Computing Cylindrical Algebraic Decomposition via Triangular Decomposition

Article · April 2009

DOI: 10.1145/1576702.1576718 · Source: arXiv

Changbo Chen
Chongqing Institute of Green and Intelligent Technology, Chinese Academy of Sciences

Marc Moreno Maza
The University of Western Ontario

Bican Xia
Peking University

Lu Yang
Chinese Academy of Sciences

Computing Cylindrical Algebraic Decomposition via Triangular Decomposition

Changbo Chen
ORCCA, University of Western Ontario (UWO)
London, Ontario, Canada
cchen252@csd.uwo.ca

Marc Moreno Maza
ORCCA, University of Western Ontario (UWO)
London, Ontario, Canada
moreno@csd.uwo.ca

Bican Xia
School of Mathematical Sciences
Peking University, Beijing, China
xbc@math.pku.edu.cn

Lu Yang
Shanghai Key Laboratory of Trustworthy Computing
East China Normal University, Shanghai, China
lyang@sei.ecnu.edu.cn

ABSTRACT

Cylindrical algebraic decomposition is one of the most important tools for computing with semi-algebraic sets, while triangular decomposition is among the most important approaches for manipulating constructible sets. In this paper, for an arbitrary finite set $F \subset \mathbb{R}[y_1, \ldots, y_n]$ we apply comprehensive triangular decomposition in order to obtain an F-invariant cylindrical decomposition of the n-dimensional complex space, from which we extract an F-invariant cylindrical algebraic decomposition of the n-dimensional real space. We report on an implementation of this new approach for constructing cylindrical algebraic decompositions.

1. INTRODUCTION

Cylindrical algebraic decomposition (CAD) is a fundamental and powerful tool in real algebraic geometry. The original algorithm introduced by Collins in 1973 [11] has been followed by many substantial ameliorations, including adjacency and clustering techniques [2], improved projection methods [25, 18, 27, 6], partially built CADs [13, 26, 29], improved stack construction [14] and efficient projection orders [16].

The main application of CAD is quantifier elimination (QE) for which other approaches are also available. Some of them have more attractive complexity results [4] than CAD. However, as pointed out by Brown and Davenport in [8], "there is the issue of whether the asymptotic cross-over points between CAD and those other QE algorithms actually occur in the range of problems that are even close to accessible with current machines". In addition, these authors observe that CAD can help solving certain QE problems [7, 19] that other QE algorithms can not.

For a finite set $F_n \subset \mathbb{R}[y_1, \ldots, y_n]$ the CAD algorithm [11] decomposes the real n-dimensional space into disjoint cells $C_1, \ldots, C_e$ together with one *sample point* $S_i \in C_i$, for all $1 \leq i \leq e$, such that the sign of each $f \in F_n$ does not change in C_i and can be determined at S_i. Besides, this decomposition is *cylindrical* in the following sense: For all $1 \leq j < n$ the projections on the first j coordinates $(y_1, \ldots, y_j)$ of any two cells are either disjoint or equal. We will make use of this notion of "cylindrical" decomposition in $\mathbb{C}^n$.

The algorithm of Collins is based on a *projection and lifting* procedure which computes from F_n a finite set $F_{n-1} \subset \mathbb{R}[y_1, \ldots, y_{n-1}]$ such that an F_n-invariant CAD of $\mathbb{R}^n$ can be constructed from an F_{n-1}-invariant CAD of $\mathbb{R}^{n-1}$. This construction and the base case $n = 1$ rely on real root isolation of univariate polynomials.

In this paper, we propose a different approach for computing CAD, which proceeds by successive transformation of an initial decomposition of the complex n-dimensional space. Our algorithm consists of three main steps:

Initial Partition: we decompose $\mathbb{C}^n$ into disjoint constructible sets $C_1, \ldots, C_e$ such that for all $1 \leq i \leq e$, for each $f \in F_n$ either f is identically zero in C_i or f vanishes at no points of C_i.

Make Cylindrical: we transform the initial partition and obtain another decomposition of $\mathbb{C}^n$ into disjoint constructible sets such that this second decomposition is cylindrical in the above sense.

Make Semi-Algebraic: from the previous decomposition we produce an F_n-invariant CAD of $\mathbb{R}^n$.

Our first motivation is to understand the relation and possible interaction between cylindrical algebraic decompositions and triangular decompositions of polynomial systems. This latter kind of decompositions have been intensively studied since the work of Wu [32]. The papers [3, 5, 20] and book [30] contain surveys of the subject. The primary goal of triangular decompositions is to provide unmixed decompositions of algebraic varieties. However, the third and fourth authors have initiated the use of triangular decompositions in real algebraic geometry [35]. Moreover, real root isolation of zero-dimensional polynomial systems can be achieved via triangular decompositions [33, 34, 10].

A second motivation of this work is to investigate the possibility of improving the practical efficiency of CAD implementation by means of modular methods and fast polynomial arithmetic. Such techniques have been successfully introduced into triangular decomposition methods [15, 24, 22]. Each of the three main steps of the algorithm proposed in this paper relies on existing sub-algorithms for triangular decompositions taken from [28, 9, 34] and for which efficient implementation in the `RegularChains` library [21] is work in progress based on the highly optimized low-level routines of the Modpn library [23].

Our third motivation is to extend to real algebraic geometry the concept of *Comprehensive Triangular Decomposition* (CTD) introduced in [9]. The relation between CAD and parametric polynomial system solving is natural as pointed in [17] and the presentation therein of Weispfenning's approach [31] for QE based on comprehensive Gröbner bases. This suggests that the algorithm proposed in this paper could support a similar QE method.

This paper is organized as follows. A summary of the theory of triangular decomposition is given in Section 2. Section 3 and Section 4 are dedicated to the first two main steps of our algorithm whereas Sections 5 presents the last one. In Section 6 we report on a preliminary experimentation of our new algorithm. No modular methods or fast polynomial arithmetic are being used yet and our code is just high-level Maple interpreted code. However our code can already process well-known examples from the literature. We also analyze the performances of the different main steps and subroutines of our algorithm and implementation. This suggests that there is a large potential for improvement by means of modular methods, for instance for the computation of GCDs, resultants (and the discriminants) of polynomials modulo regular chains.

2. TRIANGULAR DECOMPOSITION

Throughout this paper let $\mathbf{k}$ be a field of characteristic zero and $\mathbf{K}$ be the algebraic closure of $\mathbf{k}$. Let $\mathbf{k}[\mathbf{y}] := \mathbf{k}[y_1, \ldots, y_n]$ be the polynomial ring over the field $\mathbf{k}$ in variables $y_1 < \cdots < y_n$. Let $p \in \mathbf{k}[\mathbf{y}]$ be a non-constant polynomial. The greatest variable appearing in p is called the *main variable*, denoted by $\mathrm{mvar}(p)$. The integer k such that $y_k = \mathrm{mvar}(p)$ is called the *level* of p. The *separant* $\mathrm{sep}(p)$ of p w.r.t $\mathrm{mvar}(p)$, is $\partial p / \partial \mathrm{mvar}(p)$. The leading coefficient and the leading monomial of p regarded as a univariate polynomial in $\mathrm{mvar}(p)$ are called the *initial* and the *rank* of p; they are denoted by $\mathrm{init}(p)$ and $\mathrm{rank}(p)$ respectively. Let q be another polynomial of $\mathbf{k}[\mathbf{y}]$, we say $\mathrm{rank}(p)$ is less than $\mathrm{rank}(q)$ if $\mathrm{mvar}(p) < \mathrm{mvar}(q)$, or $\mathrm{mdeg}(p) < \mathrm{mdeg}(q)$ when $\mathrm{mvar}(p) = \mathrm{mvar}(q)$.

Let $F \subset \mathbf{k}[\mathbf{y}]$ be a finite polynomial set. Denote by $\langle F \rangle$ the ideal it generates in $\mathbf{k}[\mathbf{y}]$. Let h be a polynomial in $\mathbf{k}[\mathbf{y}]$, the *saturated ideal* $\langle F \rangle : h^\infty$ of $\langle F \rangle$ w.r.t h, is the set $\{q \in \mathbf{k}[\mathbf{y}] \mid \exists m \in \mathbb{N} \text{ s.t. } h^m q \in \langle F \rangle\}$, which is an ideal in $\mathbf{k}[\mathbf{y}]$. The polynomial is *regular* modulo $\langle F \rangle$ if it is neither zero, nor a zerodivisor modulo $\langle F \rangle$. Denote by $V(F)$ the *zero set* (or algebraic variety) of F in $\mathbf{K}^n$.

Let $T \subset \mathbf{k}[\mathbf{y}]$ be a *triangular set*, that is a set of non-constant polynomials with pairwise distinct main variables. We denote by $\mathrm{mvar}(T)$ the set of main variables of polynomials in T. A variable in $\mathbf{y}$ 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 $v \in \mathbf{y}$, we denote by $T_{<v}$ the subsets of T consisting of the polynomials t with main variable less than v. Let h_T be the product of the initials of polynomials in T. We denote by $\mathrm{sat}(T)$ the saturated ideal of T: if T is empty then $\mathrm{sat}(T)$ is defined as the trivial ideal $\langle 0 \rangle$, otherwise it is the ideal $\langle T \rangle : h_T^\infty$. The *quasi-component* $W(T)$ of T is defined as $V(T) \setminus V(h_T)$. Let $h \in \mathbf{k}[\mathbf{y}]$ be a polynomial. Define $Z(T, h) := W(T) \setminus V(h)$.

Let $h \in \mathbf{k}[\mathbf{y}]$ be a polynomial. The *iterated resultant* of h w.r.t. T, denoted by $\mathrm{ires}(h, T)$, is defined as follows: (1) if $h \in \mathbf{k}$ or all variables in h are free w.r.t. T, then $\mathrm{ires}(h, T) = h$; (2) otherwise, if v is the largest variable of h which is algebraic w.r.t. T, then $\mathrm{ires}(h, T) = \mathrm{ires}(r, T_{<v})$ where r is the resultant of h and the polynomial in T whose main variable is v. Iterated resultants have the following important property: the polynomial h is regular modulo $\mathrm{sat}(T)$ if and only if we have $\mathrm{ires}(h, T) \neq 0$.

We say that the triangular set T is a *regular chain* if either $T = \varnothing$ or $\mathrm{ires}(h_T, T) \neq 0$. The pair $[T, h]$ is called a *regular system* if T is a regular chain, and $\mathrm{ires}(h, T) \neq 0$. Denote by $\mathrm{sep}(T)$ the product of all $\mathrm{sep}(p)$, where $p \in T$. Then T is said to be *squarefree* if $\mathrm{ires}(\mathrm{sep}(T), T) \neq 0$. A regular system $rs = [T, h]$ is said to be *squarefree* if T is squarefree.

For a regular system $rs = [T, h]$, the rank of rs, denoted by $\mathrm{rank}(rs)$, is defined as the set of $\mathrm{rank}(p)$ for all $p \in T$. Given another regular system $rs' = [T', h']$ with $\mathrm{rank}(rs) \neq \mathrm{rank}(rs')$, we say $\mathrm{rank}(rs)$ is less than $\mathrm{rank}(rs')$ whenever the minimal element of the symmetric difference $(\mathrm{rank}(rs) \setminus \mathrm{rank}(rs')) \cup (\mathrm{rank}(rs') \setminus \mathrm{rank}(rs))$ belongs to $\mathrm{rank}(rs)$.

A *constructible set* of $\mathbf{K}^n$ 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 $\mathbf{K}^n$. For any constructible set cs of $\mathbf{K}^n$ there exist finitely many regular systems $rs_1, \ldots, rs_m$ of $\mathbf{k}[\mathbf{y}]$ such that $cs = Z(rs_1) \cup \cdots \cup Z(rs_m)$.

Example 1. Consider the polynomials in $\mathbf{k}[y_1 < y_2 < y_3]$

$$p_1 = y_2^2 + y_1 - 1 \text{ and } p_2 = y_1 y_3^2 - 1.$$

We illustrate the previous main notions as follows.

	mvar	sep	init	rank
p_1	y_2	$2y_2$	1	y_2^2
p_2	y_3	$2y_1y_3$	y_1	$y_1y_3^2$

The initial y_1 of p_2 is regular modulo $\langle p_1 \rangle$. The set $T = \{p_1, p_2\}$ is a triangular set. The iterated resultant of y_1 and

T is y_1, so T is a regular chain. The pair $[T, y_2]$ is a regular system, since $\mathrm{ires}(y_2, T) = y_1 - 1$. The quasi-component of T is the set of points in $\mathbf{K}^3$ such that $p_1 = 0$, $p_2 = 0$ and $y_1 \neq 0$, which is a constructible set.

We review three important operations Intersect, `MakePairwiseDisjoint` (MPD) and `SymmetricallyMakePairwiseDisjoint` (SMPD) proposed in [9]. Let $rs_* = [T_*, h_*]$ be a squarefree regular system of $\mathbf{k}[\mathbf{y}]$ and let p be a polynomial of $\mathbf{k}[\mathbf{y}]$ such that p is regular w.r.t $\mathrm{sat}(T_*)$. The operation $\mathsf{Intersect}(p, rs_*)$ computes a family of squarefree regular systems $\mathcal{R}$ of $\mathbf{k}[\mathbf{y}]$ such that

$$V(p) \cap Z(rs_*) = \cup_{rs \in \mathcal{R}} Z(rs),$$

and the rank of each $rs \in \mathcal{R}$ is less than that of rs_*.

For regular systems $[T_1, h_1], \ldots, [T_e, h_e]$ in $\mathbf{k}[\mathbf{y}]$, the function MPD returns regular systems $[S_1, g_1], \ldots, [S_f, g_f]$ in $\mathbf{k}[\mathbf{y}]$ s.t.

$$Z(T_1, h_1) \cup \cdots \cup Z(T_e, h_e) = Z(S_1, g_1) \cup \cdots \cup Z(S_f, g_f),$$

and for all $1 \leq i < j \leq f$ we have $Z(S_i, g_i) \cap Z(S_j, g_j) = \varnothing$.

Given a family $\mathcal{C} = \{C_1, \ldots, C_r\}$ of constructible sets of $\mathbf{K}^n$, the function SMPD returns a family $\mathcal{D} = \{D_1, \ldots, D_s\}$ of constructible sets of $\mathbf{K}^n$ such that $D_i \cap D_j = \varnothing$ for all $1 \leq i < j \leq n$, each D_j is a subset of some C_i, and each C_i can be written as a finite union of some of the D_j's. Such a $\mathcal{D}$ is called an *intersection-free basis* of $\mathcal{C}$.

3. ZERO SEPARATION

In this section, we assume $n \geq 2$ and we regard the ordered variables $y_1 < \cdots < y_{n-1}$ as parameters, denoted by $\mathbf{u}$. Let $\pi_{\mathbf{u}}$ be the projection function which sends a point $(\bar{\mathbf{u}}, \bar{y_n})$ of $\mathbf{K}^n$ to the point $\bar{\mathbf{u}}$ of the parameter space $\mathbf{K}^{n-1}$. Let $\bar{\mathbf{u}} \in \mathbf{K}^{n-1}$. We write $\pi_{\mathbf{u}}^{-1}(\bar{\mathbf{u}})$ for the set of all points $(\bar{\mathbf{u}}, \bar{y_n})$ in $\mathbf{K}^n$ such that $\pi_{\mathbf{u}}(\bar{\mathbf{u}}, \bar{y_n}) = \bar{\mathbf{u}}$.

Let $p \in \mathbf{k}[\mathbf{u}, y_n]$ be a polynomial of level n, that is, with main variable y_n. In broad terms, the goal of this section is to decompose the parameter space $\mathbf{K}^{n-1}$ into finitely many cells such that above each cell the "root structure" of p (number of roots, their multiplicity, ...) does not change. In fact, we make this problem more general by allowing algebraic constraints on the parameter $\mathbf{u}$. After some notations, we define in Definition 1 the object to be computed by the algorithm devised in this section. It can be seen as a specialization of the comprehensive triangular decomposition (CTD) to the case where the input system is a regular system and all variables but one are regarded as parameters. This algorithm is stated in Section 3.1 after two lemmas.

Notations. Let $rs = [T, h]$ be a regular system of $\mathbf{k}[\mathbf{u}, y_n]$. If y_n does not appear in rs, we denote by $Z_{\mathbf{u}}(rs)$ the zero set of rs in $\mathbf{K}^{n-1}$. If y_n does not appear in T, we write $W_{\mathbf{u}}(T)$ for the quasi-component of T in $\mathbf{K}^{n-1}$. If $\mathrm{mvar}(h) = y_n$ holds, we denote by $\mathrm{coeff}(h)$ be the set of coefficients of h when h is regarded as a polynomial in y_n with coefficients in $\mathbf{k}[\mathbf{u}]$ and by $V_{\mathbf{u}}(\mathrm{coeff}(h))$ the variety of $\mathrm{coeff}(h)$ in $\mathbf{K}^{n-1}$. Finally, if y_n is algebraic in T, letting t_n be the polynomial in T with main variable y_n, we write $T_{\mathbf{u}} = T \setminus \{t_n\}$ and $rs_{\mathbf{u}} = [T_{\mathbf{u}}, r]$, where $r = \mathrm{res}(h \cdot \mathrm{sep}(t_n), t_n)$ is the resultant of $h \cdot \mathrm{sep}(t_n)$ and t_n w.r.t y_n.

Definition 1. Let C be a constructible set of $\mathbf{K}^{n-1}$. A finite set of level n polynomials $\mathcal{P} \subset \mathbf{k}[\mathbf{u}, y_n]$ *separates above* C if for each $\alpha \in C$: (1) the initial of any $p \in \mathcal{P}$ does not vanish at α; (2) the polynomials $p(\alpha, y_n) \in \mathbf{K}[y_n]$, $p \in \mathcal{P}$, are squarefree and coprime.

Let $\mathcal{C}$ be a finite collection of pairwise disjoint constructible sets of $\mathbf{K}^{n-1}$, and, for each $C \in \mathcal{C}$, let $\mathcal{P}_C \subset \mathbf{k}[\mathbf{u}, y_n]$ be a finite set of level n polynomials. Let $rs_* = [T_*, h_*]$ be a regular system of $\mathbf{k}[\mathbf{u}, y_n]$, where $n \geq 2$ and y_n is algebraic w.r.t T. We say that the family $\{(C, \mathcal{P}_C) \mid C \in \mathcal{C}\}$ *separates* $Z(rs_*)$ if the following conditions hold:

(1) $\mathcal{C}$ is a partition of $\pi_{\mathbf{u}}(Z(rs_*))$,

(2) for each $C \in \mathcal{C}$, $\mathcal{P}_C$ separates above C,

(3) $Z(rs_*) = \bigcup_{C \in \mathcal{C}} \bigcup_{p \in \mathcal{P}_C} V(p) \cap \pi_{\mathbf{u}}^{-1}(C)$.

More generally, let cs be a constructible set of $\mathbf{K}^n$ such that there exist regular systems $rs_1, \ldots, rs_r$ of $\mathbf{k}[\mathbf{u}, y_n]$ whose zero sets form a partition of cs and such that y_n is algebraic w.r.t. the regular chain of rs_i, for all $1 \leq i \leq r$. Then, we say that the family $\{(C, \mathcal{P}_C) \mid C \in \mathcal{C}\}$ *separates* cs if $\mathcal{C}$ is a partition of $\pi_{\mathbf{u}}(cs)$ and if for all $1 \leq i \leq r$ there exists a non-empty subset $\mathcal{C}_i$ of $\mathcal{C}$ and for each $C \in \mathcal{C}_i$ a non-empty subset $\mathcal{P}_{C,i} \subseteq \mathcal{P}_C$ such that $\{(C, \mathcal{P}_{C,i}) \mid C \in \mathcal{C}_i\}$ separates $Z(rs_i)$. In this case, we have: $cs = \bigcup_{C \in \mathcal{C}} \bigcup_{p \in \mathcal{P}_C} V(p) \cap \pi_{\mathbf{u}}^{-1}(C)$.

Example 2. Consider the polynomials in $\mathbf{k}[x > b > a]$

$$p_1 = ax^2 - b \text{ and } p_2 = ax^2 + 2x + b,$$

and the constructible set $C = \{(a, b) \in \mathbf{K}^2 \mid ab(ab - 1) \neq 0\}$. For any point (a, b) of C, the two polynomials $p_1(a, b)$ and $p_2(a, b)$ of $\mathbf{K}[x]$ are squarefree and coprime. So the polynomial set $\{p_1, p_2\}$ separates above C.

Consider the regular system $rs_* = [\{p_1\}, 1]$ and the constructible sets

$$\begin{array}{l} C_1 = \{(a, b) \in \mathbf{K}^2 \mid ab \neq 0\} \\ C_2 = \{(a, b) \in \mathbf{K}^2 \mid a \neq 0 \ \& \ b = 0\} \end{array}$$

Note that the zero set of rs_* is $\{p_1 = 0 \ \& \ a \neq 0\}$. So the family $\{\ (C_1, \{p_1\}),\ (C_2, \{ax\})\ \}$ separates $Z(rs_*)$.

Given two regular systems

$$rs_1 = [\{p_1\}, b] \text{ and } rs_2 = [\{p_2, b\}, 1].$$

Consider the constructible set

$$\begin{array}{rcl} cs & = & Z(rs_1) \cup Z(rs_2) \\ & = & (V(p_1) \setminus V(ab)) \cup (V(p_2, b) \setminus V(a)). \end{array}$$

The family $\{\ (C_1, \{p_1\}),\ (C_2, \{p_2\})\ \}$ separates cs.

Lemma 1. *Let $p \in \mathbf{k}[\mathbf{u}, y_n]$ be a level n polynomial. Let $r = res(sep(p), p)$ be the resultant of $sep(p)$ and p w.r.t y_n. Then, the polynomial $p(\bar{\mathbf{u}})$ of $\mathbf{K}[y_n]$ is squarefree and $init(p)$ does not vanish at $\bar{\mathbf{u}} \in \mathbf{K}^{n-1}$, if and only if, $r(\bar{\mathbf{u}}) \neq 0$ holds.*

Observe that $\mathrm{init}(p)$ is a factor of r. So the conclusion follows directly from the specialization property of subresultants.

Lemma 2. *We have the following properties:*

(1) *If y_n does not appear in rs, then $\pi_{\mathbf{u}}(Z(rs)) = Z_{\mathbf{u}}(rs)$.*

(2) *If y_n does not appear in T and if $mvar(h) = y_n$ holds, then we have $\pi_{\mathbf{u}}(Z(rs)) = W_{\mathbf{u}}(T) \setminus V_{\mathbf{u}}(\mathrm{coeff}(h))$.*

(3) *If y_n is algebraic w.r.t T and if the regular system rs is squarefree, then $rs_{\mathbf{u}}$ is a squarefree regular system of $\mathbf{k}[\mathbf{u}]$; moreover there exists a family $\mathcal{R}'$ of squarefree regular systems of $\mathbf{k}[\mathbf{u}, y_n]$ such that:*

   (a) *the rank of each $rs' \in \mathcal{R}'$ is less than that of rs,*

   (b) *for each $[T', h'] \in \mathcal{R}'$, y_n is algebraic w.r.t T',*

   (b) *the zero sets $Z(rs')$, $rs' \in \mathcal{R}'$ and the zero set $V(t_n) \cap Z(rs_{\mathbf{u}})$ are pairwise disjoint, and we have*

   (d) *$Z(rs) = V(t_n) \cap Z(rs_{\mathbf{u}}) \ \cup \ \bigcup_{rs' \in \mathcal{R}'} Z(rs')$.*

Proof. Property (1) is clear and proving (2) is routine. We prove (3). Since rs is squarefree, using the above notations, we have

$$\mathrm{ires}(r, T) = \mathrm{ires}(r, T_{\mathbf{u}}) = \mathrm{ires}(h \cdot \mathrm{sep}(t_n), T) \neq 0.$$

This implies that r is regular w.r.t $\mathrm{sat}(T)$ and that $rs_{\mathbf{u}} = [T_{\mathbf{u}}, r]$ is a squarefree regular system of $\mathbf{k}[\mathbf{u}]$. Observe now that the zero set of rs decomposes in two disjoint parts:

$$Z(rs) = (Z(rs) \setminus V(r)) \cup (Z(rs) \cap V(r)).$$

For the first part, we have

$$Z(rs) \setminus V(r) = V(t_n) \cap Z(rs_{\mathbf{u}}).$$

For the second part, since r is regular w.r.t $\mathrm{sat}(T)$, by calling operation Intersect, we obtain a family $\mathcal{R}$ of squarefree regular systems of $\mathbf{k}[\mathbf{u}, y_n]$ such that

$$Z(rs) \cap V(r) = \bigcup_{rs' \in \mathcal{R}} Z(rs'),$$

where the rank of each $rs' \in \mathcal{R}$ is less than that of rs. Finally, applying the operation MPD to $\mathcal{R}$ we obtain a family $\mathcal{R}'$ satisfying the properties (a), (b), (c) and (d). □

3.1 The Algorithm SeparateZeros

We present now an algorithm "solving" a regular system in the sense of Definition 1. Precise specializations and algorithm steps follow.

Calling sequence. SeparateZeros$(rs_*, \mathbf{u}, n)$

Input. A (squarefree) regular system $rs_* = [T_*, h_*]$ of $\mathbf{k}[\mathbf{u}, y_n]$, where $n \geq 2$ and y_n is algebraic w.r.t T_*.

Output. A finite family $\{(C, \mathcal{P}_C) \mid C \in \mathcal{C}\}$, where $\mathcal{C}$ is a finite collection of constructible sets of $\mathbf{K}^{n-1}$, and for each $C \in \mathcal{C}$, $\mathcal{P}_C \subset \mathbf{k}[y_1, \ldots, y_n]$ is a finite set of level n polynomials, such that $\{(C, \mathcal{P}_C) \mid C \in \mathcal{C}\}$ separates the zero set of rs_*. (See Definition 1.)

Step (1). Initialize $\mathcal{R} = \{rs_*\}$ and $\mathcal{P} = \varnothing$.

Step (2). If $\mathcal{R} = \varnothing$, go to **Step** (3). Otherwise arbitrarily choose one regular system $rs = [T, h]$ from $\mathcal{R}$ and let $\mathcal{R} = \mathcal{R} \backslash \{rs\}$. Using the above notations, let $\mathcal{R}'$ be as in Property (3) of Lemma 2. Set $\mathcal{P} = \mathcal{P} \cup \{(rs_{\mathbf{u}}, t_n)\}$, set $\mathcal{R} = \mathcal{R} \cup \mathcal{R}'$ and repeat **Step** (2).

Comment. Observe that Step (2) will finally terminate since each newly added regular system into $\mathcal{R}$ has a rank less than that of the one removed from $\mathcal{R}$. When Step (2) terminates, we obtain a family $\mathcal{P}$ of pairs such that

$$Z(rs_*) = \bigcup_{(rs_{\mathbf{u}}, t_n) \in \mathcal{P}} V(t_n) \cap \pi_u^{-1}(Z_{\mathbf{u}}(rs_{\mathbf{u}})),$$

and the union is disjoint. Next, observe that for each pair $(rs_{\mathbf{u}}, t_n) \in \mathcal{P}$, the polynomial $\mathrm{init}(t_n)$ does not vanish at any point of $Z_{\mathbf{u}}(rs_{\mathbf{u}})$, by virtue of Lemma 1. Therefore, the union of all $Z_{\mathbf{u}}(rs_{\mathbf{u}})$ is equal to $\pi_{\mathbf{u}}(Z(rs_*))$.

Step (3). By means of the operation SMPD we compute an intersection-free basis of all $Z_{\mathbf{u}}(rs_{\mathbf{u}})$. Hence we obtain a partition $\mathcal{C}$ of $\pi_{\mathbf{u}}(Z(rs_*))$. Then, for each $C \in \mathcal{C}$ we define $\mathcal{P}_C$ as the set of the polynomials t_n such that there exists a regular system $rs_{\mathbf{u}}$ satisfying $(rs_{\mathbf{u}}, t_n) \in \mathcal{P}$ and $C \subseteq Z_{\mathbf{u}}(rs_{\mathbf{u}})$. Clearly $\{(C, \mathcal{P}_C) \mid C \in \mathcal{C}\}$ is a valid output.

Finally, we generalize this algorithm in order to apply it to a constructible set represented by regular systems.

Calling sequence. SeparateZeros$(\{rs_1, \ldots, rs_r\}, \mathbf{u}, n)$

Input. Regular systems $rs_1, \ldots, rs_r$ of $\mathbf{k}[\mathbf{u}, y_n]$, $n \geq 2$, whose zero sets are pairwise disjoint and such that y_n is algebraic w.r.t. the regular chain of rs_i, for all $1 \leq i \leq r$; let cs be the constructible set represented by $rs_1, \ldots, rs_r$.

Output. A finite family $\{(C, \mathcal{P}_C) \mid C \in \mathcal{C}\}$, where $\mathcal{C}$ is a finite collection of constructible sets of $\mathbf{K}^{n-1}$, and for each $C \in \mathcal{C}$, $\mathcal{P}_C \subset \mathbf{k}[y_1, \ldots, y_n]$ is a finite set of level n polynomials, such that $\{(C, \mathcal{P}_C) \mid C \in \mathcal{C}\}$ separates cs. (See Definition 1.)

Step (1). For each $1 \leq i \leq r$, call SeparateZeros$(rs_i, \mathbf{u}, n)$ obtaining $\{(C, \mathcal{P}_C) \mid C \in \mathcal{C}_i\}$ where $\mathcal{C}_i$ is a partition of $\pi_{\mathbf{u}}(Z(rs_i))$.

Step (2). By means of the operation SMPD, compute an intersection-free basis $\mathcal{D}$ of the union of the $\mathcal{C}_i$, for $1 \leq i \leq r$.

Step (3). For each $D \in \mathcal{D}$, let $\mathcal{P}_D$ be the union of the $\mathcal{P}_C$ such that $D \subseteq C$ holds. Return $\{(D, \mathcal{P}_D) \mid D \in \mathcal{D}\}$.

4. CYLINDRICAL DECOMPOSITION

In this section, we propose the notion of an *F-invariant cylindrical decomposition* of $\mathbf{K}^n$, generalizing ideas that are well-known in the case of real fields. The main algorithm and its subroutines for computing such a decomposition are stated in three subsections.

Definition 2. We state the definition by induction on n. For $n = 1$, a cylindrical decomposition of $\mathbf{K}$ is a finite collection of sets $\{D_1, \ldots, D_{r+1}\}$, where either $r = 0$ and $D_1 = \mathbf{K}$, or $r > 0$ and there exists r nonconstant coprime squarefree polynomials $p_1, \ldots, p_r$ of $\mathbf{k}[y_1]$ such that

$$D_i = \{y_1 \in \mathbf{K} \mid p_i(y_1) = 0\}, 1 \leq i \leq r,$$

and $D_{r+1} = \{y_1 \in \mathbf{K} \mid p_1(y_1) \cdots p_r(y_1) \neq 0\}$. Note that all D_i, $1 \leq i \leq r+1$ form a partition of $\mathbf{K}$. Now let $n > 1$, and let $\mathcal{D}' = \{D_1, \ldots, D_s\}$ be any cylindrical decomposition of $\mathbf{K}^{n-1}$. For each D_i, let $\{p_{i,1}, \ldots, p_{i,r_i}\}$, $r_i \geq 0$, be a set of polynomials which separates above D_i. (See Definition 1.) If $r_i = 0$, set $D_{i,1} = D_i \times \mathbf{K}$. If $r_i > 0$, set

$$D_{i,j} = \{(\alpha, y_n) \in \mathbf{K}^n \mid \alpha \in D_i \ \&\ p_{i,j}(\alpha, y_n) = 0\},$$

for $1 \leq j \leq r_i$ and set

$$D_{i,r_i+1} = \{(\alpha, y_n) \in \mathbf{K}^n \mid \alpha \in D_i \ \&\ \left(\prod_{j=1}^{r_i} p_{i,j}(\alpha, y_n)\right) \neq 0\}.$$

The collection $\mathcal{D} = \{D_{i,j} \mid 1 \leq i \leq s, 1 \leq j \leq r_i + 1\}$ is called a cylindrical decomposition of $\mathbf{K}^n$. Moreover, we say that $\mathcal{D}$ induces $\mathcal{D}'$.

Let $F = \{f_1, \ldots, f_s\}$ be a finite set of polynomials of $\mathbf{k}[y_1 < \cdots < y_n]$. A cylindrical decomposition $\mathcal{D}$ of $\mathbf{K}^n$ is called *F-invariant* if $\mathcal{D}$ is an intersection-free basis of the $s+1$ constructible sets $V(f_i)$, $1 \leq i \leq s$ and $\{y \in \mathbf{K}^n \mid f_1(y) \cdots f_s(y) \neq 0\}$.

LEMMA 3. *Let $rs_1, \ldots, rs_{r+1}$, with $r \geq 1$, be regular systems of $\mathbf{k}[y_1]$ such that their zero sets form a partition of $\mathbf{K}^1$. Then, up to renumbering, there exist polynomials $p_1, \ldots, p_r$, $h_1, \ldots, h_r, h_{r+1} \in \mathbf{k}[y_1]$ such that $rs_i = [\{p_i\}, h_i]$ for $1 \leq i \leq r$ and $rs_{r+1} = [\varnothing, h_{r+1}]$. Moreover, setting $D_i = V(p_i)$ for $1 \leq i \leq r$ and $D_{r+1} = \{y_1 \in \mathbf{K} \mid p_1(y_1) \cdots p_r(y_1) \neq 0\}$, the sets $D_1, \ldots, D_{r+1}$ form a cylindrical decomposition of $\mathbf{K}$.*

PROOF. Observe that for $1 \leq i \leq r$ we have $Z(rs_i) = V(p_i)$, as h_i and p_i have no common roots. Since the zero sets $Z(rs_1), \ldots, Z(rs_{r+1})$ form a partition of $\mathbf{K}^1$, we must have $V(h_{r+1}) = V(p_1 \cdots p_r)$. The conclusion follows. □

4.1 The Algorithm MakeCylindrical

Calling sequence. MakeCylindrical$(\mathcal{R}, n)$

Input. $\mathcal{R}$, a finite family of regular systems such that the zero sets $Z(rs)$, for all $rs \in \mathcal{R}$, form a partition of $\mathbf{K}^n$.

Output. $\mathcal{D}$, a cylindrical decomposition of $\mathbf{K}^n$ such that the zero set of each regular system in $\mathcal{R}$ is a union of some cells in $\mathcal{D}$.

Step (1)**: Base case.** If $n > 1$, go to (2). If $\mathcal{R}$ has only one element, return $\mathcal{D} = \mathbf{K}$ otherwise use the construction of Lemma 3 to return a cylindrical decomposition $\mathcal{D}$.

Step (2)**: Initialization.** Set to $\mathcal{R}_1, \mathcal{R}_2, \mathcal{R}_3$ the subset of $\mathcal{R}$ consisting of regular systems $rs = [T, h]$ such that, y_n is algebraic w.r.t T, y_n appears in h but not in T, y_n does not appear in T nor in h, respectively.

Step (3)**: Processing $\mathcal{R}_1$.** Call SeparateZeros$(\mathcal{R}_1, \mathbf{u}, n)$ (see Section 3) obtaining $\{(C, \mathcal{P}_C) \mid C \in \mathcal{C}_1\}$ where $\mathcal{C}_1$ is a partition of $\pi_{\mathbf{u}}(cs_1)$, where cs_1 is the constructible set represented by $\mathcal{R}_1$. By adding a "1" in each pair, we obtain a collection of triples $\mathcal{T}_1 = \{(C, \mathcal{P}_C, 1) \mid C \in \mathcal{C}_1\}$.

Step (4)**: Processing $\mathcal{R}_2$.** For each $rs \in \mathcal{R}_2$, compute the projection $\pi_{\mathbf{u}}(Z(rs))$ by Property (2) of Lemma 2. Set $\mathcal{C}_2 = \{\pi_{\mathbf{u}}(Z(rs)) \mid rs \in \mathcal{R}_2\}$ and $\mathcal{T}_2 = \{(C, \varnothing, 2) \mid C \in \mathcal{C}_2\}$.

Step (5)**: Processing $\mathcal{R}_3$.** For each $rs \in \mathcal{R}_3$, compute the projection $\pi_{\mathbf{u}}(Z(rs))$ by Property (1) of Lemma 2. Set $\mathcal{C}_3 = \{\pi_{\mathbf{u}}(Z(rs)) \mid rs \in \mathcal{R}_3\}$ and $\mathcal{T}_3 = \{(C, \varnothing, 3) \mid C \in \mathcal{C}_3\}$.

Comment. Since the zero sets of regular systems in $\mathcal{R}$ are pairwise disjoint, after step (3), (4), (5), we know that the element in $\mathcal{C}_3$ has no intersection with any element in $\mathcal{C}_1$ or $\mathcal{C}_2$. Note that it is possible that an element in $\mathcal{C}_1$ has intersection with some element of $\mathcal{C}_2$. So we need the following step to remove the common part between them.

Step (6)**: Merging.** Set $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3$ and $\mathcal{T} = \mathcal{T}_1 \cup \mathcal{T}_2 \cup \mathcal{T}_3$. Note that each element in $\mathcal{T}$ is a triple $(C, \mathcal{P}_C, \mathcal{I}_C)$, with $C \in \mathcal{C}$ and where $\mathcal{I}_C$ is an integer of value $1, 2$ or 3. By means of the operation SMPD, compute an intersection-free basis $\mathcal{C}'$ of $\mathcal{C}$. For each $C' \in \mathcal{C}'$, compute $\mathcal{Q}_{C'}$ (resp. $\mathcal{J}_{C'}$) the union of the $\mathcal{P}_C$ (resp. $\mathcal{I}_C$) such that $C' \subseteq C$ holds. Set $\mathcal{T}' = \{(C, \mathcal{Q}_C, \mathcal{J}_C) \mid C \in \mathcal{C}'\}$.

Step (7)**: Refinement.** To each $C \in \mathcal{C}'$, apply operation MPD to the family of regular systems representing C, so as to obtain another family $\mathcal{R}_C$ of regular systems representing C and whose zero sets are pairwise disjoint. For each $rs \in \mathcal{R}_C$, set $\mathcal{P}_{rs} = \mathcal{Q}_C$ and $\mathcal{I}_{rs} = \mathcal{J}_C$. Let $\mathcal{R}'$ be the union of the $\mathcal{R}_C$, for all $C \in \mathcal{C}'$. Set $\mathcal{T}'' = \{(Z(rs), \mathcal{P}_{rs}, \mathcal{I}_{rs}) \mid rs \in \mathcal{R}'\}$.

Comment. Recall that the union of zero sets of the $Z(rs)$, for all $rs \in \mathcal{R}$ equals $\mathbf{K}^n$. Therefore, it follows from Steps (6) and (7), that $\{Z(rs) \mid rs \in \mathcal{R}'\}$ is a partition of $\mathbf{K}^{n-1}$.

Step (8)**: Recursive call.** Call MakeCylindrical$(\mathcal{R}', n-1)$ to compute a cylindrical decomposition $\mathcal{D}'$ of $\mathbf{K}^{n-1}$ such that $Z(rs)$, for each $rs \in \mathcal{R}'$, is a union of some cells of $\mathcal{D}'$. For each $D' \in \mathcal{D}'$, observe that there exists a unique $rs \in \mathcal{R}'$ such that $D' \subseteq Z(rs)$, so set $\mathcal{P}_{D'} = \mathcal{P}_{rs}$ and $\mathcal{I}_{D'} = \mathcal{I}_{rs}$. Then, set $\mathcal{T}''' = \{(D', \mathcal{P}_{D'}, \mathcal{I}_{D'}) \mid D' \in \mathcal{D}'\}$.

Comment. By the comment below Step (5), we know that for each triple $(D', \mathcal{P}_{D'}, \mathcal{I}_{D'})$ of $\mathcal{T}'''$, the values of $\mathcal{I}_{D'}$ can only be $\{1, 2\}$, $\{2\}$ or $\{3\}$. Next, observe that for each $D' \in \mathcal{D}'$ such that $\mathcal{I}_{D'} = \{2\}$ or $\mathcal{I}_{D'} = \{3\}$ holds, we have $\mathcal{P}_{D'} = \varnothing$, whereas for each $D' \in \mathcal{D}'$ such that $\mathcal{I}_{D'} = \{1, 2\}$ the set $\mathcal{P}_{D'}$ is a nonempty finite family of level n polynomials in $\mathbf{k}[y_1, \ldots, y_n]$ such that $\mathcal{P}_{D'}$ separates above $\mathcal{D}'$. In Step (9) below, we lift the cylindrical decomposition $\mathcal{D}'$ of $\mathbf{K}^{n-1}$ to a cylindrical decomposition $\mathcal{D}$ of $\mathbf{K}^n$.

Step (9)**: Lifting.** Initialize $\mathcal{D}$ to the empty set. For each $D' \in \mathcal{D}'$ such that $\mathcal{I}_{D'} = \{2\}$ or $\mathcal{I}_{D'} = \{3\}$ holds, let $\mathcal{D} := \mathcal{D} \cup \{D' \times \mathbf{K}\}$. For each $D' \in \mathcal{D}'$ such that $\mathcal{I}_{D'} = \{1, 2\}$ holds, let $\mathcal{D} = \mathcal{D} \cup \{D_p\}$, where

$$D_p = \{(\alpha, y_n) \in \mathbf{K}^n \mid \alpha \in D' \ \text{ and } \ p(\alpha, y_n) = 0\},$$

for each $p \in \mathcal{P}_{D'}$ and let $\mathcal{D} = \mathcal{D} \cup \{D_*\}$, where

$$D_* = \{(\alpha, y_n) \in \mathbf{K}^n \mid \alpha \in D' \ \&\ \left(\prod_{p \in \mathcal{P}_{D'}} p(\alpha, y_n)\right) \neq 0\},$$

Finally, return $\mathcal{D}$. The correctness of the algorithm follows from all the comments and Definition 2.

4.2 The Algorithm InitialPartition

Calling sequence. InitialPartition(F, n)

Input. $F = \{f_1, \ldots, f_s\}$, a finite subset of $\mathbf{k}[y_1 < \cdots < y_n]$.

Output. A family $\mathcal{R}$ of regular systems, the zero sets of which form an intersection-free basis of the $s+1$ constructible sets $V(f_1), \ldots, V(f_s)$ and $\{y \in \mathbf{K}^n \mid \left(\prod_{i=1}^{s} f_i(y)\right) \neq 0\}$.

Step (1)**:** Let $\mathcal{B} = \mathsf{SMPD}(V(f_1), \ldots, V(f_s))$ be an intersection free basis of the s constructible sets $V(f_1), \ldots, V(f_s)$. For each element B of $\mathcal{B}$, we apply operation MPD to the family of regular systems representing B to compute another family $\mathcal{R}_B$ of squarefree regular systems such that the zero sets of regular systems in $\mathcal{R}_B$ are pairwise disjoint and their union is B. Let $\mathcal{R}$ be the union of all $\mathcal{R}_B$, $B \in \mathcal{B}$. Clearly the set $\{Z(rs) \mid rs \in \mathcal{R}\}$ is an intersection-free basis of the s constructible sets $V(f_1), \ldots, V(f_s)$.

Step (2)**:** Let $f = \prod_{f_i \in F} f_i$ and $rs_* = [\varnothing, f]$. Set $\mathcal{R} = \mathcal{R} \cup \{rs_*\}$. Obviously $\mathcal{R}$ is the valid output.

4.3 The Algorithm CylindricalDecompose

Calling sequence. CylindricalDecompose(F, n)

Input. F, a finite subset of $\mathbf{k}[y_1 < \cdots < y_n]$.

Output. an F-invariant cylindrical decomposition of $\mathbf{K}^n$.

Step (1)**:** If $n > 1$, go to step (2). Otherwise let $\{p_1, \ldots, p_r\}$, $r \geq 0$, be the set of irreducible divisors of non-constant elements of F. If $r = 0$, set $\mathcal{D} = \mathbf{K}$ and exit. Otherwise set

$$D_i = \{y_1 \in \mathbf{K} \mid p_i(y_1) = 0\}, 1 \leq i \leq r,$$

and $D_{r+1} = \{y_1 \in \mathbf{K} \mid p_1(y_1) \cdots p_r(y_1) \neq 0\}$. Clearly $\mathcal{D} = \{D_i \mid 1 \leq i \leq r+1\}$ is an F-invariant cylindrical decomposition of $\mathbf{K}$.

Step (2)**:** Let $\mathcal{R}$ be the output of InitialPartition(F, n).

Step (3)**:** Call algorithm MakeCylindrical$(\mathcal{R}, n)$, to compute a cylindrical decomposition $\mathcal{D}$ of $\mathbf{K}^n$ such that the zero set of each regular system in $\mathcal{R}$ is a union of some cells in $\mathcal{D}$. Clearly, $\mathcal{D}$ is an intersection-free basis of the set $\{Z(rs) \mid rs \in \mathcal{R}\}$, which implies $\mathcal{D}$ is an intersection-free basis of the $s+1$ constructible sets $V(f_1), \ldots, V(f_s)$ and $\{y \in \mathbf{K}^n \mid \left(\prod_{i=1}^{s} f_i(y)\right) \neq 0\}$. Therefore, $\mathcal{D}$ is an F-invariant cylindrical decomposition of $\mathbf{K}^n$.

5. CYLINDRICAL ALGEBRAIC DECOMPOSITION

In this section, we show how to compute a CAD of $\mathbb{R}^n$ from a cylindrical decomposition of $\mathbb{C}^n$. This section starts with reviewing basic notions for CAD [1]. A theorem (Theorem 1) due to Collins [11] is then reviewed, where the relation between complex and real roots of a polynomial with real coefficients is shown. The bridge from cylindrical decomposition to CAD is built in Corollary 1, which can be directly obtained from Collins' theorem. The main algorithm CAD and its subroutines are stated in four subsections.

A *semi-algebraic set* [4] of $\mathbb{R}^n$ is a subset of $\mathbb{R}^n$ which can be written as a finite union of sets of the form:

$$\{y \in \mathbb{R}^n \mid \forall f \in F, f(y) = 0 \text{ and } \forall g \in G, g(y) > 0\},$$

where both F and G are finite subsets of the polynomial ring $\mathbb{R}[y_1, \ldots, y_n]$.

Given an n-dimensional real space $\mathbb{R}^n$, a nonempty connected subset of $\mathbb{R}^n$ is called a *region*. For any subset S of $\mathbb{R}^n$, a *decomposition* of S is a finite collection of disjoint regions whose union is S. For a region R, the *cylinder* over R, written $Z(R)$, is $R \times \mathbb{R}^1$. Let $f_1 < \cdots < f_r, r \geq 0$ be continuous, real-valued functions defined on R. Let $f_0 = -\infty$ and $f_{r+1} = +\infty$. For any f_i, $1 \leq i \leq r$, we call the set of points $\{(a, f_i(a)) \mid a \in R\}$ the f_i*-section* of $Z(R)$. For any two functions f_i, f_{i+1}, $0 \leq i \leq r$, the set of points (a, b), where a ranges over R and $f_i(a) < b < f_{i+1}(a)$, is called the (f_i, f_{i+1})*-sector* of $Z(R)$. All the sections and sectors of $Z(R)$ can be ordered as

$$(f_0, f_1) < f_1 < \cdots < f_r < (f_r, f_{r+1}).$$

Clearly they form a decomposition of $Z(R)$, which is called a *stack* over R.

A decomposition $\mathcal{E}$ of $\mathbb{R}^n$ is *cylindrical* if either (1) $n = 1$ and $\mathcal{E}$ is a stack over $\mathbb{R}^0$, or (2) $n > 1$, and there is a cylindrical decomposition $\mathcal{E}'$ of $\mathbb{R}^{n-1}$ such that for each region R in $\mathcal{E}'$, some subset of $\mathcal{E}$ is a stack over R. Moreover, We say that $\mathcal{E}$ induces $\mathcal{E}'$. A decomposition is *algebraic* if each of its regions is a semi-algebraic set. A *cylindrical algebraic decomposition* of $\mathbb{R}^n$ is a decomposition which is both cylindrical and algebraic.

Let p be a polynomial of $\mathbb{R}[y_1, \ldots, y_n]$, and let S be a subset of $\mathbb{R}^n$. The polynomial p is *invariant* on S (and S is p-invariant), if the sign of $p(\alpha)$ does not change when α ranges over S. Let $F \subset \mathbb{R}[y_1, \ldots, y_n]$ be a finite polynomial set. We say S is F-invariant if each $p \in F$ is invariant on S. A cylindrical algebraic decomposition $\mathcal{E}$ is F-invariant if F is invariant on each region of $\mathcal{E}$.

Let p be a polynomial of $\mathbb{R}[y_1, \ldots, y_n]$, and let R be a region in $\mathbb{R}^{n-1}$. p is *delineable* on R if the real zeros of p define continuous real-valued functions $\theta_1, \ldots, \theta_s$ such that, for all $\alpha \in R$, $\theta_1(\alpha) < \cdots < \theta_s(\alpha)$, and for each θ_i there is an integer m_i such that m_i is the multiplicity of the root $\theta_i(\alpha)$ of $p(\alpha, y_n)$. Note that if $k = 0$, $V(p)$ has no intersection with $Z(R)$. Clearly when p is delineable on R, its real zeros naturally determine a stack over R.

Let $\mathcal{E}$ be a CAD of $\mathbb{R}^n$. As suggested in [1], each region $e \in \mathcal{E}$ can be represented by a pair (I, S), where I is the *index* of e and S is a *sample point* for e. The index I and the sample point S of e are defined as follows. If $n = 1$, let

$$e_1 < e_2 < \cdots < e_{2m} < e_{2m+1}, m \geq 0$$

be the elements of $\mathcal{E}$. For each e_i, the index of e_i is defined as (i). For each e_i, its sample point is any algebraic point belonging to e_i. Let $\mathcal{E}'$ be the CAD of $\mathbb{R}^{n-1}$ induced by $\mathcal{E}$. Suppose that region indices and sample points have been defined for $\mathcal{E}'$. Let

$$e_{i,1} < e_{i,2} < \cdots < e_{i,2m_i} < e_{i,2m_i+1}, m_i \geq 0$$

be the elements of $\mathcal{E}$ which form a stack over the region e_i of $\mathcal{E}'$. Let $(i_1, \ldots, i_{n-1})$ be the index of e_i. Then the index of $e_{i,j}$ is defined as $(i_1, \ldots, i_{n-1}, j)$. Let S' be a sample point of e_i. Then the sample point of $e_{i,j}$ is an algebraic point belonging to $e_{i,j}$ such that its first $n-1$ coordinates are the same as that of S'.

Theorem 1 (Collins). *Let p be a polynomial of ring $\mathbb{R}[y_1 < \cdots < y_n]$ and R be a region of $\mathbb{R}^{n-1}$. If $init(p) \neq 0$ on R and the number of distinct complex roots of p is invariant on R, then p is delineable on R.*

Corollary 1. *Let $F = \{p_1, \ldots, p_r\}$ be a finite set of polynomials in $\mathbb{R}[y_1 < \cdots < y_n]$ of level n. Let R be a region of $\mathbb{R}^{n-1}$. Assume that for every $\alpha \in R$, (1) the initial of each p_i does not vanish at α; (2) all $p_i(\alpha, y_n)$, $1 \leq i \leq r$, as polynomials of $\mathbb{R}[y_n]$, are squarefree and coprime. Then each p_i is delineable on R and the sections of $Z(R)$ belonging to different p_i and p_j are disjoint.*

Let R and F be defined as in the above corollary. Then clearly the real roots of all $p \in F$ are continuous functions on R and they together determine a stack over R. The algorithm GenerateStack, described in Section 5.2, is a direct application of the above corollary.

5.1 Real Root Isolation

Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ be an algebraic point of $\mathbb{R}^n$. Each α_i as an algebraic number is a zero of a nonconstant squarefree polynomial $t_i(y_i)$ of $\mathbb{Q}[y_i]$. Let T be the set of all $t_i(y_i)$. Clearly T is a zero dimensional squarefree regular chain of $\mathbb{Q}[\mathbf{y}]$. On the other hand, if T is a zero-dimensional regular chain of $\mathbb{Q}[\mathbf{y}]$, any real zero of T is an algebraic point of $\mathbb{R}^n$. Therefore any algebraic point α of $\mathbb{R}^n$ can be represented by a pair (T, L), where T is a zero-dimensional squarefree regular chain of $\mathbb{Q}[\mathbf{y}]$ such that $T(\alpha) = 0$ and L is an isolating cube containing α but not other zeros of T. The pair (T, L) is called a *regular chain representation* of α, which will be used to represent a sample point of CAD.

Next we provide the specification of an algorithm called IsolateZeros for isolating real zeros of univariate polynomials with real algebraic number coefficients. It is a subroutine of the algorithm NREALZERO proposed in [34] for isolating the real roots of a zero-dimensional regular chain.

Calling sequence. IsolateZeros$(\alpha^{(n-1)}, F, n)$

Input. $\alpha^{(n-1)}$ is a point of $\mathbb{R}^{n-1}$, $n \geq 1$, with a regular chain representation (T', L'). If $n = 1$, $T' = \varnothing$ and $L' = \varnothing$. $F = \{p_1, \ldots, p_r\}$ is a list of non-constant polynomials of $\mathbb{Q}[y_1, \cdots, y_n]$ of level n satisfying that (1) for $p_i \in F$, $T' \cup \{p_i\}$ is a squarefree regular chain of $\mathbb{Q}[y_1, \ldots, y_n]$; (2) all $p_i(\alpha^{(n-1)}, y_n)$, $1 \leq i \leq r$, as polynomials of $\mathbb{R}[y_n]$, are squarefree and coprime.

Output. A pair (N, ν). Let $p = \prod_{i=1}^{r} p_i$. $N = (N_1, \ldots, N_m)$ is a list of intervals with rational endpoints with $N_1 < \cdots < N_m$ such that each N_j contains exactly one real zero of $p(\alpha^{(n-1)}, y_n)$. $\nu = (\nu_1, \ldots, \nu_m)$ is list of integers, where $1 \leq \nu_i \leq r$, such that the zero of $p(\alpha^{(n-1)}, y_n)$ in N_j is a zero of $p_{\nu_j}(\alpha^{(n-1)}, y_n)$.

5.2 The Algorithm GenerateStack

Calling sequence. GenerateStack(e', F, n)

Input. e' is a region of a CAD $\mathcal{E}'$ of $\mathbb{R}^{n-1}$, $n \geq 1$, and e' is represented by its index I' and its sample point S'. Let (T', L') be the regular chain representation of S'. If $n = 1$, $I', T', L' = \varnothing$. F is a finite set of polynomials in $\mathbb{Q}[y_1, \ldots, y_n]$ of level n. The region e' and the polynomial set F satisfy the conditions specified in Corollary 1.

Output. A stack $\mathcal{S}$ over e'.

Step (1). If $F = \varnothing$, go to step (2). Otherwise call algorithm IsolateZeros(S', F, n) to isolate the real roots of polynomials in F w.r.t y_n at the sample point S' of e'. Let (N, ν) be the output. If $N \neq \varnothing$, go to step (3).

Step (2). Let $I = (I', 1)$. Let $T = T' \cup \{y_n\}$, $L = L' \times [0, 0]$, $S = (T, L)$ and return $\mathcal{S} = ((I, S))$.

Step (3). Let $N_1 = [a_1, b_1], \ldots, N_m = [a_m, b_m]$, $m > 0$ be the elements of N. For $1 \leq i \leq 2m+1$, set $I_i = (I', i)$. Let s_1 be the greatest integer less than a_1. Let s_{2m+1} be the smallest integer greater than b_m. For $1 \leq i \leq m-1$, let $s_{2i+1} = \frac{b_i + a_{i+1}}{2}$. For $0 \leq i \leq m$, Let $T_{2i+1} = T' \cup \{y_n - s_{2i+1}\}$, $L_{2i+1} = L' \times [s_{2i+1}, s_{2i+1}]$ and set $S_{2i+1} = (T_{2i+1}, L_{2i+1})$. For $1 \leq i \leq m$, let $T_{2i} = T' \cup p_{\nu_i}$, $L_{2i} = L' \times N_i$ and set $S_{2i} = (T_{2i}, L_{2i})$. Finally, set $\mathcal{S}$ be the list of all (I_i, S_i), $1 \leq i \leq 2m+1$. Then $\mathcal{S}$ is the stack over e'.

5.3 The Algorithm MakeSemiAlgebraic

Calling sequence. MakeSemiAlgebraic$(\mathcal{D}, n)$

Input. $\mathcal{D}$ is a cylindrical decomposition of $\mathbb{C}^n$, $n \geq 1$.

Output. A CAD $\mathcal{E}$ of $\mathbb{R}^n$ such that, for each element D of $\mathcal{D}$, the set $D \cap \mathbb{R}^n$ is a union of some regions in $\mathcal{E}$.

Step (1). If $n > 1$ go to (2). Otherwise let $D_1, \ldots, D_r, D_{r+1}$, $r \geq 0$ be the elements of $\mathcal{D}$. For each $1 \leq i \leq r$, let p_i be the polynomial such that $D_i = \{y_1 \mid p_i(y_1) = 0\}$. Let $\mathcal{E}$ be the output of GenerateStack$(\varnothing, \{p_1, \ldots, p_r\}, 1)$. Clearly $\mathcal{E}$ is a CAD of $\mathbb{R}^1$.

Step (2). Let $\mathcal{D}'$ be the cylindrical decomposition of $\mathbb{C}^{n-1}$ induced by $\mathcal{D}$. Call MakeSemiAlgebraic recursively to compute a CAD $\mathcal{E}'$ of $\mathbb{R}^{n-1}$.

Step (3). In this step we lift the CAD $\mathcal{E}'$ of $\mathbb{R}^{n-1}$ to $\mathcal{E}$. Initialize $\mathcal{E} = (\ )$. For each region e' of $\mathcal{E}'$, let D' be the cell of $\mathcal{D}'$ such that $e' \subset D' \cap \mathbb{R}^n$. Let $D_1, \ldots, D_r, D_{r+1}$, $r \geq 0$ be the cells of $\mathcal{D}$ such that $D' \times \mathbb{C} = \cup_{j=1}^{r+1} D_j$. For each $1 \leq j \leq r$, let p_j be the polynomial such that $D_j = \{(\alpha, y_n) \mid \alpha \in D' \ \&\ p_j(\alpha, y_n) = 0\}$. Add output of GenerateStack$(e', \{p_1, \ldots, p_r\}, n)$ into $\mathcal{E}$. Clearly $\mathcal{E}$ is a CAD of $\mathbb{R}^n$ and for each $D \in \mathcal{D}$, the set $D \cap \mathbb{R}^n$ is a union of some regions in $\mathcal{E}$.

5.4 The Algorithm CAD

Calling sequence. $\mathsf{CAD}(F, n)$

Input. F is a finite subset of $\mathbb{Q}[y_1 < \cdots < y_n]$, $n \geq 1$.

Output. An F-invariant CAD $\mathcal{E}$ of $\mathbb{R}^n$.

Step (1). Let $\mathcal{D} = \mathsf{CylindricalDecompose}(F, n)$ be an F-invariant cylindrical decomposition of $\mathbb{C}^n$.

Step (2). Call algorithm MakeSemiAlgebraic to compute a CAD $\mathcal{E}$ of $\mathbb{R}^n$ such that, for each element D of $\mathcal{D}$, the set $D \cap \mathbb{R}^n$ is a union of some regions in $\mathcal{E}$. Since $\mathcal{D}$ is an intersection-free basis of the $s+1$ constructible sets $V_{\mathbb{C}}(f_1), \ldots, V_{\mathbb{C}}(f_s)$ and $\{y \in \mathbb{C}^n \mid \left(\prod_{i=1}^s f_i(y)\right) \neq 0\}$, $\mathcal{E}$ is an intersection-free basis of the $s+1$ semi-algebraic sets $V_{\mathbb{R}}(f_1), \ldots, V_{\mathbb{R}}(f_s)$ and $\{y \in \mathbb{R}^n \mid \left(\prod_{i=1}^s f_i(y)\right) \neq 0\}$. Note that each element in $\mathcal{E}$ is connected. Therefore $\mathcal{E}$ is an F-invariant cylindrical algebraic decomposition of $\mathbb{R}^n$.

6. EXAMPLES AND EXPERIMENTATION

6.1 An Example

Let us illustrate our method by a simple and classical example. Consider the parametric parabola $p = ax^2 + bx + c$. Set the order of variables as $x > c > b > a$. The first step InitialPartition generates four regular systems, whose zero sets form a partition of $\mathbb{C}^4$.

$$r_1 := \begin{cases} c &= 0 \\ b &= 0 \\ a &= 0 \end{cases}, \quad r_2 := \begin{cases} bx + c &= 0 \\ b &\neq 0 \\ a &= 0 \end{cases},$$

$$r_3 := \begin{cases} ax^2 + bx + c &= 0 \\ a &\neq 0 \end{cases}, \quad r_4 := \left\{ \ ax^2 + bx + c \neq 0 \right. .$$

Next we trace the algorithm MakeCylindrical. Initialize the sets $\mathcal{R}_1 := \{r_2, r_3\}$, $\mathcal{R}_2 := \{r_4\}$ and $\mathcal{R}_3 := \{r_1\}$. Since x appears in the equations of r_2 and r_3, $\mathsf{SeparateZeros}(\mathcal{R}_1)$ is called to obtain a family of pairs

$$\{(C_1, \{t\}), (C_2, \{p\}), (C_3, \{q\})\},$$

defined as follows, which separates $Z(r_2) \cup Z(r_3)$.

$$\begin{array}{lcl} C_1 : \{a = 0, b \neq 0\} & \to & \{t\} : \{bx + c\} \\ C_2 : \{a(4ac - b^2) \neq 0\} & \to & \{p\} : \{ax^2 + bx + c\} \\ C_3 : \{4ac - b^2 = 0, a \neq 0\} & \to & \{q\} : \{2ax + b\} \end{array}$$

The projection of $Z(r_4)$ is the values such that a, b, c do not vanish simultaneously, denoted by C_4. The projection of $Z(r_1)$ is the set $\{a = b = c = 0\}$, denoted by C_5.

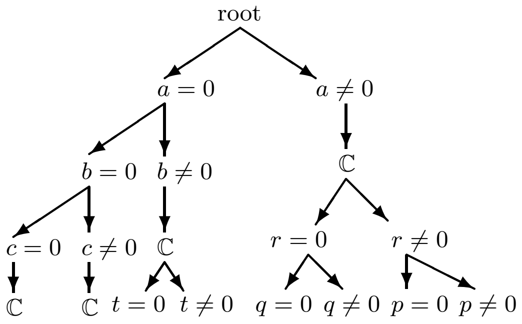
Note that C_1, C_2, C_3 are all subsets of C_4. In the **Merging** step, by calling SMPD, we get another set $C_6 := \{a = b = 0, c \neq 0\}$ such that C_1, C_2, C_3, C_5 and C_6 are pairwise disjoint and their union is $\mathbb{C}^3$. Moreover, for each C_i, there is a family of polynomials and indices associated to it.

C_1	C_2	C_3	C_5	C_6
$\{t\}$	$\{p\}$	$\{q\}$	$\varnothing$	$\varnothing$
$\{1,2\}$	$\{1,2\}$	$\{1,2\}$	$\{3\}$	$\{2\}$

Since each C_i is already the zero set of some regular system,

$$\mathsf{MakeCylindrical}(\{C_1, C_2, C_3, C_5, C_6\}, 3)$$

is called recursively to compute a cylindrical decomposition of $\mathbb{C}^3$. By the **Lifting** step, we finally obtain a p-invariant cylindrical decomposition of $\mathbb{C}^4$. Let $r = 4ac - b^2$, the decomposition can be described by the following tree.



To compute a p-invariant CAD of $\mathbb{R}^4$ from the above tree is straightforward. Starting from the root, one first obtains the trivial zero 0 of a, which decomposes $a \neq 0$ into two connected cells $a < 0$ and $a > 0$. The real line is thus divided into three parts. For each part, one then substitutes its sample point into its children which are equations, from where one can determine the sample points for the children which are inequations. Continuing in this manner, one finally obtains a CAD of $\mathbb{R}^4$ with 27 cells. The number of cells is the same as that obtained in [6]. In fact, it is the minimal number of cells one can obtain for a p-invariant CAD of $\mathbb{R}^4$.

6.2 Experimental Results

In this section, we present experimental results obtained with an implementation of the algorithms presented in this paper. Our code is in MAPLE 12 running on a computer with Intel Core 2 Quad CPU (2.40GHz) and 3.0GB total memory. The test examples, listed in appendix for the reader's convenience, are taken from diverse papers [16, 1, 13, 25, 6, 14, 12] on CAD. The time-out for a test run is set to 2 hours.

In Table 1, we show the total computation time of CAD and the time spent on three main phases of it, which are InitialPartition (Partition for short), MakeCylindrical (M.C. for short) and MakeSemiAlgebraic (M.S.A. for short). We also report the number of elements ($N_{\mathbb{R}}$) in the CAD. Aborted computations due to time-out are marked with "-". From the table, one can see that, except examples 14 and 16, the steps of the algorithm dedicated to computations in complex space dominate the step taking place in the real space.

In Table 2, we show the total computation time of the algorithm CylindricalDecompose (C.D. for short) and the time spent on three main operations of it, which are respectively SeparateZeros(Separate for short), MPD and SMPD. We can see that the cost of algorithm CylindricalDecompose is dominated by SMPD. The number of elements ($N_{\mathbb{C}}$) in the cylindrical decomposition of $\mathbb{C}^n$ is also reported.

The data reported in two tables shows that SMPD is the dominant operation, which computes intensively GCDs of polynomials modulo regular chains. This suggests that the modular methods and efficient implementation techniques in [15, 24, 22] (use of FFT-based polynomial arithmetic, ...) have a large potential for improving the implementation of our CAD algorithm.

Sys	Partition	M.C.	M.S.A.	Total	$N_{\mathbb{R}}$
1	0.024	0.096	0.024	0.144	27
2	1.184	2.856	1.048	5.088	895
3	0.004	7.512	0.704	8.220	233
4	0.264	1.368	1.080	2.716	421
5	0.016	0.052	0.116	0.184	55
6	0.108	0.156	0.120	0.384	41
7	2.704	3.600	1.360	7.664	893
8	0.380	1.608	1.196	3.184	365
9	0.288	0.532	0.264	1.084	209
10	5.668	48.079	18.833	72.640	3677
11	0.252	1.192	0.620	2.068	563
12	2.664	135.028	88.142	225.862	20143
13	10.576	35.846	6.905	53.335	4949
14	5.728	71.760	2520.354	2597.878	27547
15	690.731	2513.817	299.250	3503.954	66675
16	895.435	2064.469	-	-	-
17	0.052	-	-	-	-
18	-	-	-	-	-

Table 1 Timing (s) and number of cells for CAD

Sys	Separate	MPD	SMPD	Total	$N_{\mathbb{C}}$
1	0.020	0.012	0.084	0.156	8
2	0.508	0.252	2.268	4.052	63
3	3.856	0.836	2.460	7.880	24
4	0.280	0.088	1.036	1.648	65
5	0.032	0.008	0.012	0.064	7
6	0.036	0.012	0.092	0.268	13
7	1.100	0.652	2.416	6.320	58
8	0.536	0.144	1.040	2.008	55
9	0.120	0.032	0.384	0.816	26
10	3.204	0.756	49.031	54.119	594
11	0.128	0.032	0.960	1.416	49
12	8.508	2.024	125.104	138.188	856
13	2.040	1.784	42.578	47.002	407
14	5.741	2.092	64.875	76.956	983
15	83.469	62.736	3066.071	3232.073	2974
16	66.516	377.664	2501.947	2959.904	5877

Table 2 Timing (s) and number of cells for C.D.

7. CONCLUSION

We have presented a new approach for computing cylindrical algebraic decompositions. Our main motivation is to understand the relations between CADs and triangular decompositions, studying how the efficient techniques developed for the latter ones can benefit to the former ones.

Our method can be applied for solving QE problems directly. However, to solve practical problems efficiently, our method needs to be equipped with existing techniques, like partially built CADs, for utilizing the specific feature of input problems. Such issues will be addressed in a future paper.

8. REFERENCES

[1] D. S. Arnon, G. E. Collins, and S. McCallum. Cylindrical algebraic decomposition I: the basic algorithm. *SIAM J. Comput.*, 13(4):865–877, 1984.

[2] D. S. Arnon, G. E. Collins, and S. McCallum. Cylindrical algebraic decomposition II: an adjacency algorithm for the plane. *SIAM J. Comput.*, 13(4):878–889, 1984.

[3] P. Aubry, D. Lazard, and M. Moreno Maza. On the theories of triangular sets. *J. Symb. Comp.*, 28(1-2):105–124, 1999.

[4] S. Basu, R. Pollack, and M. F. Roy. *Algorithms in real algebraic geometry*, volume 10 of *Algorithms and Computations in Mathematics*. Springer-Verlag, 2006.

[5] F. Boulier, F. Lemaire, and M. Moreno Maza. Well known theorems on triangular systems and the D5 principle. In *Proc. of* Transgressive Computing 2006, Granada, Spain, 2006.

[6] C. W. Brown. Improved projection for cylindrical algebraic decomposition. *J. Symb. Comput.*, 32(5):447–465, 2001.

[7] C. W. Brown. Simple cad construction and its applications. *J. Symb. Comput.*, 31(5):521–547, 2001.

[8] C. W. Brown and J. H. Davenport. The complexity of quantifier elimination and cylinrical algebraic decomposition. In *Proc. ISSAC'07*, pages 54–60.

[9] C. Chen, O. Golubitsky, F. Lemaire, M. Moreno Maza, and W. Pan. *Comprehensive Triangular Decomposition*, volume 4770 of *Lecture Notes in Computer Science*, pages 73–101. 2007.

[10] J. S. Cheng, X. S. Gao, and C. K. Yap. Complete numerical isolation of real zeros in zero-dimensional triangular systems. In *ISSAC*, pages 92–99, 2007.

[11] G. E. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decomposition. *Springer Lecture Notes in Computer Science*, 33:515–532, 1975.

[12] G. E. Collins. Quantifier elimination by cylindrical algebraic decomposition–twenty years of progress. In B. Caviness and J. Johnson, editors, *Quantifier Elimination and Cylindical Algebraic Decomposition, Texts and Mongraphs in Symbolic Computation*, pages 8–23. Springer, 1998.

[13] G. E. Collins and H. Hong. Partial cylindrical algebraic decomposition. *Journal of Symbolic Computation*, 12(3):299–328, 1991.

[14] G. E. Collins, J. R. Johnson, and W. Krandick. Interval arithmetic in cylindrical algebraic decomposition. *J. Symb. Comput.*, 34(2):145–157, 2002.

[15] X. Dahan, M. Moreno Maza, É. Schost, W. Wu, and Y. Xie. Lifting techniques for triangular decompositions. In *ISSAC'05*, pages 108–115, 2005.

[16] A. Dolzmann, A. Seidl, and T. Sturm. Efficient projection orders for cad. In *Proc. ISSAC '04*, pages 111–118. ACM, 2004.

[17] A. Dolzmann, T. Sturm, and V. Weispfenning. Real quantifier elimination in practice. In *Algorithmic Algebra and Number Theory*, pages 221–247, 1998.

[18] H. Hong. An improvement of the projection operator in cylindrical algebraic decomposition. In *ISSAC '90*, pages 261–264. ACM, 1990.

[19] H. Hong. Simple solution formula construction in cylindrical algebraic decomposition based quantifier elimination. In *ISSAC '92*, pages 177–188. ACM, 1992.

[20] É. Hubert. Notes on triangular sets and triangulation-decomposition algorithms. I. Polynomial systems. In *Symbolic and numerical scientific computation (Hagenberg, 2001)*, volume 2630 of *LNCS*, pages 1–39. Springer, 2003.

[21] F. Lemaire, M. Moreno Maza, and Y. Xie. The `RegularChains` library. In Ilias S. Kotsireas, editor, Maple Conference 2005, pages 355–368, 2005.

[22] X. Li, M. Moreno Maza, and W. Pan. Computations modulo regular chains, 2009. Submitted to ISSAC'09.

[23] X. Li, M. Moreno Maza, R. Rasheed, and É. Schost. The Modpn library: Bringing fast polynomial arithmetic into Maple. In *MICA'08*, 2008.

[24] X. Li, M. Moreno Maza, and É. Schost. Fast arithmetic for triangular sets: From theory to practice. In *ISSAC'07*, pages 269–276. ACM, 2007.

[25] S. McCallum. An improved projection operation for cylindrical algebraic decomposition of 3-dimensional space. *J. Symb. Comput.*, 5(1-2):141–161, 1988.

[26] S. McCallum. Solving polynomial strict inequalities using cylindrical algebraic decomposition. *The Computer Journal*, 36(5):432–438, 1993.

[27] S. McCallum. An improved projection operator for cylindrical algebraic decomposition. In B. Caviness and J. Johnson, editors, *Quantifier Elimination and Cylindical Algebraic Decomposition, Texts and Mongraphs in Symbolic Computation*. Springer, 1998.

[28] M. Moreno Maza. On triangular decompositions of algebraic varieties. Technical Report TR 4/99, NAG Ltd, Oxford, UK, 1999. Presented at the MEGA-2000 Conference, Bath, England.

[29] A. Strzeboński. Solving systems of strict polynomial inequalities. *J. Symb. Comput.*, 29(3):471–480, 2000.

[30] D. M. Wang. *Elimination Methods*. Springer, Wein, New York, 2000.

[31] V. Weispfenning. A new approach to quantifier elimination for real algebra, in quantifier elimination and cylindrical algebraic decomposition. In B. Caviness and J. Johnson, editors, *Quantifier Elimination and Cylindical Algebraic Decomposition, Texts and Mongraphs in Symbolic Computation*, pages 376–392. Springer, 1998.

[32] W. T. Wu. A zero structure theorem for polynomial equations solving. *MM Research Preprints*, 1:2–12, 1987.

[33] B. Xia and L. Yang. An algorithm for isolating the real solutions of semi-algebraic systems. *J. Symb. Comput.*, 34(5):461–477, 2002.

[34] B. Xia and T. Zhang. Real solution isolation using interval arithmetic. *Comput. Math. Appl.*, 52(6-7):853–860, 2006.

[35] L. Yang, X. Hou, and B. Xia. A complete algorithm for automated discovering of a class of inequality-type theorems. *Science in China, Series* **F**, 44(6):33–49, 2001.

APPENDIX

1. Parametric parabola
$\{ax^2 + bx + c\}, x > c > b > a.$

2. Whitney umbrella
$\{x - uv, y - v, z - u^2\}, v > u > z > y > x.$

3. Quartic
$\{x^4 + px^2 + qx + r\}, x > p > q > r.$

4. Sphere and catastrophe
$\{z^2 + y^2 + x^2 - 1, z^3 + xz + y\}, x > y > z.$

5. Arnon-84
$\{y^4 - 2y^3 + y^2 - 3x^2y + 2x^4\}, y > x.$

6. Arnon-84-2
$\{144y^2 + 96x^2y + 9x^4 + 105x^2 + 70x - 98,$
$xy^2 + 6xy + x^3 + 9x\}, y > x.$

7. A real implicitization problem
$\{x - uv, y - uv^2, z - u^2\}, v > u > z > y > x.$

8. Ball and circular cylinder
$\{x^2 + y^2 + z^2 - 1, x^2 + (y + z - 2)^2 - 1\}, z > y > x.$

9. Termination of term rewrite system
$\{x - r, y - r, x^2(1 + 2y)^2 - y^2(1 + 2x^2)\}, r > x > y.$

10. Collins and Johnson
$\{3a^2r + 3b^2 - 2ar - a^2 - b^2,$
$3a^2r + 3b^2r - 4ar + r - 2a^2 - 2b^2 + 2a,$
$a - 1/2, b, r, r - 1\}, r > a > b.$

11. Range of lower bounds
$\{a, az^2 + bz + c, ax^2 + bx + c - y\},$
$z > c > b > a > x > y.$

12. X-axis ellipse problem
$\{b^2(x - c)^2 + a^2y^2 - a^2b^2,$
$x^2 + y^2 - 1\}, y > x > b > c > a.$

13. Davenport and Heintz
$\{a - d, b - c, a - c, b - 1, a^2 - b\}, a > b > c > d.$

14. Hong-90
$\{r + s + t, rs + st + tr - a, rst - b\},$
$t > s > r > b > a.$

15. Solotareff-3
$\{r, r - 1, u + 1, u - v, v - 1,$
$3u^2 + 2ru - a, 3v^2 + 2rv - a,$
$u^3 + ru^2 - au + a - r - 1,$
$v^3 + rv^2 - av - 2b - a + r + 1\},$
$b > u > v > r > a.$

16. Collision problem
$\{\frac{17}{16}t - 6, \frac{17}{16}t - 10, x - \frac{17}{16}t + 1,$
$x - \frac{17}{16}t - 1, y - \frac{17}{16}t + 9, y - \frac{17}{16}t + 7,$
$(x - t)^2 + y^2 - 1\}, t > x > y.$

17. McCallum trivariate random polynomial
$\{(y - 1)z^4 + xz^3 + x(1 - y)z^2 + (y - x - 1)z + y\},$
$z > y > x.$

18. Ellipse problem
$\{b^2(x - c)^2 + a^2(y - d)^2 - a^2b^2, a, b, x^2 + y^2 - 1\},$
$y > x > d > c > b > a.$