Verifying tolerant systems using polynomial approximations

Pavithra Prabhakar

University of Illinois at Urbana-Champaign

Joint work with Vladimeros Vladimerou, Mahesh Viswanathan and Geir Dullerud

12 September 2009

Outline

Motivation

- Hybrid system: mixed discrete-continuous behavior.
  - Embedded processors, electronic controllers.
- Complex continuous behavior.
  - Approximate into system with simple continuous dynamics.
- Polynomial approximations.
  - Decidable properties: Reachability in bounded executions.

Overview of results

- Given $\mathcal{H}$, construct $Poly_\epsilon(\mathcal{H})$.
  - Approximate simulation: Every execution of $\mathcal{H}$ is closely simulated by an execution of $Poly_\epsilon(\mathcal{H})$.
  - Tight simulation: $Poly_\epsilon(\mathcal{H})$ is ϵ-simulated by an overapproximation of $\mathcal{H}$.
  - If the approximation satisfies certain properties, then one can infer that the original system satisfies certain properties.

Overview of results

- Given $\mathcal{H}$, construct $Poly_\epsilon(\mathcal{H})$.
  - Approximate simulation: Every execution of $\mathcal{H}$ is closely simulated by an execution of $Poly_\epsilon(\mathcal{H})$.
  - Tight simulation: $Poly_\epsilon(\mathcal{H})$ is ϵ-simulated by an overapproximation of $\mathcal{H}$.
  - If the approximation satisfies certain properties, then one can infer that the original system satisfies certain properties.
- Verifying Tolerant systems.
  - Systems whose property does not change with small perturbations in the parameters.
  - Verifying the approximation is equivalent to verifying the original system.

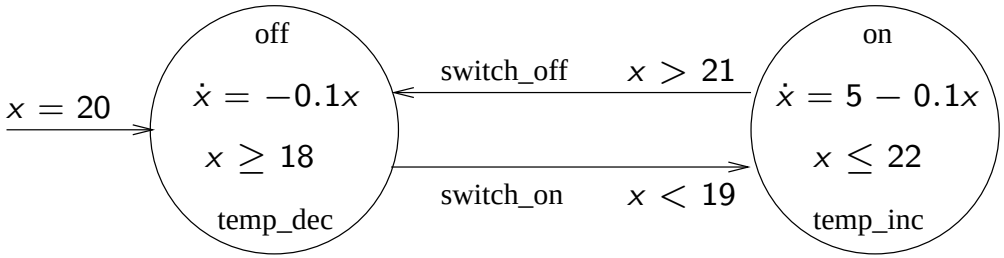
Outline

Hybrid system

A hybrid automaton $\mathcal{H}$ is a tuple $\mathcal{H} = (Loc, Actions, Labels, q_0, edges, Cont, Cont_0, flow, invariant, guard, reset, \mathcal{L})$:

- Loc - finite set of locations,
- $Actions$ - finite set of action labels,
- $Labels$ -finite set of location labels,
- $loc_0 \in Loc$ - initial location,
- $edges \subseteq Loc \times Actions \times Loc$,
- $Cont = \mathbb{R}^n$ - set of continuous states,
- $Cont_0 \subseteq Cont$ - initial continuous states,
- $flow : Loc \times Cont \rightarrow (\mathbb{R}_+ \rightarrow Cont)$,
- $invariant : Loc \rightarrow 2^{Cont}$,
- $guard : edges \rightarrow 2^{Cont}$,
- $reset : edges \rightarrow 2^{Cont \times Cont}$, and
- $\mathcal{L} : Loc \rightarrow Labels$ - location labelling function.

Example: thermostat



- $Loc = \{off, on\}$, $loc_0 = off$,
- $Actions = \{switch\_on, switch\_off\}$,
- $Labels = \{temp\_dec, temp\_inc\}$,
- $edges = \{(off, switch\_on, on), (on, switch\_off, off)\}$,
- $Cont = \mathbb{R}$, $Cont_0 = \{20\}$,
- $flow(off, x, t) = xe^{-0.1t}$ and $flow(on, x, t) = \cdots$,
- $invariant(off) = \{x \mid x \geq 18\}$ and $invariant(on) = \cdots$,
- $guard(off, switch\_on, on) = \{x \mid x < 19\}$ and $guard(on, switch\_off, off) = \cdots$,
- $reset(off, switch\_on, on) = reset(on, switch\_off, off) = \{(x, x) \mid x \in \mathbb{R}\}$,
- $\mathcal{L}(off) = temp\_dec, \mathcal{L}(on) = temp\_inc$.

Transition system

$\mathcal{T} = (Q, \Sigma, Prop, \{\rightarrow_a\}_{a \in \Sigma}, \langle\langle \cdot \rangle\rangle)$, where:

- Q is a (finite or infinite) set of states,
- Σ is a finite set of trasition labels,
- $Prop$ is a (finite or infinite) set of state labels,
- $\rightarrow_a \subseteq Q \times Q$, and
- $\langle\langle \cdot \rangle\rangle : Q \rightarrow Prop$.

Semantics of Hybrid Systems

$[\![\mathcal{H}]\!] = (Q, \Sigma, Prop, \{\rightarrow_a\}_{a\in\Sigma}, \langle\!\langle\cdot\rangle\!\rangle)$:

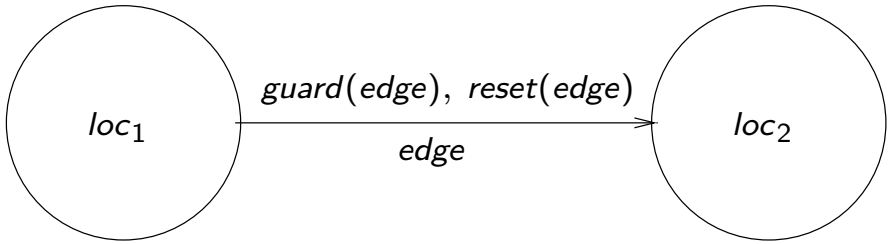
- $Q = Loc \times X$,
- $\Sigma = Actions \cup \mathbb{R}_{\geq 0}$,
- $Prop = Labels \times \mathbb{R}^n$,
- $(l, x) \rightarrow_a (l', x')$:
  - Discrete transitions: $a \in Actions$,
  - Continuous transitions: $a \in \mathbb{R}_{\geq 0}$,
- $\langle\!\langle (l, x) \rangle\!\rangle = (\mathcal{L}(l), x)$.

Semantics of HS

Discrete transitions

$(loc_1, x_1) \rightarrow_a (loc_2, x_2)$ iff $\exists edge = (loc_1, a, loc_2)$:

- $x_1 \in guard(edge)$, and
- $(x_1, x_2) \in reset(edge)$.

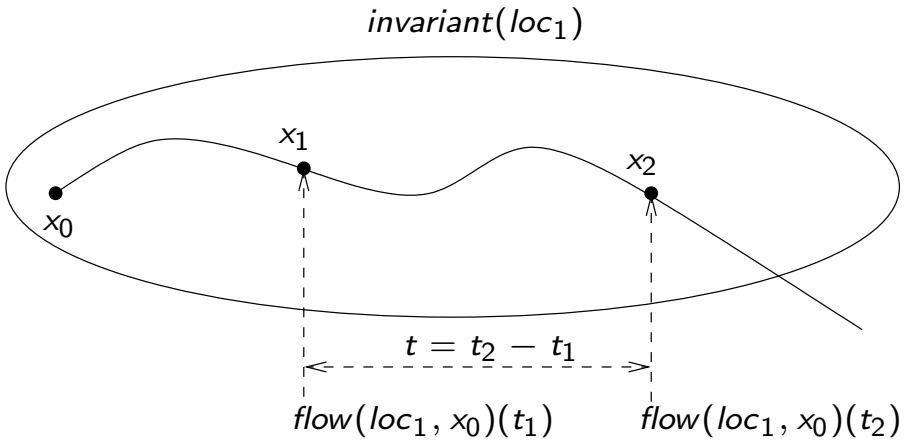


Semantics of HS

Continuous transitions

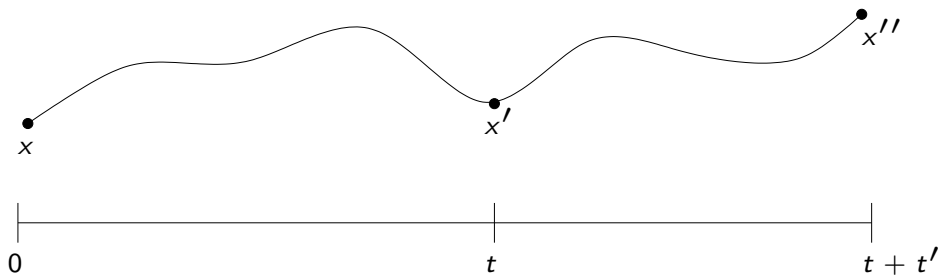
$(loc_1, x_1) \rightarrow_t (loc_2, x_2)$ iff

- $loc_1 = loc_2$,
- $\exists x_0, t_1, t_2$ such that $flow(loc_1, x_0)(t_1) = x_1$, $flow(loc_1, x_0)(t_2) = x_2$, $t = t_2 - t_1$ and for all $t' \in [0, t_2]$, $flow(loc_1, x_0)(t') \in invariant(loc_1)$.



Consistent Flows

- $flow(loc, x)$ is continuous and $flow(loc, x)(0) = x$.
- $flow(loc, x)(t + t') = flow(loc, x')(t')$ where $x' = flow(loc, x)(t)$.



Outline

Outline

Stone-Weierstrass Theorem

Polynomial function

A function $f : \mathbb{R}^n \rightarrow \mathbb{R}$ is a polynomial function if there exists a polynomials $P(x_1, \cdots, x_n)$ such that for all $v \in \mathbb{R}^n$, $f(v) = P(v)$.

Stone-Weierstrass Theorem

Polynomial function

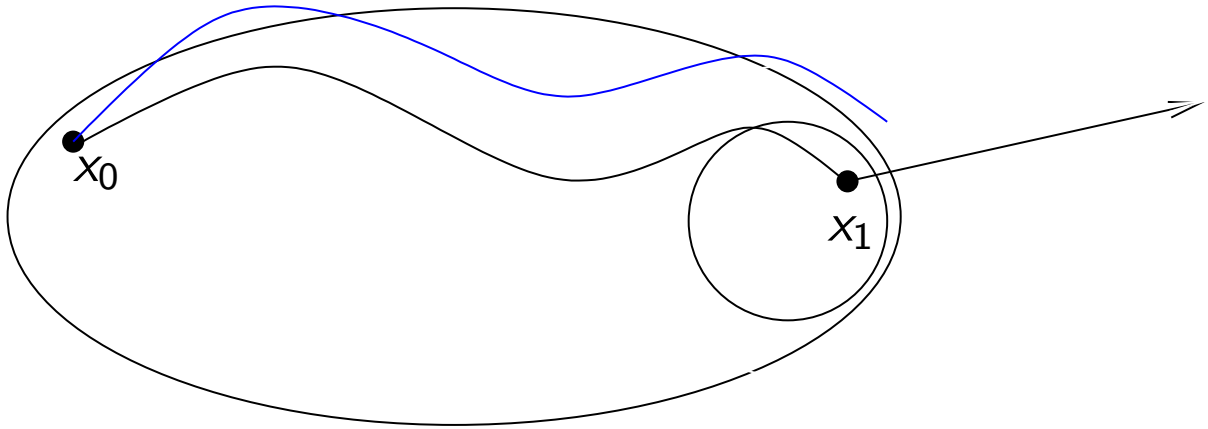
A function $f : \mathbb{R}^n \rightarrow \mathbb{R}$ is a polynomial function if there exists a polynomials $P(x_1, \cdots, x_n)$ such that for all $v \in \mathbb{R}^n$, $f(v) = P(v)$.

Theorem

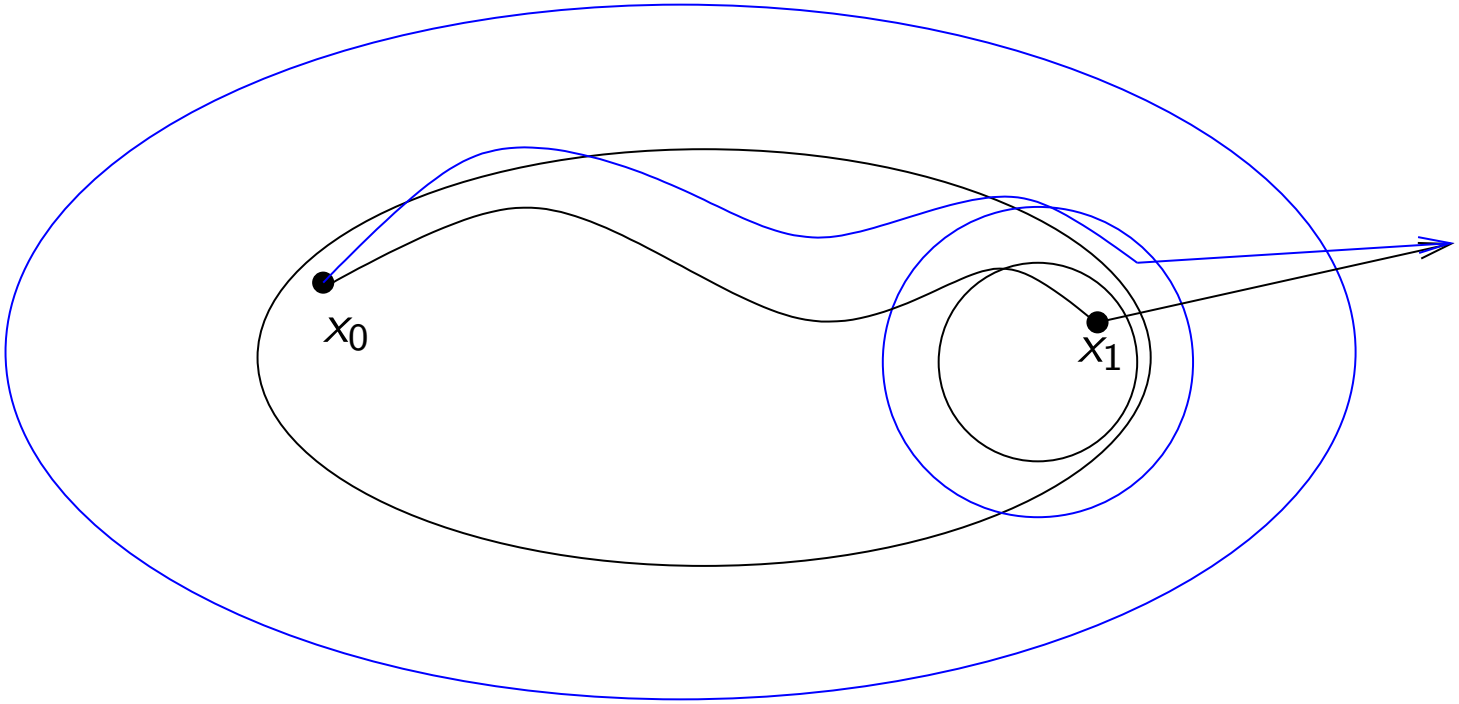
Given any continuous function $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$, a compact subset K of $\mathbb{R}^n$ and $\epsilon > 0$, there exists a polynomial function $P : \mathbb{R}^n \rightarrow \mathbb{R}^m$ such that

$$|f(x) - P(x)| < \epsilon, \forall x \in K.$$

Polynomial approximation of $\mathcal{H}$

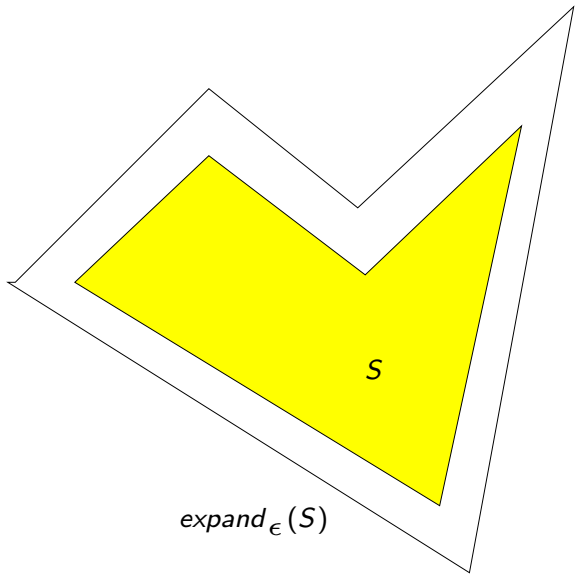


Polynomial approximation of $\mathcal{H}$



Expansion of a set

Given a set $S \subseteq \mathbb{R}^n$ and $\epsilon > 0$,
$expand_\epsilon(S) = \{x \mid \exists y \in S, |x - y| < \epsilon\}$.



Polynomial approximation of $\mathcal{H}$

$Poly_\epsilon(\mathcal{H})$ is given by:

- Continuous state space: (x_0, t, x) such that $x = flow(x_0, t)$.
- Polynomial flow function: value of the function at location l, continuous state (x_0, t_1, x_1) and time t is given by $(x_0, t_1 + t, P_{\epsilon,l}(x_0, t_1 + t))$.
- Invariant of a location l: $invariant(l) \times \mathbb{R}_{\geq 0} \times expand_\epsilon(invariant(l))$.
- Guard of an edge e: $invariant(l) \times \mathbb{R}_{\geq 0} \times expand_\epsilon(guard(e)))$.
- Reset of an edge e: $((x_0, t_1, x_1), (x_2, 0, x_2))$ such that $(x_1', x_2) \in reset(e)$ for some x' with $|x' - x| \leq \epsilon$.
- Label of state $(l, (x_0, t_1, x_1))$: $\mathcal{L}(l, x)$.

$Poly_\epsilon(\mathcal{H})$ "closely" simulates $\mathcal{H}$.

Outline

Metric space

A metric space $\mathcal{M}$ is a pair (M, d) where M is a set and $d : M \times M \to \mathbb{R}_{\geq 0} \cup \{\infty\}$ such that for all m_1, m_2 and m_3,

1. (Non-negativity) $d(m_1, m_2) \geq 0$.
2. (Identity of indiscernibles) $d(m_1, m_2) = 0$ if and only if $m_1 = m_2$.
3. (Symmetry) $d(m_1, m_2) = d(m_2, m_1)$.
4. (Triangle inequality) $d(m_1, m_3) \leq d(m_1, m_2) + d(m_2, m_3)$.

Metric Transition System

A transition system with a distance metric d on $Prop$ is a metric transition system.

$[\![\mathcal{H}]\!]$ as a metric transition system

- $Prop = Labels \times \mathbb{R}^n$.
- $d((l, x), (l', x')) = |x - x'|$ if $l = l'$ and ∞ otherwise.

Simulation

Given transition systems $\mathcal{T}_1$ and $\mathcal{T}_2$ over Σ and *Prop*, $R \subseteq Q_1 \times Q_2$ is said to be a *simulation* between $\mathcal{T}_1$ and $\mathcal{T}_2$ if and only if for all $(q_1, q_2) \in R$:

1. $\langle\langle q_1 \rangle\rangle_1 = \langle\langle q_2 \rangle\rangle_2$, and
2. if $q_1 \rightarrow_a q_1'$ then there is a q_2' s.t. $q_2 \rightarrow_a q_2'$ and $(q_1', q_2') \in R$.

ϵ-simulation

Given metric transition systems $\mathcal{T}_1$ and $\mathcal{T}_2$ over Σ and $(Prop, d)$, $R \subseteq Q_1 \times Q_2$ is said to be an ϵ-simulation between $\mathcal{T}_1$ and $\mathcal{T}_2$ if and only if for all $(q_1, q_2) \in R$:

1. $d(\langle\langle q_1 \rangle\rangle_1, \langle\langle q_2 \rangle\rangle_2) < \epsilon$, and
2. if $q_1 \rightarrow_a q_1'$ then there is a q_2' s.t. $q_2 \rightarrow_a q_2'$ and $(q_1', q_2') \in R$.

We say $T_1 \preceq_\epsilon T_2$.

Safe Henessy-Milner Logic (SHM)

SHM(Σ, *Prop*)

$$\phi ::= P \mid [a]\phi \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2$$

Safe Henessy-Milner Logic (SHM)

SHM(Σ, *Prop*)

$$\phi ::= P \mid [a]\phi \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2$$

$SatFor(q) = \{\phi \in SHM \mid T, q \models \phi\}$.

Safe Henessy-Milner Logic (SHM)

SHM(Σ, *Prop*)

$$\phi ::= P \mid [a]\phi \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2$$

$SatFor(q) = \{\phi \in SHM \mid T, q \models \phi\}$.

Theorem (Milner)

Let $\mathcal{T}_1$ and $\mathcal{T}_2$ be two transition systems and let q_1 be a state of $\mathcal{T}_1$ and q_2 be a state of $\mathcal{T}_2$. Then:

1. $q_1 \preceq q_2$ *implies* $SatFor(q_2) \subseteq SatFor(q_1)$.
2. $\mathcal{T}_2$ *is finite branching and* $SatFor(q_2) \subseteq SatFor(q_1)$ *implies* $q_1 \preceq q_2$.

Logical characterization of ϵ-simulations

$shrink_\epsilon(\phi)$

Replace each P in ϕ by
$shrink_\epsilon(P) = \{x \mid \forall x', |x' - x| < \epsilon \implies x' \in P\}$.

Logical characterization of ϵ-simulations

$shrink_\epsilon(\phi)$

Replace each P in ϕ by
$shrink_\epsilon(P) = \{x \mid \forall x', |x' - x| < \epsilon \implies x' \in P\}$.

Theorem

Let $\mathcal{T}_1$ and $\mathcal{T}_2$ be two metric transition systems. Let q_1 and q_2 be states in $\mathcal{T}_1$ and $\mathcal{T}_2$ respectively. Then

1. $q_1 \preceq_\epsilon q_2 \Rightarrow SatFor(q_2) \subseteq shrink_\epsilon(SatFor(q_1))$.
2. *$\mathcal{T}_2$ is finite branching and $SatFor(q_2) \subseteq shrink_\epsilon(SatFor(q_1))$ $\Rightarrow q_1 \preceq_\epsilon q_2$.*

Outline

Relating $\mathcal{H}$ and $Poly_\epsilon \mathcal{H}$

Approximate simulation:

Theorem

$[\![\mathcal{H}]\!] \preceq_\epsilon [\![Poly_\epsilon(\mathcal{H})]\!]$.

Relating $\mathcal{H}$ and $Poly_\epsilon \mathcal{H}$

Approximate simulation:

Theorem

$[\![\mathcal{H}]\!] \preceq_\epsilon [\![Poly_\epsilon(\mathcal{H})]\!]$.

Tightness of approximation:

$expand_\epsilon(\mathcal{H})$

Expand the invariants, guards and resets of $\mathcal{H}$.

Relating $\mathcal{H}$ and $Poly_\epsilon\mathcal{H}$

Approximate simulation:

Theorem

$[\![\mathcal{H}]\!] \preceq_\epsilon [\![Poly_\epsilon(\mathcal{H})]\!]$.

Tightness of approximation:

$expand_\epsilon(\mathcal{H})$

Expand the invariants, guards and resets of $\mathcal{H}$.

Theorem

$[\![Poly_\epsilon(\mathcal{H})]\!] \preceq_\epsilon [\![expand_{2\epsilon}(\mathcal{H})]\!]$.

Properties of polynomial approximation

Application to verification

- $q_1 \preceq_\epsilon q_2 \Rightarrow \mathit{SatFor}(q_2) \subseteq \mathit{shrink}_\epsilon(\mathit{SatFor}(q_1))$.
- If $\mathit{Poly}_\epsilon(\mathcal{H}) \models \mathit{shrink}(\phi)$, then $\mathcal{H} \models \phi$.
- $\mathit{Poly}_\epsilon(\mathcal{H}) \models \mathit{shrink}(\phi)$ decidable when the invariants, guards, resets of $\mathcal{H}$ and atomic propositions in ϕ are all definable in $(\mathbb{R}, <, +, \cdot)$.

Properties of polynomial approximation

Application to verification

- $q_1 \preceq_\epsilon q_2 \Rightarrow \mathit{SatFor}(q_2) \subseteq \mathit{shrink}_\epsilon(\mathit{SatFor}(q_1))$.
- If $\mathit{Poly}_\epsilon(\mathcal{H}) \models \mathit{shrink}(\phi)$, then $\mathcal{H} \models \phi$.
- $\mathit{Poly}_\epsilon(\mathcal{H}) \models \mathit{shrink}(\phi)$ decidable when the invariants, guards, resets of $\mathcal{H}$ and atomic propositions in ϕ are all definable in $(\mathbb{R}, <, +, \cdot)$.

What if $\mathit{Poly}_\epsilon(\mathcal{H}) \not\models \mathit{shrink}(\phi)$?

Outline

Tolerant systems

ϵ-tolerance

$$\mathcal{H} \models \phi \implies \mathit{expand}_\epsilon(\mathcal{H}) \models \mathit{shrink}_\epsilon(\phi).$$

Tolerant systems

ϵ-tolerance

$\mathcal{H} \models \phi \implies expand_\epsilon(\mathcal{H}) \models shrink_\epsilon(\phi)$.

Theorem

$\mathcal{H}$ 2ϵ-tolerant with respect to ϕ implies:

$$\mathcal{H} \models \phi \Leftrightarrow Poly_\epsilon(\mathcal{H}) \models shrink_\epsilon(\phi).$$

Tolerant systems

Theorem

Deciding whether $\mathcal{H}$ is ϵ-tolerant with respect to ϕ is equivalent to deciding if $\mathcal{H} \models \phi$.

Nevertheless, we have

- $Poly_\epsilon(\mathcal{H}) \models shrink_\epsilon(\phi)$ implies $\mathcal{H} \models \phi$.
- $Poly_\epsilon(\mathcal{H}) \not\models shrink_\epsilon(\phi)$ implies either $\mathcal{H} \not\models \phi$ or $\mathcal{H}$ is not tolerant.

Stone Weierstrass Theorem in Practice

- Taylor approximation by taking the first few terms of the Taylor expansion.
- Bernstein polynomial approximates the function by sampling at various points.
- When given as a differential equation, collocation methods can be used.

Conclusions

- Presented a technique to approximate hybrid systems with arbitrary flows by hybrid systems with polynomial flows.
- For tolerant systems, verfying its safety is equivalent to verifying polynomial approximation.
- Gave a logical characterization of the ϵ-simulation.