Computing Cylindrical Algebraic Decomposition via Triangular Decomposition

Changbo Chen, Marc Moreno Maza, Bican Xia and Lu Yang

University of Western Ontario, Canada
Massachusetts Institute of Technology, USA
Peking University, China
East China Normal University, China

July 29, 2009

Background

Cylindrical algebraic decomposition (CAD) is a fundamental tool in real algebraic geometry. It was introduced by Collins in 1973 and has been followed by lots of improvements, like

- improved projection methods
  (McCallum 88, 98, Hong 90, Brown 01)
- partially built CADs
  (Collins and Hong 91, McCallum 93, Strzeboński 00)
- improved stack construction
  (Collins, Johnson and Krandick 02)
- efficient projection orders
  (Dolzmann, Seidl and Sturm 04)
- ...

Motivation

1. Understand the relations and possible interactions between CAD and triangular decompositions of polynomial systems.

Motivation

1. Understand the relations and possible interactions between CAD and triangular decompositions of polynomial systems.

2. Investigate the possibility of improving the practical efficiency of CAD implementation by means of modular methods and fast polynomial arithmetic, being developed for triangular decompositions.

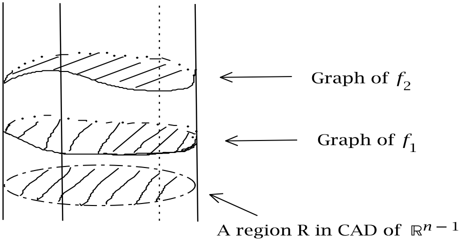
Cylindrical Algebraic Decomposition (I)

A cylindrical algebraic decomposition of $\mathbb{R}^n$ can be defined inductively as follows.

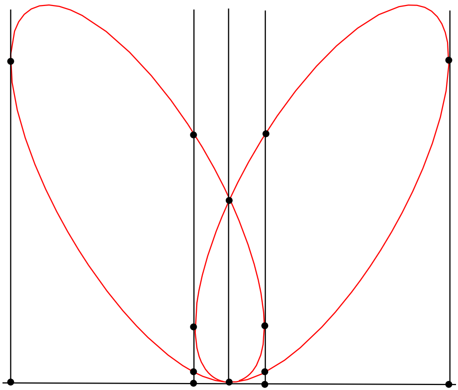
- $n = 1$. A CAD of $\mathbb{R}$ is a finite partition of the real line into points and open intervals.

Cylindrical Algebraic Decomposition (II)

- $n > 1$. Given a CAD D' of $\mathbb{R}^{n-1}$, one builds a CAD D of $\mathbb{R}^n$ as follows. Above each region R of D':
  - consider finitely many disjoint graphs (called *sections*) of continuous real-valued algebraic functions,
  - decomposing the cylinder $R \times \mathbb{R}^1$, into sections and *sectors* (located between two consecutive sections), which form a stack over R,
  - then all the sections and sectors are the elements of D.



A Cylindrical Algebraic Decomposition of $\mathbb{R}^2$ Induced by the Tacnode Curve



Tacnode curve: $y^4 - 2y^3 + y^2 - 3x^2y + 2x^4 = 0$.

Algorithm of Collins

Projection: Starting from the input $F_n \subset \mathbb{Q}[y_1, \ldots, y_n]$, repeatedly apply a projection operator to eliminate the variables one by one until a set of univariate polynomials are obtained

$$F_n \to F_{n-1} \to \cdots \to F_1$$

such that an F_k-invariant CAD of $\mathbb{R}^k$ can be constructed from an F_{k-1}-invariant CAD of $\mathbb{R}^{k-1}$, for $2 \leq k \leq n$.

Lifting: One isolates the real roots of polynomial in F_1 and deduces a CAD of $\mathbb{R}^1$. For each region of the CAD of $\mathbb{R}^1$, one evaluates the polynomials of F_2 at a *sample point* and isolates their real roots, from which one produces a stack over the region. Continuing in this manner, one finally obtains a CAD of $\mathbb{R}^n$.

Another View of CAD

A CAD of $\mathbb{R}^n$ is a partition of $\mathbb{R}^n$, where

- all the cells are cylindrically arranged, that is for all $1 \leq j < n$ the projections on the first j coordinates $(y_1, \ldots, y_j)$ of any two cells are either identical or disjoint.
- each cell is a connected semi-algebraic subset, called a region

For $F_n \subset \mathbb{Q}[y_1, \ldots, y_n]$, a CAD of $\mathbb{R}^n$ is F_n-invariant if above each region of it, the sign of each $f \in F_n$ is constant.

Our Method

F_n: a set of polynomials of $\mathbb{Q}[y_1, \ldots, y_n]$.

Initial Partition: we decompose $\mathbb{C}^n$ into disjoint constructible sets $C_1, \ldots, C_e$ such that 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 partition of $\mathbb{C}^n$ into disjoint constructible sets such that this second decomposition is cylindrical.

Make Semi-Algebraic: from the previous decomposition we produce an F_n-invariant CAD of $\mathbb{R}^n$ via real root isolation of zero-dimensional regular chains.

The Three Phases

$$F_n \subset \mathbb{Q}[y_1, \cdots, y_n]$$

$$\downarrow$$

$\boxed{\text{Initial Partition}}$

$$\downarrow$$

$\mathcal{C}$: a partition of $\mathbb{C}^n$ into constructible sets

$$\downarrow$$

$\boxed{\text{Make Cylindrical}}$

$$\downarrow$$

$\mathcal{D}$: a cylindrically arranged partition of $\mathbb{C}^n$ into constructible sets

$$\downarrow$$

$\boxed{\text{Make SemiAlgebraic}}$

$$\downarrow$$

An F_n-invariant CAD of $\mathbb{R}^n$

Representation of Constructible Sets

A pair $R = [T, h]$ is called a regular system if T is a regular chain, and h is a polynomial which is regular w.r.t $\mathrm{sat}(T)$.

Theorem (CGLMP, CASC2007)

Every constructible set can be written as a finite union of the zero sets of regular systems.

The constructible set

$$\left\{ \begin{array}{rcl} x(1+y)-s & = & 0 \\ y(1+x)-s & = & 0 \\ x+y-1 & \neq & 0 \end{array} \right. \tag{1}$$

can be represented by two regular systems

$$R_1 : \left| \begin{array}{l} T_1 = \left\{ \begin{array}{l} (y+1)x - s \\ y^2 + y - s \end{array} \right. \\ h_1 = y - 2s + 1 \end{array} \right. \qquad R_2 : \left| \begin{array}{l} T_2 = \left\{ \begin{array}{l} x+1 \\ y+1 \\ s \end{array} \right. \\ h_2 = 1 \end{array} \right.$$

Initial Partition

Let $F_n = \{f_1, \ldots, f_s\}$ be a finite subset of $\mathbb{Q}[y_1 < \cdots < y_n]$. We compute an intersection free basis of the $s+1$ sets $f_1 = 0, \ldots, f_s = 0$ and $f_1 \cdots f_s \neq 0$, where each element is represented a regular system and their sets from a partition of $\mathbb{C}^n$.

Consider the parametric parabola $p = ax^2 + bx + c$, where $x > c > b > a$. InitialPartition decomposes $\mathbb{C}^4$ into four pairwise disjoint sets, each of which is the zero set of a regular system.

$$r_1 := \left\{ \begin{array}{ccc} c & = & 0 \\ b & = & 0 \\ a & = & 0 \end{array} \right. , \quad r_2 := \left\{ \begin{array}{ccc} bx + c & = & 0 \\ b & \neq & 0 \\ a & = & 0 \end{array} \right. ,$$

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

The Three Phases

$$F_n \subset \mathbb{Q}[y_1, \cdots, y_n]$$

$$\downarrow$$

$$\boxed{\text{Initial Partition}}$$

$$\downarrow$$

$\mathcal{C}$: a partition of $\mathbb{C}^n$ into constructible sets

$$\downarrow$$

$$\boxed{\text{Make Cylindrical}}$$

$$\downarrow$$

$\mathcal{D}$: a cylindrically arranged partition of $\mathbb{C}^n$ into constructible sets

$$\downarrow$$

$$\boxed{\text{Make SemiAlgebraic}}$$

$$\downarrow$$

An F_n-invariant CAD of $\mathbb{R}^n$

Separate Zeros

Let $rs = [T, h]$ be a regular system of $\mathbb{Q}[y_1 < \cdots < y_n]$. We see $y_1, \ldots, y_{n-1}$ as parameters, denoted by $\mathbf{u}$, and regard rs as a parametric system in $\mathbf{u}$, that we solve via comprehensive triangular decomposition.

As a result, we obtain a partition of the projection onto the $\mathbf{u}$-space of $Zero(rs)$ such that, above each cell R of the partition, $Zero(rs)$ equals the union of the zero sets of some polynomials $p_1, \ldots, p_r \in \mathbb{R}[y_1, \ldots, y_n]$, where

- the initial of each p_j does not vanish on R,
- the p_j's are squarefree and pairwise coprime at any point of R.

For the regular system

$$r_3 := \begin{cases} ax^2 + bx + c & = & 0 \\ a & \neq & 0 \end{cases}$$

Calling SeparateZeros(r_3) will get

$$\begin{array}{lcl} \{a(4ac - b^2) \neq 0\} & \rightarrow & \{ax^2 + bx + c\} \\ \{4ac - b^2 = 0, a \neq 0\} & \rightarrow & \{2ax + b\} \end{array}$$

Make Cylindrical

By calling SeparateZeros recursively, MakeCylindrical produces a cylindrical decomposition of $\mathbb{C}^n$, defined inductively as folows.

Make Cylindrical

By calling SeparateZeros recursively, MakeCylindrical produces a cylindrical decomposition of $\mathbb{C}^n$, defined inductively as folows.

- $n = 1$. A cylindrical decomposition of $\mathbb{C}$ is either $\mathbb{C}$ itself or of the form $p_1 = 0, \cdots, p_r = 0$ and $p_1 \cdots p_r \neq 0$ where $p_1, \ldots, p_r$ are nonconstant coprime squarefree polynomials of $\mathbb{Q}[y_1]$.

Make Cylindrical

By calling SeparateZeros recursively, MakeCylindrical produces a cylindrical decomposition of $\mathbb{C}^n$, defined inductively as folows.

• $n = 1$. A cylindrical decomposition of $\mathbb{C}$ is either $\mathbb{C}$ itself or of the form $p_1 = 0, \cdots, p_r = 0$ and $p_1 \cdots p_r \neq 0$ where $p_1, \ldots, p_r$ are nonconstant coprime squarefree polynomials of $\mathbb{Q}[y_1]$.

• $n > 1$. Given a cylindrical decomposition $\mathcal{D}'$ of $\mathbb{C}^{n-1}$, one builds a cylindrical decomposition $\mathcal{D}$ of $\mathbb{C}^n$. For each cell D_i of $\mathbb{C}^{n-1}$:

Make Cylindrical

By calling SeparateZeros recursively, MakeCylindrical produces a cylindrical decomposition of $\mathbb{C}^n$, defined inductively as folows.

• $n = 1$. A cylindrical decomposition of $\mathbb{C}$ is either $\mathbb{C}$ itself or of the form $p_1 = 0, \cdots, p_r = 0$ and $p_1 \cdots p_r \neq 0$ where $p_1, \ldots, p_r$ are nonconstant coprime squarefree polynomials of $\mathbb{Q}[y_1]$.

• $n > 1$. Given a cylindrical decomposition $\mathcal{D}'$ of $\mathbb{C}^{n-1}$, one builds a cylindrical decomposition $\mathcal{D}$ of $\mathbb{C}^n$. For each cell D_i of $\mathbb{C}^{n-1}$:

- either $D_i \times \mathbb{C}$ is an element of $\mathcal{D}$, or

Make Cylindrical

By calling SeparateZeros recursively, MakeCylindrical produces a cylindrical decomposition of $\mathbb{C}^n$, defined inductively as folows.

• $n = 1$. A cylindrical decomposition of $\mathbb{C}$ is either $\mathbb{C}$ itself or of the form $p_1 = 0, \cdots, p_r = 0$ and $p_1 \cdots p_r \neq 0$ where $p_1, \ldots, p_r$ are nonconstant coprime squarefree polynomials of $\mathbb{Q}[y_1]$.

• $n > 1$. Given a cylindrical decomposition $\mathcal{D}'$ of $\mathbb{C}^{n-1}$, one builds a cylindrical decomposition $\mathcal{D}$ of $\mathbb{C}^n$. For each cell D_i of $\mathbb{C}^{n-1}$:

- either $D_i \times \mathbb{C}$ is an element of $\mathcal{D}$, or
- there exists $r_i > 0$ $p_{i,1}, \ldots, p_{i,r_i} \in \mathbb{R}[y_1, \ldots, y_n]$ such that

Make Cylindrical

By calling SeparateZeros recursively, MakeCylindrical produces a cylindrical decomposition of $\mathbb{C}^n$, defined inductively as folows.

- $n = 1$. A cylindrical decomposition of $\mathbb{C}$ is either $\mathbb{C}$ itself or of the form $p_1 = 0, \cdots, p_r = 0$ and $p_1 \cdots p_r \neq 0$ where $p_1, \ldots, p_r$ are nonconstant coprime squarefree polynomials of $\mathbb{Q}[y_1]$.
- $n > 1$. Given a cylindrical decomposition $\mathcal{D}'$ of $\mathbb{C}^{n-1}$, one builds a cylindrical decomposition $\mathcal{D}$ of $\mathbb{C}^n$. For each cell D_i of $\mathbb{C}^{n-1}$:
  - either $D_i \times \mathbb{C}$ is an element of $\mathcal{D}$, or
  - there exists $r_i > 0$ $p_{i,1}, \ldots, p_{i,r_i} \in \mathbb{R}[y_1, \ldots, y_n]$ such that
    - the initial of each p_j does not vanish on D_i and,

Make Cylindrical

By calling SeparateZeros recursively, MakeCylindrical produces a cylindrical decomposition of $\mathbb{C}^n$, defined inductively as folows.

• $n = 1$. A cylindrical decomposition of $\mathbb{C}$ is either $\mathbb{C}$ itself or of the form $p_1 = 0, \cdots, p_r = 0$ and $p_1 \cdots p_r \neq 0$ where $p_1, \ldots, p_r$ are nonconstant coprime squarefree polynomials of $\mathbb{Q}[y_1]$.

• $n > 1$. Given a cylindrical decomposition $\mathcal{D}'$ of $\mathbb{C}^{n-1}$, one builds a cylindrical decomposition $\mathcal{D}$ of $\mathbb{C}^n$. For each cell D_i of $\mathbb{C}^{n-1}$:

- either $D_i \times \mathbb{C}$ is an element of $\mathcal{D}$, or
- there exists $r_i > 0$ $p_{i,1}, \ldots, p_{i,r_i} \in \mathbb{R}[y_1, \ldots, y_n]$ such that
  - the initial of each p_j does not vanish on D_i and,
  - the p_j's are squarefree and pairwise coprime at all $\mathbf{u} \in D_i$,

Make Cylindrical

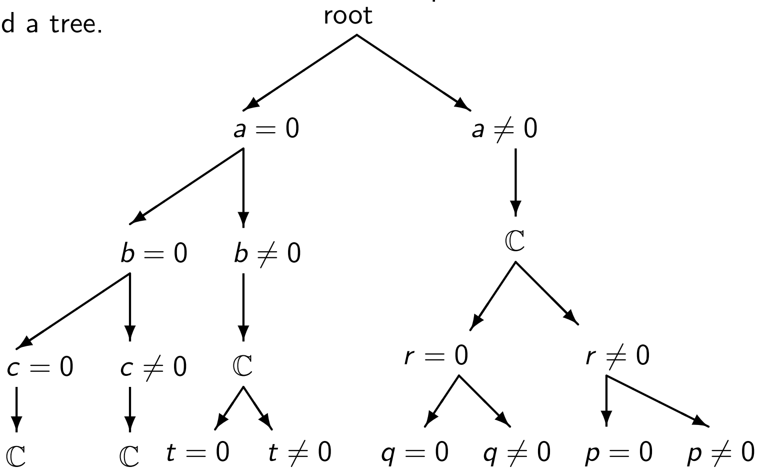
By calling SeparateZeros recursively, MakeCylindrical produces a cylindrical decomposition of $\mathbb{C}^n$, defined inductively as folows.

• $n = 1$. A cylindrical decomposition of $\mathbb{C}$ is either $\mathbb{C}$ itself or of the form $p_1 = 0, \cdots, p_r = 0$ and $p_1 \cdots p_r \neq 0$ where $p_1, \ldots, p_r$ are nonconstant coprime squarefree polynomials of $\mathbb{Q}[y_1]$.

• $n > 1$. Given a cylindrical decomposition $\mathcal{D}'$ of $\mathbb{C}^{n-1}$, one builds a cylindrical decomposition $\mathcal{D}$ of $\mathbb{C}^n$. For each cell D_i of $\mathbb{C}^{n-1}$:

- either $D_i \times \mathbb{C}$ is an element of $\mathcal{D}$, or
- there exists $r_i > 0$ $p_{i,1}, \ldots, p_{i,r_i} \in \mathbb{R}[y_1, \ldots, y_n]$ such that
  - the initial of each p_j does not vanish on D_i and,
  - the p_j's are squarefree and pairwise coprime at all $\mathbf{u} \in D_i$,
  - $D_i \times (p_1 = 0), \cdots, D_i \times (p_r = 0)$ and $D_i \times (p_1 \cdots p_r \neq 0)$ are in $\mathcal{D}$.

The algorithm MakeCylindrical takes r_1, r_2, r_3 and r_4 as input and outputs a cylindrical decomposition of $\mathbb{C}^4$. Let $t = bx + c$, $q = 2ax + b$, and $r = 4ac - b^2$, the decomposition can be described a tree.



The Three Phases

$$F_n \subset \mathbb{Q}[y_1, \cdots, y_n]$$

$$\downarrow$$

$$\boxed{\text{Initial Partition}}$$

$$\downarrow$$

$\mathcal{C}$: a partition of $\mathbb{C}^n$ into constructible sets

$$\downarrow$$

$$\boxed{\text{Make Cylindrical}}$$

$$\downarrow$$

$\mathcal{D}$: a cylindrically arranged partition of $\mathbb{C}^n$ into constructible sets

$$\downarrow$$

$$\boxed{\text{Make SemiAlgebraic}}$$

$$\downarrow$$

An F_n-invariant CAD of $\mathbb{R}^n$

Make SemiAlgebraic (I)

Theorem (Collins)

Let $p \in \mathbb{R}[y_1 < \cdots < y_n]$ *and* R *be a region of* $\mathbb{R}^{n-1}$*. If init*(p) *does not vanish* R *and the number of distinct complex roots of* p *is invariant on* R*, then* p *is* delineable *on* R*, that is,* $V(p)$ *is the union of finitely many disjoint graphs of continuous functions over* R*.*

Make SemiAlgebraic (II)

Corollary

Let $\{p_1, \ldots, p_r\} \subset \mathbb{R}[y_1 < \cdots < y_n]$ *and let* R *be a region of* $\mathbb{R}^{n-1}$. *Assume that for all* $\alpha \in R$*:*

- *each* $\mathrm{init}(p_j)$ *does not vanish at* α*;*
- *all* $p_j(\alpha, y_n)$*, as polynomials of* $\mathbb{R}[y_n]$*, are squarefree and coprime.*

Then each p_j *is delineable on* R *and any two sections of the cylinder over* R*, given by different* p_i *and* p_j*, are disjoint.*

By Collins' theorem and its corollary, one derives a CAD of $\mathbb{R}^n$ from a cylindrical decomposition of $\mathbb{C}^n$, by means real root isolation of zero-dimensional regular chains.

Maple Demo

Special thanks to James H. Davenport and John May for the piecewise construction.

Comparing with Collins' Algorithm

Consider the parametric parabola $p = ax^2 + bx + c$, where $x > c > b > a$.

- Our algorithm produces a p-invariant CAD of $\mathbb{R}^4$ with 27 cells, which is minimal.
- By Collins-Hong or McCallum projection operator, one produces the following polynomials during the projection phase:

  $$ax^2 + bx + c, b^2 - 4ac, c, b, a.$$

  In the lifting phase, one then obtains a CAD of $\mathbb{R}^4$ with 115 cells (Brown 01)!
- If Brown-McCallum projection operator is applied, one could also obtain a CAD of $\mathbb{R}^4$ with 27 cells (Brown 01). However, this projection operator may fail in some (rare) cases.

Sys	InitialPartition	MakeCylindrical	MakeSemiAlgebraic	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

Observation

- For most examples the steps of the algorithm dedicated to computations in complex space, where GCDs of polynomials modulo regular chains are computed intensively, dominate the step taking place in the real space.

- The data suggests that the modular methods and efficient implementation techniques being developed in `RegularChains` library have a large potential for improving our current implementation.

Conclusion

- We have introduced an intermediate concept, cylindrical decomposition of the complex space, from which a CAD of $\mathbb{R}^n$ can easily be extracted.
- W.r.t Collins-Hong projection operator, even for simple examples, our approaches tends to produce much less cells due to its case discussion feature.
- W.r.t Brown-McCallum projection operator, it can always generate a CAD while the Brown-McCallum projection operator may fail (rarely).

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-Catastrophe: $\{z^2 + y^2 + x^2 - 1, z^3 + xz + y\}, x > y > z$.
5. Tacnode curve: $\{y^4 - 2y^3 + y^2 - 3x^2y + 2x^4\}, y > x$.
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-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
$\{b^2(x-c)^2+a^2(y-d)^2-a^2b^2, a, b, x^2+y^2-1\},$
$y>x>d>c>b>a.$