# The Symbolic Computation group

April 15$^{th}$, 2009

# Overview

1. What is Symbolic Computation? (D. Sevilla)
2. Application of Symbolic Computation to Robotics (B. Moore)
3. Symbolic Computation for boundary problems (G. Regensburger)

# What is Symbolic Computation?

Symbolic computation:

# What is Symbolic Computation?

Symbolic computation:

. . . computation with symbols?

# What is Symbolic Computation?

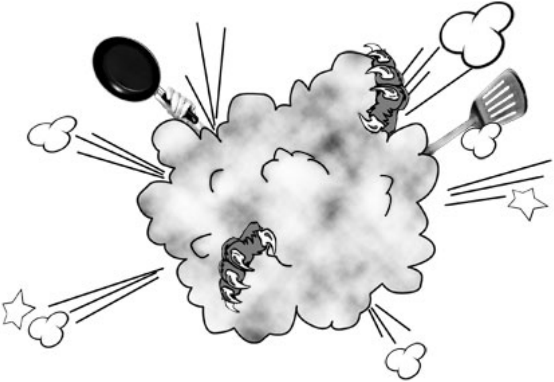
Symbolic computation:

... computation with symbols?

$$333049652 \cdot 34745674584 = \square$$

# Group discussion

Figure: SC group trying to define “Symbolic Computation”



# Symbolic Computation by example

> "Symbolic Computation is defined not so much by problems, but by the way we approach problems."

> "Solve (parametric) classes of problems rather than problems, and study the (algebraic) structures and algorithms involved in this."

We will try to give a flavour of Symbolic Computation by means of examples.

# Parameters and classes of problems

**Problem**

Solve $x^2 - 4x + 3 = 0$.

# Parameters and classes of problems

**Problem**

Solve $x^2 - 4x + 3 = 0$.

**Solution**

Brute force; complete the square.

# Parameters and classes of problems

**Problem**

Solve $x^2 - 4x + 3 = 0$.

**Solution**

Brute force; complete the square.

**Problem**

Solve $ax^2 + bx + c = 0$.

# Parameters and classes of problems

**Problem**

Solve $x^2 - 4x + 3 = 0$.

**Solution**

Brute force; complete the square.

**Problem**

Solve $ax^2 + bx + c = 0$.

**Solution**

Complete the square; use the formula.

# Parameters and classes of problems

**Problem**

Solve $x^2 - 4x + 3 = 0$.

**Solution**

Brute force; complete the square.

**Problem**

Solve $ax^2 + bx + c = 0$.

**Solution**

Complete the square; use the formula.

**Problem**

Solve any polynomial equation.

# Parameters and classes of problems

**Problem**

Solve $x^2 - 4x + 3 = 0$.

**Solution**

Brute force; complete the square.

**Problem**

Solve $ax^2 + bx + c = 0$.

**Solution**

Complete the square; use the formula.

**Problem**

Solve any polynomial equation.

**Solution**

Algebra $\rightarrow$ not always explicit formula

- Numeric flavour: approximation, intervals, etc.
- Symbolic flavour: algorithm to decide expressibility by radicals
  - ✓ Yes: compute
  - ✓ No: $x = \alpha \rightarrow \ldots$

# System of polynomial equations

## Problem: polynomial system

Solve the system

$$P_1(x_1, \ldots, x_n) = \cdots = P_m(x_1, \ldots, x_n) = 0$$

where $\quad P_i(x_1, \ldots, x_n) = \sum c_{i,\underline{e}}\, x_1^{e_1} \cdots x_n^{e_n}, \quad i = 1, \ldots, m.$

# System of polynomial equations

## Problem: polynomial system

Solve the system

DECIDE
COUNT
COMPUTE

$$P_1(x_1, \ldots, x_n) = \cdots = P_m(x_1, \ldots, x_n) = 0$$

where $$P_i(x_1, \ldots, x_n) = \sum c_{i,\underline{e}}\, x_1^{e_1} \cdots x_n^{e_n}, \quad i = 1, \ldots, m.$$

# System of polynomial equations

## Problem: polynomial system

Solve the system

DECIDE
COUNT
COMPUTE

$$P_1(x_1, \dots, x_n) = \cdots = P_m(x_1, \dots, x_n) = 0$$

where $P_i(x_1, \dots, x_n) = \sum c_{i,\underline{e}}\, x_1^{e_1} \cdots x_n^{e_n}, \quad i = 1, \dots, m.$

## Simpler problem: inhomogeneous linear system

Solve the system

DECIDE
COUNT
COMPUTE

$$P_1(x_1, \dots, x_n) = \cdots = P_m(x_1, \dots, x_n) = 0$$

where $P_i(x_1, \dots, x_n) = b_i + \sum a_{ij}\, x_j, \quad i = 1, \dots, m.$

# Solution: Gröbner bases

## Solving an inhomogeneous linear system

$$\left(\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array}\right) \leftrightsquigarrow \left(\begin{array}{cccc|c} c_{11} & c_{12} & \cdots & c_{1n} & d_1 \\ 0 & c_{22} & \cdots & c_{2n} & d_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & c_{mn} & d_m \end{array}\right)$$

Gaussian elimination $+$ solve row by row from bottom to top.

# Solution: Gröbner bases

## Solving an inhomogeneous linear system

$$\left(\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array}\right) \leftrightsquigarrow \left(\begin{array}{cccc|c} c_{11} & c_{12} & \cdots & c_{1n} & d_1 \\ 0 & c_{22} & \cdots & c_{2n} & d_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & c_{mn} & d_m \end{array}\right)$$

Gaussian elimination $+$ solve row by row from bottom to top.

## Solving a polynomial system

Gröbner bases computations allow, among other things,

a polynomial version of Gaussian elimination

Disclaimer: can be VERY SLOW to compute!

# Example: Solving a polynomial system

## Example

$$x^2 + y + z = 1$$
$$x + y^2 + z = 1$$
$$x + y + z^2 = 1$$

# Example: Solving a polynomial system

## Example

$$\begin{aligned} x^2 + y + z &= 1 \\ x + y^2 + z &= 1 \\ x + y + z^2 &= 1 \end{aligned}$$

## Elimination step

$$\begin{aligned} x + y + z^2 &= 1 \\ y^2 - y - z^2 + z &= 0 \\ 2yz^2 + z^4 - z^2 &= 0 \\ z^6 - 4z^4 + 4z^3 - z^2 &= 0 \end{aligned}$$

# Example: Solving a polynomial system

## Example

$$\begin{aligned} x^2 + y + z &= 1 \\ x + y^2 + z &= 1 \\ x + y + z^2 &= 1 \end{aligned}$$

## Elimination step

$$\begin{aligned} x + y + z^2 &= 1 & \qquad (x, y, z) \\ y^2 - y - z^2 + z &= 0 & \qquad (y, z) \\ 2yz^2 + z^4 - z^2 &= 0 & \qquad (y, z) \\ z^6 - 4z^4 + 4z^3 - z^2 &= 0 & \qquad (z) \end{aligned}$$

# Example: Solving a polynomial system

## Example

$$
\begin{aligned}
x^2 + y + z &= 1 \\
x + y^2 + z &= 1 \\
x + y + z^2 &= 1
\end{aligned}
$$

## Elimination step

$$
\begin{array}{rrl}
x + y + z^2 = 1 & (x, y, z) & \rightarrow\ x \\
y^2 - y - z^2 + z = 0 & (y, z) & \multirow{2}{*}{$\left.\right\} \rightarrow\ y$} \\
2yz^2 + z^4 - z^2 = 0 & (y, z) & \\
z^6 - 4z^4 + 4z^3 - z^2 = 0 & (z) & \rightarrow\ z
\end{array}
$$

# Example: Solving a polynomial system

## Example

$$
\begin{aligned}
x^2 + y + z &= 1 \\
x + y^2 + z &= 1 \\
x + y + z^2 &= 1
\end{aligned}
$$

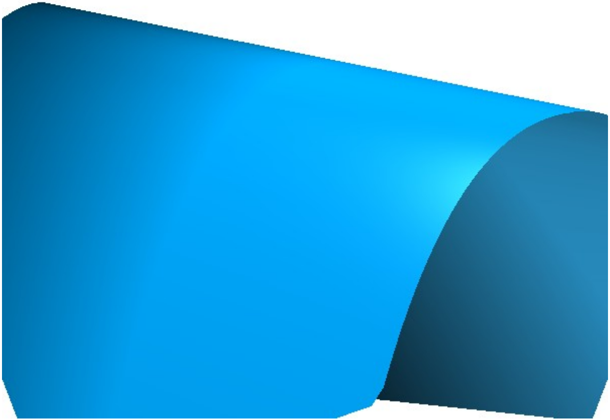
## Elimination step

$$
\begin{array}{rcl}
x + y + z^2 = 1 & (x, y, z) & \rightarrow x \\
y^2 - y - z^2 + z = 0 & (y, z) & \\
2yz^2 + z^4 - z^2 = 0 & (y, z) & \Big\} \rightarrow y \\
z^6 - 4z^4 + 4z^3 - z^2 = 0 & (z) & \rightarrow z
\end{array}
$$

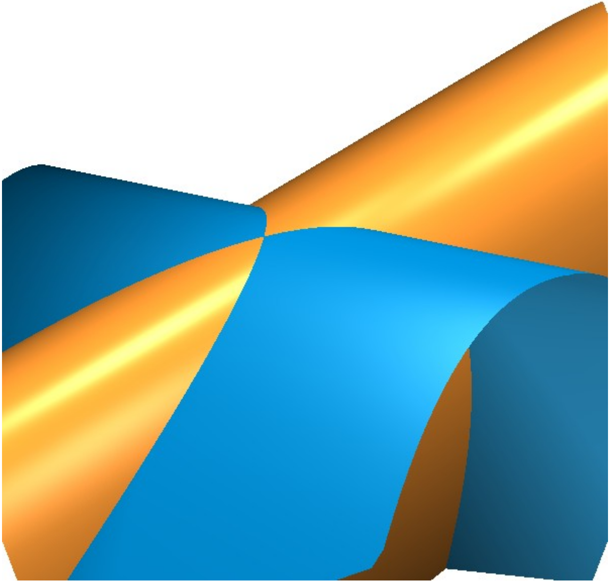
## Solution

$$
(1, 0, 0),\ (0, 1, 0),\ (0, 0, 1),
$$
$$
(-1 \pm \sqrt{2}, -1 \pm \sqrt{2}, -1 \pm \sqrt{2})
$$

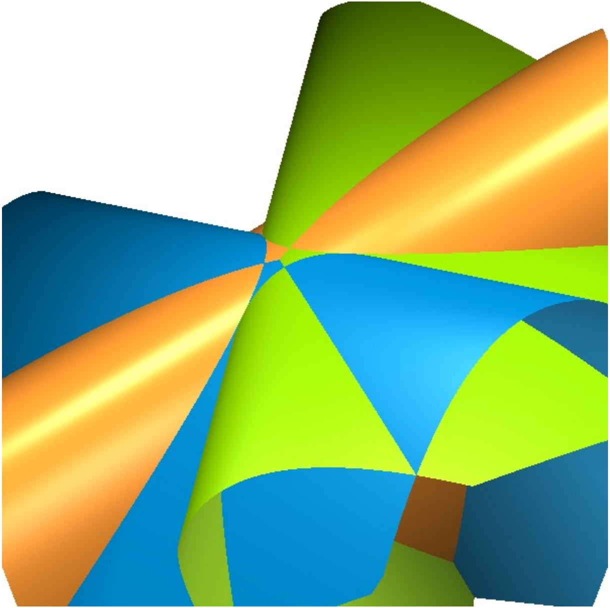
# One surface



# Two surfaces



# Three surfaces



# Dimension of the solution set

## Definition

A set of variables is independent iff all the leading monomials of the Gröbner basis contain variables outside the set.

## Example

$$\begin{aligned} x + y + z^2 &= 1 \\ y^2 - y - z^2 + z &= 0 \\ 2yz^2 + z^4 - z^2 &= 0 \\ z^6 - 4z^4 + 4z^3 - z^2 &= 0 \end{aligned} \qquad \longrightarrow \qquad \varnothing$$

# Dimension of the solution set

## Definition

A set of variables is independent iff all the leading monomials of the Gröbner basis contain variables outside the set.

## Example

$$\begin{aligned} x + y + z^2 &= 1 \\ y^2 - y - z^2 + z &= 0 \\ 2yz^2 + z^4 - z^2 &= 0 \\ z^6 - 4z^4 + 4z^3 - z^2 &= 0 \end{aligned} \quad \rightarrow \quad \varnothing,\ \{z\}$$

# Dimension of the solution set

## Definition

A set of variables is independent iff all the leading monomials of the Gröbner basis contain variables outside the set.

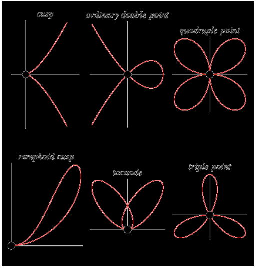
## Example

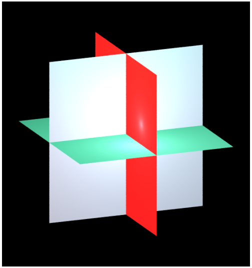
$$\begin{aligned} x + y + z^2 &= 1 \\ y^2 - y - z^2 + z &= 0 \\ 2yz^2 + z^4 - z^2 &= 0 \\ z^6 - 4z^4 + 4z^3 - z^2 &= 0 \end{aligned} \quad \rightarrow \quad \emptyset,\ \{z\}$$

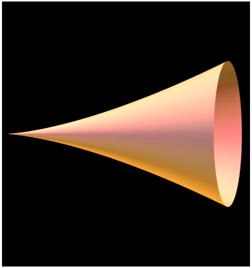
## Theorem

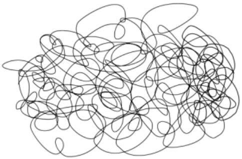
The dimension of the solution set is the maximum of the sizes of sets of independent variables of a Gröbner basis (0-dimensional = finite set)

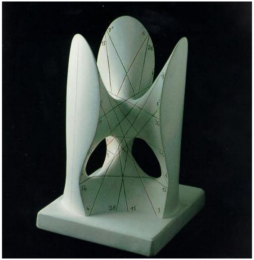
# Algebraic geometry

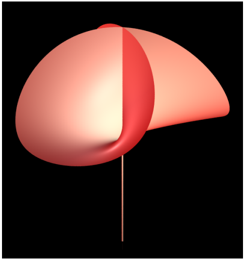




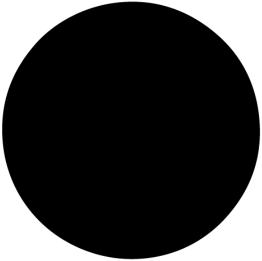


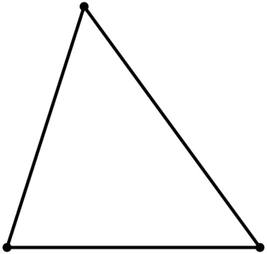


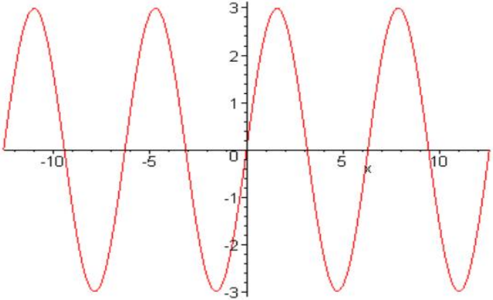


# Algebraic geometry in RICAM

# Non-algebraic sets







# Implicit vs. parametric

## How to represent infinitely many solutions?

The set of $\mathbb{R}^2$ given by $x^2 + y^2 = 1$ is infinite. How to obtain explicitly as many solutions as we want?

# Implicit vs. parametric

## How to represent infinitely many solutions?

The set of $\mathbb{R}^2$ given by $x^2 + y^2 = 1$ is infinite. How to obtain explicitly as many solutions as we want?

$$x^2 + y^2 = 1 \quad \Leftrightarrow^* \quad x = \frac{2t}{t^2+1}, \quad y = \frac{t^2-1}{t^2+1} \quad \text{for some } t \in \mathbb{R}$$

# Implicit vs. parametric

## How to represent infinitely many solutions?

The set of $\mathbb{R}^2$ given by $x^2 + y^2 = 1$ is infinite. How to obtain explicitly as many solutions as we want?

$$x^2 + y^2 = 1 \quad \Leftrightarrow^* \quad x = \frac{2t}{t^2+1}, \quad y = \frac{t^2-1}{t^2+1} \quad \text{for some } t \in \mathbb{R}$$

## Definition: parametrizable

An algebraic set of dimension $d$ is called parametrizable iff it can be written$^*$ as

$$x_1 = u_1(t_1, \ldots, t_d), \ \ldots, \ x_n = u_n(t_1, \ldots, t_d), \quad t_i \in \mathbb{R}$$

where $u_j$ are rational functions.

# Implicit vs. parametric

## How to represent infinitely many solutions?

The set of $\mathbb{R}^2$ given by $x^2 + y^2 = 1$ is infinite. How to obtain explicitly as many solutions as we want?

$$x^2 + y^2 = 1 \quad \Leftrightarrow^* \quad x = \frac{2t}{t^2+1}, \quad y = \frac{t^2-1}{t^2+1} \quad \text{for some } t \in \mathbb{R}$$

## Definition: parametrizable

An algebraic set of dimension $d$ is called parametrizable iff it can be written$^*$ as

$$x_1 = u_1(t_1, \ldots, t_d), \ \ldots, \ x_n = u_n(t_1, \ldots, t_d), \quad t_i \in \mathbb{R}$$

where $u_j$ are rational functions.

## Conversion

- Parametrization $\rightarrow$ equation: “easy” (eliminate the $t_i$)
- Equation $\rightarrow$ parametrization: not so easy!

# Curve parametrization

## The genus of a curve

An algebraic curve has a genus, which is an integer $\geq 0$.

Examples:

- Conics have genus 0.
- Elliptic curves have genus 1.
- Hyperelliptic curves have arbitrarily high genus.

# Curve parametrization

## The genus of a curve

An algebraic curve has a genus, which is an integer $\geq 0$.

Examples:

- Conics have genus 0.
- Elliptic curves have genus 1.
- Hyperelliptic curves have arbitrarily high genus.

## Parametrizability theorem for curves

A curve is parametrizable iff it has genus 0.

(Corollary: most curves are not parametrizable.)

There exist good algorithms to decide and compute this.

# Radical curve parametrization

## Extending the class of parametrizations

Example: the curve $y^2 = x^3 - x$ (an elliptic curve) has genus 1, thus it is not parametrizable.

# Radical curve parametrization

## Extending the class of parametrizations

Example: the curve $y^2 = x^3 - x$ (an elliptic curve) has genus 1, thus it is not parametrizable.

But: $x = t,\ y = \sqrt{t^3 - t}$ parametrizes it. (?)

# Radical curve parametrization

## Extending the class of parametrizations

Example: the curve $y^2 = x^3 - x$ (an elliptic curve) has genus 1, thus it is not parametrizable.

But: $x = t,\ y = \sqrt{t^3 - t}$ parametrizes it. (?)

Remember that "parametrizations" are rational!

# Radical curve parametrization

## Extending the class of parametrizations

Example: the curve $y^2 = x^3 - x$ (an elliptic curve) has genus 1, thus it is not parametrizable.

But: $x = t, \ y = \sqrt{t^3 - t}$ parametrizes it. (?)

Remember that “parametrizations” are rational!

## Radical parametrizations

By allowing just one square root we can parametrize:

- all elliptic (genus 1) curves
- all hyperelliptic curves

## Problem

Given a curve $F(x, y) = 0$, to decide if it admits a radical parametrization, and to compute one in the affirmative case.

# Surface parametrization

## Parametrizability theorem for surfaces

A surface is parametrizable iff its generalized genus is zero.

(Holds only for the complex case, not for the real case.)

## Algorithm

Developed by J. Schicho. Currently being implemented.

Until 2006, the singularity analysis was the main bottleneck. This step is now quite efficient, due to work by former colleague T. Beck.

# Algorithmic real algebraic geometry

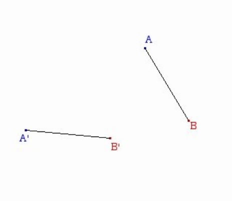
## Definition

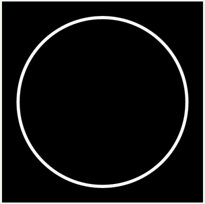
A semialgebraic set is the solution of a semialgebraic system

$$P_1(x_1, \ldots, x_n) \blacksquare 0, \quad \ldots, \quad P_m(x_1, \ldots, x_n) \blacksquare 0$$

where each $\blacksquare$ is one of $=, \neq, <, >, \leqslant, \geqslant$.

## Examples



## Theorem

Semialgebraic sets are closed under finite unions, arbitrary intersections, and complement.

# Quantifier elimination

## Definitions

- A quantifier is one of $\forall, \exists$.
- A quantifier-free formula is an expresion in $\underline{x} = (x_1, \ldots, x_n)$ consisting of polynomial (in)equalities over $\mathbb{R}$, $f_i(\underline{x}) \blacksquare 0$, combined with the Boolean operators $\wedge$ (and), $\vee$ (or) and $\Rightarrow$ (implies).
- A formula is an expression

$$(\blacklozenge\, x_1) \ldots (\blacklozenge\, x_s) \quad \mathcal{F}(f_1(\underline{x}), \ldots, f_r(\underline{x}))$$

  where each $\blacklozenge$ is a quantifier and $\mathcal{F}$ is quantifier-free.
- Each variable is quantified or free.

## Examples

$$(\forall x) \quad [(x \geq 0) \;\Rightarrow\; (x^2 + ax + b \geq 0)]$$

$$(\forall a)\,(\forall \epsilon)\,(\exists \delta)\,(\forall x) \quad [((x \neq a) \wedge ((x-a)^2 < \delta^2)) \;\Rightarrow\; ((x^3 - a^3)^2 < \epsilon^2)]$$

# Quantifier elimination results

## Elimination examples

$$(\exists x) \quad [(ax^2 + bx + c = 0)] \quad \Leftrightarrow \quad [(b^2 - 4ac \geq 0)]$$

# Quantifier elimination results

## Elimination examples

$$(\exists x) \quad [(ax^2 + bx + c = 0)] \quad \Leftrightarrow \quad [(b^2 - 4ac \geq 0) \ \wedge (a \neq 0)]$$

# Quantifier elimination results

## Elimination examples

$$(\exists x) \quad [(ax^2 + bx + c = 0)] \quad \Leftrightarrow \quad \begin{array}{l} [(b^2 - 4ac \geq 0) \;\wedge (a \neq 0)] \\ \vee\; [(a = 0) \wedge (b \neq 0)] \\ \vee\; [(a = 0) \wedge (c = 0)] \end{array}$$

# Quantifier elimination results

## Elimination examples

$$(\exists x) \quad [(ax^2 + bx + c = 0)] \quad \Leftrightarrow \quad [(b^2 - 4ac \geq 0) \ \wedge (a \neq 0)] \vee [(a = 0) \wedge (b \neq 0)] \vee [(a = 0) \wedge (c = 0)]$$

Mathematica : `Resolve`

# Quantifier elimination results

## Elimination examples

$$(\exists x) \quad [(ax^2 + bx + c = 0)] \quad \Leftrightarrow \quad \begin{array}{l} [(b^2 - 4ac \geq 0) \ \wedge (a \neq 0)] \\ \vee \ [(a = 0) \wedge (b \neq 0)] \\ \vee \ [(a = 0) \wedge (c = 0)] \end{array}$$

Mathematica : `Resolve`

## Theorem (Tarski-Seidenberg)

For every first-order formula over the real field there exists an equivalent quantifier-free formula. Furthermore, there is an explicit algorithm to compute this quantifier-free formula.

# Quantifier elimination results

## Elimination examples

$$(\exists x) \quad [(ax^2 + bx + c = 0)] \quad \Leftrightarrow \quad \begin{array}{l} [(b^2 - 4ac \geq 0) \ \wedge (a \neq 0)] \\ \vee \ [(a = 0) \wedge (b \neq 0)] \\ \vee \ [(a = 0) \wedge (c = 0)] \end{array}$$

Mathematica : `Resolve`

## Theorem (Tarski-Seidenberg)

For every first-order formula over the real field there exists an equivalent quantifier-free formula. Furthermore, there is an explicit algorithm to compute this quantifier-free formula.

## Geometric interpretation

The projection of a semialgebraic set is semialgebraic.

# Algebraic structure for differential equations

## Definition: differential algebra

- a field $K$
- a $K$-algebra $A$
  - $x \cdot y = y \cdot x$
  - $x \cdot (y + z) = x \cdot y + x \cdot z$
  - $(cx) \cdot y = c(x \cdot y)$
- a derivation $\partial \colon A \to A$
  - Linear: $\partial(cx) = c(\partial x), \quad \partial(x + y) = \partial x + \partial y$
  - Leibniz rule: $\partial(x \cdot y) = x \cdot \partial y + y \cdot \partial x$

# Algebraic structure for differential equations

## Definition: differential algebra

- a field $K$ (think of $\mathbb{R}$)
- a $K$-algebra $A$ (think of $C^\infty$ functions $\mathbb{R} \to \mathbb{R}$)
  - $x \cdot y = y \cdot x$
  - $x \cdot (y + z) = x \cdot y + x \cdot z$
  - $(cx) \cdot y = c(x \cdot y)$
- a derivation $\partial \colon A \to A$ (think of $dt$)
  - Linear: $\partial(cx) = c(\partial x), \quad \partial(x + y) = \partial x + \partial y$
  - Leibniz rule: $\partial(x \cdot y) = x \cdot \partial y + y \cdot \partial x$

# Elimination in differential equations

## Example: Differential system

$$x' = 0.7y + \sin(2.5z), \quad y' = 1.4x + \cos(2.5z), \quad 1 = x^2 + y^2$$

In order to apply Euler's scheme we need an equation $z' = f(x, y, z)$.

# Elimination in differential equations

## Example: Differential system

$$x' = 0.7y + \underbrace{\sin(2.5z)}_{= s}, \quad y' = 1.4x + \underbrace{\cos(2.5z)}_{= c}, \quad 1 = x^2 + y^2$$

In order to apply Euler's scheme we need an equation $z' = f(x, y, z)$.

## Algebraic differential system

$$\begin{array}{lll} x' = 0.7y + s, & y' = 1.4x + c, & 1 = x^2 + y^2, \\ s' = 2.5z'c, & c' = -2.5z's, & 1 = s^2 + c^2. \end{array}$$

# Elimination in differential equations

## Example: Differential system

$$x' = 0.7y + \underbrace{\sin(2.5z)}_{=s}, \quad y' = 1.4x + \underbrace{\cos(2.5z)}_{=c}, \quad 1 = x^2 + y^2$$

In order to apply Euler's scheme we need an equation $z' = f(x, y, z)$.

## Algebraic differential system

$$\begin{aligned} x' &= 0.7y + s, & y' &= 1.4x + c, & 1 &= x^2 + y^2, \\ s' &= 2.5z'c, & c' &= -2.5z's, & 1 &= s^2 + c^2. \end{aligned}$$

## Elimination step

$$z' = \frac{3500 - 12348y^6 + 13230cxy^4 + 25809y^4 - 14700xy^2c - \cdots}{25\,(441y^6 - 882y^4 + 541y^2 - 100)}$$