mathcal{R}} \mathbf{W}(R)\right) \bigcup \left(\bigcup_{(g,C)\in\mathcal{G},\ |C|=|T_{<v}|} \mathbf{W}(C\cup T_{\geqslant v})\right)\\
&\subseteq \overline{\mathbf{W}(T_{<v}\cup T_{\geqslant v})}\\
&= \overline{\mathbf{W}(T)},
\end{aligned}$$

which implies,

$$
\begin{aligned}
\mathbf{Z}(T,h) &= \mathbf{Z}(T,hh_T) \\
&\subseteq \left(\bigcup_{R\in\mathcal{R},\ hh_T\notin \mathrm{Sat}(R)} \mathbf{Z}(R,hh_T) \right) \bigcup \left(\bigcup_{(g,C)\in\mathcal{G},\ |C|=|T_{<v}|} \mathbf{Z}(C\cup T_{\geqslant v},hh_T) \right) \\
&\subseteq \overline{\mathbf{W}(T)} \setminus \mathbf{V}(hh_T) = \mathbf{Z}(T,h).
\end{aligned}
$$

So (i) holds. When $|\mathcal{G}|>1$, by Notation 1, (ii) and $(iii.b)$ hold.

If $|C|=|T_{<v}|$, by Proposition 5 of [15], we conclude that $(iii.a)$ holds.

Lemma 10. *Assume that* $\mathrm{Sat}(T_{<v}) = \mathrm{Sat}(T'_{<v})$ *but* $\mathrm{Sat}(T_{\leqslant v}) \neq \mathrm{Sat}(T'_{\leqslant v})$ *and that* v *is algebraic w.r.t both* T *and* T'. *Define* $p=T_v$, $p'=T'_v$ *and*

$$\mathcal{G} = \mathbf{GCD}(p,p',T_{<v}).$$

If $|\mathcal{G}|=1$, *let* $\mathcal{G}=\{(g,C)\}$. *Then the following properties hold*

(i) $C=T_{<v}$.

(ii) *If* $g\in\mathbb{K}$, *then*

$$\mathbf{Z}(T,h)\setminus\mathbf{Z}(T',h') = \mathbf{Z}(T,h).$$

(iii) *If* $g\notin\mathbb{K}$ *and* $\mathrm{mvar}(g)<v$, *then* g *is regular w.r.t* $\mathrm{Sat}(T)$ *and*

$$
\begin{aligned}
&\mathbf{Z}(T,h)\setminus\mathbf{Z}(T',h') \\
&= \mathbf{Z}(T,gh) \bigsqcup \left(\mathbf{Z}(g,T,hh_T)\setminus\mathbf{Z}(T',h')\right).
\end{aligned}
$$

(iv) *Assume that* $\mathrm{mvar}(g)=v$.

$(iv.a)$ *If* $\mathrm{mdeg}(g)=\mathrm{mdeg}(p)$, *defining*

$$
\begin{aligned}
q' &= \mathrm{pquo}(p',p,T'_{<v}) \\
D'_p &= T'_{<v}\cup\{p\}\cup T'_{>v} \\
D'_{q'} &= T'_{<v}\cup\{q'\}\cup T'_{>v},
\end{aligned}
$$

then we have

$$\mathbf{Z}(T,h)\setminus\mathbf{Z}(T',h') = \mathbf{Z}(T,h)\setminus\mathbf{Z}(D'_p,h'h_{T'}),$$

$\mathrm{rank}(D'_p)<\mathrm{rank}(T')$ *and* $h'h_{T'}$ *is regular w.r.t* $\mathrm{Sat}(D'_p)$.

$(iv.b)$ *If* $\mathrm{mdeg}(g)<\mathrm{mdeg}(p)$, *defining*

$$
\begin{aligned}
q &= \mathrm{pquo}(p,g,T_{<v}) \\
D_g &= T_{<v}\cup\{g\}\cup T_{>v} \\
D_q &= T_{<v}\cup\{q\}\cup T_{>v},
\end{aligned}
$$

then we have: D_g *and* D_q *are regular chains such that* $\mathrm{rank}(D_g)<\mathrm{rank}(T)$, $\mathrm{rank}(D_q)<\mathrm{rank}(T)$, hh_T *is regular w.r.t* $\mathrm{Sat}(D_g)$ *and* $\mathrm{Sat}(D_q)$, *and*

$$\mathbf{Z}(T,h) = \mathbf{Z}(D_g,hh_T)\bigcup\mathbf{Z}(D_q,hh_T)\bigcup\mathbf{Z}(h_g,T,hh_T).$$

PROOF. Since $|\mathcal{G}| = 1$, by the specification of the operation $\mathbf{GCD}$ and Notation 1, (i) holds. Therefore we have

$$\text{Sat}(C) = \text{Sat}(T_{<v}) = \text{Sat}(T'_{<v}) \tag{1}$$

There exist polynomials A and B such that

$$g \equiv Ap + Bp' \quad \text{mod} \quad \text{Sat}(C). \tag{2}$$

From (2), we have

$$\mathbf{V}(\text{Sat}(C)) \subseteq \mathbf{V}(g - Ap - Bp') \tag{3}$$

Therefore, we deduce

$$\begin{aligned}
&\mathbf{W}(T) \bigcap \mathbf{W}(T') \\
&= \mathbf{W}(T_{<v} \cup p \cup T_{\geqslant v}) \bigcap \mathbf{W}(T'_{<v} \cup p' \cup T'_{\geqslant v}) \\
&\subseteq (\mathbf{W}(T_{<v}) \cap \mathbf{V}(p)) \bigcap (\mathbf{W}(T'_{<v}) \cap \mathbf{V}(p')) \\
&\subseteq \mathbf{V}(\text{Sat}(T_{<v})) \bigcap \mathbf{V}(p) \bigcap \mathbf{V}(p') && \text{by (1)} \\
&\subseteq \mathbf{V}(g - Ap - Bp') \bigcap \mathbf{V}(p) \bigcap \mathbf{V}(p') && \text{by (3)} \\
&\subseteq \mathbf{V}(g).
\end{aligned}$$

that is

$$\mathbf{W}(T) \bigcap \mathbf{W}(T') \subseteq \mathbf{V}(g). \tag{4}$$

Now we prove (ii). When $g \in \mathbb{K}$, $g \neq 0$, from (4) we deduce

$$\mathbf{W}(T) \bigcap \mathbf{W}(T') = \emptyset. \tag{5}$$

Thus we have

$$\begin{aligned}
&\mathbf{Z}(T, h) \setminus \mathbf{Z}(T', h') \\
&= (\mathbf{W}(T) \setminus \mathbf{V}(h)) \setminus (\mathbf{W}(T') \setminus \mathbf{V}(h')) \\
&= (\mathbf{W}(T) \setminus \mathbf{V}(h)) && \text{by (5)} \\
&= \mathbf{Z}(T, h).
\end{aligned}$$

Now we prove (iii). Since $C = T_{<v}$ and $\text{mvar}(g)$ is smaller than or equal to v, by the specification of $\mathbf{GCD}$, g is regular w.r.t $\text{Sat}(T)$. We have following decompositions

$$\begin{aligned}
\mathbf{Z}(T, h) &= \mathbf{Z}(T, gh) \bigsqcup \mathbf{Z}(g, T, hh_T), \\
\mathbf{Z}(T', h') &= \mathbf{Z}(T', gh') \bigsqcup \mathbf{Z}(g, T', h'h_{T'}).
\end{aligned}$$

On the other hand,

$$\begin{aligned}
&\mathbf{Z}(T, gh) \bigcap \mathbf{Z}(T', gh') \\
&= (\mathbf{W}(T) \cap \mathbf{V}(gh)^c) \bigcap (\mathbf{W}(T') \cap \mathbf{V}(gh')^c) \\
&\subseteq (\mathbf{W}(T) \cap \mathbf{V}(g)^c) \bigcap (\mathbf{W}(T') \cap \mathbf{V}(g)^c) \\
&= (\mathbf{W}(T) \cap \mathbf{W}(T')) \bigcap \mathbf{V}(g)^c \\
&= \emptyset \qquad \text{by } (4).
\end{aligned}$$

Therefore,

$$\begin{aligned}
&\mathbf{Z}(T, h) \setminus \mathbf{Z}(T', h') \\
&= (\mathbf{Z}(T, gh) \setminus \mathbf{Z}(T', gh')) \bigsqcup (\mathbf{Z}(g, T, hh_T) \setminus \mathbf{Z}(T', h')) \\
&= \mathbf{Z}(T, gh) \bigsqcup (\mathbf{Z}(g, T, hh_T) \setminus \mathbf{Z}(T', h'))\,.
\end{aligned}$$

Now we prove $(iv.a)$. First, both h' and h'_T are regular w.r.t $\text{Sat}(C) = \text{Sat}(T_{<v}) = \text{Sat}(T'_{<v})$. From the construction of D'_p, we have $h'h_{T'}$ is regular w.r.t $\text{Sat}(D'_p)$.

Assume that $\text{mvar}(g) = v$ and $\text{mdeg}(g) = \text{mdeg}(p)$. We note that $\text{mdeg}(p') > \text{mdeg}(p)$ holds. Otherwise we would have $\text{mdeg}(g) = \text{mdeg}(p) = \text{mdeg}(p')$ which implies:

$$p \in \text{Sat}(T'_{\geqslant v}) \text{ and } p' \in \text{Sat}(T_{\geqslant v}). \tag{6}$$

Thus

$$\begin{aligned}
\text{Sat}(T_{\leqslant v}) &= \langle T_{\leqslant v} \rangle : h_{T_{\leqslant v}}^{\infty} = \langle T_{<v} \cup p \rangle : h_{T_{\leqslant v}}^{\infty} \\
&\subseteq \text{Sat}(T'_{\leqslant v}) : h_{T_{\leqslant v}}^{\infty} \qquad\qquad \text{by } (6) \\
&= \text{Sat}(T'_{\leqslant v}),
\end{aligned}$$

that is $\text{Sat}(T_{\leqslant v}) \subseteq \text{Sat}(T'_{\leqslant v})$. Similarly, $\text{Sat}(T'_{\leqslant v}) \subseteq \text{Sat}(T_{\leqslant v})$ holds. So we have $\text{Sat}(T'_{\leqslant v}) = \text{Sat}(T_{\leqslant v})$, a contradiction.

Hence, $\text{mvar}(q') = v$.

By Lemma 6 [15], we know that D'_p and $D'_{q'}$ are regular chains. Then with Theorem 7 [15] and Lifting Theorem [15], we know

$$\begin{aligned}
\mathbf{Z}(T', h') &\subseteq \mathbf{Z}(D'_p, h') \bigcup \mathbf{Z}(D'_{q'}, h') \bigcup \mathbf{Z}(h_p, T', h') \\
&\subseteq \overline{\mathbf{W}(T')} \setminus \mathbf{V}(h').
\end{aligned}$$

By Lemma 2, we have

$$\mathbf{Z}(T', h') = \mathbf{Z}(D'_p, h'h_{T'}) \bigcup \mathbf{Z}(D'_{q'}, h'h_{T'}) \bigcup \mathbf{Z}(h_p, T', h'h_{T'}).$$

Since

$$\begin{aligned}
\mathbf{Z}(D'_{q'}, h'h_{T'}) &= \mathbf{Z}(D'_{q'}, h_p h' h_{T'}) \bigcup \mathbf{Z}(h_p, D'_{q'}, h'h'_T) \\
&= \mathbf{Z}(D'_{q'}, p h_p h' h_{T'}) \bigcup \mathbf{Z}(p, D'_{q'}, h_p h' h'_T) \bigcup \mathbf{Z}(h_p, D'_{q'}, h'h'_T)
\end{aligned}$$

and

$$\mathbf{Z}(p, D'_{q'}, h_p h' h'_T) \subseteq \mathbf{Z}(D'_p, h' h_{T'})$$
$$\mathbf{Z}(h_p, D'_{q'}, h' h'_T) \subseteq \mathbf{Z}(h_p, T', h' h_{T'}),$$

we deduce

$$\mathbf{Z}(T', h') = \mathbf{Z}(D'_p, h' h_{T'}) \bigsqcup \mathbf{Z}(D'_{q'}, p h' h_{T'}) \bigsqcup \mathbf{Z}(h_p, T', h' h_{T'}).$$

Now observe that

$$\mathbf{Z}(T, h) \bigcap \mathbf{Z}(D'_{q'}, p h' h_{T'}) = \emptyset, \text{ and}$$
$$\mathbf{Z}(T, h) \bigcap \mathbf{Z}(h_p, T', h' h_{T'}) = \emptyset.$$

We obtain

$$\mathbf{Z}(T, h) \setminus \mathbf{Z}(T', h') = \mathbf{Z}(T, h) \setminus \mathbf{Z}(D'_p, h' h_{T'}).$$

Finally we prove $(iv.b)$. We assume that $\mathrm{mvar}(g) = v$ and $\mathrm{mdeg}(g) < \mathrm{mdeg}(p)$; this implies $\mathrm{mvar}(q) = v$. Applying Lemma 6 in [15] we know that D_g and D_q are regular chains and satisfy the desired rank condition. Then by Theorem 7 [15] and Lifting Theorem [15] we have

$$\mathbf{Z}(T, h) = \mathbf{Z}(D_g, h h_T) \bigcup \mathbf{Z}(D_q, h h_T) \bigcup \mathbf{Z}(h_g, T, h h_T).$$

This completes the whole proof.

Definition 7. *Given two pairs of ranks* $(\mathrm{rank}(T_1), \mathrm{rank}(T'_1))$ *and* $(\mathrm{rank}(T_2), \mathrm{rank}(T'_2))$, *where* T_1, T_2, T'_1, T'_2 *are triangular sets. We define the product order* $<_p$ *of Ritt order* $<_r$ *on them as follows*

$$(\mathrm{rank}(T_2), \mathrm{rank}(T'_2)) <_p (\mathrm{rank}(T_1), \mathrm{rank}(T'_1))$$
$$\Longleftrightarrow \begin{cases} \mathrm{rank}(T_2) <_r \mathrm{rank}(T_1) \;\; \textit{or} \\ \mathrm{rank}(T_2) = \mathrm{rank}(T_1), \;\; \mathrm{rank}(T'_2) <_r \mathrm{rank}(T'_1). \end{cases}$$

In the following theorems, we prove the termination and correctness separately. Along with the proof of Theorem 2, we show the rank conditions are satisfied which is part of the correctness. The remained part, say zero set decomposition, will be proved in Theorem 3.

Theorem 2. *Algorithms* **Difference** *and* **DifferenceLR** *terminate and satisfy the rank conditions in their specifications.*

PROOF. The following two statements need to be proved

(i) **Difference** terminates with $\mathrm{rank}(\mathbf{Difference}([T, h], [T', h'])) \leqslant_r \mathrm{rank}([T, h])$,
(ii) **DifferenceLR** terminates with $\mathrm{rank}(\mathbf{DifferenceLR}(\mathcal{L}, \mathcal{R})) \leqslant_r \mathrm{rank}(\mathcal{L})$.

We prove them by induction on the product order $<_p$.

(1) Base case: there are no recursive calls to **Difference** or **DifferenceLR**. The termination of both algorithms is clear. By line $2, 18$ of the algorithm **Difference**, rank(**Difference**($[T, h], [T', h']$)) $\leqslant_r$ rank($[T, h]$). By line $2, 4$ of the algorithm **DifferenceLR**, rank(**DifferenceLR**($\mathcal{L}, \mathcal{R}$)) $\leqslant_r$ rank($\mathcal{L}$).
(2) Induction hypothesis: assume that both (i) and (ii) hold with inputs whose ranks are smaller than the rank of $([T, h], [T', h'])$ w.r.t. $<_p$.
(3) By (1), if no recursive calls occur in one branch, then (i) and (ii) already hold. When recursive calls occur, by line $8, 11, 21, 25, 30, 31, 32, 41, 46$ and Lemma 6, 8, 9, 10, we know the inputs of recursive calls to both **Difference** and **DifferenceLR** have smaller ranks than rank($([T, h], [T', h'])$) w.r.t $<_p$. By induction hypothesis, (i) holds. Finally, by line $8, 15$ of algorithm **DifferenceLR** and (i), (ii) holds.

Theorem 3. *Both* **Difference** *and* **DifferenceLR** *satisfy their specifications.*

PROOF. By Theorem 2, **Difference** and **DifferenceLR** terminate and satisfy their rank conditions. So it suffices to prove the correctness of **Difference** and **DifferenceLR**, that is

(i) $\mathbf{Z}(T, h) \setminus \mathbf{Z}(T', h') = \mathbf{Z}(\mathbf{Difference}([T, h], [T', h']))$,
(ii) $\mathbf{Z}(\mathcal{L}) \setminus \mathbf{Z}(\mathcal{R}) = \mathbf{Z}(\mathbf{DifferenceLR}(\mathcal{L}, \mathcal{R}))$.

We prove them by induction on the product order $<_p$.

(1) Base case: no recursive calls to **Difference** and **DifferenceLR** occur. First, by line $2, 18$ of the algorithm **Difference** and Lemma 6, 7, 10, (i) holds. Second, by line $2, 4$ of the algorithm **DifferenceLR**, (ii) holds.
(2) Induction hypothesis: assume that both (i) and (ii) hold with inputs whose ranks are smaller than the rank of $([T, h], [T', h'])$ w.r.t. $<_p$.
(3) By (1), if no recursive calls occur, (i) and (ii) already hold. When there are recursive calls, we first show (i) holds. From the proof of Theorem 2, in **Difference**, the inputs of recursive calls to **Difference** and **DifferenceLR** will have smaller ranks w.r.t. the product order $<_p$. Therefore, by (2), line 7, 8, 11, 20, 21, 25, 30, 31, 32, 41, 46 and Lemma 6, 8, 9, 10, (i) holds.
Finally, by (i) and line $5 - 18$ of algorithm **DifferenceLR**, (ii) holds.

4 Decomposition into Pairwise Disjoint Constructible Sets

We assume that **DifferenceLR**($\mathcal{L}, \mathcal{R}$) returns a list of regular systems sorted by increasing rank.

Definition 8. *Let $\mathcal{S}$ be a list of regular systems sorted by increasing rank. If $\mathcal{S}$ is empty or consists of a single regular system $[T, h]$, define $\mathbf{MPD}(\mathcal{S}) = \mathcal{S}$. Otherwise, let $\mathcal{S} = \mathcal{L} + \mathcal{R}$, where $|\mathcal{L}| = |\mathcal{R}|$ or $|\mathcal{L}| = |\mathcal{R}| + 1$ (and $+$ denotes concatenation of lists). Define*

$$\mathbf{MPD}(\mathcal{S}) = \mathbf{MPD}(\mathbf{DifferenceLR}(\mathcal{L}, \mathcal{R})) + \mathbf{MPD}(\mathcal{R}).$$

Definition 9. *For a regular system $S = [T, h]$, let $\mathbf{Z}_0(S)$ denote the zero set of S considered as a regular system in $\hat{\mathbb{K}}[\mathrm{mvar}(T)] := \overline{\mathbb{K}(Y \setminus \mathrm{mvar}(T))}[\mathrm{mvar}(T)]$.*

Lemma 11. *For every regular system S, $\mathbf{Z}_0(S)$ is non-empty and finite.*

Proof. If the regular system $S = [T, h]$ is considered in $\hat{\mathbb{K}}[\mathrm{mvar}(T)]$, it remains to be a regular system and, moreover, T becomes a zero-dimensional regular chain. We have therefore

$$\mathbf{Z}_0(S) = \mathbf{W}_{\hat{\mathbb{K}}}(T) \setminus \mathbf{V}_{\hat{\mathbb{K}}}(h) = \mathbf{V}_{\hat{\mathbb{K}}}(T).$$

Definition 10. *For a finite set of regular systems $\mathcal{S} = \{[T_1, h_1], \ldots, [T_k, h_k]\}$ such that $\mathrm{rank}(T_1) = \cdots = \mathrm{rank}(T_k)$, define*

$$\mathbf{Z}_0(\mathcal{S}) = \mathbf{Z}_0([T_1, h_1]) \cup \ldots \cup \mathbf{Z}_0([T_k, h_k]).$$

For an arbitrary finite set of regular systems $\mathcal{S}$, let $\mathcal{S}_{\mathrm{rank}(\mathcal{S})}$ denote the subset of regular systems of maximal rank. Define $\mathbf{Z}_0(\mathcal{S}) = \mathbf{Z}_0(\mathcal{S}_{\mathrm{rank}(\mathcal{S})})$.

Lemma 12. *Let $\mathcal{S}$ be a list of regular systems sorted by increasing rank represented as a concatenation of two non-empty sublists: $\mathcal{S} = \mathcal{L} + \mathcal{R}$. Let $\mathcal{C} = \mathbf{DifferenceLR}(\mathcal{L}, \mathcal{R})$. Then either $\mathrm{rank}(\mathcal{C}) < \mathrm{rank}(\mathcal{S})$, or $|\mathbf{Z}_0(\mathcal{C})| < |\mathbf{Z}_0(\mathcal{S})|$.*

Proof. If $\mathrm{rank}(\mathcal{L}) < \mathrm{rank}(\mathcal{S})$, then $\mathrm{rank}(\mathcal{C}) < \mathrm{rank}(\mathcal{S})$ by Theorem 2. Otherwise, $\mathrm{rank}(\mathcal{L}) = \mathrm{rank}(\mathcal{S})$ and, since $\mathcal{S}$ is sorted by increasing rank, the rank of every system in $\mathcal{R}$ equals $\mathrm{rank}(\mathcal{S})$. By Theorem 2, we have $\mathrm{rank}(\mathcal{C}) \leq \mathrm{rank}(\mathcal{S})$. In case of strict inequality we are done, so assume that $\mathrm{rank}(\mathcal{C}) = \mathrm{rank}(\mathcal{S})$.

Denote $r = \mathrm{rank}(\mathcal{L}) = \mathrm{rank}(\mathcal{C}) = \mathrm{rank}(\mathcal{R}) = \mathrm{rank}(\mathcal{S})$. We have:

$$\bigcup_{C \in \mathcal{C}_r} \mathbf{Z}(C) \subseteq \bigcup_{A \in \mathcal{L}_r} \mathbf{Z}(A) \setminus \bigcup_{B \in \mathcal{R}} \mathbf{Z}(B),$$

which implies

$$\mathbf{Z}_0(\mathcal{C}) \subseteq \mathbf{Z}_0(\mathcal{L}) \setminus \bigcup_{B \in \mathcal{R}} \mathbf{Z}_0(B).$$

Since, by Lemma 11, $\mathbf{Z}_0(\mathcal{S}) = \mathbf{Z}_0(\mathcal{L}) \cup \mathbf{Z}_0(\mathcal{R})$ is finite and $\bigcup_{B \in \mathcal{R}} \mathbf{Z}(B) \neq \varnothing$, we obtain the desired $|\mathbf{Z}_0(\mathcal{C})| < |\mathbf{Z}_0(\mathcal{S})|$.

Lemma 13. *For any list $\mathcal{S}$ of regular systems, $\mathcal{D} = \mathbf{MPD}(\mathcal{S})$ is well-defined.*

Proof. We define a well-order on the set of all sorted finite lists of regular systems and prove the statement by induction on this well-order.

For a non-empty list $\mathcal{S}$, let $\phi(\mathcal{S}) = (\mathrm{rank}(\mathcal{S}), \mathbf{Z}_0(\mathcal{S}), |\mathcal{S}|)$. Let $\mathcal{L} \prec \mathcal{R}$ iff $\phi(\mathcal{L}) <_{\mathrm{lex}} \phi(\mathcal{R})$. Since $<_{\mathrm{lex}}$ is the lexicographic product of three well-orders, $<_{\mathrm{lex}}$ is a well-order, whence so is $\prec$. Define the empty list to be less than any non-empty list w.r.t. $\prec$.

For empty and singleton lists $\mathcal{S}$, $\mathbf{MPD}(\mathcal{S})$ is well-defined. Let $\mathcal{S}$ be a non-singleton and non-empty list. Assume that $\mathbf{MPD}(\mathcal{S}')$ is defined for all lists $\mathcal{S}'$ such that $\mathcal{S}' \prec \mathcal{S}$. Let, as in Definition 8, $\mathcal{S} = \mathcal{L} + \mathcal{R}$, where $|\mathcal{L}| = |\mathcal{R}|$ or $|\mathcal{L}| = |\mathcal{R}| + 1$. Then by

Lemma 12, $\mathbf{Difference}(\mathcal{L}, \mathcal{R}) \prec \mathcal{S}$. Also, $\text{rank}(\mathcal{R}) \leq \text{rank}(\mathcal{S})$, $\mathbf{Z}_0(\mathcal{R}) \leq \mathbf{Z}_0(\mathcal{S})$, and $|\mathcal{R}| < |\mathcal{S}|$, whence $\mathcal{R} \prec \mathcal{S}$. This implies that $\mathbf{MPD}(\mathcal{S})$ is well-defined according to Definition 8.

Note that Definition 8 yields a recursive algorithm for computing $\mathbf{MPD}(\mathcal{S})$, which terminates according to the previous lemma. The output of this algorithm is a decomposition of the union of zero-sets of regular systems in $\mathcal{S}$ into a disjoint union of zero-sets of regular systems:

Proposition 2. *For all distinct regular systems $R, S \in \mathcal{D} = \mathbf{MPD}(\mathcal{S})$, we have $\mathbf{Z}(R) \cap \mathbf{Z}(S) = \varnothing$, and*

$$\bigcup_{R \in \mathcal{S}} \mathbf{Z}(S) = \bigcup_{S \in \mathcal{D}} \mathbf{Z}(D).$$

PROOF. Follows immediately from the definition of $\mathbf{MPD}$.

In the following section, to compute comprehensive triangular decompositions, we will see that $\mathbf{SMPD}$ (strongly make pairwise disjoint) is really required. Given a set of regular systems $A_1, \cdots, A_s$, $\mathbf{SMPD}$ compute another set of regular systems $B_1, \cdots, B_t$ whose zero sets are pairwise disjoint, such that each $\mathbf{Z}(A_i)$ writes as a union of some of the $\mathbf{Z}(B_1), \cdots, \mathbf{Z}(B_t)$.

Algorithm 3. SMPD$(\mathcal{S})$

if $|\mathcal{S}| \leq 1$ **then**
  output $\mathcal{S}$
end if
Let $[T_0, h_0] \in \mathcal{S}, \mathcal{S} \leftarrow \mathcal{S} \setminus \{[T_0, h_0]\}$
$\mathcal{S} \leftarrow$ **SMPD**$(\mathcal{S})$
for $[T, h] \in \mathcal{S}$ **do**
  $\mathcal{A} \leftarrow \mathbf{Difference}([T, h], [T_0, h_0])$
  $\mathcal{B} \leftarrow \mathbf{DifferenceLR}([T, h], \mathcal{A})$
  output **MPD**$(\mathcal{A})$
  output **MPD**$(\mathcal{B})$
end for
$\mathcal{C} \leftarrow \mathbf{DifferenceLR}([T_0, h_0], \mathcal{S})$
output **MPD**$(\mathcal{C})$

Proposition 3. *The Algorithm* $\mathbf{SMPD}$ *terminates and is correct.*

PROOF. It follows directly from the termination and correctness of algorithms $\mathbf{Difference}$, $\mathbf{DifferenceLR}$ and $\mathbf{MPD}$.

5 Comprehensive Triangular Decomposition

In this section we introduce the concept of comprehensive triangular decomposition of an algebraic variety. We propose an algorithm for computing this decomposition and apply it to compute the set of all parameter values at which a given parametric system has an empty or an infinite set of solutions.

Notation 2. *From now on, we assume that $n = m + d$, the variables $Y_1, \ldots, Y_d$ are renamed $U_1, \ldots, U_d$ and viewed as parameters, whereas $Y_{d+1}, \ldots, Y_n$ are renamed $X_1, \ldots, X_m$ and regarded as unknowns.*

If the polynomial set $F \subset \mathbb{K}[Y]$ involves polynomials from $\mathbb{K}[U]$ only, we denote by $\mathbf{V}^U(F)$ its variety in $\overline{\mathbb{K}}^d$. Similarly, if the regular chain $T \subset \mathbb{K}[Y]$ involves polynomials from $\mathbb{K}[U]$ only, we denote by $\mathbf{W}^U(T)$ its quasi-component in $\overline{\mathbb{K}}^d$.

Notation 3. *Let $p \in \mathbb{K}[U][X]$ be a polynomial. We denote by $\mathbf{V}^U(p)$ the variety of $\overline{\mathbb{K}}^d$, consisting of the common roots of the coefficients of p, when p is regarded as a polynomial with variables in X and coefficients in $\mathbb{K}[U]$. Then, we define $\mathbf{V}^U(F)$ as the intersection of all $\mathbf{V}^U(p)$ for $p \in F$.*

For $u \in \overline{\mathbb{K}}^d$, we denote by $p(u)$ the polynomial of $\overline{\mathbb{K}}[X]$ obtained by evaluating p at $U_1 = u_1, \ldots, U_d = u_d$. Clearly, for all $u \in \overline{\mathbb{K}}^d$, the polynomial $p(u)$ is identically null iff $u \in \mathbf{V}^U(p)$. Then, we denote by $F(u)$ the set of all non-zero $p(u)$ for $p \in F$.

Definition 11. *Let $T \subset \mathbb{K}[U, X]$ be a regular chain. The* defining set of T w.r.t. U, *denoted by $\mathbf{D}^U(T)$, is the constructible set of $\overline{\mathbb{K}}^d$ given by*

$$\mathbf{D}^U(T) = \mathbf{W}^U(T \cap \mathbb{K}[U]) \setminus \mathbf{V}^U(\mathrm{res}(h_{T_{>U_d}}, T_{>U_d})).$$

Let $u \in \mathbf{W}^U(T \cap \mathbb{K}[U])$. We say that the regular chain T specializes well at u *if $T(u)$ is a regular chain in $\overline{\mathbb{K}}[X]$ such that* $\mathrm{rank}(T(u)) = \mathrm{rank}(T_{>U_d})$.

Remark 2. *Since $\mathbf{D}^U(T)$ is a constructible set, by Lemma 5, there exists an algorithm to compute a set of regular systems $\mathcal{R}^U(T)$, such that $\mathbf{D}^U(T) = \mathbf{Z}(\mathcal{R}^U(T))$.*

Lemma 14. *Let $T \subset \mathbb{K}[U, X]$ be a regular chain with* $\mathrm{mvar}(T) \subseteq X$ *and let $u \in \overline{\mathbb{K}}^d$. We have*

$$u \notin \mathbf{V}^U(\mathrm{res}(h_T, T)) \iff \mathrm{res}(h_{T(u)}, T(u)) \neq 0 \text{ and } h_T(u) \neq 0.$$

PROOF. "$\Leftarrow$" If $h_T(u) \neq 0$ and $\mathrm{res}(h_{T(u)}, T(u)) \neq 0$, then

$$\mathrm{res}(h_{T(u)}, T(u)) = \mathrm{res}(h_T(u), T(u)) \neq 0,$$

which implies $\mathrm{res}(h_T, T)(u) \neq 0$. So $u \notin \mathbf{V}^U(\mathrm{res}(h_T, T))$.

"$\Rightarrow$" We prove this by induction on $|T|$.

If $|T| = 1$, then $u \notin \mathbf{V}^U(\mathrm{res}(h_T, T))$ implies $h_T(u) \neq 0$ and therefore

$$\mathrm{res}(h_{T(u)}, T(u)) = h_{T(u)} = h_T(u) \neq 0.$$

Now we assume that the conclusion holds for $|T| = n - 1$. If $|T| = n$, let v be the largest variable in $\mathrm{mvar}(T)$. Since $u \notin \mathbf{V}^U(\mathrm{res}(h_T, T))$, we have

$$\mathrm{res}(h_T, T)(u) = \mathrm{res}(h_T, T_{<v})(u) \neq 0.$$

Therefore, $\mathrm{res}(h_{T_{<v}}, T_{<v})(u) \neq 0$. By induction hypothesis, we know $h_{T_{<v}}(u) \neq 0$. By the specialization property of resultant, $\mathrm{res}(h_T(u), T_{<v}(u)) \neq 0$ and therefore $h_T(u) \neq 0$. So $\mathrm{res}(h_T, T)(u) \neq 0$ implies $\mathrm{res}(h_{T(u)}, T(u)) \neq 0$.

Proposition 4. *Let $T \subset \mathbb{K}[U, X]$ be a regular chain and let $u \in \mathbf{W}^U(T \cap \mathbb{K}[U])$. The regular chain T specializes well at $u \in \overline{\mathbb{K}}^d$ if and only if $u \in \mathbf{D}^U(T)$.*

PROOF. Assume that $u \in \mathbf{D}^U(T)$. We prove that T specializes well at u. From Lemma 14 we have

$$\mathrm{res}(h_{T_{>U_d}(u)}, T_{>U_d}(u)) \neq 0 \text{ and } h_{T_{>U_d}}(u) \neq 0.$$

With $u \in \mathbf{W}^U(T \cap \mathbb{K}[U])$, which implies $(T \cap \mathbb{K}[U])(u) = \{0\}$, we conclude that $\mathrm{rank}(T(u)) = \mathrm{rank}(T_{>U_d})$. Moreover, by Theorem 1, $T(u)$ is a regular chain. Therefore, the regular chain T specializes well at u. The converse implication is proved similarly.

Definition 12. *Let $T \subset \mathbb{K}[U, X]$ be a regular chain. The* comprehensive quasi-component *of T* w.r.t. *U, denoted by $\mathbf{W}_C(T)$, is defined by*

$$\mathbf{W}_C(T) = \mathbf{W}(T) \cap \Pi_U^{-1}(\mathbf{D}^U(T)).$$

Proposition 5. *Let $T \subset \mathbb{K}[U, X]$ be a regular chain. The following properties hold:*

(1) *We have:* $\mathbf{W}_C(T) = \mathbf{W}(T) \setminus \Pi_U^{-1}(\mathbf{V}^U(\mathrm{res}(h_{T>U_d}, T_{>U_d})))$.
(2) *We have:* $\Pi_U(\mathbf{W}_C(T)) = \mathbf{D}^U(T)$.

PROOF. It follows from Definition 11 and Lemma 14.

Definition 13. *Let $F \subset \mathbb{K}[U, X]$ be a finite polynomial set. A* comprehensive triangular decomposition *of $\mathbf{V}(F)$ is given by :*

1. *a finite partition $\mathcal{C}$ of $\Pi_U(\mathbf{V}(F))$,*
2. *for each $C \in \mathcal{C}$ a set of regular chains $\mathcal{T}_C$ of $\mathbb{K}[U, X]$ such that for $u \in C$ each of the regular chains $T \in \mathcal{T}_C$ specializes well at u and we have for all $u \in C$*

$$\mathbf{V}(F(u)) = \bigcup_{T \in \mathcal{T}_C} \mathbf{W}(T(u)).$$

We will compute the above comprehensive triangular decomposition with the help of the following auxiliary concept:

Definition 14. *Let $F \subset \mathbb{K}[U, X]$ be a finite polynomial set. A* pre-comprehensive triangular decomposition *(PCTD) of $\mathbf{V}(F)$ is a family of regular chains $\mathcal{T}$ satisfying the following property: for each $u \in \overline{\mathbb{K}}^d$, let $\mathcal{T}_u$ be the subfamily of all regular chains in $\mathcal{T}$ that specialize well at u; then*

$$\mathbf{V}(F(u)) = \bigcup_{T \in \mathcal{T}_u} \mathbf{W}(T(u)).$$

Proposition 6. *Let $F \subset \mathbb{K}[U, X]$ be a finite polynomial set. A triangular decomposition $\mathcal{T}$ of $\mathbf{V}(F)$ is a pre-comprehensive triangular decomposition if and only if*

$$\mathbf{V}(F) = \bigcup_{T \in \mathcal{T}} W_C(T).$$

PROOF. It follows from the definition of $W_C(T)$, Proposition 4 and the definition of pre-comprehensive triangular decomposition.

Algorithm 4. PCTD(F)

Input: A finite set $F \subset \mathbb{K}[U, X]$.
Output: A PCTD of $\mathbf{V}(F)$.

$\mathcal{T} \leftarrow$ **Triangularize**(F)
while $\mathcal{T} \neq \emptyset$ **do**
  let $T \in \mathcal{T}$, $\mathcal{T} \leftarrow \mathcal{T} \setminus \{T\}$
  output T
  $G \leftarrow$ COEFFICIENTS(res$(h_{T_{>U_d}}, T_{>U_d}), U)$
  $\mathcal{T} \leftarrow \mathcal{T} \cup$ **Triangularize**(G, T)
end while

Proposition 7. *Algorithm 4 computes a pre-comprehensive triangular decomposition of* $\mathbf{V}(F)$.

PROOF. The loop satisfies the following invariant: the union of all $\mathbf{W}(T)$, where T ranges over $\mathcal{T}$, and of the $\mathbf{W}(T')$, where T' ranges over the current output, equals $\mathbf{V}(F)$. Indeed, the invariant holds at the beginning, when the output is empty; and for the regular chain T taken from $\mathcal{T}$ at the current iteration, we have $\mathbf{W}(T) \setminus \mathbf{W}_C(T) = \mathbf{V}(G) \cap \mathbf{W}(T)$ by Proposition 5 (1). Then, correctness of the algorithm follows from Proposition 6 and the fact that at the end $\mathcal{T} = \varnothing$.

Since polynomials in G do not involve the main variables of T, by Lemma 3 they are regular w.r.t Sat(T). Then by Lemma 1, either the output of **Triangularize**(G, T) is empty or the dimensions of the regular chains computed by **Triangularize**(G, T) are strictly less than that of T. Therefore, the algorithm terminates.

Proposition 8. *Algorithm 5 computes a comprehensive triangular decomposition of* $F \subset \mathbb{K}[U, X]$.

PROOF. Let $\mathcal{T}$ be the output of $\mathbf{PCTD}(F)$. By Proposition 6 and Proposition 5 (2), we have

$$\Pi_U(\mathbf{V}(F)) = \bigcup_{T \in \mathcal{T}} \mathbf{D}^U(T).$$

Then the conclusion follows from the definition of comprehensive triangular decomposition, Proposition 3, 7 and Remark 2.

Given a polynomial set $F \subset \mathbb{K}[U, X]$, a natural question is to describe the points u of $\overline{\mathbb{K}}^d$ for which the specialized system $F(u)$ admits a finite and positive number of solutions in $\overline{\mathbb{K}}^m$. This question is formalized by the following definition.

Definition 15. *The* discriminant set of F *is defined as the set of all points* $u \in \overline{\mathbb{K}}^d$ *for which* $\mathbf{V}(F(u))$ *is empty or infinite.*

Algorithm 5. $\mathbf{CTD}(F)$

Input: A finite set $F \subset \mathbb{K}[U, X]$.
Output: A CTD of $\mathbf{V}(F)$.

1: $\mathcal{T} \leftarrow$ **PCTD**(F)
2: $\mathcal{S} \leftarrow \emptyset$
3: **for** $T \in \mathcal{T}$ **do**
4: $\quad \mathcal{S} \leftarrow \mathcal{S} \cup \mathcal{R}^U(T)$
5: **end for**
6: $\mathcal{S} \leftarrow \mathbf{SMPD}(\mathcal{S})$
7: **while** $\mathcal{S} \neq \emptyset$ **do**
8: $\quad$ let $C \in \mathcal{S}, \mathcal{S} \leftarrow \mathcal{S} \setminus C$
9: $\quad \mathcal{T}_C \leftarrow$ regular chains in $\mathcal{T}$ associated to C
10: $\quad$ **output** $(C, \mathcal{T}_C)$
11: **end while**

Theorem 4. *If $\mathcal{T}$ is a pre-comprehensive triangular decomposition of $\mathbf{V}(F)$, then the following is the discriminant set of F:*

$$\left(\bigcup_{\substack{T \in \mathcal{T} \\ X \not\subseteq \mathrm{mvar}(T)}} \mathbf{D}^U(T) \right) \cup \left(\bigcap_{\substack{T \in \mathcal{T} \\ X \subseteq \mathrm{mvar}(T)}} \overline{\mathbb{K}}^d \setminus \mathbf{D}^U(T) \right).$$

PROOF. By Proposition 4, for every parameter value $u \in \overline{\mathbb{K}}^d$, the set $\{T(u) \mid T \in \mathcal{T} \text{ and } u \in \mathbf{D}^U(T)\}$ is a triangular decomposition of $\mathbf{V}(F(u))$ into regular chains. In particular, if there exists no $T \in \mathcal{T}$ such that $u \in \mathbf{D}^U(T)$ holds, then $\mathbf{V}(F(u)) = \emptyset$.

Therefore, u yields finitely many solutions (and at least one) if and only if the following conditions hold:

– u belongs to at least one $\mathbf{D}^U(T)$ such that $X \subseteq \mathrm{mvar}(T)$, i.e., $T(u)$ is a zero-dimensional regular chain.
– u does not belong to any $\mathbf{D}^U(T)$ such that $X \not\subseteq \mathrm{mvar}(T)$, i.e., $T(u)$ is a positive-dimensional regular chain.

Remark 3. *By Theorem 4 and Proposition 8, we have completely answered the two problems proposed in the introduction.*

6 Implementation

We have implemented the algorithm for computing comprehensive triangular decompositions (CTD) based on *RegularChains* library in Maple 11. Our main function `CTD` calls essentially three functions

– `Triangularize`, computing a triangular decomposition of the input system F,
– `PCTD`, deducing a pre-comprehensive triangular decomposition of F,
– `SMPD`, obtaining a comprehensive triangular decomposition of F.

Table 1. Solving timings and number of cells of `CTD`

Sys	Name	`Triangularize`	`PCTD`	`SMPD`	`CTD`	#Cells
1	MontesS1	0.089	0.002	0.031	0.122	3
2	MontesS2	0.031	0.002	0	0.033	1
3	MontesS3	0.103	0.006	0.005	0.114	2
4	MontesS4	0.101	0.016	0	0.117	1
5	MontesS5	0.383	0.022	0.465	0.870	11
6	MontesS6	0.395	0.019	0.121	0.535	4
7	MontesS7	0.416	0.215	0.108	0.739	4
8	MontesS8	0.729	0.001	0.016	0.746	2
9	MontesS9	0.945	0.116	3.817	4.878	23
10	MontesS10	5.325	0.684	1.138	7.147	10
11	MontesS11	0.757	0.208	12.302	13.267	28
12	MontesS12	14.199	2.419	10.114	26.732	10
13	MontesS13	0.415	0.143	1.268	1.826	9
14	MontesS14	41.167	31.510	0.303	72.980	4
15	MontesS15	6.919	0.579	1.123	8.621	5
16	MontesS16	6.963	0.083	2.407	9.453	21
17	AlkashiSinus	0.716	0.191	0.574	1.481	6
18	Bronstein	2.526	0.017	0.548	3.091	6
19	Gerdt	3.863	0.006	0.733	4.602	5
20	Hereman-2	1.826	0.019	0.020	1.865	2
21	Lanconelli	2.056	0.336	3.430	5.822	14
22	genLinSyst-3-2	1.624	0.275	25.413	27.312	32
23	genLinSyst-3-3	9.571	1.824	1097.291	1108.686	116
24	Wang93	6.795	37.232	11.828	55.855	8
25	Maclane	12.955	0.403	54.197	67.555	21
26	Neural	15.279	19.313	0.530	35.122	4
27	Leykin-1	1261.751	86.460	27.180	1375.391	57
28	Lazard-ascm2001	60.698	2817.801	–	–	–
29	Pavelle	–	–	–	–	–
30	Cheaters-homotopy	–	–	–	–	–

We provide comparative benchmarks with MAPLE implementations of related methods for solving parametric polynomial systems, namely: *decomposition into regular systems* by Wang [19] and *discussing parametric Gröbner bases* by Montes [14]. Corresponding MAPLE functions are `RegSer` and `DISPGB`, respectively.

Note that the specifications of these three methods are different. The outputs of `CTD` and `DISPGB` depend on the choice of the parameter sets, whereas `RegSer` does not require to specify parameters. `RegSer` decomposes the input system into pairwise disjoint constructible sets given by regular systems. `CTD` computes a comprehensive triangular decomposition, and thus a family of triangular decompositions with a partition of the parameter space. `DISPGB` computes a family of comprehensive Gröbner bases with a partition of the parameter space.

We run `CTD` in Maple 11 using an Intel Pentium 4 processor (3.20GHz CPU, 2.0GB total memory, and Red Hat 4.0.0-9); we set the time-out to 1 hour. Due to the current availability of `RegSer` and `DISPGB`, the timings obtained by these two functions are

Table 2. Solving timings and number of components/cells in three algorithms

	DISPGB		RegSer		CTD	
Sys	Time (s)	# Cells	Time (s)	# Components	Time (s)	# Cells
1	0.509	2	0.021	3	0.122	3
2	0.410	2	0.021	1	0.033	1
3	0.550	2	0.060	3	0.114	2
4	1.511	2	0.070	1	0.117	1
5	1.030	3	0.099	4	0.870	11
6	1.350	4	0.049	5	0.535	4
7	1.609	2	0.180	4	0.739	4
8	2.181	3	0.150	4	0.746	2
9	10.710	5	0.171	7	4.878	23
10	9.659	5	0.329	5	7.147	10
11	0.489	3	0.260	9	13.267	28
12	259.730	5	2.381	23	26.732	10
13	5.830	9	0.199	9	1.826	9
14	–	–	–	–	72.980	4
15	30.470	7	0.640	10	8.621	5
16	61.831	7	6.060	22	9.453	21
17	4.619	6	0.150	5	1.481	6
18	8.791	5	0.319	6	3.091	6
19	20.739	5	3.019	10	4.602	5
20	101.251	2	0.371	7	1.865	2
21	43.441	4	0.330	7	5.822	14
22	–	–	0.350	18	27.312	32
23	–	–	2.031	61	1108.686	116
24	–	–	4.040	6	55.855	8
25	83.210	11	–	–	67.555	21
26	–	–	–	–	35.122	4
27	–	–	–	–	1375.391	57
28	–	–	–	–	–	–
29	–	–	–	–	–	–
30	–	–	–	–	–	–

performed in Maple 8 on Intel Pentium 4 machines (1.60GHz CPU, 513MB memory and Red Hat Linux 3.2.2-5); and the time-out is 2 hours. The 30 test-systems used in our experimentation are chosen from [13,18,21].

As shown in the above two tables, our implementation of the CTD algorithm can solve all problems which can be solved by the other methods. In addition, the `CTD` can solve 4 test-systems which are out of reach of the other two methods, generally due to memory consumption.

7 Conclusion

Comprehensive triangular decomposition is a powerful tool for the analysis of parametric polynomial systems: its purpose is to partition the parameter space into regions, so that within each region the "geometry" of the algebraic variety of the specialized system is the same for all values of the parameters.

As the main technical tool, we proposed an algorithm that represents the difference of two constructible sets as finite unions of regular systems. From there, we have deduced an algorithmic solution for a set theoretical instance of the coprime factorization problem: refining a family of constructible sets into a family of pairwise disjoint constructible sets.

We have reported on an implementation of our algorithm computing CTDs, based on the `RegularChains` library in MAPLE. Our comparative benchmarks, with MAPLE implementations of related methods for solving parametric polynomial systems, illustrate the good performances of our CTD code.

References

1. Aubry, P., Lazard, D., Moreno Maza, M.: On the theories of triangular sets. J. Symb. Comp. 28(1-2), 105–124 (1999)
2. Bernstein, D.J.: Factoring into coprimes in essentially linear time. J. Algorithms 54(1), 1–30 (2005)
3. Boulier, F., Lemaire, F., Moreno Maza, M.: Well known theorems on triangular systems and the D5 principle. In: Proc. of Transgressive Computing 2006, Granada, Spain (2006)
4. Caviness, B., Johnson, J. (eds.): Quantifier Elimination and Cylindical Algebraic Decomposition, Texts and Mongraphs in Symbolic Computation. Springer, Heidelberg (1998)
5. Chen, F., Wang, D. (eds.): Geometric Computation. Lecture Notes Series on Computing, vol. 11. World Scientific Publishing Co., Singapore, New Jersey (2004)
6. Chou, S.C., Gao, X.S.: Computations with parametric equations. In: Proc. ISAAC'91, Bonn, Germany, pp. 122–127 (1991)
7. Chou, S.C., Gao, X.S.: Solving parametric algebraic systems. In: Proc. ISSAC'92, Berkeley, California, pp. 335–341 (1992)
8. Dahan, X., Moreno Maza, M., Schost, É., Xie, Y.: On the complexity of the D5 principle. In: Proc. of Transgressive Computing 2006, Granada, Spain (2006)
9. Duval, D.: Algebraic Numbers: an Example of Dynamic Evaluation. J. Symb. Comp. 18(5), 429–446 (1994)
10. Gómez Díaz, T.: Quelques applications de l'évaluation dynamique. PhD thesis, Université de Limoges (1994)
11. Kalkbrener, M.: A generalized euclidean algorithm for computing triangular representations of algebraic varieties. J. Symb. Comp. 15, 143–167 (1993)
12. Lazard, D., Rouillier, F.: Solving parametric polynomial systems. Technical Report 5322, INRIA (2004)
13. Manubens, M., Montes, A.: Improving dispgb algorithm using the discriminant ideal (2006)
14. Montes, A.: A new algorithm for discussing gröbner bases with parameters. J. Symb. Comput. 33(2), 183–208 (2002)
15. Moreno Maza, M.: On triangular decompositions of algebraic varieties. Technical Report TR 4/99, NAG Ltd, Oxford, UK (1999), `http://www.csd.uwo.ca/~moreno`
16. Samuel, P., Zariski, O.: Commutative algebra. D. Van Nostrand Company, INC (1967)
17. Suzuki, A., Sato, Y.: A simple algorithm to compute comprehensive Gröbner bases. In: Proc. ISSAC'06, pp. 326–331. ACM Press, New York (2006)
18. The SymbolicData Project (2000–2006), `http://www.SymbolicData.org`
19. Wang, D.M.: Computing triangular systems and regular systems. Journal of Symbolic Computation 30(2), 221–236 (2000)

20. Wang, D.M.: Decomposing polynomial systems into simple systems. J. Symb. Comp. 25(3), 295–314 (1998)
21. Wang, D.M.: Elimination Methods. Springer, Wein, New York (2000)
22. Weispfenning, V.: Comprehensive grobner bases. J. Symb. Comp. 14, 1–29 (1992)
23. Weispfenning, V.: Canonical comprehensive grobner bases. In: ISSAC 2002, pp. 270–276. ACM Press, New York (2002)
24. Wu, W.T.: A zero structure theorem for polynomial equations solving. MM Research Preprints 1, 2–12 (1987)
25. Wu, W.T.: On a projection theorem of quasi-varieties in elimination theory. MM Research Preprints 4, 40–53 (1989)
26. Yang, L., Hou, X.R., Xia, B.C.: A complete algorithm for automated discovering of a class of inequality-type theorem. Science in China, Series E 44(6), 33–49 (2001)