Triangular decomposition of semi-algebraic systems

Presented by Marc Moreno Maza[1]
joint work with
Changbo Chen[1], James H. Davenport[2], John P. May[3],
Bican Xia[4], Rong Xiao[1]

[1]University of Western Ontario

[2]University of Bath (England)

[3]Maplesoft (Canada)

[4]Peking University (China)

Algebra Seminar
University of Western Ontario
February 4, 2011

Plan

Solving polynomial systems? What does this mean?

The algebra text book says:

For $F \subset \mathbf{k}[x_1, \ldots, x_n]$ this is simply

- a *primary decomposition* of $\langle F \rangle$ or
- the *irreducible decomposition* of $V(F)$ (the zero set of F in $\overline{\mathbf{k}}^n$).

The computer algebra system does well:

For $F \subset \mathbf{k}[x_1, \ldots, x_n]$, with $\mathbf{k} = \mathbb{Z}/p\mathbb{Z}$ or $\mathbf{k} = \mathbb{Q}$,

- computing a *Gröbner basis* of $\langle F \rangle$ or
- computing a *triangular decomposition* of $V(F)$.

But most scientists and engineers need:

- For $F \subset \mathbb{Q}[x_1, \ldots, x_n]$, a useful description of the points of $V(F)$ whose coordinates are real.
- For $F \subset \mathbb{Q}[u_1, \ldots, u_d][x_1, \ldots, x_n]$, the real $(x_1, \ldots, x_n)$-solutions as a function of the real parameter $(u_1, \ldots, u_d)$.

Solving polynomial systems? What does this mean?

The algebra text book says:

For $F \subset \mathbf{k}[x_1, \ldots, x_n]$ this is simply

- a *primary decomposition* of $\langle F \rangle$ or
- the *irreducible decomposition* of $V(F)$ (the zero set of F in $\overline{\mathbf{k}}^n$).

The computer algebra system does well:

For $F \subset \mathbf{k}[x_1, \ldots, x_n]$, with $\mathbf{k} = \mathbb{Z}/p\mathbb{Z}$ or $\mathbf{k} = \mathbb{Q}$,

- computing a *Gröbner basis* of $\langle F \rangle$ or
- computing a *triangular decomposition* of $V(F)$.

But most scientists and engineers need:

- For $F \subset \mathbb{Q}[x_1, \ldots, x_n]$, a useful description of the points of $V(F)$ whose coordinates are real.
- For $F \subset \mathbb{Q}[u_1, \ldots, u_d][x_1, \ldots, x_n]$, the real $(x_1, \ldots, x_n)$-solutions as a function of the real parameter $(u_1, \ldots, u_d)$.

Solving polynomial systems? What does this mean?

The algebra text book says:

For $F \subset \mathbf{k}[x_1, \ldots, x_n]$ this is simply

- a *primary decomposition* of $\langle F \rangle$ or
- the *irreducible decomposition* of $V(F)$ (the zero set of F in $\overline{\mathbf{k}}^n$).

The computer algebra system does well:

For $F \subset \mathbf{k}[x_1, \ldots, x_n]$, with $\mathbf{k} = \mathbb{Z}/p\mathbb{Z}$ or $\mathbf{k} = \mathbb{Q}$,

- computing a *Gröbner basis* of $\langle F \rangle$ or
- computing a *triangular decomposition* of $V(F)$.

But most scientists and engineers need:

- For $F \subset \mathbb{Q}[x_1, \ldots, x_n]$, a useful description of the points of $V(F)$ whose coordinates are real.
- For $F \subset \mathbb{Q}[u_1, \ldots, u_d][x_1, \ldots, x_n]$, the real $(x_1, \ldots, x_n)$-solutions as a function of the real parameter $(u_1, \ldots, u_d)$.

Solving for the real solutions: classical techniques

In dimension zero over $\mathbb{Q}$:

For $F \subset \mathbb{Q}[x_1, \ldots, x_n]$, if $V(F)$ is finite, many standard and efficient techniques apply to identify the real solutions.

In (generic) dimension zero over $\mathbb{Q}[u_1, \ldots, u_d]$:

For $F \subset \mathbb{Q}[u_1, \ldots, u_d][x_1, \ldots, x_n]$ and an integer r one can determine "generic" conditions on $u_1, \ldots, u_d$ for F to admit exactly r real $(x_1, \ldots, x_n)$-solutions

For arbitrary systems:

For $F \subset \mathbb{Q}[x_1, \ldots, x_n]$, one can partition $\mathbb{R}^n$ into *cylindrical cells* where the sign of each $f \in F$ does not change.

Solving for the real solutions: classical techniques

In dimension zero over $\mathbb{Q}$:

For $F \subset \mathbb{Q}[x_1, \ldots, x_n]$, if $V(F)$ is finite, many standard and efficient techniques apply to identify the real solutions.

In (generic) dimension zero over $\mathbb{Q}[u_1, \ldots, u_d]$:

For $F \subset \mathbb{Q}[u_1, \ldots, u_d][x_1, \ldots, x_n]$ and an integer r one can determine "generic" conditions on $u_1, \ldots, u_d$ for F to admit exactly r real $(x_1, \ldots, x_n)$-solutions

For arbitrary systems:

For $F \subset \mathbb{Q}[x_1, \ldots, x_n]$, one can partition $\mathbb{R}^n$ into *cylindrical cells* where the sign of each $f \in F$ does not change.

Solving for the real solutions: classical techniques

In dimension zero over $\mathbb{Q}$:

For $F \subset \mathbb{Q}[x_1, \ldots, x_n]$, if $V(F)$ is finite, many standard and efficient techniques apply to identify the real solutions.

In (generic) dimension zero over $\mathbb{Q}[u_1, \ldots, u_d]$:

For $F \subset \mathbb{Q}[u_1, \ldots, u_d][x_1, \ldots, x_n]$ and an integer r one can determine "generic" conditions on $u_1, \ldots, u_d$ for F to admit exactly r real $(x_1, \ldots, x_n)$-solutions

For arbitrary systems:

For $F \subset \mathbb{Q}[x_1, \ldots, x_n]$, one can partition $\mathbb{R}^n$ into *cylindrical cells* where the sign of each $f \in F$ does not change.

Real root isolation for zero-dimensional systems

Applications Places System moreno

Untitled (1)* - [Server 1] - Maple 14

Format Table Drawing Plot Spreadsheet Tools Window Help

```
with(RegularChains) : with(SemiAlgebraicSetTools) : with(ParametricSystemTools) : with(ParametricSystem
R := PolynomialRing([x, y, z]); F := [x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1];
```

polynomial_ring

$$\left[x^2 + y + z - 1,\ y^2 + x + z - 1,\ x + y + z^2 - 1\right]$$

```
dec := Triangularize(F, R); map(Display, dec, R);
```

[regular_chain, regular_chain, regular_chain, regular_chain]

$$\left[\begin{cases} x - z = 0 \\ y - z = 0 \\ z^2 + 2z - 1 = 0 \end{cases},\ \begin{cases} x = 0 \\ y = 0 \\ z - 1 = 0 \end{cases},\ \begin{cases} x = 0 \\ y - 1 = 0 \\ z = 0 \end{cases},\ \begin{cases} x - 1 = 0 \\ y = 0 \\ z = 0 \end{cases}\right]$$

$$boxes := \left[seq\left(op\left(RealRootIsolate\left(rc, R, 'rerr' = \frac{1}{2^9}\right)\right), rc = dec\right)\right];\ map\left(Display, boxes, R\right.$$

[box, box, box, box, box]

$$\left[\begin{cases} x = \left[\frac{3393}{8192}, \frac{6791}{16384}\right] \\ y = \left[\frac{3393}{8192}, \frac{6791}{16384}\right] \\ z = \left[\frac{217167}{524288}, \frac{868669}{2097152}\right] \end{cases},\ \begin{cases} x = \left[-\frac{4947}{2048}, -\frac{2471}{1024}\right] \\ y = \left[-\frac{4947}{2048}, -\frac{2471}{1024}\right] \\ z = \left[-\frac{79109}{32768}, -\frac{316435}{131072}\right] \end{cases},\ \begin{cases} x = 0 \\ y = 0 \\ z = 1 \end{cases},\ \begin{cases} x = 0 \\ y = 1 \\ z = 0 \end{cases},\ \begin{cases} x = 1 \\ y = 0 \\ z = 0 \end{cases}\right.$$

Real root classification: generically 0-dimensional systems

Applications Places System moreno

Untitled (1)* - [Server 1] - Maple 14

Format Table Drawing Plot Spreadsheet Tools Window Help

with(*RegularChains*) : *with*(*SemiAlgebraicSetTools*) : *with*(*ParametricSystemTools*) : with(ParametricSystem

$R := PolynomialRing([x, y, z, \text{epsilon}]);\ F := [x\text{^}2 + y + z - 1, x + y\text{^}2 + z - 1, x + y + z\text{^}2 - 1 + \text{epsilon}];$

polynomial_ring

$$[x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1 + \varepsilon]$$

$dec := Triangularize(F, R);\ map(Equations, dec, R);$

[*regular_chain*, *regular_chain*]

$$[[2x + z^2 + \varepsilon - 1, 2y + z^2 + \varepsilon - 1, z^4 + (2\varepsilon - 4)z^2 + 4z - 4\varepsilon - 1 + \varepsilon^2], [x + y - 1, y^2 - y + z, z^2 + \varepsilon$$

For which values of epsilon does F have 2 solutions each of which has a positive x-coordinate?

$rrc := RealRootClassification(F, [\ ], [x], [\ ], 1, 2, R); Display(rrc[1][1], R); Display(rrc[2], R)$

[[*regular_semi_algebraic_set*], *border_polynomial*]

$$\begin{cases} \varepsilon < 0 \textbf{ and } 16\varepsilon < -1 \textbf{ and } 5\varepsilon - 1 \neq 0 \textbf{ and } 16\varepsilon^2 - 71\varepsilon + 2 \neq 0 \\ \textbf{or } \varepsilon > 0 \textbf{ and } 16\varepsilon + 1 \neq 0 \textbf{ and } 5\varepsilon < 1 \textbf{ and } 16\varepsilon^2 - 71\varepsilon + 2 > 0 \end{cases}$$

$$\left[\varepsilon, \varepsilon - \frac{1}{5}, \varepsilon + \frac{1}{16}, \varepsilon^2 - \frac{71}{16}\varepsilon + \frac{1}{8}\right]$$

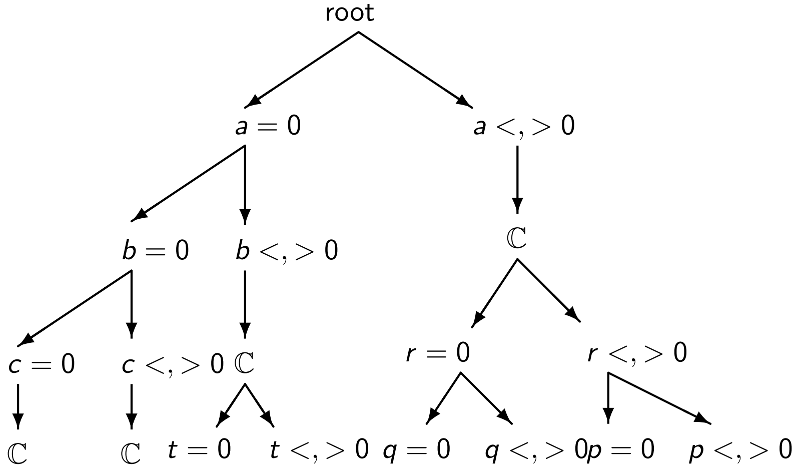
For which values of epsilon does F have 5 solutions ?

$rrc := RealRootClassification(F, [\ ], [\ ], [\ ], 1, 5, R);\ Display(rrc[2], R)$

[[ ], *border_polynomial*]

$$\left[\varepsilon, \varepsilon + \frac{1}{16}, \varepsilon^2 - \frac{71}{16}\varepsilon + \frac{1}{8}\right]$$

Cylindrical algebraic decomposition of $\{ax^2 + bx + c\}$



The cylindrical algebraic decomposition of $\{ax^2 + bx + c\}$ is given by the tree above, where $t = bx + c$, $q = 2ax + b$, and $r = 4ac - b^2$. This is the best possible output for that method, leading to **27 cells**!

Can a computer program be as good as a high-school student?

For the equation $ax^2 + bx + c = 0$, can a computer program produce?

$$\begin{cases} ax^2 + bx + c = 0 \\ a \neq 0 \wedge b^2 - 4ac > 0 \end{cases} \qquad \begin{cases} 2ax + b = 0 \\ 4ac - b^2 = 0 \\ a \neq 0 \end{cases}$$

$$\begin{cases} bx + c = 0 \\ a = 0 \\ b \neq 0 \end{cases} \qquad \begin{cases} c = 0 \\ b = 0 \\ a = 0 \end{cases}$$

Yes, our new algorithm RealTriangularize can do that!

Applications Places System moreno

Untitled (1)* - [Server 1] - Maple 14

ormat Table Drawing Plot Spreadsheet Tools Window Help

with(RegularChains) : *with(SemiAlgebraicSetTools)* : *with(ParametricSystemTools)* : with(ParametricSystemT

$R := PolynomialRing([x, c, b, a]);\ F := [a \cdot x^2 + b \cdot x + c];$

polynomial_ring

$$[a\,x^2 + b\,x + c]$$

Solving for the real solutions:

$RealTriangularize(F, R, output = record);$

$$\left\{\begin{array}{c} a\,x^2 + b\,x + c = 0 \\ -4\,c\,a + b^2 > 0 \\ a \neq 0 \end{array}\right., \left\{\begin{array}{c} b\,x + c = 0 \\ b \neq 0 \\ a = 0 \end{array}\right., \left\{\begin{array}{c} c = 0 \\ b = 0 \\ a = 0 \end{array}\right., \left\{\begin{array}{c} 2\,a\,x + b = 0 \\ 4\,a\,c - b^2 = 0 \\ a \neq 0 \end{array}\right.$$

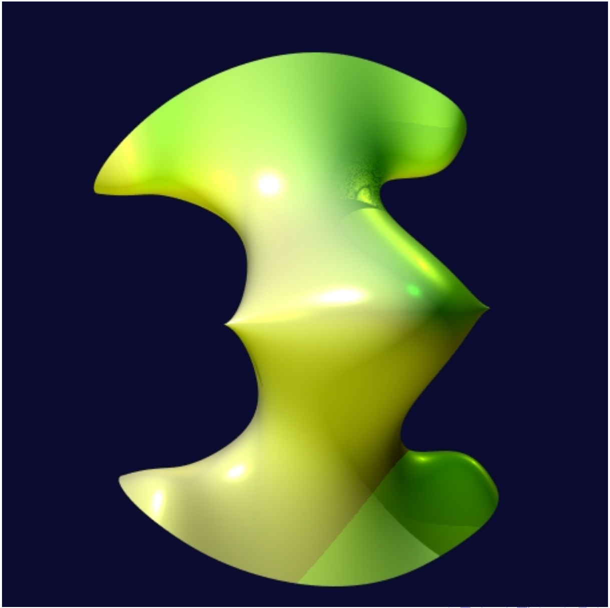
Solving **for** *the complex solutions*

$dec := Triangularize(F, R, output = lazard);\ map(Display, dec, R);$

[regular_chain, regular_chain, regular_chain]

$$\left[\left\{\begin{array}{c} a\,x^2 + b\,x + c = 0 \\ a \neq 0 \end{array}\right., \left\{\begin{array}{c} b\,x + c = 0 \\ a = 0 \\ b \neq 0 \end{array}\right., \left\{\begin{array}{c} c = 0 \\ b = 0 \\ a = 0 \end{array}\right.\right]$$

RealTriangularize applied to the *Eve* surface (1/2)



RealTriangularize applied to the *Eve* surface (2/2)

Applications Places System moreno

Untitled (1)* - [Server 1] - Maple 14

ormat Table Drawing Plot Spreadsheet Tools Window Help

$R := PolynomialRing([x, y, z]);\ F := [5*x\wedge 2 + 2*x*z\wedge 2 + 5*y\wedge 6 + 15*y\wedge 4 + 5*z\wedge 2 - 15*y\wedge 5 - 5*y\wedge 3$

$$polynomial\_ring$$

$$[5\,x^2 + 2\,x\,z^2 + 5\,y^6 + 15\,y^4 + 5\,z^2 - 15\,y^5 - 5\,y^3]$$

$RealTriangularize(F, R, output = record);$

$$\left\{\begin{array}{l} 5\,x^2 + 2\,z^2\,x + 5\,y^6 + 15\,y^4 - 5\,y^3 - 15\,y^5 + 5\,z^2 = 0 \\ 25\,y^6 - 75\,y^5 + 75\,y^4 - z^4 - 25\,y^3 + 25\,z^2 < 0 \end{array}\right. ,$$

$$\left\{\begin{array}{c} 5\,x + z^2 = 0 \\ 25\,y^6 - 75\,y^5 + 75\,y^4 - 25\,y^3 - z^4 + 25\,z^2 = 0 \\ 64\,z^4 - 1600\,z^2 + 25 > 0 \\ z \neq 0 \\ z - 5 \neq 0 \\ z + 5 \neq 0 \end{array}\right. , \left\{\begin{array}{c} x = 0 \\ y - 1 = 0 \\ z = 0 \end{array}\right. , \left\{\begin{array}{c} x = 0 \\ y = 0 \\ z = 0 \end{array}\right. , \left\{\begin{array}{c} x + 5 = 0 \\ y - 1 = 0 \\ z - 5 = 0 \end{array}\right. ,$$

$$\left\{\begin{array}{c} x + 5 = 0 \\ y = 0 \\ z - 5 = 0 \end{array}\right. , \left\{\begin{array}{c} x + 5 = 0 \\ y - 1 = 0 \\ z + 5 = 0 \end{array}\right. , \left\{\begin{array}{c} x + 5 = 0 \\ y = 0 \\ z + 5 = 0 \end{array}\right. , \left\{\begin{array}{c} 5\,x + z^2 = 0 \\ 2\,y - 1 = 0 \\ 64\,z^4 - 1600\,z^2 + 25 = 0 \end{array}\right.$$

Plan

Triangular Set

Definition

$T \subset \mathbf{k}[x_n > \cdots > x_1]$ is a *triangular set* if $T \cap \mathbf{k} = \emptyset$ and $\mathrm{mvar}(p) \neq \mathrm{mvar}(q)$ for all $p, q \in T$ with $p \neq q$.

Theorem (J.F. Ritt, 1932)

Let $V \subset \mathbf{K}^n$ be an irreducible variety and $F \subset \mathbf{k}[x_1, \cdots, x_n]$ s.t. $V = V(F)$. Then, one can compute a (reduced) triangular set $T \subset \langle F \rangle$ s.t.

$$(\forall\ g \in \langle \mathbf{F} \rangle)\ \ \mathrm{prem}(g, T) = 0.$$

Theorem (W.T. Wu, 1987)

Let $V \subset \mathbf{K}^n$ be a variety and let $F \subset \mathbf{k}[x_1, \cdots, x_n]$ s.t. $V = V(F)$. Then, one can compute a (reduced) triangular set $T \subset \langle F \rangle$ s.t.

$$(\forall\ g \in F)\ \ \mathrm{prem}(g, T) = 0.$$

Unfortunately, this procedure cannot decide whether $V = \emptyset$ holds or not.

Triangular Set

Definition

$T \subset \mathbf{k}[x_n > \cdots > x_1]$ is a *triangular set* if $T \cap \mathbf{k} = \emptyset$ and $\mathrm{mvar}(p) \neq \mathrm{mvar}(q)$ for all $p, q \in T$ with $p \neq q$.

Theorem (J.F. Ritt, 1932)

Let $V \subset \mathbf{K}^n$ be an irreducible variety and $F \subset \mathbf{k}[x_1, \cdots, x_n]$ s.t. $V = V(F)$. Then, one can compute a (reduced) triangular set $T \subset \langle F \rangle$ s.t.

$$(\forall\ g \in \langle \mathbf{F} \rangle) \ \ \mathrm{prem}(g, T) = 0.$$

Theorem (W.T. Wu, 1987)

Let $V \subset \mathbf{K}^n$ be a variety and let $F \subset \mathbf{k}[x_1, \cdots, x_n]$ s.t. $V = V(F)$. Then, one can compute a (reduced) triangular set $T \subset \langle F \rangle$ s.t.

$$(\forall\ g \in F) \ \ \mathrm{prem}(g, T) = 0.$$

Unfortunately, this procedure cannot decide whether $V = \emptyset$ holds or not.

Triangular Set

Definition

$T \subset \mathbf{k}[x_n > \cdots > x_1]$ is a *triangular set* if $T \cap \mathbf{k} = \emptyset$ and $\mathrm{mvar}(p) \neq \mathrm{mvar}(q)$ for all $p, q \in T$ with $p \neq q$.

Theorem (J.F. Ritt, 1932)

Let $V \subset \mathbf{K}^n$ be an irreducible variety and $F \subset \mathbf{k}[x_1, \cdots, x_n]$ s.t. $V = V(F)$. Then, one can compute a (reduced) triangular set $T \subset \langle F \rangle$ s.t.

$$(\forall\ g \in \langle \mathbf{F} \rangle)\ \ \mathrm{prem}(g, T) = 0.$$

Theorem (W.T. Wu, 1987)

Let $V \subset \mathbf{K}^n$ be a variety and let $F \subset \mathbf{k}[x_1, \cdots, x_n]$ s.t. $V = V(F)$. Then, one can compute a (reduced) triangular set $T \subset \langle F \rangle$ s.t.

$$(\forall\ g \in F)\ \ \mathrm{prem}(g, T) = 0.$$

Unfortunately, this procedure cannot decide whether $V = \emptyset$ holds or not.

Regular chain

Definition

Let $T \subset \mathbf{k}[x_n > \cdots > x_1]$ be a triangular set. For all $t \in T$ write $\mathrm{init}(t) := \mathrm{lc}(t, \mathrm{mvar}(t))$ and $h_T := \prod_{t \in T} \mathrm{init}(t)$. The *quasi-component* and *saturated ideal* of T are:

$$W(T) := V(T) \setminus V(h_T) \text{ and } \mathrm{sat}(T) = \langle T \rangle : h_T^{\infty}$$

Theorem (F. Boulier, F. Lemaire and M.M.M. 2006)

We have: $\overline{W(T)} = V(\mathrm{sat}(T))$. *Moreover, if* $\mathrm{sat}(T) \neq \langle 1 \rangle$ *then* $\mathrm{sat}(T)$ *is strongly equi-dimensional.*

Definition (M. Kalkbrner, 1991 - L. Yang, J. Zhang 1991)

T is a *regular chain* if $T = \emptyset$ or $T := T' \cup \{t\}$ with $\mathrm{mvar}(t)$ maximum s.t.

- T' is a regular chain,
- $\mathrm{init}(t)$ is regular modulo $\mathrm{sat}(T')$

Regular chain

Definition

Let $T \subset \mathbf{k}[x_n > \cdots > x_1]$ be a triangular set. For all $t \in T$ write $\mathrm{init}(t) := \mathrm{lc}(t, \mathrm{mvar}(t))$ and $h_T := \prod_{t \in T} \mathrm{init}(t)$. The *quasi-component* and *saturated ideal* of T are:

$$W(T) := V(T) \setminus V(h_T) \quad \text{and} \quad \mathrm{sat}(T) = \langle T \rangle : h_T^{\infty}$$

Theorem (F. Boulier, F. Lemaire and M.M.M. 2006)

We have: $\overline{W(T)} = V(\mathrm{sat}(T))$. Moreover, if $\mathrm{sat}(T) \neq \langle 1 \rangle$ then $\mathrm{sat}(T)$ is strongly equi-dimensional.

Definition (M. Kalkbrner, 1991 - L. Yang, J. Zhang 1991)

T is a *regular chain* if $T = \emptyset$ or $T := T' \cup \{t\}$ with $\mathrm{mvar}(t)$ maximum s.t.

- T' is a regular chain,
- $\mathrm{init}(t)$ is regular modulo $\mathrm{sat}(T')$

Regular chain

Definition

Let $T \subset \mathbf{k}[x_n > \cdots > x_1]$ be a triangular set. For all $t \in T$ write $\mathrm{init}(t) := \mathrm{lc}(t, \mathrm{mvar}(t))$ and $h_T := \prod_{t \in T} \mathrm{init}(t)$. The *quasi-component* and *saturated ideal* of T are:

$$W(T) := V(T) \setminus V(h_T) \;\; \text{and} \;\; \mathrm{sat}(T) = \langle T \rangle : h_T^{\infty}$$

Theorem (F. Boulier, F. Lemaire and M.M.M. 2006)

We have: $\overline{W(T)} = V(\mathrm{sat}(T))$. *Moreover, if* $\mathrm{sat}(T) \neq \langle 1 \rangle$ *then* $\mathrm{sat}(T)$ *is strongly equi-dimensional.*

Definition (M. Kalkbrner, 1991 - L. Yang, J. Zhang 1991)

T is a *regular chain* if $T = \emptyset$ or $T := T' \cup \{t\}$ with $\mathrm{mvar}(t)$ maximum s.t.

- T' is a regular chain,
- $\mathrm{init}(t)$ is regular modulo $\mathrm{sat}(T')$

Regular chain: alternative definition

Regular chain: algorithmic properties

Definition

Let $T \subset \mathbf{k}[x_n > \cdots > x_1]$ be a triangular set and $p \in \mathbf{k}[x_n > \cdots > x_1]$. If T is empty then, the *iterated resultant* of p w.r.t. T is $\mathrm{res}(T, p) = p$. Otherwise, writing $T = T_{<w} \cup T_w$

$$\mathrm{res}(T, p) \;=\; \begin{cases} p & \text{if } \deg(p, w) = 0 \\ \mathrm{res}(T_{<w}, \mathrm{res}(T_w, p, w)) & \text{otherwise} \end{cases}$$

Theorem (P. Aubry, D. Lazard, M.M.M.)

T is a regular chain *iff*

$$\{p \mid \mathrm{prem}(p, T) = 0\} \;=\; \mathrm{sat}(T)$$

Theorem (L. Yang, J. Zhang 1991)

p is regular modulo $\mathrm{sat}(T)$ *iff*

$$\mathrm{res}(T, p) \neq 0$$

Regular chain: algorithmic properties

Definition

Let $T \subset \mathbf{k}[x_n > \cdots > x_1]$ be a triangular set and $p \in \mathbf{k}[x_n > \cdots > x_1]$. If T is empty then, the *iterated resultant* of p w.r.t. T is $\mathrm{res}(T, p) = p$. Otherwise, writing $T = T_{<w} \cup T_w$

$$\mathrm{res}(T, p) \quad = \quad \begin{cases} p & \text{if } \deg(p, w) = 0 \\ \mathrm{res}(T_{<w}, \mathrm{res}(T_w, p, w)) & \text{otherwise} \end{cases}$$

Theorem (P. Aubry, D. Lazard, M.M.M.)

T is a regular chain *iff*

$$\{p \mid \mathrm{prem}(p, T) = 0\} \quad = \quad \mathrm{sat}(T)$$

Theorem (L. Yang, J. Zhang 1991)

p is regular modulo $\mathrm{sat}(T)$ iff

$$\mathrm{res}(T, p) \neq 0$$

Regular chain: algorithmic properties

Definition

Let $T \subset \mathbf{k}[x_n > \cdots > x_1]$ be a triangular set and $p \in \mathbf{k}[x_n > \cdots > x_1]$. If T is empty then, the *iterated resultant* of p w.r.t. T is $\mathrm{res}(T, p) = p$. Otherwise, writing $T = T_{<w} \cup T_w$

$$\mathrm{res}(T, p) \quad = \quad \begin{cases} p & \text{if } \deg(p, w) = 0 \\ \mathrm{res}(T_{<w}, \mathrm{res}(T_w, p, w)) & \text{otherwise} \end{cases}$$

Theorem (P. Aubry, D. Lazard, M.M.M.)

T is a regular chain *iff*

$$\{p \mid \mathrm{prem}(p, T) = 0\} \quad = \quad \mathrm{sat}(T)$$

Theorem (L. Yang, J. Zhang 1991)

p is regular modulo $\mathrm{sat}(T)$ *iff*

$$\mathrm{res}(T, p) \neq 0$$

Triangular decomposition of an algebraic variety

Kalkbrener triangular decomposition

Let $F \subset \mathbf{k}[\mathbf{x}]$. A family of regular chains $T_1, \ldots, T_e$ of $\mathbf{k}[\mathbf{x}]$ is called a Kalkbrener triangular decomposition of $V(F)$ if

$$V(F) = \cup_{i=1}^{e} V(\mathrm{sat}(T_i)).$$

Wu-Lazard triangular decomposition

Let $F \subset \mathbf{k}[\mathbf{x}]$. A family of regular chains $T_1, \ldots, T_e$ of $\mathbf{k}[\mathbf{x}]$ is called a Wu-Lazard triangular decomposition of $V(F)$ if

$$V(F) = \cup_{i=1}^{e} W(T_i)$$

Triangular decomposition of an algebraic variety

Kalkbrener triangular decomposition

Let $F \subset \mathbf{k}[\mathbf{x}]$. A family of regular chains $T_1, \ldots, T_e$ of $\mathbf{k}[\mathbf{x}]$ is called a Kalkbrener triangular decomposition of $V(F)$ if

$$V(F) = \cup_{i=1}^{e} V(\mathrm{sat}(T_i)).$$

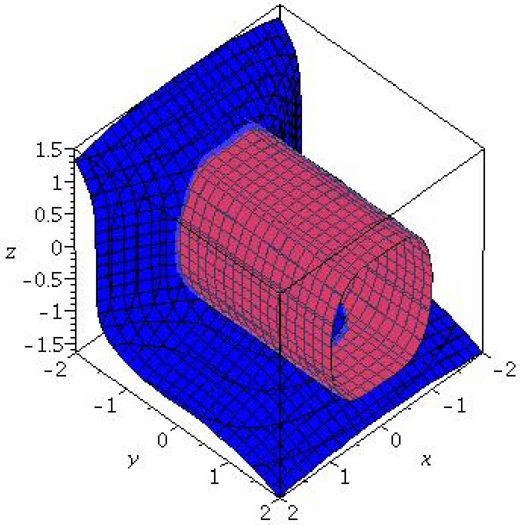
Wu-Lazard triangular decomposition

Let $F \subset \mathbf{k}[\mathbf{x}]$. A family of regular chains $T_1, \ldots, T_e$ of $\mathbf{k}[\mathbf{x}]$ is called a Wu-Lazard triangular decomposition of $V(F)$ if

$$V(F) = \cup_{i=1}^{e} W(T_i)$$

Triangularize applied to *sofa* and *cylinder* (1/2)

$$x^2 + y^3 + z^5 = x^4 + z^2 - 1 = 0$$



Triangularize applied to *sofa* and *cylinder* (2/2)

Applications Places System — Sun Feb 13, 10:36 PM — changbo

/home/changbo/src/maple/triade/mapleP4/lib/cylinder.mw - [Server 1] - Maple 14

File Edit View Insert Format Table Drawing Plot Spreadsheet Tools Window Help

```
> R := PolynomialRing([z, y, x]): F := [x^2+y^3+z^5, x^4+z^2-1]: dec :=
  Triangularize(F, R): map(Display, dec, R);
```

$$\left[\left\{\begin{array}{c} (-2x^4+x^8+1)\,z+x^2+y^3=0 \\ y^6+2x^2y^3+10x^{12}-10x^8+x^{20}-5x^{16}+6x^4-1=0 \\ -2x^4+x^8+1\neq 0 \end{array}\right.\right]$$

```
> dec := Triangularize(F, R, output=lazard): map(Display, dec, R);
```

$$\left[\left\{\begin{array}{c} (-2x^4+x^8+1)\,z+x^2+y^3=0 \\ y^6+2x^2y^3+10x^{12}-10x^8+x^{20}-5x^{16}+6x^4-1=0 \\ -2x^4+x^8+1\neq 0 \end{array}\right., \left\{\begin{array}{c} z=0 \\ y^2+y+1=0 \\ x^2+1=0 \end{array}\right.,\right.$$

$$\left\{\begin{array}{c} z=0 \\ y-1=0 \\ x^2+1=0 \end{array}\right., \left\{\begin{array}{c} z=0 \\ y^2-y+1=0 \\ x+1=0 \end{array}\right., \left\{\begin{array}{c} z=0 \\ y^2-y+1=0 \\ x-1=0 \end{array}\right., \left\{\begin{array}{c} z=0 \\ y+1=0 \\ x+1=0 \end{array}\right.,$$

$$\left.\left\{\begin{array}{c} z=0 \\ y+1=0 \\ x-1=0 \end{array}\right.\right]$$

Ready

Plan

Regular chain: specialization properties

Notation

Let $T \subset \mathbb{Q}[x_1 < \ldots < x_n]$ be a regular chain with $\mathbf{y} := \{\mathrm{mvar}(t) \mid t \in T\}$ and $\mathbf{u} := \mathbf{x} \setminus \mathbf{y} = u_1, \ldots, u_d$. Hence $\mathrm{sat}(T)$ has dimension d.

- *Recall that h_T is the product of the $\mathrm{init}(t)$, for $t \in T$.*
- *Denote by s_T the product of the $\mathrm{discrim}(\mathrm{t}, \mathrm{mvar}(t))$.*

Definition

We say that T *specializes well* at a point $u \in \mathbb{R}^d$ if $h_T(u) \neq 0$ and the triangular set $T(u)$ is a regular chain generating a radical ideal.

Theorem (X. Hou, B. Xia, L. Yang, 2001)

Define $BP_T := \mathrm{res}(T, h_T)\,\mathrm{res}(T, s_T)$, the border polynomial of T. Then

- *T specializes well at $u \in \mathbb{R}^d$ if and only if $BP_T(u) \neq 0$.*
- *For each connected component C of $BP_T(u) \neq 0$, the number of real solutions of $T(u)$ is constant for $u \in C$.*

Regular chain: specialization properties

Notation

Let $T \subset \mathbb{Q}[x_1 < \ldots < x_n]$ *be a regular chain with* $\mathbf{y} := \{\mathrm{mvar}(t) \mid t \in T\}$ *and* $\mathbf{u} := \mathbf{x} \setminus \mathbf{y} = u_1, \ldots, u_d$. *Hence* $\mathrm{sat}(T)$ *has dimension* d.

- *Recall that* h_T *is the product of the* $\mathrm{init}(t)$, *for* $t \in T$.
- *Denote by* s_T *the product of the* $\mathrm{discrim}(\mathrm{t}, \mathrm{mvar}(t))$.

Definition

We say that T *specializes well* at a point $u \in \mathbb{R}^d$ if $h_T(u) \neq 0$ and the triangular set $T(u)$ is a regular chain generating a radical ideal.

Theorem (X. Hou, B. Xia, L. Yang, 2001)

Define $BP_T := \mathrm{res}(T, h_T)\,\mathrm{res}(T, s_T)$, *the* border polynomial *of* T. *Then*

- *T specializes well at* $u \in \mathbb{R}^d$ *if and only if* $BP_T(u) \neq 0$.
- *For each connected component* C *of* $BP_T(u) \neq 0$, *the number of real solutions of* $T(u)$ *is constant for* $u \in C$.

Regular chain: specialization properties

Notation

Let $T \subset \mathbb{Q}[x_1 < \ldots < x_n]$ *be a regular chain with* $\mathbf{y} := \{\mathrm{mvar}(t) \mid t \in T\}$ *and* $\mathbf{u} := \mathbf{x} \setminus \mathbf{y} = u_1, \ldots, u_d$*. Hence* $\mathrm{sat}(T)$ *has dimension* d*.*

- *Recall that* h_T *is the product of the* $\mathrm{init}(t)$*, for* $t \in T$*.*
- *Denote by* s_T *the product of the* $\mathrm{discrim}(\mathrm{t}, \mathrm{mvar}(t))$*.*

Definition

We say that T *specializes well* at a point $u \in \mathbb{R}^d$ if $h_T(u) \neq 0$ and the triangular set $T(u)$ is a regular chain generating a radical ideal.

Theorem (X. Hou, B. Xia, L. Yang, 2001)

Define $BP_T := \mathrm{res}(T, h_T)\,\mathrm{res}(T, s_T)$, *the* border polynomial *of* T*. Then*

- T *specializes well at* $u \in \mathbb{R}^d$ *if and only if* $BP_T(u) \neq 0$*.*
- *For each connected component* C *of* $BP_T(u) \neq 0$*, the number of real solutions of* $T(u)$ *is constant for* $u \in C$*.*

Border polynomial and specialization

Example (bad specialization of a regular chain)

$$T := \begin{cases} x_4 x_5{}^2 + 2x_5 + 1 \\ (x_1 + x_2) x_3{}^2 + x_3 + 1 \\ x_1{}^2 - 1. \end{cases} \qquad T_{x_2, x_4 = -1, 1} := \begin{cases} x_5{}^2 + 2x_5 + 1 \\ (x_1 - 1) x_3{}^2 + x_3 + 1 \\ x_1{}^2 - 1. \end{cases}$$

Example (border polynomial)

$$\mathrm{res}(\mathrm{dis}(t_2), t_1)\, \mathrm{res}(\mathrm{res}(\mathrm{dis}(t_3), t_2), t_1).\, \mathrm{res}(\mathrm{init}(t_2), t_1)\, \mathrm{res}(\mathrm{res}(\mathrm{init}(t_3), t_2), t_1).$$

For the above regular chain, it is

$$(4x_2 + 3)(4x_2 - 5)(x_2^2 - 1)(x_4 - 1)x_4$$

Border polynomial and specialization

Example (bad specialization of a regular chain)

$$T := \begin{cases} x_4 x_5{}^2 + 2x_5 + 1 \\ (x_1 + x_2) x_3{}^2 + x_3 + 1 \\ x_1{}^2 - 1. \end{cases} \qquad T_{x_2, x_4 = -1, 1} := \begin{cases} x_5{}^2 + 2x_5 + 1 \\ (x_1 - 1) x_3{}^2 + x_3 + 1 \\ x_1{}^2 - 1. \end{cases}$$

Example (border polynomial)

$$\mathrm{res}(\mathrm{dis}(t_2), t_1)\, \mathrm{res}(\mathrm{res}(\mathrm{dis}(t_3), t_2), t_1).\, \mathrm{res}(\mathrm{init}(t_2), t_1)\, \mathrm{res}(\mathrm{res}(\mathrm{init}(t_3), t_2), t_1).$$

For the above regular chain, it is

$$(4x_2 + 3)(4x_2 - 5)(x_2^2 - 1)(x_4 - 1)x_4$$

Regular semi-algebraic system

Notation

- *Let* $T \subset \mathbb{Q}[x_1 < \ldots < x_n]$ *be a regular chain with* $\mathbf{y} := \{\mathrm{mvar}(t) \mid t \in T\}$ *and* $\mathbf{u} := \mathbf{x} \setminus \mathbf{y} = u_1, \ldots, u_d$.
- *Let* P *be a finite set of polynomials, s.t. every* $f \in P$ *is regular modulo* $\mathrm{sat}(T)$.
- *Let* $\mathcal{Q}$ *be a quantifier-free formula of* $\mathbb{Q}[\mathbf{u}]$.

Definition

We say that $R := [\mathcal{Q}, T, P_>]$ is a regular semi-algebraic system if:

(i) $\mathcal{Q}$ defines a non-empty open semi-algebraic set S in $\mathbb{R}^d$,

(ii) the regular system $[T, P]$ specializes well at every point u of S

(iii) at each point u of S, the specialized system $[T(u), P(u)_>]$ has at least one real solution.

Define

$$Z_{\mathbb{R}}(R) = \{(u, y) \mid \mathcal{Q}(u), t(u, y) = 0, p(u, y) > 0, \forall (t, p) \in T \times P\}.$$

Regular semi-algebraic system

Notation

- *Let* $T \subset \mathbb{Q}[x_1 < \ldots < x_n]$ *be a regular chain with* $\mathbf{y} := \{\mathrm{mvar}(t) \mid t \in T\}$ *and* $\mathbf{u} := \mathbf{x} \setminus \mathbf{y} = u_1, \ldots, u_d$.
- *Let* P *be a finite set of polynomials, s.t. every* $f \in P$ *is regular modulo* $\mathrm{sat}(T)$.
- *Let* $\mathcal{Q}$ *be a quantifier-free formula of* $\mathbb{Q}[\mathbf{u}]$.

Definition

We say that $R := [\mathcal{Q}, T, P_>]$ is a regular semi-algebraic system if:

(*i*) $\mathcal{Q}$ defines a non-empty open semi-algebraic set S in $\mathbb{R}^d$,

(*ii*) the regular system $[T, P]$ specializes well at every point u of S

(*iii*) at each point u of S, the specialized system $[T(u), P(u)_>]$ has at least one real solution.

Define

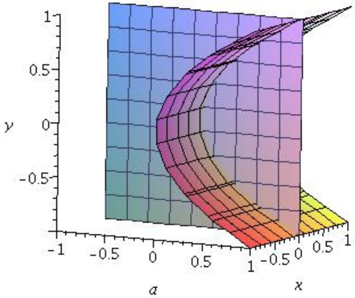
$$Z_{\mathbb{R}}(R) = \{(u, y) \mid \mathcal{Q}(u), t(u, y) = 0, p(u, y) > 0, \forall (t, p) \in T \times P\}.$$

Example

The system $[\mathcal{Q}, T, P_>]$, where

$$\mathcal{Q} := a > 0, \;\; T := \begin{cases} y^2 - a = 0 \\ x = 0 \end{cases}, \;\; P_> := \{y > 0\}$$

is a regular semi-algebraic system.



Triangular decompositions of semi-algebraic systems (1/2)

Proposition

Let $R := [\mathcal{Q}, T, P_>]$ be a regular semi-algebraic system of $\mathbb{Q}[u_1, \ldots, u_d, \mathbf{y}]$. Then the zero set of R is a nonempty semi-algebraic set of dimension d.

Theorem

Every semi-algebraic system $\mathcal{S}$ can be decomposed as a finite union of regular semi-algebraic systems such that the union of their zero sets is the zero set of $\mathcal{S}$. We call it a (full) triangular decomposition of $\mathcal{S}$.

Triangular decompositions of semi-algebraic systems (2/2)

Notation

Let $\mathcal{S} = [F, N_{\geq}, P_{>}, H_{\neq}]$ be a semi-algebraic system of $\mathbb{Q}[\mathbf{x}]$. Let c be the dimension of the constructible set of $\mathbb{C}^n$ corresponding to $\mathcal{S}$.

Definition

A finite set of regular semi-algebraic systems R_i is called a lazy triangular decomposition of $\mathcal{S}$ if

- for each i, $Z_{\mathbb{R}}(R_i) \subseteq Z_{\mathbb{R}}(\mathcal{S})$ holds, and
- there exists $G \subset \mathbb{Q}[\mathbf{x}]$ such that

$$Z_{\mathbb{R}}(\mathcal{S}) \setminus \left(\cup_{i=1}^{t} Z_{\mathbb{R}}(R_i)\right) \subseteq Z_{\mathbb{R}}(G),$$

  where the complex zero set $V(G)$ has dimension less than c.

A detailed example

Original problem

Consider the following question (Brown, McCallum, ISSAC'05): when does $p(z) = z^3 + az + b$ have a non-real root $x + iy$ satisfying $xy < 1$.

The equivalent quantifier elimination problem

$(\exists x \in \mathbb{R})(\exists y \in \mathbb{R})[f = g = 0 \wedge y \neq 0 \wedge xy - 1 < 0]$, where

- $f = \mathrm{Re}(p(x + iy)) = x^3 - 3xy^2 + ax + b$
- $g = \mathrm{Im}(p(x + i))/y = 3x^2 - y^2 + a$

The semi-algebraic system to solve

$$\mathcal{S} := \begin{cases} f = 0, \\ g = 0, \\ y \neq 0, \\ xy - 1 < 0 \end{cases}$$

A lazy triangular decomposition

The command LazyRealTriangularize($[f, g, y \neq 0, xy-1 < 0], [y, x, b, a]$) returns the following:

$$\begin{cases} [\{t_1 = 0, t_2 = 0, 1 - xy > 0\}] & h_1 > 0, h_2 \neq 0 \\ \%\mathtt{LazyRealTriangularize}([t_1 = 0, t_2 = 0, f = 0, \\ h_1 = 0, 1 - xy > 0, y \neq 0], [y, x, b, a]) & h_1 = 0 \\ \%\mathtt{LazyRealTriangularize}([t_1 = 0, t_2 = 0, f = 0, \\ h_2 = 0, 1 - xy > 0, y \neq 0], [y, x, b, a]) & h_2 = 0 \\ [\,] & \text{otherwise} \end{cases}$$

where

$$t_1 = 8x^3 + 2ax - b, t_2 = 3x^2 - y^2 + a,$$
$$h_1 = 4a^3 + 27b^2,$$
$$h_2 = -4a^3b^2 - 27b^4 + 16a^4 + 512a^2 + 4096.$$

A full triangular decomposition

Evaluate the output with the `value` command, which yields

$$\begin{cases} [\{t_1 = 0, t_2 = 0, 1 - xy > 0\}] & h_1 > 0, h_2 \neq 0 \\ [\,] & h_1 = 0 \\ [\{t_3 = 0, t_4 = 0, h_2 = 0\}] & h_2 = 0 \\ [\,] & \text{otherwise} \end{cases}$$

where

$$\begin{aligned} t_3 &= (2a^3 + 32a + 18b^2)x - a^2 b - 48b \\ t_4 &= xy + 1 \\ h_1 &= 4a^3 + 27b^2, \\ h_2 &= -4a^3 b^2 - 27b^4 + 16a^4 + 512a^2 + 4096 \end{aligned}$$

Plan

Outline of the algorithm

Definition

Let $[T, P]$ be as before and $B \subset \mathbb{Q}[\mathbf{u}]$. We say that $[B_{\neq}, T, P_{>}]$ is a pre-regular semi-algebraic system of $\mathbb{Q}[\mathbf{u}, \mathbf{y}]$ if $[T, P]$ specializes well at every point of $B(\mathbf{u}) \neq 0$.

Computation in complex space

$$Z_{\mathbb{R}}(F, N_{\geq}, P_{>}, H_{\neq})$$
$$\downarrow$$
$$\bigcup Z_{\mathbb{R}}(B_{\neq}, T, P_{>})$$

Computation in real space

$$[B_{\neq}, T, P_{>}]$$
$$\downarrow$$
$$\mathcal{Q} := \exists \mathbf{y}\,(B(\mathbf{u}) \neq 0,\, T(\mathbf{u}, \mathbf{y}) = 0,\, P(\mathbf{u}, \mathbf{y}) > 0)$$
$$\downarrow$$
$$\text{output } [\mathcal{Q}, T, P_{>}], \text{ where } \mathcal{Q} \neq \text{false}$$

Fingerprint polynomial set

Definition

Let $R := [B_{\neq}, T, P_{>}]$. Let $D \subset \mathbb{Q}[\mathbf{u}]$. Let dp and b be the product of D and B. We call D a *fingerprint polynomial set* (FPS) of R if:

(*i*) for all $\alpha \in \mathbb{R}^d$, $b \in B$: $dp(\alpha) \neq 0 \quad \Rightarrow \quad b(\alpha) \neq 0$,

(*ii*) for all $\alpha, \beta \in \mathbb{R}^d$ with $\alpha \neq \beta$ and $dp(\alpha) \neq 0$, $dp(\beta) \neq 0$, if for $p \in D$, $\mathrm{sign}(p(\alpha)) = \mathrm{sign}(p(\beta))$, then $R(\alpha)$ has real solutions iff $R(\beta)$ does.

Open projection operator (Brown-McCalumn operator)

Let A be a squarefree basis in $\mathbb{Q}[u_1 < \cdots < u_d]$. Define

$$\mathrm{oproj}(A, u_d) := \bigcup_{f \in A} \mathrm{lc}(f, u_d) \cup \bigcup_{f \in A} \mathrm{discrim}(f, u_d) \cup \bigcup_{f,g \in A} \mathrm{res}(f, g, u_d).$$

Theorem

For $A \subset \mathbb{Q}[u_1, \ldots, u_d]$, *let* $\mathrm{oaf}(A) = \mathrm{der}(A, u_d) \cup \mathrm{oaf}(\mathrm{oproj}(\mathrm{der}(A, u_d), u_{d-1}))$. *If* $R := [B_{\neq}, T, P_{>}]$ *is a PRSAS, then,* $\mathrm{oaf}(B)$ *is a fingerprint polynomial*

Fingerprint polynomial set

Definition

Let $R := [B_{\neq}, T, P_{>}]$. Let $D \subset \mathbb{Q}[\mathbf{u}]$. Let dp and b be the product of D and B. We call D a *fingerprint polynomial set* (FPS) of R if:

(i) for all $\alpha \in \mathbb{R}^d$, $b \in B$: $dp(\alpha) \neq 0 \quad \Rightarrow \quad b(\alpha) \neq 0$,

(ii) for all $\alpha, \beta \in \mathbb{R}^d$ with $\alpha \neq \beta$ and $dp(\alpha) \neq 0$, $dp(\beta) \neq 0$, if for $p \in D$, $\mathrm{sign}(p(\alpha)) = \mathrm{sign}(p(\beta))$, then $R(\alpha)$ has real solutions iff $R(\beta)$ does.

Open projection operator (Brown-McCalumn operator)

Let A be a squarefree basis in $\mathbb{Q}[u_1 < \cdots < u_d]$. Define

$$\mathrm{oproj}(A, u_d) := \bigcup_{f \in A} \mathrm{lc}(f, u_d) \cup \bigcup_{f \in A} \mathrm{discrim}(f, u_d) \cup \bigcup_{f,g \in A} \mathrm{res}(f, g, u_d).$$

Theorem

For $A \subset \mathbb{Q}[u_1, \ldots, u_d]$, *let* $\mathrm{oaf}(A) = \mathrm{der}(A, u_d) \cup \mathrm{oaf}(\mathrm{oproj}(\mathrm{der}(A, u_d), u_{d-1}))$. *If* $R := [B_{\neq}, T, P_{>}]$ *is a PRSAS, then,* $\mathrm{oaf}(B)$ *is a fingerprint polynomial*

A detailed example (1/3)

Applications Places System moreno

/home/moreno/src/Talks/ApplMath-UWO-2011/bp-fps.mw* - [Server 1] - Maple 14

nat Table Drawing Plot Spreadsheet Tools Window Help

RealRootIsolate, RefineBox, RefineListBox, RemoveRedundantComponents, RepresentingBox, RepresentingChain, RepresentingQuantifierFreeFormula, RepresentingRootIndex, VariableOrdering]

```
> F := [x^2+y+a, y^2+b*x+a];
```

$$F := [y + x^2 + a,\ y^2 + b\,x + a]$$

```
> R := PolynomialRing([y, x, b, a]);
```

$$R := polynomial\_ring$$

```
> dec := Triangularize(F, R);
  rc := dec[1];
```

$$dec := [regular\_chain]$$

$$rc := regular\_chain$$

```
> Display(rc, R);
```

$$\begin{cases} y + x^2 + a = 0 \\ x^4 + 2\,a\,x^2 + b\,x + a^2 + a = 0 \end{cases}$$

```
> rceqs := Info(rc, R);
```

$$rceqs := [y + x^2 + a,\ x^4 + 2\,a\,x^2 + b\,x + a^2 + a]$$

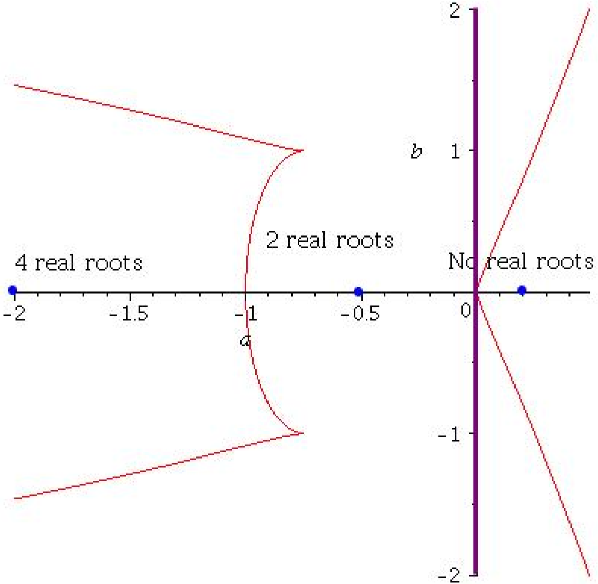
```
> bp := discrim(rceqs[2],x);
```

$$bp := 256\,b^2\,a^3 - 27\,b^4 + 288\,b^2\,a^2 + 256\,a^4 + 256\,a^3$$

```
> with(plots);
```

[*animate, animate3d, animatecurve, arrow, changecoords, complexplot, complexplot3d, conformal,*

A detailed example (2/3)



A detailed example (3/3)

Applications Places System moreno Fri 4 Feb,

Format Table Drawing Plot Spreadsheet Tools Window Help

polynomial_ring

$$[x^2+y+a,\ y^2+b\,x+a]$$

$dec := Triangularize(F, R) : rc := dec[1] : Display(rc, R);$

$$\begin{cases} y+x^2+a=0 \\ x^4+2\,a\,x^2+b\,x+a^2+a=0 \end{cases}$$

$LazyRealTriangularize(F, R, output = record);$

$$\left[\begin{cases} y+x^2+a=0 \\ x^4+2\,a\,x^2+b\,x+a^2+a=0 \\ 256\,b^2\,a^3-27\,b^4+288\,b^2\,a^2+256\,a^4+256\,a^3<0 \\ a\neq 0 \end{cases},\ \begin{cases} y+x^2+a=0 \\ x^4+2\,a\,x^2+b\,x+a^2+a=0 \\ 256\,b^2\,a^3-27\,b^4+288\,b^2\,a^2+256\,a^4+256\,a^3>0 \\ a<0 \end{cases}\right.,$$

$\%LazyRealTriangularize\big([a=0, y+x^2+a=0, y^2+b\,x+a=0, x^4+2\,a\,x^2+b\,x+a^2+a=0], polynomial\_ring, output = record\big),$
$\%LazyRealTriangularize\big([y+x^2+a=0, y^2+b\,x+a=0, 256\,b^2\,a^3-27\,b^4+288\,b^2\,a^2+256\,a^4+256\,a^3=0, x^4+2\,a\,x^2+b\,x+a^2+a=0], polynomial\_ring, output = record\big)$

Plan

LazyRealTriangularize for a system of equations

Algorithm 1: LazyRealTriangularize($\mathcal{S}$)

Input: a semi-algebraic system $\mathcal{S} = [F, \emptyset, \emptyset, \emptyset]$
Output: a lazy triangular decomposition of $\mathcal{S}$

$\mathcal{T} :=$ Triangularize(F)
for $T_i \in \mathcal{T}$ **do**
  $Bp_i :=$ BorderPolynomial($T_i, \emptyset$)
  solve $\exists \mathbf{y}(Bp_i(\mathbf{u}) \neq 0, T_i(\mathbf{u}, \mathbf{y}) = 0)$,
  and let $\mathcal{Q}_i$ be the resulting quantifier-free formula
  if $\mathcal{Q}_i \neq$ *false* **then** output $[\mathcal{Q}_i, T_i, \emptyset]$

Complexity results (1/2)

Assumptions

($\mathbf{H_0}$) $V(F)$ is equidimensional of dimension d,

($\mathbf{H_1}$) $x_1, \ldots, x_d$ are algebraically independent modulo each associated prime ideal of the ideal generated by F in $\mathbb{Q}[\mathbf{x}]$,

($\mathbf{H_2}$) F consists of $m := n - d$ polynomials, $f_1, \ldots, f_m$.

Geometrical formulation

Hypotheses ($\mathbf{H_0}$) and ($\mathbf{H_1}$) are equivalent to the existence of regular chains $T_1, \ldots, T_e$ of $\mathbb{Q}[x_1, \ldots, x_n]$ such that

- $x_1, \ldots, x_d$ are free w.r.t. each T_i
- $V(F) = V(\mathrm{sat}(T_1)) \cup \ldots \cup V(\mathrm{sat}(T_e))$.

Complexity results (2/2)

Notation

Let n, m, δ, $\hbar$ be respectively the number of variables, number of polynomials, maximum total degree and height of polynomials in F.

Proposition

Within $m^{O(1)}(\delta^{O(n^2)})^{d+1} + \delta^{O(m^4)O(n)}$ operations in $\mathbb{Q}$, one can compute a Kalkbrener triangular decomposition $E_1, \ldots, E_e$ of $V(F)$, where each polynomial of each E_i

- has total degree upper bounded by $O(\delta^{2m})$,
- has height upper bounded by $O(\delta^{2m}(m\hbar + dm\log(\delta) + n\log(n)))$.

From which, a lazy triangular decomposition of F can be computed in $\left(\delta^{n^2} n 4^n\right)^{O(n^2)} \hbar^{O(1)}$ bit operations.

Plan

Notations

Table 1 Notions for Tables 2 and 3

symbol	meaning
#e	number of equations in the system
#v	number of variables in the equations
d	max total degree of the equations
G	Groebner:-Basis (with plex order) in MAPLE 13
T	Triangularize in REGULARCHAINS library of MAPLE
LR	lazy RealTriangularize implemented in MAPLE
R	complete RealTriangularize implemented in MAPLE
Q	QEPCAD B
$> 1h$	the examples cannot be solved in 1 hour
FAIL	QEPCAD B failed due to prime list exhausted

Timings for algebraic varieties

Table 2 Timings for algebraic varieties

system	#v/#e/d	G	T	LR
Hairer-2-BGK	13/ 11/ 4	25	1.924	2.396
Collins-jsc02	5/ 4/ 3	876	0.296	0.820
Leykin-1	8/ 6/ 4	103	3.684	3.924
8-3-config-Li	12/ 7/ 2	109	5.440	6.360
Lichtblau	3/ 2/ 11	126	1.548	11
Cinquin-3-3	4/ 3/ 4	64	0.744	2.016
Cinquin-3-4	4/ 3/ 5	$> 1h$	10	22
DonatiTraverso-rev	4/ 3/ 8	154	7.100	7.548
Cheaters-homotopy-1	7/ 3/ 7	3527	174	$> 1h$
hereman-8.8	8/ 6/ 6	$> 1h$	33	62
L	12/ 4/ 3	$> 1h$	0.468	0.676
dgp6	17/19/ 2	27	60	63
dgp29	5/ 4/ 15	84	0.008	0.016

Timings for semi-algebraic systems

Table 3 Timings for semi-algebraic systems

system	#v/#e/d	T	LR	R	Q
BM05-1	4/ 2/ 3	0.008	0.208	0.568	86
BM05-2	4/ 2/ 4	0.040	2.284	$> 1h$	FAIL
Solotareff-4b	5/ 4/ 3	0.640	2.248	924	$> 1h$
Solotareff-4a	5/ 4/ 3	0.424	1.228	8.216	FAIL
putnam	6/ 4/ 2	0.044	0.108	0.948	$> 1h$
MPV89	6/ 3/ 4	0.016	0.496	2.544	$> 1h$
IBVP	8/ 5/ 2	0.272	0.560	12	$> 1h$
Lafferriere37	3/ 3/ 4	0.056	0.184	0.180	10
Xia	6/ 3/ 4	0.164	2.192	230.198	$> 1h$
SEIT	11/ 4/3	0.400	33.914	$> 1h$	$> 1h$
p3p-isosceles	7/ 3/ 3	1.348	$> 1h$	$> 1h$	$> 1h$
p3p	8/ 3/ 3	210	$> 1h$	$> 1h$	FAIL
Ellipse	6/ 1/ 3	0.012	0.904	$> 1h$	$> 1h$

Plan

Conclusion

- We have proposed adaptations of the notions of regular chains and triangular decompositions in order to solve semi-algebraic systems symbolically.
- We have shown that any such system can be decomposed into finitely many *regular semi-algebraic systems*.
- We propose two specifications of such a decomposition and present corresponding algorithms:
- Under some assumptions, one type of decomposition (`LazyRealTriangularize`) can be computed in singly exponential time w.r.t. the number of variables.
- We have implemented both types of decompositions and reported on comparative benchmarks.
- Our experimental results suggest that these approaches are promising.

Work in progress

- We have obtained geometrical invariants for the notion of border polynomial.
- We have improved the performances of our algorithms by avoiding unnecessary recursive calls
- We have developed an incremental algorithms for decomposing semi-algebraic systems
- We have procedures for performing set theoretical operations on semi-algebraic sets.
- As a consequence we can produce decomposition free of redundant components.

Thank you!

Plan

Laurent's model for the mad cow disease (1/4)

The dynamical system ruling the transformation

The normal form PrP^C is harmless, while the infectious form PrP^{S_c} catalyzes a transformation from the normal form to the infectious one.

$$\begin{cases} \frac{\mathrm{d}x}{\mathrm{d}t} & = & k_1 - k_2 x - a x \frac{(1+by^n)}{1+cy^n} \\ \frac{\mathrm{d}y}{\mathrm{d}t} & = & a x \frac{(1+by^n)}{1+cy^n} - k_4 y \end{cases}$$

where $x = \left[PrP^C\right]$, $y = \left[PrP^{S_c}\right]$ and where b, c, n, a, k_4, k_1 are biological constants which can be set as follows:

$$b = 2, \quad c = 1/20, \quad n = 4, \quad a = 1/10, \quad k_4 = 50 \ \text{ and } \ k_1 = 800.$$

The dynamical system to study

$$\begin{cases} \frac{\mathrm{d}x}{\mathrm{d}t} & = & \frac{16000+800y^4-20k_2x-k_2xy^4-2x-4xy^4}{20+y^4} \\ \frac{\mathrm{d}y}{\mathrm{d}t} & = & \frac{2(x+2xy^4-500y-25y^5)}{20+y^4} \end{cases}$$

Laurent's model for the mad cow disease (2/4)

The semi-algebraic system to be solved

$$\mathcal{S} := \begin{cases} 16000 + 800y^4 - 20k_2x - k_2xy^4 - 2x - 4xy^4 & = & 0 \\ 2(x + 2xy^4 - 500y - 25y^5) & = & 0 \\ k_2 & > & 0 \end{cases}$$

Computations (1/5)

LazyRealTriangularize to this system, yields the following regular semi-algebraic system (and unevaluated recursive calls)

$$\begin{cases} (2y^4 + 1)x - 500y - 25y^5 = 0 \\ (k_2 + 4)y^5 - 64y^4 + (20k_2 + 2)y - 32 = 0 \\ (k_2 > 0) \ \wedge \ (R_1 \neq 0) \end{cases}$$

where

$$R_1 = 100000k_2^8 + 1250000k_2^7 + 5410000k_2^6 + 8921000k_2^5 - 9161219950k_2^4 - 5038824999k_2^3 - 1665203348k_2^2 - 882897744k_2 + 1099528405056.$$

Laurent's model for the mad cow disease (3/4)

Computations (2/5)

Through the computation of sample points, we easily obtain the following observation. Whenever $R_1 > 0$ holds, the system has 1 equilibrium, while $R_2 < 0$ implies that the system has 3 equilibria.

Computations (3/5)

Now we study the stability of those equilibria. To this end, we consider the two Hurwitz determinants.
Adding to $\mathcal{S}$ the constraints $\{\Delta_1 > 0, a_2 > 0\}$

$$\Delta_1 = 54y^8 + 40k_2y^4 + 2082y^4 - 312xy^3 + 20040 + k_2y^8 + 400k_2,$$
$$a_2 = 20000k_2 + 2000 + 50k_2y^8 + 200y^8 + 2000k_2y^4 - 312k_2xy^3 + 4100y^4.$$

we obtain a new semi-algebraic system $\mathcal{S}'$.

Laurent's model for the mad cow disease (4/4)

Computations (4/5)

Applying LazyRealTriangularize to $\mathcal{S}'$ in conjunction with sample point computations brings the following conclusion. If $R_1 > 0$, then the system has 1 asymptotically stable hyperbolic equilibria.

Computations (5/5)

If $R_1 < 0$ and $R_2 \neq 0$, then System has 2 asymptotically equilibria, where R_2 is given by:

$$R_2 = 10004737927168k_2^9 + 624166300700672k_2^8 + 7000539052537600k_2^7$$
$$+ 45135589467012800k_2^6 - 840351411856453750k_2^5 - 5009800435224844687 5k_2^4$$
$$- 2738816898945500000 0k_2^3 - 8675209266696000000k_2^2$$
$$+ 1029609173568000000 0k_2 + 5932546064102400000 0.$$

To further investigate the number of asymptotically stable hyperbolic equilibria on the hypersurface $R_2 = 0$ and the equilibria when $R_1 = 0$, one can apply SamplePoints on $\mathcal{S}'$, which produces 14 points.

Program verification: an example from Lafferriere (1/4)

Reachability computation

This problem reduces to determine the set

$$\{(y_1, y_2) \in \mathbb{R}^2 \mid (\exists a \in \mathbb{R})(\exists z \in \mathbb{R})\,(0 \le a) \wedge (z \ge 1) \wedge (h_1 = 0) \wedge (h_2 = 0)\}$$

where

$$h_1 = 3\,y_1 - 2\,a(-z^4 + z) \ \ \text{and} \ \ h_2 = 2\,y_2 z^2 - a(z^4 - 1).$$

The semi-algebraic system to be solved

One wishes to compute the projection of the semi-algebraic set defined by

$$(0 \le a) \wedge (z \ge 1) \wedge (h_1 = 0) \wedge (h_2 = 0)$$

onto the (y_1, y_2)-plane.
For the variable ordering $a > z > y_1 > y_2$. we obtain the five following regular semi-algebraic systems R_1 to R_5

Program verification: an example from Lafferriere (2/4)

The triangular decomposition (1/3)

$$R_2^T = \begin{cases} a \\ y_1 \\ y_2 \end{cases} \qquad R_2^P = \{\ z > 1$$

$$R_3^T = \begin{cases} z-1 \\ y_1 \\ y_2 \end{cases} \qquad R_3^P = \{\ 0 < a$$

$$R_4^T = \begin{cases} a \\ z-1 \\ y_1 \\ y_2 \end{cases}$$

The projection on the (y_1, y_2)-plane of $Z_{\mathbb{R}}(R_2) \cup Z_{\mathbb{R}}(R_3) \cup Z_{\mathbb{R}}(R_4)$ is clearly equal to the $(y_1, y_2) = (0, 0)$ point.

Program verification: an example from Lafferriere (3/4)

The triangular decomposition (2/3)

$$R_1^T = \begin{cases} (z^4 - 1)\, a - 2\, z^2 y_2 \\ 4\, y_2\, z^5 + 4\, y_2\, z^4 + (3\, y_1 + 4\, y_2)\, z^3 + 3\, y_1\, z^2 + 3\, y_1\, z + 3\, y_1 \end{cases}$$

$$R_1^{\mathcal{Q}} = \begin{cases} (y_1 + y_2 < 0) \wedge (y_1 < 0) \wedge (0 < y_2) \\ 3y_1^5 - 6y_2y_1^4 - 63y_2^2y_1^3 + 192y_2^3y_1^2 + 112y_2^4y_1 + 16y_2^5 \neq 0 \end{cases}$$

$$R_1^P = \{\ z > 1$$

The projection on the (y_1, y_2)-plane of $Z_{\mathbb{R}}(R_1)$ is given by $Z_{\mathbb{R}}(R_1^{\mathcal{Q}})$.

Program verification: an example from Lafferriere (4/4)

The triangular decomposition (3/3)

$$R_5^T = \begin{cases} (z^4 - 1)\, a - 2\, z^2 y_2 \\ t_z \\ 3\, {y_1}^5 - 6\, y_2\, {y_1}^4 - 63\, {y_2}^2 {y_1}^3 + 192\, {y_2}^3 {y_1}^2 + 112\, {y_2}^4 y_1 + 16\, {y_2}^5 \end{cases}$$

$$R_5^Q = \{\ 0 < y_2 \qquad R_5^P = \{\ z > 1$$

where t_z is a large polynomial of degree 4 in z.
The polynomial with main variable y_1, say t_{y_1} is delineable above $0 < y_2$.
Using a sample point we check that t_{y_1} admits a single real root.

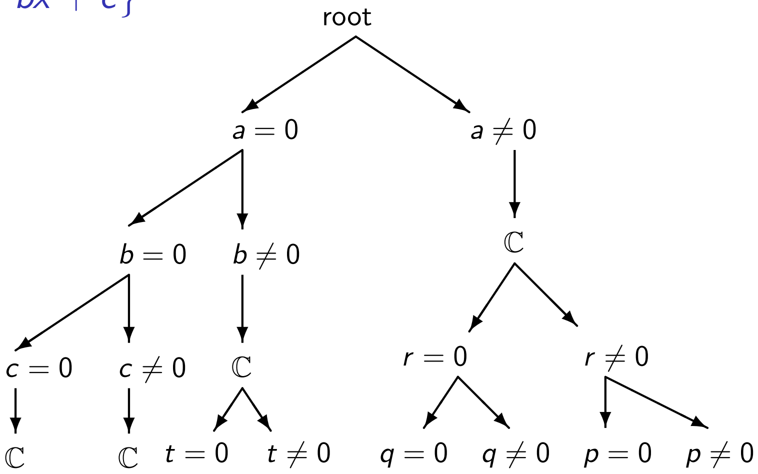
Conclusion

It follows that the projection on the (y_1, y_2)-plane of $Z_{\mathbb{R}}(R_5)$ is given by:

$$(0 < y_2) \wedge (3\, {y_1}^5 - 6\, y_2\, {y_1}^4 - 63\, {y_2}^2 {y_1}^3 + 192\, {y_2}^3 {y_1}^2 + 112\, {y_2}^4 y_1 + 16\, {y_2}^5).$$

Plan

Recall: cylindrical algebraic decomposition of $\{ax^2 + bx + c\}$



The cylindrical algebraic decomposition of $\{ax^2 + bx + c\}$ is given by the tree above, where $t = bx + c$, $q = 2ax + b$, and $r = 4ac - b^2$. This is the best possible output for that method.

Cylindrical algebraic decomposition of $\mathbb{R}^n$ (1/2)

Definition

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 $(x_1, \ldots, x_j)$ of any two cells are either identical or disjoint.
- each cell is a connected semi-algebraic subset, called a region

Complexity of CAD

Unfortunately the number of cells can be **doubly exponential** in n.

Case of $n = 1$

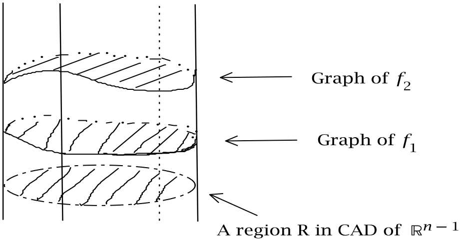
This is a finite partition of the real line into points and open intervals.

Cylindrical algebraic decomposition of $\mathbb{R}^n$ (2/2)

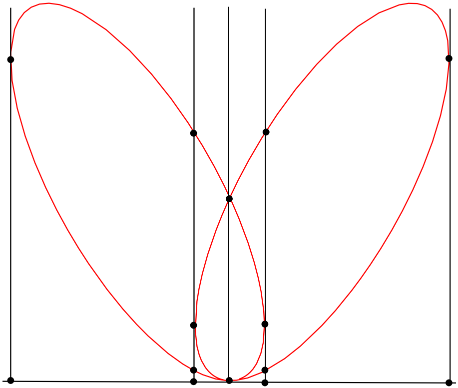
Case of $n > 1$

From a CAD D' of $\mathbb{R}^{n-1}$, one builds a CAD D of $\mathbb{R}^n$. Above each $R \in D'$:

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

RealTriangularize applied to the Tacnode Curve

```
> R := PolynomialRing([x,y]);
> F := [y^4-2*y^3+y^2-3*x^2*y+2*x^4];
> RealTriangularize(F, R, output=record);
{    4        2    4      3    2
{ 2 x  - 3 y x  + y  - 2 y  + y  = 0
{
{              0 < y                             { x = 0
{                                              , {                 ,
{            y - 1 <> 0                          { y = 0
{
{            2
{        8 y  - 16 y < 1

    {   x = 0               {    2
    {                     , { 2 x  - 3 = 0         ,
    { y - 1 = 0             {
                            {   y - 1 = 0

    {        2
    { 32 y x  - 48 y - 3 = 0
    {
    {      2
    {  8 y  - 16 y - 1 = 0
```