SpaceEx:
Vers un passage à l’échelle dans la vérification des systèmes hybrides

Goran Frehse, Rajarshi Ray, Alexandre Donzé, Olivier Lebeltel, Rodolfo Ripado, Thao Dang, Oded Maler
Université Grenoble 1 Joseph Fourier – Verimag, France

Scott Cotton
Complex and Adaptive Systems Lab, University College Dublin, Ireland

Antoine Girard
Laboratoire Jean Kuntzmann, France

Colas Le Guernic
New York University CIMS

Réunion SDH/MEA
Paris, 3 février 2011
Outline

- Computing Reachable States
- Efficient Set Operations using Support Functions
- SpaceEx Verification Platform
Outline

- Computing Reachable States
- Efficient Set Operations using Support Functions
- SpaceEx Verification Platform
Nondeterministic Affine Dynamics

● Linear dynamics plus inputs:

\[ \dot{x} = Ax + Bu, \quad x \in \mathbb{R}^n, u \in U \subseteq \mathbb{R}^p \]

- variables \( x_1, \ldots, x_n \), inputs \( u_1, \ldots, u_p \)

● Input \( u \) models nondeterminism

\[ \dot{x} \in Ax + BU \]

- used later for overapproximating nonlinear dynamics
Hybrid Automaton Model: Bouncing Ball

Free fall:
\[ x \geq 0 \]
\[ \dot{x} = v \]
\[ \dot{v} = -g \]

Bounce:
\[ x = 0 \land v < 0 \]
\[ v := -cv \]
Computing Reachable States

- Compute sets of successor states
  - discrete transitions: $Post_d(R)$
  - time elapse: $Post_c(R)$

\[ R_1 = Post_c(R_0) \]
\[ R_2 = Post_d(R_1) \]
\[ R_3 = Post_c(R_2) \]
Reachability by Time-Discretization

● **Goal:**
  - Compute sequence $\Omega_k$ over bounded time $[0,N\delta]$ such that:
    $$\text{Reach}_{[0,N\delta]}(X_{Ini}) \subseteq \Omega_0 \cup \Omega_1 \cup \ldots \cup \Omega_N$$

● **Approach:**
  - Refine $\Omega_k$ by recurrence:
    $$\Omega_{k+1} = e^{A\delta} \Omega_k \oplus V$$
  - Condition for $\Omega_0$:
    $$\text{Reach}_{[0,\delta]}(X_{Ini}) \subseteq \Omega_0$$

E. Asarin, O. Bournez, T. Dang, and O. Maler. Approximate Reachability Analysis of Piecewise-Linear Dynamical Systems. HSCC'00
Time-Discretization with Convex Hull

● Overapproximating $\text{Reach}_{[0,\delta]}$: $\text{Reach}_{[0,\delta]}(X_{\text{Ini}})$, $\text{Conv}(X_0, X_1)$, $\text{Bloat}(\text{Conv}(X_0, X_1))$
Time-Discretization with Convex Hull

Bouncing Ball:
Effect of the Time Step on Accuracy

(a) $\delta = 0.5$  
(b) $\delta = 0.2$  
(c) $\delta = 0.05$
Nondeterministic Affine Dynamics

- Overapproximated Solution in Discretized Time
  
  \[ V = \text{box with radius } \frac{e^{\|A\|\delta} - 1}{\|A\|} \sup_{u \in U} \|Bu\| \]

\[
\begin{align*}
\Omega_0 &= Bloat(Conv(X_{Ini}, e^{A\delta} X_{Ini})) \oplus V \\
\Omega_{k+1} &= e^{A\delta} \Omega_k \oplus V
\end{align*}
\]

- Minkowski Sum: \( A \oplus B = \{a + b \mid a \in A, b \in B\} \)
Nondeterministic Affine Dynamics

\[ \Omega_2 = e^{A\delta} \Omega_1 \oplus V \]
Outline

- Computing Reachable States
- Efficient Set Operations using Support Functions
- SpaceEx Verification Platform
Support Functions

\[ \rho_P(d) = \max_{x \in P} d^T x \]

max. signed distance of \( P \) to origin projected in direction \( d \)
If we know the value of $\rho_P(d)$, we know $P$ is in the halfspace

$$\{ x \mid d^T x \leq \rho_P(d) \}$$
If we know $\rho_P(d_1), \rho_P(d_2), \ldots$ we know $P$ is inside the intersection of the halfspaces

$= \text{outer polyhedral approx.}$
Overapproximation with Template Directions

(a) box

(b) octagonal

(c) 16 uniform
Computing with Support Functions

- Many set operations are simple operations on support functions
  - Affine Transform: \( \rho_{AP}(d) = \rho_P(A^T d) \)
  - Minkowski sum: \( \rho_{P \oplus Q}(d) = \rho_P(d) + \rho_Q(d) \)
  - Convex hull: \( \rho_{chull(P,Q)}(d) = \max(\rho_P(d), \rho_Q(d)) \)

- Problems:
  - Containment: use outer/inner polyhedral approx.
  - Intersection: intersection with halfspace
    = scalar convex minimization problem

C. Le Guernic, A. Girard. Reachability analysis of hybrid systems using support functions. CAV’09
## Comparison of Set Representations

<table>
<thead>
<tr>
<th>Operators</th>
<th>Polyhedra</th>
<th>Zonotopes</th>
<th>Support Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Constraints</td>
<td>Vertices</td>
<td></td>
</tr>
<tr>
<td>Affine transform</td>
<td>-</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>Minkowski sum</td>
<td>--</td>
<td>-</td>
<td>++</td>
</tr>
<tr>
<td>Intersection</td>
<td>++</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Containment</td>
<td>++</td>
<td>-</td>
<td>?</td>
</tr>
<tr>
<td>Convex hull</td>
<td>--</td>
<td>++</td>
<td>-</td>
</tr>
</tbody>
</table>

- indicates not supported
+ indicates supported
C. Le Guernic, A. Girard. Reachability analysis of hybrid systems using support functions. CAV'09
Clustering

• After discrete jump, every convex set spawns a new flowpipe

- Reduce number to avoid explosion
- How many sets?
- Bound approximation error
Clustering

- After discrete jump, every convex set spawns a new flowpipe

- Template hull of all sets

  $\Rightarrow$ 1 set, big error

large error
Clustering

- After discrete jump, every convex set spawns a new flowpipe

- Template hull up to given error bound

  ⇒ low number of sets

- Small error
Even a low number of sets might be still too much

- 2 sets ⇒ possibly $2^k$ sets at iteration $k$
- aggregate using convex hull

⇒ 1 set, good accuracy
Outline

- Computing Reachable States
- Efficient Set Operations using Support Functions
- SpaceEx Verification Platform
SpaceEx Platform - Architecture

Model Editor

System Model

User Options

Specification

Visualization

Text Output / File Download

Web Browser

Web Server

Web Interface

local
remote / Virtual Machine

SpaceEx Analysis Core

User Options

Visualization

Text Output / File Download
SpaceEx Model Editor

- Construct hierarchical models

Editing Automata = basic components

Composing Components (nested, hierarchical)
SpaceEx Model Editor

- Connecting Components
SpaceEx Web Interface

http://spaceex.imag.fr/
Example: Filtered Switched Oscillator

- **Switched oscillator**
  - 2 state variables
  - similar to many circuits
    (Buck converters,…)

- **plus** $m^{th}$ **order filter**
  - dampens output signal

- **Piecewise affine dynamics**
  - 4 discrete states
  - total $2 + m$ continuous state variables
Filtered Switched Oscillator

- 2\textsuperscript{nd} order oscillator + 4\textsuperscript{th} order filter
  - 6 state variables

\[ m = 2n \] box constraints (axis directions)

\[ m = 2n^2 \] octagonal constraints \((\pm x_i \pm x_j)\)
Empirical Complexity Measurements

- **Filtered Oscillator**: Average time per iteration
  - fixed constraints (200), varying dimension

\[
t \quad O(n), \text{ expected from LP}
\]
Empirical Complexity Measurements

- **Filtered Oscillator**: Average time per iteration
  - fixed dimension (8 variables), varying nb of constraints

\[
y = 0.0048x^{1.5745}
\]

\[O(m^2), \text{ ok for LP}\]
Empirical Complexity Measurements

- **Filtered Oscillator**: Total runtime $\sim O(nm^2)$
Clustering & Aggregation Experiments

- **57 sets ⇒ impossible without clustering/aggregation**

(a) 30% clustering (3 flowpipes)

(b) 30% clustering, then convex hull aggregation

(c) Constraint hull aggregation

(d) Convex hull aggregation

Time:

- 11.5 sec
- 3.6 sec
- 3.4 sec
- 8.2 sec
Clustering & Aggregation Experiments

- 57 sets ⇒ impossible without clustering/aggregation

\[ 36 \]

\[ 11.5 \text{ sec} \]

\[ 3.6 \text{ sec} \]

\[ 3.4 \text{ sec} \]

\[ 8.2 \text{ sec} \]

speed & accuracy: combine clustering & aggregation

(a) 30% clustering, then convex

(c) Constraint hull aggregation

(d) Convex hull aggregation
Example: Overhead Crane

- **State variables**
  - position \( x \), speed \( y \)
  - line angle \( y \), angle rate \( w \)

- **Inputs**
  - motor force \( u \)
  - gravity (const.)

- **Outputs**
  - \( x, v \)
  - not measured: \( y, w \)

- **Double Integrator System**
  - marginally stable, tricky

\[
\begin{align*}
\dot{x} &= v \\
\dot{v} &= b_{21}u + b_{22}g \\
y &= w \\
\dot{w} &= -a_{43}y - b_{41}u
\end{align*}
\]
Overhead Crane – Uncontrolled Plant

- Double integrator + purely imaginary Eigenvalues
  $\Rightarrow$ very sensitive to errors

error increases with time – only in $x$!
Overhead Crane – Uncontrolled Plant

- Use variable time step...

- time step adjustment for constant error bound

- time step decreases slowly
Overhead Crane – Observer

- Validation of observer quality
  - Standard: Simulation of “representative trajectories”

- Using reachability
  - Error bounds over range of initial states & inputs
Overhead Crane - Controller

- Evaluation of swing (angle range)

- Over small initial range: 
  \([-0.17, 0.12]\)

- Over full operating range: 
  \([-0.17, 0.17]\)
Controlled Helicopter

- 28\textsuperscript{th} order linear model
  - 8\textsuperscript{th} order model of an (actual) helicopter
  - 20\textsuperscript{th} order disturbance rejection controller

- Reachability of single initial state: 4.2s

Controlled Helicopter

- **28\textsuperscript{th} order linear model**
  - 8\textsuperscript{th} order model of an (actual) helicopter
  - 20\textsuperscript{th} order disturbance rejection controller

- **Reachability of (large) set of initial states: 24s**

\[ \text{error} \leq 0.025 \]

\[ \text{time step} \quad 0.01 \]
Controlled Helicopter

- **28**\(^{th}\) order linear model
  - 8\(^{th}\) order model of an (actual) helicopter
  - 20\(^{th}\) order disturbance rejection controller

- **Reachability of (large) set of initial states**: 14.5s

**Error**: \(\leq 0.025\)

**Variable time step**: 0.01 – 0.04
Controlled Helicopter

- Comparison of two controllers for nondeterministic inputs

(a) Roll stabilization

(b) Pitch stabilization
Conclusions

- **Old problems solved**
  - no more explosion with number of variables

- **New problems, but “softer”**
  - complexity increases with accuracy needed (less explosive)
  - nb. of constraints (for fixed error bound: exponential)

- **Case Studies needed**
  - analysis difficulties depend on particular case

- **Download SpaceEx: spaceex.imag.fr**
Bibliography

**Affine Dynamics**

**Support Functions**
- C. Le Guernic, A. Girard. Reachability analysis of hybrid systems using support functions. CAV’09
- G. Frehse, R. Ray. Design Principles for an Extendable Verification Tool for Hybrid Systems. ADHS’09
Verification Tools for Hybrid Systems

- **HyTech: LHA**
  - [http://embedded.eecs.berkeley.edu/research/hytech/](http://embedded.eecs.berkeley.edu/research/hytech/)

- **PHAVer: LHA + affine dynamics**
  - [http://www-verimag.imag.fr/~frehse/](http://www-verimag.imag.fr/~frehse/)

- **d/dt: affine dynamics + controller synthesis**
  - [http://www-verimag.imag.fr/~tdang/Tool-ddt/ddt.html](http://www-verimag.imag.fr/~tdang/Tool-ddt/ddt.html)

- **Matisse Toolbox: zonotopes**
  - [http://www.seas.upenn.edu/~agirard/Software/MATISSE/](http://www.seas.upenn.edu/~agirard/Software/MATISSE/)

- **HSOLVER: nonlinear systems**

- **and more...**