VERIMAC
E. Asarin, T. Danes, and O. Maler

Continuous and Hybrid Systems

d/dt: A Tool for Reachability Analysis of
Outline

1. Introduction
2. Reachability problem and our approach
3. Reachability technique for non-linear continuous systems
4. Reachability technique for linear continuous systems
5. Analysis of hybrid systems: verification and controller synthesis
6. The tool d/t
Numerical approximation of the reachable set

\[ \Leftrightarrow \]

Exact symbolic computation: applicable for restricted classes

- Intersection with other sets
  - Representation of reachable sets that can be tested for
  - Characterizing the set of states reachable from the set \( \mathcal{F} \)
  
  \[ x(t) \in \mathcal{F}, \text{ set of initial states} \]
  \[ x(t) \in \mathcal{V}, \text{ bounded subset of } \mathcal{R}^n \]

The basic problem for Continuous Systems
\[
((\mathcal{A})^{[1\tau,0]\varrho})^{[\varrho,0]} = (\mathcal{A})^{[\varrho,1+1\tau,0]\varrho} = (\mathcal{A})^{(\infty,0]\varrho} = (\mathcal{A})^{(0,0]\varrho} = (\mathcal{A})^\varrho
\]

Semigroup property: \( \varrho \rightarrow \) reachable set
\[ I \supseteq \mathcal{A} \text{ set of states reachable from } I \text{ in time } \tau \]
\[ [\tau,1+\tau] = I \text{ and } a \text{ time interval } \mathcal{X} \subseteq \mathcal{A} \]

Reachability operators
Perform set union equivalence testing

Compute $g_0^{i+1}$ of a set $M_i$

Problems

Until $\left( I_{1-\gamma d_0} = \gamma d_1 \right)$

$I_1 - \gamma d_0 \cap I_{1-\gamma d_0} = \gamma d_1$

$I_1 + \gamma = \gamma$

Repeat

$\gamma = 0$

$H = \{ 0 \}$

Abstract Algorithm for Computing $g(M)$
Approximation by Orthogonal Polyhedra

- Reachable sets are often non-convex ⇒ difficulty in representing and manipulating arbitrary non-convex polyhedra

⇒ Orthogonal Polyhedra
  - Canonical representation, relatively efficient manipulation
  - Easy termination checking
  - Over-approximation (verification), under-approximation (synthesis)

Arbitrary polyhedra

Orthogonal polyhedra
Approximation by Orthogonal Polyhedra (cont’d)

Accumulation of over-approximation errors
Consider the evolution in the outward normal direction of each face of $\mathcal{P}$.

The set is polyhedral $\mathcal{P}$ is the union of its faces.

Continuity of trajectories $\Rightarrow$ Continuity of trajectories from the boundary $\mathcal{P}$.

Reachability technique, inspired by [Greenstreet 96]

A non-linear continuous system: $x'(t) = f(x)$, $x(0) = x_0$ is the set of initial states.
Face $e$ 

$\phi_{(e)}^N$ max of $f^e$ over $f^e$ face $e$ 

projection of $\mathbf{x}$ on the outward normal vector $\mathbf{u}$ of $\mathcal{N}_{(e)}$ 

Step 2 - More precise approximation 

intectors starting from $\mathcal{N}$ for at least $t$ time. 

Step 1 - Rough approximation: neighborhood $\mathcal{N}$ such that all 

Face Tilting Technique
Orthogonal polyhedra are closed under the lift-time operation — Faces can be systematically enumerated using orthogonal polyhedra.

Face Lift: using Orthogonal Polyhedra
We exploit this property to approximate $\varphi(H)$, which can be computed by a finite number of integrations.

\begin{itemize}
  \item $x_{FA}^\varphi = (x_{FA}^\varphi, 1) \in \varphi(H)$, with $\{x_{FA}^\varphi = (x_{FA}^\varphi, 1)\}$ is the set of initial states, $FA = FA^\varphi = (FA^\varphi, 1)$.
\end{itemize}

A linear continuous system: $x = FA$, $H$ is the set of initial states.

Reachability of Linear Continuous Systems.
Approximate Computation of \( \varphi(H) \)
Example
Linear Systems with Uncertain Input
Example of Linear Continuous Systems with Input
Hybrid Dynamical Systems

\[ (x)^T_H = \frac{x}{1^T_H} \in x \]

\[ (x)^f = x \]

\[ (x)^T_I = \frac{x}{1^I} \in x \]

\[ (x)^R + x^{bb}A = (x)^{bb}H \]

reset functions associated with transitions affine of the form

reseting conditions

switching conditions

quadrants

convex polyhedra

polyhedra

switching conditions

stability conditions

stability

convex conditions

convex

differential equations

continuous dynamics of the models are defined by differential equations

several models (discrete states, locations)
Reachability by discrete transitions (discrete-successors) • Reachable sets by discrete transitions (continuos-successors) • Reachable sets by continuous dynamics

Reachability procedure requires the computation of

changed according to the reset function

By discrete transitions: Location changes, and \( x \) can be

By continuous dynamics: Location remains constant, and \( x \)

The state \((b, x)\) of the system can change in two ways:

Reachability analysis of Hybrid Systems
Boolean and geometric operations on polyhedra

\[ (\{bH \cup b\overline{b}C \cup A\}, b\overline{b}H) \]

Set of discrete-successors of set \( A \) by transition from \( b \) to \( \overline{b} \)

Computation of discrete-successors

Computation of continuous-successors

Reachability Technique for Hybrid Systems
Example
The states which can stay in \( F \) and reach \( C \):

\[
[0.02, 0.06] \times [-0.05, 0.02] = C
\]

\[
\begin{pmatrix}
-3.0 & -0.5 \\
4.0 & -0.5
\end{pmatrix} = A
\]

Given two subsets \( F \) and \( C \), calculate \( F \cup C \).

**Example:** \( F \cup C \)
Future work

- Improved interaction with linear continuous dynamics
- Safety verification for hybrid systems
- Safety verification of hybrid systems
- Hybrid systems
- Non-linear continuous systems
- Linear continuous systems
- Reachability analysis

Three functionalities

The tool d/
Some Related Works

- Verification via mathematical programming [Bemporad and Morari 99]
- Verifying 01- and Σ01-Properties [Pappas, Latier and Yovine 99; Anai and Katoen 99]
- Flow-Pipe Approximation [Chutinan and Krogh 99]
- and Variations 00
- Ellipsoidal Techniques [Kurzhanski and Valyi 97; Kurzhanski]
- Intersection Projection [Greenstreet 96]