Deductive Verification of Continuous Dynamical Systems

Ankur Taly

Dept. of Computer Science, Stanford University

(Joint work with Ashish Tiwari, SRI International.)

What are Continuous Dynamical Systems (CDS)?

- Modeling formalism for systems with continuous dynamics.
  Example: Motion of a projectile under gravity.
- Dynamics are specified as differential equations over suitable state space.
- Multiple continuous dynamical systems combined together using a discrete switching logic give rise to Hybrid systems.
  Example: Thermostat with *on* and *off* modes.
- This work: Design a rigorous procedure for verifying safety properties of CDS.
- First step towards rigorous safety analysis of Hybrid systems.

Formal definition

CDS

A CDS is specified as tuple $(\mathtt{X}, \mathtt{Init}, f)$

- $\mathtt{X}$ is a finite set of variables interpreted over the reals $\mathbb{R}$ and $\mathbb{R}^{\mathtt{X}}$ is the set of all valuations of the variables $\mathtt{X}$,
- $\mathtt{Init} \subseteq \mathbb{R}^{\mathtt{X}}$ is the set of initial states,
- $f : \mathbb{R}^{\mathtt{X}} \mapsto \mathbb{R}^{\mathtt{X}}$ is a lipschitz continuous vector field that specifies the continuous dynamics.

Lipschitz continuity of f guarantees unique solutions for the initial value problem(ivp) $\frac{d\mathtt{X}(t)}{dt} = f(\mathtt{X}(t))$, $\mathtt{X}(0) = \vec{x}_0$. Henceforth we use $F(\vec{x}_0, t)$ to denote such a solution.

Semantics: Given a CDS : $(\mathtt{X}, \mathtt{Init}, f)$,

$$[[\mathrm{CDS}]] \quad := \quad \{F_1 : [0, \infty) \mapsto \mathbb{R}^{\mathtt{X}} \quad | \quad F_1(t) = F(\vec{x}_0, t), \quad \vec{x}_0 \in \mathtt{Init} \quad \}$$

Formal definition

CDS

A $\mathtt{CDS}$ is specified as tuple $(\mathtt{X}, \mathtt{Init}, f)$

- $\mathtt{X}$ is a finite set of variables interpreted over the reals $\mathbb{R}$ and $\mathbb{R}^{\mathtt{X}}$ is the set of all valuations of the variables $\mathtt{X}$,
- $\mathtt{Init} \subseteq \mathbb{R}^{\mathtt{X}}$ is the set of initial states,
- $f : \mathbb{R}^{\mathtt{X}} \mapsto \mathbb{R}^{\mathtt{X}}$ is a lipschitz continuous vector field that specifies the continuous dynamics.

Lipschitz continuity of f guarantees unique solutions for the initial value problem(ivp) $\frac{d\mathtt{X}(t)}{dt} = f(\mathtt{X}(t))$, $\mathtt{X}(0) = \vec{\mathtt{x}}_0$. Henceforth we use $F(\vec{\mathtt{x}}_0, t)$ to denote such a solution.

Semantics: Given a $\mathtt{CDS} : (\mathtt{X}, \mathtt{Init}, f)$,

$$[[\mathtt{CDS}]] \;:=\; \{F_1 : [0, \infty) \mapsto \mathbb{R}^{\mathtt{X}} \;\mid\; F_1(t) = F(\vec{\mathtt{x}}_0, t), \quad \vec{\mathtt{x}}_0 \in \mathtt{Init} \;\}$$

The Safety problem for CDS

Given a $\mathtt{CDS} : (\mathtt{X}, \mathtt{Init}, f)$,

- $\mathtt{Reach}(\mathtt{CDS})$ is defined as $\{\vec{\mathtt{x}} \in \mathbb{R}^{\mathtt{X}} \mid \exists F \in [[\mathtt{CDS}]], \exists t \geq 0 : \vec{\mathtt{x}} = F(t)\}$
- A (safety) property, $\mathtt{Safe}$, is simply a subset of the state space $\mathbb{R}^{\mathtt{X}}$.
- A property $\mathtt{Safe}$ is an invariant (for the system $\mathtt{CDS}$) if $\mathtt{Reach}(\mathtt{CDS}) \subseteq \mathtt{Safe}$.

Safety Verification Problem

Given a continuous dynamical system $\mathtt{CDS}$ and a safety property $\mathtt{Safe}$, determine if $\mathtt{Safe}$ is an invariant for $\mathtt{CDS}$.

Verification approaches

- Explicit computation of an over-approximation of the set of reachable states (fixed point based approaches):
  - Good for systems with pure discrete flows.
  - Inefficient for systems with non-linear continuous flows.
  - Proving soundness and completeness is diffucult.
  - Termination is an issue.
- This work: Deductive Verification
  - Inductive invariants and Constraint solving.
  - Symbolic approach.
  - Soundness and relative completeness can be rigorously proven.

Soundness and Completeness

We seek a deductive verification rule $R(\mathtt{CDS}, \mathtt{Safe})$ which has the following properties:

1. **Soundness**: Whenever the rule returns true, $\mathtt{Reach}(\mathtt{CDS}) \subseteq \mathtt{Safe}$.
2. **Completeness**: For all CDS and safety properties Safe, if $\mathtt{Reach}(\mathtt{CDS}) \subseteq \mathtt{Safe}$ holds then the rule returns true.
3. **Decidable**

This Work: A sound and decidable rule, relatively complete over a large class of systems.

Soundness and Completeness

We seek a deductive verification rule $R(\mathtt{CDS}, \mathtt{Safe})$ which has the following properties:

1. **Soundness**: Whenever the rule returns true, $\mathtt{Reach}(\mathtt{CDS}) \subseteq \mathtt{Safe}$.
2. **Completeness**: For all $\mathtt{CDS}$ and safety properties $\mathtt{Safe}$, if $\mathtt{Reach}(\mathtt{CDS}) \subseteq \mathtt{Safe}$ holds then the rule returns true.
3. **Decidable**

This Work: A sound and decidable rule, relatively complete over a large class of systems.

Inductive Invariants (Discrete systems)

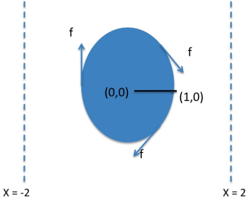
Inductive Invariant

An invariant $I(\vec{x})$ is inductive iff $I(\vec{x}) \Rightarrow I(Next(\vec{x}))$.

What is $Next(\vec{x})$ for continuous systems ?

Example:

$\mathtt{Init} = \{0 \leq x \leq 1, y = 0\}$; $\frac{dx}{dt} = y, \frac{dy}{dt} = -x$;
$\mathtt{Safe} = -2 \leq x \leq 2$



Inwards

Define $\mathtt{Inwards}(\mathtt{Inv}, f, \vec{x})$ as the predicate
$\exists t_0 > 0 : \forall 0 \leq t < t_0 : F(\vec{x}, t) \in \mathtt{Inv}$

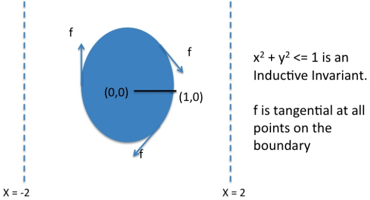
Inductive Invariants (Discrete systems)

Inductive Invariant

An invariant $I(\vec{x})$ is inductive iff $I(\vec{x}) \Rightarrow I(Next(\vec{x}))$.

What is $Next(\vec{x})$ for continuous systems ?

Example:
$\texttt{Init} = \{0 \leq x \leq 1, y = 0\}; \frac{dx}{dt} = y, \frac{dy}{dt} = -x;$
$\texttt{Safe} = -2 \leq x \leq 2$



Inwards

Define $\texttt{Inwards}(\texttt{Inv}, f, \vec{x})$ as the predicate
$\exists t_0 > 0 : \forall 0 \leq t < t_0 : F(\vec{x}, t) \in \texttt{Inv}$

Rule based on Inductive Invariants

Sound and Complete Rule

Exists closed set $\mathtt{Inv}$,

$$\frac{\begin{array}{lll} \text{[Init]} & \forall \vec{x} & \vec{x} \in \mathtt{Init} \implies \vec{x} \in \mathtt{Inv} \\ \text{[Inductiveness]} & \forall \vec{x} \in \partial\mathtt{Inv} : & \mathtt{Inwards}(\mathtt{Inv}, f, \vec{x}) \\ \text{[Safety]} & \forall \vec{x} & \vec{x} \in \mathtt{Inv} \implies \vec{x} \in \mathtt{Safe} \end{array}}{\mathtt{CDS}\ \textit{is safe}}$$

Inductive invariant

Any closed set $\mathtt{Inv}$ satisfying conditions Init and Inductiveness is said to be an inductive invariant for the $\mathtt{CDS}$.

Issues: General form of the above rule is $\exists \mathtt{Inv} : \forall \vec{x} : \phi(\mathtt{Inv}, \vec{x})$

1. Second order quantifier $\exists \mathtt{Inv}$.
2. Predicate ϕ makes use of solution function F.

Getting rid of the second order quantifier

Bounded Verification approach: Bound the search for `Inv` by restricting to a template $\psi(\vec{\mathrm{u}}, \vec{\mathrm{x}})$. The verification rule now is $\exists \vec{\mathrm{u}} : \forall \vec{\mathrm{x}} : \phi(\psi(\vec{\mathrm{u}}, \vec{\mathrm{x}}), \vec{\mathrm{x}})$.

- Focus on polynomial `CDS`
  - `Init` is specified as $p \geq 0$ for some polynomial p.
  - Each component of field $f(\vec{\mathrm{x}})$ is a polynomial.
- Restrict the search for `Inv` to sets of the form $p \geq 0$ where p is a polynomial with unknown coefficients.
- Recall: Exists-forall formulas in theory of Reals are decidable.
- We loose completeness but can try for relative completeness.

Relative Completeness

Our goal is to prove relative completeness to the class of polynomial `CDS` and safety properties `Safe` for which there is an inductive invariant of the form $p \geq 0$ such that $p \geq 0 \Rightarrow$ `Safe`.

Getting rid of the second order quantifier

Bounded Verification approach: Bound the search for `Inv` by restricting to a template $\psi(\vec{u}, \vec{x})$. The verification rule now is $\exists\vec{u} : \forall\vec{x} : \phi(\psi(\vec{u}, \vec{x}), \vec{x})$.

- Focus on polynomial `CDS`
  - `Init` is specified as $p \geq 0$ for some polynomial p.
  - Each component of field $f(\vec{x})$ is a polynomial.
- Restrict the search for `Inv` to sets of the form $p \geq 0$ where p is a polynomial with unknown coefficients.
- Recall: Exists-forall formulas in theory of Reals are decidable.
- We loose completeness but can try for relative completeness.

Relative Completeness

Our goal is to prove relative completeness to the class of polynomial `CDS` and safety properties `Safe` for which there is an inductive invariant of the form $p \geq 0$ such that $p \geq 0 \Rightarrow$ `Safe`.

Removing dependence on solution function F

Recall: $\mathtt{Inwards}(\mathtt{Inv}, f, \vec{\mathrm{x}})$ is defined as
$\exists t_0 > 0 : \forall 0 \leq t < t_0 : F(\vec{\mathrm{x}}, t) \in \mathtt{Inv}$

- $\mathtt{Inv}$ is specified using the template $p \geq 0$. Intuitively,
  - Since f is lipschitz, direction of $f(\vec{\mathrm{x}})$ determines direction of $F(\vec{\mathrm{x}}, t)$ for t very close to 0.
  - Inwards can be determined by analyzing the dot-product of $f(\vec{\mathrm{x}})$ with normal to surface $p = 0$.
- We now present practical and intuitive approximations of $\mathtt{Inwards}$ and analyze the soundness and relative completeness of resulting procedures.
- Many of these procedures are already present in the literature but without rigorous analysis of soundness and completeness.

Removing dependence on solution function F

Recall: $\texttt{Inwards}(\texttt{Inv}, f, \vec{x})$ is defined as
$\exists t_0 > 0 : \forall 0 \leq t < t_0 : F(\vec{x}, t) \in \texttt{Inv}$

- $\texttt{Inv}$ is specified using the template $p \geq 0$. Intuitively,
  - Since f is lipschitz, direction of $f(\vec{x})$ determines direction of $F(\vec{x}, t)$ for t very close to 0.
  - Inwards can be determined by analyzing the dot-product of $f(\vec{x})$ with normal to surface $p = 0$.
- We now present practical and intuitive approximations of $\texttt{Inwards}$ and analyze the soundness and relative completeness of resulting procedures.
- Many of these procedures are already present in the literature but without rigorous analysis of soundness and completeness.

Procedure 1 (Tiwari and Gulwani, Prajna)

Approximation for Inwards

$\texttt{Inwards}(p \geq 0, f, \vec{\mathrm{x}}) := \vec{\nabla}(p) \cdot f \geq 0 := \Sigma_{x \in \mathrm{X}} \frac{\partial p}{\partial x} \frac{dx}{dt} \geq 0$

The inductiveness condition is:
$p = 0 \Rightarrow \vec{\nabla} p \cdot f(\vec{\mathrm{x}}) \geq 0$

Relative Completeness holds but Soundness fails !

Unsoundness Example

Let $\frac{dx}{dt} = 1$ be the dynamics and $x = 0$ be the initial state. The above rule proves that $-x^2 \geq 0$ is inductive since $-x^2 = 0 \Rightarrow -2x * 1 \geq 0$.

Procedure 1 (Tiwari and Gulwani, Prajna)

Approximation for Inwards

$$\texttt{Inwards}(p \geq 0, f, \vec{\mathrm{x}}) := \vec{\nabla}(p) \cdot f \geq 0 := \Sigma_{x \in \mathrm{X}} \frac{\partial p}{\partial x} \frac{dx}{dt} \geq 0$$

The inductiveness condition is:

$p = 0 \Rightarrow \vec{\nabla} p \cdot f(\vec{\mathrm{x}}) \geq 0$

Relative Completeness holds but Soundness fails !

Unsoundness Example

Let $\frac{dx}{dt} = 1$ be the dynamics and $x = 0$ be the initial state. The above rule proves that $-x^2 \geq 0$ is inductive since $-x^2 = 0 \Rightarrow -2x * 1 \geq 0$.

Procedure 2

Approximation for Inwards

$\texttt{Inwards}(p \geq 0, f, \vec{x}) := L_f(p)(\vec{x}) > 0 \equiv: \vec{\nabla}(p) \cdot f > 0$

The inductiveness condition is:
$p = 0 \Rightarrow \vec{\nabla} p \cdot f(\vec{x}) > 0$

Soundness holds but Relative Completeness fails !

Incompleteness Example

Let $\frac{dx}{dt} = y$, $\frac{dy}{dt} = -x$, be the dynamics; $0 \leq x \leq 1 \wedge y = 0$ be the initial state and Safe be $x^2 + y^2 > 1$.

- The safety of the system can only be shown using $x^2 + y^2 \leq 1$.
- The vector field is tangential at all points on $x^2 + y^2 = 1$. Therefore $\vec{\nabla}(p) \cdot f(\vec{x}) = 0$ for all $\vec{x}$ such that $p = 0$ (here p is $1 - x^2 - y^2$).

Procedure 2

Approximation for Inwards

$$\texttt{Inwards}(p \geq 0, f, \vec{x}) := L_f(p)(\vec{x}) > 0 \equiv: \vec{\nabla}(p) \cdot f > 0$$

The inductiveness condition is:

$p = 0 \Rightarrow \vec{\nabla} p \cdot f(\vec{x}) > 0$

Soundness holds but Relative Completeness fails !

Incompleteness Example

Let $\frac{dx}{dt} = y, \frac{dy}{dt} = -x$, be the dynamics; $0 \leq x \leq 1 \wedge y = 0$ be the initial state and $\texttt{Safe}$ be $x^2 + y^2 > 1$.

- The safety of the system can only be shown using $x^2 + y^2 \leq 1$.
- The vector field is tangential at all points on $x^2 + y^2 = 1$. Therefore $\vec{\nabla}(p) \cdot f(\vec{x}) = 0$ for all $\vec{x}$ such that $p = 0$ (here p is $1 - x^2 - y^2$).

Procedure 3

Approximation for `Inwards`

- The polynomial $P(u, \vec{x}) = -x^2$ in the previous example had points where $\vec{\nabla} P$ is 0 and so the check $\vec{\nabla}(p) \cdot f(\vec{\mathrm{x}}) \geq 0$ failed.
- We call a polynomial P as smooth if $\forall \vec{x} : P(\vec{x}) = 0 \Rightarrow \vec{\nabla} P(\vec{x}) \neq 0$
- Search over the space of smooth polynomials only.

The inductiveness condition is

$p = 0 \Rightarrow \vec{\nabla}(p) \neq 0 \bigwedge$

$p = 0 \Rightarrow \vec{\nabla} p \cdot f(\vec{\mathrm{x}}) \geq 0$

Soundness holds but relatively completeness still fails !

Not all polynomial `CDS` have smooth inductive invariant sets

Procedure 3

Approximation for `Inwards`

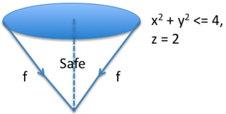
- The polynomial $P(u, \vec{x}) = -x^2$ in the previous example had points where $\vec{\nabla} P$ is 0 and so the check $\vec{\nabla}(p) \cdot f(\vec{x}) \geq 0$ failed.
- We call a polynomial P as smooth if $\forall \vec{x} : P(\vec{x}) = 0 \Rightarrow \vec{\nabla} P(\vec{x}) \neq 0$
- Search over the space of smooth polynomials only.

The inductiveness condition is
$p = 0 \Rightarrow \vec{\nabla}(p) \neq 0 \bigwedge$
$p = 0 \Rightarrow \vec{\nabla} p \cdot f(\vec{x}) \geq 0$
Soundness holds but relatively completeness still fails !
Not all polynomial `CDS` have smooth inductive invariant sets

Procedure 3 contd.

Incompleteness example

Let $\frac{dx}{dt} = -x$, $\frac{dy}{dt} = -y$, $\frac{dz}{dt} = -z$ be the dynamics. Let $\texttt{Safe} := -x^2 - y^2 + z^2 >= 0$ and $\texttt{Init} := z = 2 \bigwedge x^2 + y^2 <= 4$. This system is safe, however its safety can only be proven using the invariant $P := -x^2 - y^2 + z^2 >= 0$, which is not a *smooth* polynomial (since $\vec{\nabla} P$ is 0 at the origin).

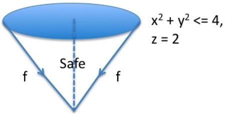


- The problem is trickier than we thought.
- Lets go back to the foundations !

Procedure 3 contd.

Incompleteness example

Let $\frac{dx}{dt} = -x$, $\frac{dy}{dt} = -y$, $\frac{dz}{dt} = -z$ be the dynamics. Let $\texttt{Safe} := -x^2 - y^2 + z^2 >= 0$ and $\texttt{Init} := z = 2 \bigwedge x^2 + y^2 <= 4$. This system is safe, however its safety can only be proven using the invariant $P := -x^2 - y^2 + z^2 >= 0$, which is not a *smooth* polynomial (since $\vec{\nabla} P$ is 0 at the origin).



- The problem is trickier than we thought.
- Lets go back to the foundations !

Sound and Relatively Complete procedures

We present two procedures to compute $\texttt{Inwards}(p \geq 0, f, \vec{\mathrm{x}})$, without computing the solution F, for invariant sets specified as $p \geq 0$ for some polynomial p:

1. Based on Tangent cone and Nagumo's theorem.
2. Based on Lie Derivatives.

Resulting rules from both approaches are sound and relatively complete but are not in general decidable.
We will later present a decidable approximation for the rule based on Tangent cones.

Computing Inwards using Nagumo's theorem

Tangent Cone

Let $\mathtt{S} \subset \mathbb{R}^n$ be a closed set. Given any $\vec{\mathtt{x}} \in \mathbb{R}^n$, the tangent cone to $\mathtt{S}$ at $\vec{\mathtt{x}}$ is the set

$$T(\mathtt{S})(\vec{\mathtt{x}}) \quad := \quad \{\vec{\mathtt{z}} \in \mathbb{R}^n \mid \liminf_{\alpha \to 0} \frac{\mathtt{d}(\vec{\mathtt{x}} + \alpha\vec{\mathtt{z}}, \mathtt{S})}{\alpha} = 0\} \qquad (1)$$

where $\mathtt{d}(\vec{\mathtt{x}}, \mathtt{S}) := \inf_{\vec{\mathtt{y}} \in \mathtt{S}} ||\vec{\mathtt{x}} - \vec{\mathtt{y}}||$ is the distance of $\vec{\mathtt{x}}$ from $\mathtt{S}$

Nagumo's theorem

Given a CDS : $\{\mathtt{Init}, \mathtt{X}, f\}$ and a closed set $\mathtt{Inv}$, $\mathtt{Inwards}(\mathtt{Inv}, f, \vec{\mathtt{x}})$ hold iff $\vec{\mathtt{x}} \in T(\mathtt{Inv})(\vec{\mathtt{x}})$.

Thus given a polynomial $p \geq 0$, $f(\vec{\mathtt{x}}) \in T(p \geq 0)(\vec{\mathtt{x}})$ is sufficient to compute $\mathtt{Inwards}(p \geq 0, f, \vec{\mathtt{x}})$.

Computing Inwards using Nagumo's theorem

Tangent Cone

Let $\mathtt{S} \subset \mathbb{R}^n$ be a closed set. Given any $\vec{\mathtt{x}} \in \mathbb{R}^n$, the tangent cone to $\mathtt{S}$ at $\vec{\mathtt{x}}$ is the set

$$T(\mathtt{S})(\vec{\mathtt{x}}) \quad := \quad \{\vec{\mathtt{z}} \in \mathbb{R}^n \mid \liminf_{\alpha \to 0} \frac{\mathtt{d}(\vec{\mathtt{x}} + \alpha\vec{\mathtt{z}}, \mathtt{S})}{\alpha} = 0\} \qquad (1)$$

where $\mathtt{d}(\vec{\mathtt{x}}, \mathtt{S}) := \inf_{\vec{\mathtt{y}} \in \mathtt{S}} ||\vec{\mathtt{x}} - \vec{\mathtt{y}}||$ is the distance of $\vec{\mathtt{x}}$ from $\mathtt{S}$

Nagumo's theorem

Given a $\mathtt{CDS} : \{\mathtt{Init}, \mathtt{X}, f\}$ and a closed set $\mathtt{Inv}$, $\mathtt{Inwards}(\mathtt{Inv}, f, \vec{\mathtt{x}})$ hold iff $\vec{\mathtt{x}} \in T(\mathtt{Inv})(\vec{\mathtt{x}})$.

Thus given a polynomial $p \geq 0$, $f(\vec{\mathtt{x}}) \in T(p \geq 0)(\vec{\mathtt{x}})$ is sufficient to compute $\mathtt{Inwards}(p \geq 0, f, \vec{\mathtt{x}})$.

Computing Inwards using Lie Derivatives

Central Idea: Compute $\mathtt{Inwards}(p \geq 0, f, \vec{x})$ by checking the time derivative $\frac{dp}{dt}$ at $\vec{x}$.

- For any polynomial p, $\frac{dp}{dt} = \vec{\nabla} p \cdot f$
- For any polynomial p, define $L_f^{(n)}(p)$ as the n-th derivative of p with respect to time.

$$L_f^{(n)}(p) \quad := \quad \begin{cases} \vec{\nabla} p \cdot f & \text{if } n = 1 \\ \frac{dL_f^{(n-1)}(p)}{dt} & \text{otherwise} \end{cases} \qquad (2)$$

Computing Inwards

$\mathtt{Inwards}(p \geq 0, f, \vec{x})$ can be computed as

$\bigwedge_{i=1}^{k-1} L_f^{(i)}(p) = 0 \Rightarrow L_f^{(k)}(p) \geq 0$ for $k = 1, 2, \ldots$.

Note that for polynomial f, $L_f^n(p)$ is a polynomial for all n.

Inference Rules

$$\frac{\begin{array}{l}(S1)\ \texttt{Init}(\vec{x}) \implies p(\vec{x}) \geq 0 \\ (S2)\ p(\vec{x}) = 0 \implies f(\vec{x}) \in T(p \geq 0)(\vec{x}) \\ (S3)\ p(\vec{x}) \geq 0 \implies \texttt{Safe}(\vec{x})\end{array}}{\texttt{CDS}\ \textit{is Safe}}$$

$$\frac{\begin{array}{l}(T1)\ \texttt{Init}(\vec{x}) \implies p(\vec{x}) \geq 0 \\ (T2)\ p = 0 \implies (\bigwedge_{i=1}^{k-1} L_f^{(i)}(p) = 0 \Rightarrow L_f^{(k)}(p) \geq 0) \\ \quad \text{for } k = 1, 2, \ldots \\ (T3)\ p(\vec{x}) \geq 0 \implies \texttt{Safe}(\vec{x})\end{array}}{\texttt{CDS}\ \textit{is Safe}}$$

Theorem

For all CDS and safety property Safe

- Soundness: If Inv satisfies Conditions (S1), (S2) and (S3) or Conditions (T1), (T2) and (T3), then $\texttt{Reach}(\texttt{CDS}) \subseteq \texttt{Safe}$.
- Relative Completeness: If $\texttt{Reach}(\texttt{CDS}) \subseteq \texttt{Safe}$ and there is an inductive invariant $p \geq 0$ such that $p \geq 0 \implies \texttt{Safe}$, then $p \geq 0$ also satisfies Conditions (S1), (S2) and (S3) as well as Conditions (T1), (T2) and (T3).

Effectively checkable approximation for Tangent cone based procedure

Given a polynomial p and a point $\vec{x}$ such that $p(\vec{x}) = 0$, we want to check if

$$\liminf_{\alpha \to 0} \frac{\mathtt{d}(\vec{x} + \alpha f(\vec{x}), p \geq 0)}{\alpha} = 0$$

This is equivalent to

$$\exists \alpha_0 > 0 : \forall 0 \leq \alpha \leq \alpha_0 : \exists g_\alpha : \liminf_{\alpha \to 0} \frac{\mathtt{d}(\vec{x} + \alpha f(\vec{x}), p \geq 0, g_\alpha)}{\alpha} = 0$$

where $\mathtt{d}(\vec{x} + \alpha f(\vec{x}), p \geq 0, g_\alpha)$ is distance of $\vec{x} + \alpha f(\vec{x})$ from $p \geq 0$, along direction g_α.

Approximation

$\exists g : \exists \alpha_0 > 0 : \forall 0 \leq \alpha \leq \alpha_0 : \liminf_{\alpha \to 0} \frac{\mathtt{d}(\vec{x} + \alpha f(\vec{x}), p \geq 0, g)}{\alpha} = 0$

Effectively checkable approximation for Tangent cone based procedure

Given a polynomial p and a point $\vec{x}$ such that $p(\vec{x}) = 0$, we want to check if

$$\liminf_{\alpha \to 0} \frac{\mathtt{d}(\vec{x} + \alpha f(\vec{x}), p \geq 0)}{\alpha} = 0$$

This is equivalent to

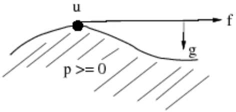
$$\exists \alpha_0 > 0 : \forall 0 \leq \alpha \leq \alpha_0 : \exists g_\alpha : \liminf_{\alpha \to 0} \frac{\mathtt{d}(\vec{x} + \alpha f(\vec{x}), p \geq 0, g_\alpha)}{\alpha} = 0$$

where $\mathtt{d}(\vec{x} + \alpha f(\vec{x}), p \geq 0, g_\alpha)$ is distance of $\vec{x} + \alpha f(\vec{x})$ from $p \geq 0$, along direction g_α.

Approximation

$\exists g : \exists \alpha_0 > 0 : \forall 0 \leq \alpha \leq \alpha_0 : \liminf_{\alpha \to 0} \frac{\mathtt{d}(\vec{x} + \alpha f(\vec{x}), p \geq 0, g)}{\alpha} = 0$

Effectively checkable approximation contd.



Either f moves inside OR there exists a direction g which makes $p = 0$ sufficiently quickly.

Notation

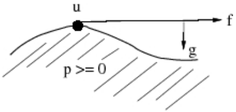
Let $p(\vec{x}+\vec{y})_i$ denote i^{th} homogeneous component of $p(\vec{x}+\vec{y})$ when viewed as a polynomial in $\vec{y}$.

$$\mathrm{pos}(p,\vec{x},\vec{u}) := \bigvee_{k=1}^{n} (p(\vec{x}+\vec{y})_k(\vec{u}) > 0 \wedge \bigwedge_{i=1}^{k-1} p(\vec{x}+\vec{y})_i(\vec{u}) = 0)$$

$$\mathrm{kneg}(p,\vec{x},\vec{u},k) := (p(\vec{x}+\vec{y})_k(\vec{u}) < 0 \wedge \bigwedge_{i=1}^{k-1} p(\vec{x}+\vec{y})_i(\vec{u}) = 0)$$

$$\mathrm{zero}(p,\vec{x},\vec{u}) := \bigwedge_{i=1}^{n} p(\vec{x}+\vec{y})_i(\vec{u}) = 0 \quad \mathrm{neg}(p,\vec{x},\vec{u}) := \bigvee_{i=1}^{n} \mathrm{kneg}(p,\vec{x},\vec{u},i)$$

Effectively checkable approximation contd.



Either f moves inside OR there exists a direction g which makes $p = 0$ sufficiently quickly.

Notation

Let $p(\vec{x}+\vec{y})_i$ denote i^{th} homogeneous component of $p(\vec{x}+\vec{y})$ when viewed as a polynomial in $\vec{y}$.

$$\begin{aligned}
\mathtt{pos}(p,\vec{x},\vec{u}) &:= \bigvee_{k=1}^{n} (p(\vec{x}+\vec{y})_k(\vec{u}) > 0 \wedge \bigwedge_{i=1}^{k-1} p(\vec{x}+\vec{y})_i(\vec{u}) = 0) \\
\mathtt{kneg}(p,\vec{x},\vec{u},k) &:= (p(\vec{x}+\vec{y})_k(\vec{u}) < 0 \wedge \bigwedge_{i=1}^{k-1} p(\vec{x}+\vec{y})_i(\vec{u}) = 0) \\
\mathtt{zero}(p,\vec{x},\vec{u}) &:= \bigwedge_{i=1}^{n} p(\vec{x}+\vec{y})_i(\vec{u}) = 0 \quad \mathtt{neg}(p,\vec{x},\vec{u}) := \bigvee_{i=1}^{n} \mathtt{kneg}(p,\vec{x},\vec{u},i)
\end{aligned}$$

Effectively checkable approximation contd.

$$(F1)\ \texttt{Init} \implies p \geq 0$$

$$(F2)\ p = 0 \Rightarrow \neg\texttt{neg}(p, \vec{\texttt{x}}, f) \vee \bigvee_{k=2}^{n} (\texttt{kneg}(p, \vec{\texttt{x}}, f, k) \wedge \bigvee_{l<k} (\exists g : \texttt{pos}(p_l, f, g) \wedge \bigwedge_{j<l} \texttt{zero}(p_j, f, g)))$$

$$\frac{(F3)\ p \geq 0 \Rightarrow \texttt{Safe}}{\texttt{CDS}\ \textit{is safe}}$$

Theorem

For all CDS and safety property Safe

- Soundness: If Inv satisfies Conditions (F1), (F2) and (F3) then Reach(CDS) $\subseteq$ Safe.
- Relative Completeness: If Reach(CDS) $\subseteq$ Safe and there is an inductive invariant $p \geq 0$ such that $p \geq 0 \implies$ Safe and $p \geq 0$ is a convex, then $p \geq 0$ also satisfies Conditions (F1), (F2) and (F3).

Open Problem: Sound and Relatively Complete rules for the entire class of polynomial CDS with polynomial inductive invariants.

Effectively checkable approximation contd.

$$(F1)\ \texttt{Init} \implies p \geq 0$$

$$(F2)\ p = 0 \Rightarrow \neg\texttt{neg}(p, \vec{\mathtt{x}}, f) \vee \bigvee_{k=2}^{n} (\texttt{kneg}(p, \vec{\mathtt{x}}, f, k) \wedge \bigvee_{l<k} (\exists g : \texttt{pos}(p_l, f, g) \wedge \bigwedge_{j<l} \texttt{zero}(p_j, f, g)))$$

$$\frac{(F3)\ p \geq 0 \Rightarrow \texttt{Safe}}{\texttt{CDS}\ \textit{is safe}}$$

Theorem

For all CDS and safety property Safe

- Soundness: If Inv satisfies Conditions (F1), (F2) and (F3) then $\texttt{Reach}(\texttt{CDS}) \subseteq \texttt{Safe}$.
- Relative Completeness: If $\texttt{Reach}(\texttt{CDS}) \subseteq \texttt{Safe}$ and there is an inductive invariant $p \geq 0$ such that $p \geq 0 \implies \texttt{Safe}$ and $p \geq 0$ is a convex, then $p \geq 0$ also satisfies Conditions (F1), (F2) and (F3).

Open Problem: Sound and Relatively Complete rules for the entire class of polynomial CDS with polynomial inductive invariants.

Ongoing and Future Work

Ongoing Work:

- Deductive techniques for synthesizing switching logic for safe hybrid systems: search for controlled inductive invariants (VMCAI'09).
- Deductive techniques for checking reachability: search for Lyapunov functions (submitted to HSCC'09).

Future Work:

- Extend the verification rule to full-fledged hybrid systems.
- Deductive techniques for verifying other properties like stability, reachability+safety etc.
- Design good exists-forall solvers to automate the verification/synthesis procedure.

Thank You !