Decidability of the Reachability for a Family of Linear Vector Fields

Ting Gan[1], Mingshuai Chen[2], Liyun Dai[1], Bican Xia[1], and Naijun Zhan[2]

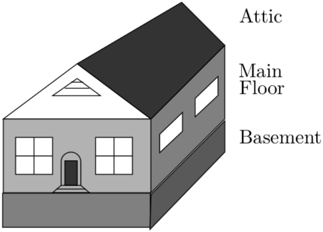
[1] LMAM & School of Mathematical Sciences, Peking University
[2] State Key Lab. of Computer Science, Institute of Software, Chinese Academy of Sciences

Shanghai, October 2015

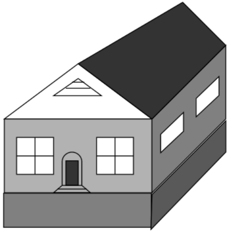
Outline

Example : Home Heating

Example : Home Heating

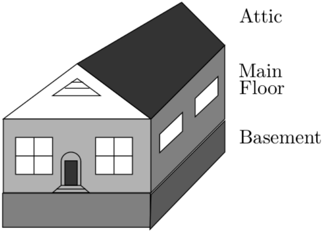


Example : Home Heating



$x_3(t)$ = Temperature in the attic,
$x_2(t)$ = Temperature in the living area,
$x_1(t)$ = Temperature in the basement,
t = Time in hours.

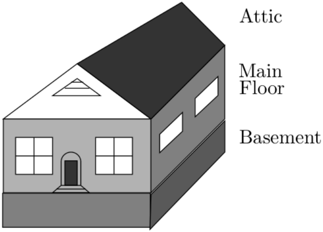
Example : Home Heating



$x_3(t)$ = Temperature in the attic,
$x_2(t)$ = Temperature in the living area,
$x_1(t)$ = Temperature in the basement,
t = Time in hours.

$$
\begin{aligned}
\dot{x}_1 &= \frac{1}{2}(45 - x_1) + \frac{1}{2}(x_2 - x_1),\\
\dot{x}_2 &= \frac{1}{2}(x_1 - x_2) + \frac{1}{4}(35 - x_2) + \frac{1}{4}(x_3 - x_2) + 20,\\
\dot{x}_3 &= \frac{1}{4}(x_2 - x_3) + \frac{3}{4}(35 - x_3),
\end{aligned}
$$

Example : Home Heating



$x_3(t)$ = Temperature in the attic,
$x_2(t)$ = Temperature in the living area,
$x_1(t)$ = Temperature in the basement,
t = Time in hours.

$$\begin{aligned}
\dot{x}_1 &= \frac{1}{2}(45 - x_1) + \frac{1}{2}(x_2 - x_1),\\
\dot{x}_2 &= \frac{1}{2}(x_1 - x_2) + \frac{1}{4}(35 - x_2) + \frac{1}{4}(x_3 - x_2) + 20,\\
\dot{x}_3 &= \frac{1}{4}(x_2 - x_3) + \frac{3}{4}(35 - x_3),
\end{aligned}$$

with the initial set $\mathrm{X} = \{(x_1, x_2, x_3)^T \mid 1 - (x_1 - 45)^2 - (x_2 - 35)^2 - (x_3 - 35)^2 > 0\}$.

Example : Home Heating

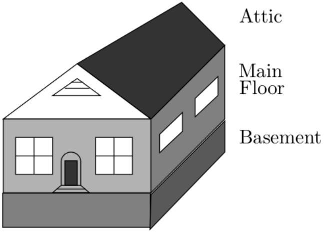
$x_3(t)$ = Temperature in the attic,
$x_2(t)$ = Temperature in the living area,
$x_1(t)$ = Temperature in the basement,
t = Time in hours.

$$\begin{aligned}
\dot{x_1} &= \frac{1}{2}(45 - x_1) + \frac{1}{2}(x_2 - x_1), \\
\dot{x_2} &= \frac{1}{2}(x_1 - x_2) + \frac{1}{4}(35 - x_2) + \frac{1}{4}(x_3 - x_2) + 20, \\
\dot{x_3} &= \frac{1}{4}(x_2 - x_3) + \frac{3}{4}(35 - x_3),
\end{aligned}$$

with the initial set $\mathrm{X} = \{(x_1, x_2, x_3)^T \mid 1 - (x_1 - 45)^2 - (x_2 - 35)^2 - (x_3 - 35)^2 > 0\}$.

Is it possible for the temperature x_2 getting over than $70^\circ F$ (unsafe) ?

Example : Home Heating



$x_3(t)$ = Temperature in the attic,
$x_2(t)$ = Temperature in the living area,
$x_1(t)$ = Temperature in the basement,
t = Time in hours.

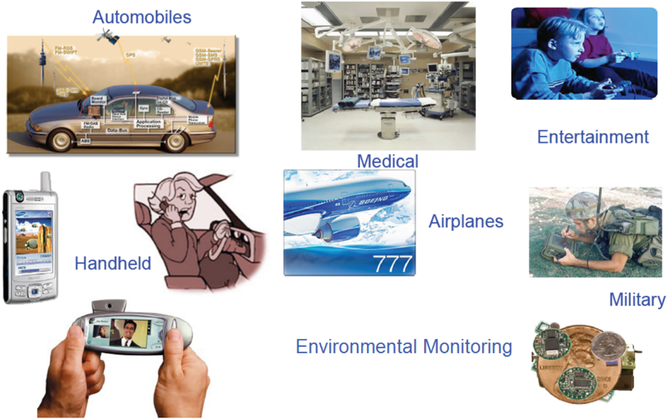
$$\begin{aligned}\dot{x_1} &= \frac{1}{2}(45 - x_1) + \frac{1}{2}(x_2 - x_1),\\ \dot{x_2} &= \frac{1}{2}(x_1 - x_2) + \frac{1}{4}(35 - x_2) + \frac{1}{4}(x_3 - x_2) + 20,\\ \dot{x_3} &= \frac{1}{4}(x_2 - x_3) + \frac{3}{4}(35 - x_3),\end{aligned}$$

with the initial set $\mathrm{X} = \{(x_1, x_2, x_3)^T \mid 1 - (x_1 - 45)^2 - (x_2 - 35)^2 - (x_3 - 35)^2 > 0\}$.

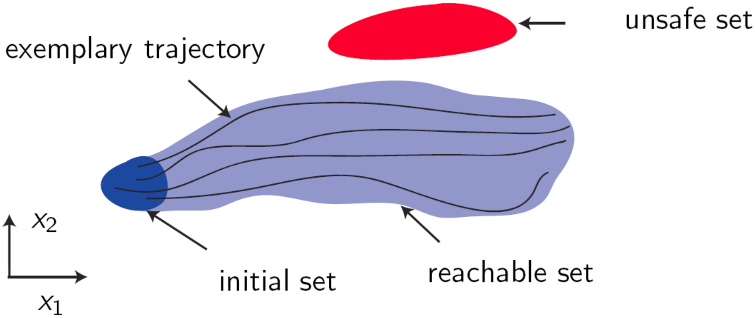
Is it possible for the temperature x_2 getting over than $70^\circ F$ (unsafe) ? **UNBOUNDED.**

Hybrid Systems

Hybrid systems exhibit combinations of discrete jumps and continuous evolution, many of which are Safety-critical.



Safety Verification Using Reachable Sets [1]



- System is safe, if no trajectory enters the unsafe set.

1. The figure is taken from [M. Althoff, 2010].

Tarski Algebra and Quantifier Elimination

- Tarski Algebra ($T(\mathbb{R})$)= real numbers with arithmetic and ordering.

Example

$$\varphi := \forall x \exists y : x^2 + xy + b > 0 \wedge x + ay^2 + b \leq 0$$

Tarski Algebra and Quantifier Elimination

- Tarski Algebra ($T(\mathbb{R})$)= real numbers with arithmetic and ordering.

Example

$$\varphi := \forall x \exists y : x^2 + xy + b > 0 \wedge x + ay^2 + b \leq 0$$

- Quantifier Elimination :

$$T(\mathbb{R}) \models \varphi \longleftrightarrow \varphi'$$

Example

$$T(\mathbb{R}) \models \underbrace{\forall x \exists y (x^2 + xy + b > 0 \wedge x + ay^2 + b \leq 0)}_{\varphi} \longleftrightarrow \underbrace{a < 0 \wedge b > 0}_{\varphi'}$$

Quantifier Elimination

Survey of QE Algorithms

- Tarski's algorithm [Tarski 51] : the first one, but its complexity is nonelementary, impratical, simplified by Seidenberg [Seidenberg 54].
- Collins' algorithm [Collins 76] : based on cylindrical algebraic decomposition (CAD), double exponential in the number of variables, improved by Hoon Hong [Hoon Hong 92] by combining with SAT engine partial cylindrical algebraic decomposition (PCAD), implemented in many computer algebra tools, e.g., QEPCAD,REDLOG, ...
- Ben-Or, Kozen and Reif's algorithm [Ben-Or, Kozen & Reif 86] : double exponential in the number of variables using sequential computation, single exponential using parallel computation, based on Sturm sequence and Sturm Theorem.
- More efficient algorithms [Grigor'ev & Vorobjov 88, Grigor'ev 88], [Renegar 89], [Heintz, Roy & Solerno 89], [Basu,Pollack & Roy 96] : mainly based on BKR's approach, double exponential in the number of quantifier alternation, no implementation yet.

Tarski's Conjecture (TC)

- Whether the extension of TA with *exponentiation* is decidable ?

Tarski's Conjecture (TC)

- Whether the extension of TA with *exponentiation* is decidable ?
- TC is still open.

Tarski's Conjecture (TC)

- Whether the extension of TA with *exponentiation* is decidable ?
- TC is still open.
- In 2008, Strzebonski showed the decidability of $\mathcal{T}_e$, the extension of TA with polynomial exponential functions (PEFs) :

$$f(t, \mathbf{x}) = \sum_{i=0}^{m} f_i(t, \mathbf{x}) e^{\lambda_i t}$$

LDSs with Inputs

- Linear dymamical systems (LDSs) with inputs are differential equations of the form

$$\dot{\xi} = A\xi + \mathbf{u}, \tag{1}$$

where $\xi(t) \in \mathbb{R}^n$, $A \in \mathbb{R}^{n \times n}$, and $\mathbf{u} : \mathbb{R} \to \mathbb{R}^n$ is a continuous function vector which is called the *input*.

LDSs with Inputs

- Linear dymamical systems (LDSs) with inputs are differential equations of the form

$$\dot{\xi} = A\xi + \mathbf{u}, \tag{1}$$

where $\xi(t) \in \mathbb{R}^n$, $A \in \mathbb{R}^{n\times n}$, and $\mathbf{u} : \mathbb{R} \to \mathbb{R}^n$ is a continuous function vector which is called the *input*.

- The *forward reachable set* :

$$Post(\mathrm{X}) = \{\mathbf{y} \in \mathbb{R}^n \mid \exists \mathbf{x} \exists t : \mathbf{x} \in \mathrm{X} \wedge t \geq 0 \wedge \Phi(\mathbf{x}, t) = \mathbf{y}\} \tag{2}$$

LDSs with Inputs

- Linear dymamical systems (LDSs) with inputs are differential equations of the form

$$\dot{\xi} = A\xi + \mathbf{u}, \tag{1}$$

where $\xi(t) \in \mathbb{R}^n$, $A \in \mathbb{R}^{n \times n}$, and $\mathbf{u} : \mathbb{R} \to \mathbb{R}^n$ is a continuous function vector which is called the *input*.

- The *forward reachable set* :

$$Post(\mathrm{X}) = \{\mathbf{y} \in \mathbb{R}^n \mid \exists \mathbf{x} \exists t : \mathbf{x} \in \mathrm{X} \wedge t \geq 0 \wedge \Phi(\mathbf{x}, t) = \mathbf{y}\} \tag{2}$$

- **Reachability problem :**

$$\mathcal{F}(\mathrm{X}, \mathrm{Y}) := \exists \mathbf{x} \exists \mathbf{y} \exists t : \mathbf{x} \in \mathrm{X} \wedge \mathbf{y} \in \mathrm{Y} \wedge t \geq 0 \wedge \Phi(\mathbf{x}, t) = \mathbf{y}.$$

Decidability Results of the Reachability of LDSs

In [LPY 2001], Lafferriere, Pappas and Yovine proved the decidability of the reachability problems of the following three families of LDSs :

1. A is *nilpotent*, i.e. $A^n = 0$, and each component of $\mathbf{u}$ is a polynomial ;
2. A is *diagonalizable* with rational eigenvalues, and each component of $\mathbf{u}$ is of the form $\sum_{i=1}^{m} c_i e^{\lambda_i t}$, where λ_is are rational and c_is are subject to semi-algebraic constraints ;
3. A is *diagonalizable* with purely imaginary eigenvalues, and each component of $\mathbf{u}$ of the form $\sum_{i=1}^{m} c_i \sin(\lambda_i t) + d_i \cos(\lambda_i t)$, where λ_is are rationals and c_is and d_is are subject to semi-algebraic constraints.

Decidability Results of the Reachability of LDSs

In [LPY 2001], Lafferriere, Pappas and Yovine proved the decidability of the reachability problems of the following three families of LDSs :

1. A is *nilpotent*, i.e. $A^n = 0$, and each component of $\mathbf{u}$ is a polynomial ;
2. A is *diagonalizable* with *real* eigenvalues, and each component of $\mathbf{u}$ is of the form $\sum_{i=1}^{m} c_i e^{\lambda_i t}$, where λ_is are *reals* and c_is are subject to semi-algebraic constraints ;
3. A is *diagonalizable* with purely imaginary eigenvalues, and each component of $\mathbf{u}$ of the form $\sum_{i=1}^{m} c_i \sin(\lambda_i t) + d_i \cos(\lambda_i t)$, where λ_is are rationals and c_is and d_is are subject to semi-algebraic constraints.

Decidability of the Reachability for a Family of $\mathrm{LDS}_{\mathrm{PEF}}$

Definition ($\mathrm{LDS}_{\mathrm{PEF}}$)

A Family of LDSs with diagonalizable matrices with real eigenvalues, and polynomial-exponential inputs ($\mathrm{LDS}_{\mathrm{PEF}}$) :

$$\dot{\xi} = A\xi + \mathbf{u},$$

where

- $A = QDQ^{-1}$, where $D = diag(\lambda_1, \cdots, \lambda_n)$, and $\lambda_1, \cdots, \lambda_n \in \mathbb{R}$;
- $\mathbf{u} = (u_1, u_2, \cdots, u_n)^T$, $u_i = \sum_{k=0}^{r_i} g_{ik}(t)e^{\mu_{ik}t}$, $i = 1, 2, \cdots, n$

Computing Reachable Sets

$$\xi(t) = \Phi(\mathbf{x}, t) = e^{At}\mathbf{x} + \int_0^t e^{A(t-\tau)}\mathbf{u}(\tau)d\tau, \quad (3)$$

$$e^{At} = e^{QDQ^{-1}t} = Q \begin{bmatrix} e^{\lambda_1 t} & & \\ & \ddots & \\ & & e^{\lambda_n t} \end{bmatrix} Q^{-1}, \quad (4)$$

$$(e^{At})_{ij} = \sum_{k=1}^{n} q_{ik} q_{kj}^{-} e^{\lambda_k t}, \quad (5)$$

$$(e^{At}\mathbf{x})_i = \sum_{j=1}^{n} (e^{At})_{ij} x_j = \sum_{j=1}^{n}\sum_{k=1}^{n} q_{ik} q_{kj}^{-} x_j e^{\lambda_k t} \quad (6)$$

$$= \sum_{k=1}^{n}\left(\sum_{j=1}^{n} q_{ik} q_{kj}^{-} x_j\right) e^{\lambda_k t} = \sum_{k=1}^{n} \alpha_{ik}(\mathbf{x}) e^{\lambda_k t}, \quad (7)$$

Computing Reachable Sets

- $(\Phi(\mathbf{x}, t))_i = \sum_{k=1}^{n} \alpha_{ik}(\mathbf{x}) e^{\lambda_k t} + \sum_{j=0}^{c_i} \psi_{ij}(t) e^{\theta_{ij} t}$.
- The solution $\Phi(\mathbf{x}, t)_i$ can be reduced to

$$\Phi(\mathbf{x}, t)_i = \sum_{j=1}^{s_i} \phi_{ij}(\mathbf{x}, t) e^{\nu_{ij} t},$$

Computing Reachable Sets

- $(\Phi(\mathbf{x}, t))_i = \sum_{k=1}^{n} \alpha_{ik}(\mathbf{x}) e^{\lambda_k t} + \sum_{j=0}^{c_i} \psi_{ij}(t) e^{\theta_{ij} t}$.
- The solution $\Phi(\mathbf{x}, t)_i$ can be reduced to

$$\Phi(\mathbf{x}, t)_i = \sum_{j=1}^{s_i} \phi_{ij}(\mathbf{x}, t) e^{\nu_{ij} t},$$

Forward Reachable Sets Revisited

$$Post(\mathrm{X}) = \{\mathbf{y} \mid \exists \mathbf{x} \exists t : \mathbf{x} \in \mathrm{X} \wedge t \geq 0 \wedge \bigwedge_{i=1}^{n} \sum_{j=1}^{s_i} \phi_{ij}(\mathbf{x}, t) e^{\nu_{ij} t} = y_i\}$$

Computing Reachable Sets

The Reachability Revisited

Given two semi-algebraic sets

$$\mathrm{X} = \{\mathbf{x} \in \mathbb{R}^n \mid p_1(\mathbf{x}) > 0, \cdots, p_{J_1}(\mathbf{x}) > 0\},$$

$$\mathrm{Y} = \{\mathbf{y} \in \mathbb{R}^n \mid p_{J_1+1}(\mathbf{y}) > 0, \cdots, p_J(\mathbf{y}) > 0\},$$

$$\mathcal{F}(\mathrm{X}, \mathrm{Y}) := \exists \mathbf{x} \exists \mathbf{y} \exists t : \mathbf{x} \in \mathrm{X} \wedge \mathbf{y} \in \mathrm{Y} \wedge t \geq 0 \wedge \bigwedge_{i=1}^{n} \sum_{j=1}^{s_i} \phi_{ij}(\mathbf{x}, t) e^{\nu_{ij} t} = y_i \tag{8}$$

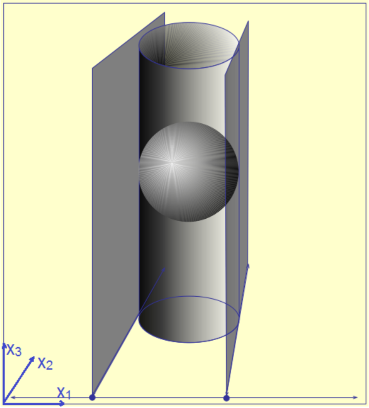
Theorem (Decidability of the Reachability of $\mathrm{LDS}_{\mathrm{PEF}}$)

The reachability problem of $\mathrm{LDS}_{\mathrm{PEF}}$ *is decidable if* $\mathcal{T}_e$ *is decidable.*

Cylindrical Algebraic Decomposition (CAD) [2]

$$\exists x_1 \exists x_2 \exists x_3 : f_1 > 0 \wedge f_2 \geq 0 \wedge f_3 > 0 \wedge f_4 \leq 0?$$

$$f_1 = {x_1}^2 + {x_2}^2 + {x_3}^2 - 4$$
$$f_2 = {x_1}^2 + {x_2}^2 - 4$$
$$f_3 = x_1 + 2$$
$$f_4 = x_1 - 2$$

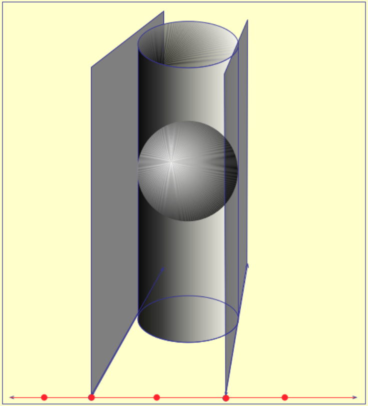


2. Taken from Thomas Sturm.

Cylindrical Algebraic Decomposition (CAD)

$\exists x_1 \exists x_2 \exists x_3 : f_1 > 0 \wedge f_2 \geq 0 \wedge f_3 > 0 \wedge f_4 \leq 0?$

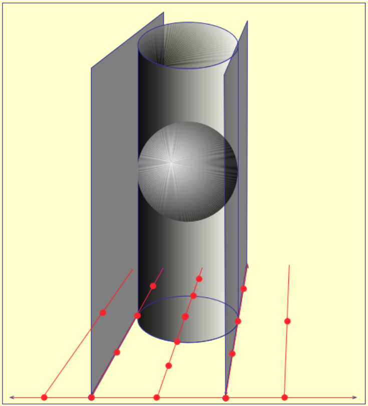
$$f_1 = {x_1}^2 + {x_2}^2 + {x_3}^2 - 4$$
$$f_2 = {x_1}^2 + {x_2}^2 - 4$$
$$f_3 = x_1 + 2$$
$$f_4 = x_1 - 2$$



Cylindrical Algebraic Decomposition (CAD)

$\exists x_1 \exists x_2 \exists x_3 : f_1 > 0 \wedge f_2 \geq 0 \wedge f_3 > 0 \wedge f_4 \leq 0?$

$$f_1 = {x_1}^2 + {x_2}^2 + {x_3}^2 - 4$$
$$f_2 = {x_1}^2 + {x_2}^2 - 4$$
$$f_3 = x_1 + 2$$
$$f_4 = x_1 - 2$$



Cylindrical Algebraic Decomposition (CAD)

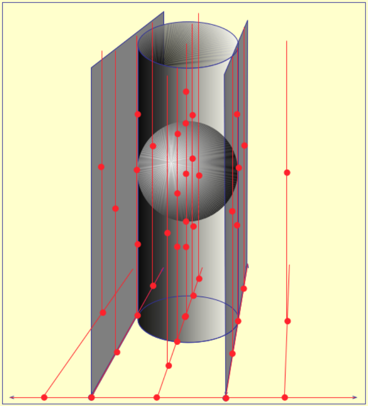
$\exists x_1 \exists x_2 \exists x_3 : f_1 > 0 \wedge f_2 \geq 0 \wedge f_3 > 0 \wedge f_4 \leq 0?$

$f_1 = {x_1}^2 + {x_2}^2 + {x_3}^2 - 4$

$f_2 = {x_1}^2 + {x_2}^2 - 4$

$f_3 = x_1 + 2$

$f_4 = x_1 - 2$



Decision Procedure for $\mathcal{T}_e$

Definition (CAD(openCAD))

For a polynomial $f(x_1, \ldots, x_n) \in \mathbb{R}[x_1, \ldots, x_n]$, a CAD (openCAD) defined by f under the order $x_1 \prec x_2 \prec \cdots \prec x_n$ is a set of sample points in $\mathbb{R}^n$ obtained through the following three phases :

- **Projection :** Apply CAD (openCAD) projection operator on f to get a set of projection polynomials

$$\{f_n = f(x_1, \ldots, x_n), f_{n-1}(x_1, \ldots, x_{n-1}), \ldots, f_1(x_1)\};$$

- **Base :** Choose a rational point in each of the (open) intervals defined by the real roots of f_1 ;
- **Lifting :** Substitute each sample point in $\mathbb{R}^{i-1}$ for $(x_1, \ldots, x_{i-1})$ in f_i to get a univariate polynomial $f_i'(x_i)$, and then, as in Base phase, choose sample points for $f_i'(x_i)$. Repeat this process for i from 2 to n.

Decision Procedure for $\mathcal{T}_e$

Step 1 Check whether $X \cap Y = \emptyset$, if not $\Rightarrow$ unsafe.

Decision Procedure for $\mathcal{T}_e$

Step 1 Check whether $\mathrm{X} \cap \mathrm{Y} = \emptyset$, if not $\Rightarrow$ unsafe.

Step 2 Translate the problem to an openCAD solvable problem if X and Y are open sets (otherwise a CAD solvable problem) :

$$\mathcal{F} := \exists \mathbf{x} \exists t \bigwedge_{j=1}^{J} p_j(\mathbf{x}, t) > 0 \wedge t > 0.$$

Decision Procedure for $\mathcal{T}_e$

Step 1 Check whether $\mathrm{X} \cap \mathrm{Y} = \emptyset$, if not $\Rightarrow$ unsafe.

Step 2 Translate the problem to an openCAD solvable problem if X and Y are open sets (otherwise a CAD solvable problem) :

$$\mathcal{F} := \exists \mathbf{x} \exists t \bigwedge_{j=1}^{J} p_j(\mathbf{x}, t) > 0 \wedge t > 0.$$

Step 3 Eliminate $x_1, \cdots, x_n$ one by one using CAD (openCAD) projection operator on $\prod_{j=1}^{J} p_j$ and obtain a set of projection polynomials $\{q_n(x_1, \ldots, x_n, t) = \prod_{j=1}^{J} p_j, q_{n-1}(x_2, \ldots, x_n, t)\}, \ldots, q_0(t)\}$.

Decision Procedure for $\mathcal{T}_e$

Step 4 Isolate the real roots of the resulted PEF q_0 based on ***Rolle's theorem***.

Decision Procedure for $\mathcal{T}_e$

Step 4 Isolate the real roots of the resulted PEF q_0 based on ***Rolle's theorem***.

Step 5 Lift the solution using openCAD or CAD lifting procedure according to the order $t, x_n, \cdots, x_1$ based on the projection factor $\{q_0, \cdots, q_n\}$, and obtain a set S of *sample points*.

Decision Procedure for $\mathcal{T}_e$

Step 4 Isolate the real roots of the resulted PEF q_0 based on ***Rolle's theorem***.

Step 5 Lift the solution using openCAD or CAD lifting procedure according to the order $t, x_n, \cdots, x_1$ based on the projection factor $\{q_0, \cdots, q_n\}$, and obtain a set S of *sample points*.

Step 6 Check if $\mathcal{F}$ holds by testing if there exists α in S such that $\wedge_{j=1}^{J} p_j(\alpha) \rhd 0$.

Isolating Real Roots of PEFs

Theorem 1.

Let $f(t)$ be a PEF, $f'(t)$ the derivative of $f(t)$ w.r.t. t, $I = (a, b)$ a non-empty open interval, and $\mathcal{L}_I(f') = \{I_j | j = 1, \ldots, J\}$ a real root isolation of f' in I, in which $I_j = (a_j, b_j)$ with

$$a = b_0 < a_1 < b_1 < \cdots < a_J < b_J < a_{J+1} = b.$$

Furthermore, there is no real root of $f(t) = 0$ in any closed interval $[a_j, b_j]$, $1 \leq j \leq J$. Then,

$$\{\ (b_j, a_{j+1}) \mid f(b_j)f(a_{j+1}) < 0,\ 0 \leq j \leq J\ \}$$

is a real root isolation of $f(t) = 0$ in I.

Proof.

Attributes to ***Rolle's theorem*** (cf. differential mean value theorem).

Basic Idea

Example (A Running Example)

$$f(t) = t + 1 + e^{\sqrt{2}t} - (t+2)e^{\sqrt{5}t}$$

Basic Idea

Example (A Running Example)

$$f(t) = t + 1 + e^{\sqrt{2}t} - (t+2)e^{\sqrt{5}t}$$

Step 1 Computing Lower and Upper Bounds :

$$L(f) = -4, \quad U(f) = 12.$$

Basic Idea

Step 2 Constructing a sequence of derivatives :

$$S_0 = f(t) = t + 1 + e^{\sqrt{2}t} - (t+2)e^{\sqrt{5}t}$$

$$S_1 = f'(t) = 1 + \sqrt{2}e^{\sqrt{2}t} - (\sqrt{5}t + 2\sqrt{5} + 1)e^{\sqrt{5}t}$$

$$f''(t) = 0 + 2e^{\sqrt{2}t} - (5t + 2\sqrt{5} + 10)e^{\sqrt{5}t}$$

$$S_2 = f''(t)e^{-\sqrt{2}t} = 2 - (5t + 2\sqrt{5} + 10)e^{(\sqrt{5}-\sqrt{2})t}$$

$$S_3 = S_2' = 0 + 0 + he^{(\sqrt{5}-\sqrt{2})t}$$

where $h = -(5(\sqrt{5} - \sqrt{2})t + 15 + 10\sqrt{5} - 2\sqrt{10} - 10\sqrt{2})$.

Basic Idea

Step 2 Constructing a sequence of derivatives :

$$S_0 = f(t) = t + 1 + e^{\sqrt{2}t} - (t+2)e^{\sqrt{5}t}$$

$$S_1 = f'(t) = 1 + \sqrt{2}e^{\sqrt{2}t} - (\sqrt{5}t + 2\sqrt{5} + 1)e^{\sqrt{5}t}$$

$$f''(t) = 0 + 2e^{\sqrt{2}t} - (5t + 2\sqrt{5} + 10)e^{\sqrt{5}t}$$

$$S_2 = f''(t)e^{-\sqrt{2}t} = 2 - (5t + 2\sqrt{5} + 10)e^{(\sqrt{5}-\sqrt{2})t}$$

$$S_3 = S_2' = 0 + 0 + he^{(\sqrt{5}-\sqrt{2})t}$$

where $h = -(5(\sqrt{5} - \sqrt{2})t + 15 + 10\sqrt{5} - 2\sqrt{10} - 10\sqrt{2})$.

$S_3 = 0$ if and only if $h = 0$, while the real zeros of h can be easily achieved by any real root isolation procedure for polynomials.

Basic Idea

Step 3 Isolating all real roots of the sequence of derivatives :

- For $h(t) = 0$,

$$t = -\frac{15 + 10\sqrt{5} - 2\sqrt{10} - 10\sqrt{2}}{5(\sqrt{5} - \sqrt{2})} \in (-5, -4).$$

Basic Idea

Step 3 Isolating all real roots of the sequence of derivatives :

- For $h(t) = 0$,

$$t = -\frac{15 + 10\sqrt{5} - 2\sqrt{10} - 10\sqrt{2}}{5(\sqrt{5} - \sqrt{2})} \in (-5, -4).$$

- As $(-5, -4) \cap (-4, 12) = \emptyset$, there is no real root of $S_3 = 0$ in $(-4, 12)$. Hence, we have $\mathcal{L}_{(-4,12)}(S_3) = \emptyset$.

Basic Idea

Step 3 Isolating all real roots of the sequence of derivatives :

- For $h(t) = 0$,

$$t = -\frac{15 + 10\sqrt{5} - 2\sqrt{10} - 10\sqrt{2}}{5(\sqrt{5} - \sqrt{2})} \in (-5, -4).$$

- As $(-5, -4) \cap (-4, 12) = \emptyset$, there is no real root of $S_3 = 0$ in $(-4, 12)$. Hence, we have $\mathcal{L}_{(-4,12)}(S_3) = \emptyset$.
- $\mathcal{L}_{(-4,12)}(S_2) = \{(-2, -1)\}$.
- $\mathcal{L}_{(-4,12)}(S_1) = \{(-0.59375, -0.390625)\}$.
- $\mathcal{L}_{(-4,12)}(f) = \{(-4, -0.59375), (-0.390625, 12)\}$.

Implementation

- A prototype in *Mathematica*, called *LinR*, which takes a specific *LDS* reachability problem as input, and gives either *False* if the problem is not satisfiable, or *True* otherwise associated with some counterexamples.
- Both the tool and the forthcoming case studies can be found at `http://lcs.ios.ac.cn/~chenms/tools/LinR.tar.bz2`

Illustrating Examples

Example (Constructed)

Consider the following LDS

$$\dot{\xi} = \begin{bmatrix} \sqrt{2} & & \\ & -\sqrt{2} & \\ & & -1 \end{bmatrix} \xi + \begin{bmatrix} 1-t \\ te^{t} \\ e^{-t} \end{bmatrix}.$$

Let

$$\mathrm{X} = \{(x_1, x_2, x_3)^T \mid 1 - x_1^2 - x_2^2 - x_3^2 > 0\},$$
$$\mathrm{Y} = \{(y_1, y_2, y_3)^T \mid y_1 + y_2 + y_3 + 2 < 0\}.$$

The safety property to be verified is to check if some state in Y is reachable from X.

Illustrating Examples

- Obviously, $\mathrm{X} \cap \mathrm{Y} = \emptyset$.
- $\xi(t) = \begin{bmatrix} x_1 e^{\sqrt{2}t} + \frac{\sqrt{2}t-\sqrt{2}+1}{2} + \frac{\sqrt{2}-1}{2} e^{\sqrt{2}t} \\ x_2 e^{-\sqrt{2}t} + \frac{(1+\sqrt{2})t-1}{3+2\sqrt{2}} e^{t} + \frac{e^{-\sqrt{2}t}}{3+2\sqrt{2}} \\ x_3 e^{-t} + te^{-t} \end{bmatrix}.$
- The reachability problem becomes

$$\mathcal{F} = \exists x_1 \exists x_2 \exists x_3 \exists t.\ \Phi(x_1, x_2, x_3, t);$$

$$\Phi(x_1, x_2, x_3, t) = 1 - x_1^2 - x_2^2 - x_3^2 > 0$$

$$\wedge\ x_1 e^{\sqrt{2}t} + x_2 e^{-\sqrt{2}t} + x_3 e^{-t} + h(t) < 0 \wedge t > 0,$$

where $h(t) = \frac{e^{-\sqrt{2}t}}{3+2\sqrt{2}} + te^{-t} + \frac{\sqrt{2}t-\sqrt{2}+5}{2} + \frac{(1+\sqrt{2})t-1}{3+2\sqrt{2}} e^{t} + \frac{\sqrt{2}-1}{2} e^{\sqrt{2}t}$.

Illustrating Examples

- Using the *projection operator* to eliminate x_1, x_2, x_3 successively (Step 3), we have

$$
\begin{aligned}
q_3(x_1, x_2, x_3, t) &= (x_1^2 + x_2^2 + x_3^2 - 1)(ax_1 + bx_2 + cx_3 + h) \\
q_2(x_2, x_3, t) &= a(x_2^2 + x_3^2 - 1) \\
&\quad (-a^2 + a^2x_2^2 + a^2x_3^2 + b^2x_2^2 + 2bcx_2x_3 + 2bhx_2 + c^2x_3^2 + 2chx_3 + h^2), \\
q_1(x_3, t) &= a(x_3 - 1)(x_3 + 1)(a^2 + b^2)(2chx_3 + h^2 - b^2 + b^2x_3^2 + c^2x_3^2) \\
&\quad (-a^2 + a^2x_3^2 + 2chx_3 + h^2 - b^2 + b^2x_3^2 + c^2x_3^2), \\
q_0(t) &= ab(c - h)(c + h)(a^2 + b^2)(b^2 + c^2)(b^2 + c^2 - h^2)(a^2 + b^2 + c^2) \\
&\quad (a^2 + b^2 + c^2 - h^2),
\end{aligned}
$$

where $a = e^{\sqrt{2}t}$, $b = e^{-\sqrt{2}t}$ and $c = e^{-t}$.

Illustrating Examples

- Isolate all real roots of $q_0(t) = 0$ in $(0, +\infty)$ (Step 4)

$$\mathcal{L}(q_0) = \{(1.08, 1.29)\}$$

- Lift the real root isolation in the order t, x_3, x_2, x_1 (Step 5), and we finally obtain 48 sample points in which the sample point $\{-0.835, -0.212, 0.184, 2.\}$ satisfies Φ, which implies that the safety property is not satisfied with the counter example starting from $(-0.835, -0.212, 0.184) \in X$, and ending at time $t = 2$.

Illustrating Examples

Example (Biochemical : nutrient flow in an aquarium)

Consider a vessel of water containing a radioactive isotope, to be used as a tracer for the food chain, which consists of aquatic plankton varieties phytoplankton A and zooplankton B. Let $\xi_1(t)$ be the isotope concentration in the water, $\xi_2(t)$ the isotope concentration in A and $\xi_3(t)$ the isotope concentration in B. The dynamics of the vessel is modeled by the following LDS

$$\dot{\xi} = A\xi, \text{ where } A = \begin{bmatrix} -3 & 6 & 5 \\ 2 & -12 & 0 \\ 1 & 6 & -5 \end{bmatrix}.$$

The initial radioactive isotope concentrations $\xi_1(0) = x_1 > 0, \xi_2(0) = 0, \xi_3(0) = 0$.

The safety property of our concern is whether $\forall t > 0\ \xi_1(t) \geq \xi_2(t) + \xi_3(t)$.

A more general problem : For which $n_1, n_2 \in \mathbb{N}$ such that $\mathcal{F}(n_1, n_2) = \exists x_1 > 0\ \exists t > 0\ \xi_1(t) < n_1\xi_2(t) + n_2\xi_3(t)$ holds.

Illustrating Examples

Example (Physics : home heating)

Consider a typical home with attic, basement and insulated main floor. Let $x_3(t), x_2(t), x_1(t)$ be the temperature in the attic, main living area and basement respectively, and t is the time in hours. Assume it is winter time, the outside temperature is nearly $35° F$, and the basement earth temperature is nearly $45° F$. Suppose a small electric heater is turned on, and it provides a $20° F$ rise per hour. We want to verify that the temperature in main living area will never reach too high (maybe $70° F$). Analyze the changing temperatures in the three levels using Newton's cooling law and given the value of the cooling constants, we obtain the model as follows :

$$\dot{x_1} = \frac{1}{2}(45 - x_1) + \frac{1}{2}(x_2 - x_1), \dot{x_2} = \frac{1}{2}(x_1 - x_2) + \frac{1}{4}(35 - x_2) + \frac{1}{4}(x_3 - x_2) + 20,$$
$$\dot{x_3} = \frac{1}{4}(x_2 - x_3) + \frac{3}{4}(35 - x_3),$$

with the initial set $\mathrm{X} = \{(x_1, x_2, x_3)^T \mid 1 - (x_1 - 45)^2 - (x_2 - 35)^2 - (x_3 - 35)^2 > 0\}$ and the unsafe set $\mathrm{Y} = \{(y_1, y_2, y_3)^T \mid y_2 - 70 > 0\}$.

Evaluation Results for Open Constraints

LDS	Time (sec)					Memory (kb)				
	LinR	*CT1D*	*dReach*	*HSolver*	*Flow**	*LinR*	*CT1D*	*dReach*	*HSolver*	*Flow**
Constructed	1.35	×	37.36	–	–	112	×	3812	–	–
Biochemical	0.03	0.20	0.71	–	–	131	2018	3816	–	–
Physics	1.68	×	0.05	0.72	16.50	166	×	3812	1076932	113492

× : the verification fails by non-termination within reasonable amount of time (10 hours)

– : the verification fails because of giving an answer as "safety unknown"

Table 1. Evaluation results of different methods

Evaluation Results for Closed Constraints

LinR	CT1D	QEPCAD	dReach	HSolver	Flow*
39	33	57	110	--	--

Table : Time consumption (in milliseconds) on Example 3.4 from [LPY2001]

Comparison with Strzebonski's Decision Procedure

	Strzebonski's	Ours
CAD	complete CAD	openCAD
real root isolation	weak Fourier sequence	Rolle's theorem
assumption	Schanuel's Conjecture	no multiple real root of PEFs

Concluding Remarks

- The decidability of the reachability problem of a family of LDSs, whose state parts are linear, and input parts are possibly with exponential expressions.
- The decidability is achieved by showing the decidability of the extension of TA.
- A sound and complete decision procedure for unbounded verification under the assumption that PEFs have no multiple real roots.