An Approximation Algorithm for Box Abstraction of Transition Systems on Real Vector Fields

(This is a revised version of a paper presented in SICE2009.)

Kunihiko HIRAISHI and Koichi KOBAYASHI,
JAIST
Predicate abstraction for Hybrid Systems

- Predicate abstraction is a powerful technique for extracting finite-state models from infinite-state systems.
- Predicate abstraction has also been applied to the verification of hybrid systems [Alur00, Alur02, Alur06].
- Given a hybrid system with linear dynamics and a set of linear predicates, the verifier performs a search of *the finite discrete quotient* whose states correspond to the truth assignments to the input predicates.
- We propose a technique that can be used for *accelerating* the computation of abstract state spaces for hybrid systems.
Predicate abstraction: example (1)

\[
\begin{bmatrix}
    x_1(t+1) \\
    x_2(t+1)
\end{bmatrix} = \alpha \cdot \begin{bmatrix}
    \cos \beta \pi & -\sin \beta \pi \\
    \sin \beta \pi & \cos \beta \pi
\end{bmatrix} \cdot \begin{bmatrix}
    x_1(t) \\
    x_2(t)
\end{bmatrix}
\]

\(\alpha = 0.8,\)
\(\beta = 1/6 \ (x_1 \leq 0, \ x_2 > 0);\)
\(\beta = -1/6 \ (x_1 > 0, \ x_2 > 0);\)
\(\beta = 1/8 \ (x_1 \leq 0, \ x_2 \leq 0);\)
\(\beta = -1/8 \ (x_1 > 0, \ x_2 \leq 0).\)

A PieceWise Linear System
Predicate abstraction: example (2)

Predicates $\Pi = \{ \pi_i \}$

$x_1 \leq k \ (k = -1, 0, 1)$,

$x_2 \leq k \ (k = -1, 0, 1)$.

Abstract states $B$

$S_1 = [1,1,1,1,1,1]$, …,

$S_{10} = [0,1,1,0,0,1]$, …,

$S_{16} = [0,0,0,0,0,0]$.

Transitions

$S_{10} \rightarrow S_{11} \equiv \exists x \in S_{10} \exists x' \in S_{11}. \ x \rightarrow x'$

(over-approximation)
Exact computation

\[ b(v_1, \ldots, v_n) : \text{an abstract states with state variables } v_1, \ldots, v_n \]

\[ C_\Pi(b) \subseteq \mathbb{R}^n : \text{Concretization of } b \]

\[ \pi(R) \in \{0, 1\}^m : \text{Discretization of region } R \]

\[ \text{Im}(R) \subseteq \mathbb{R}^n : \text{Image of region } R \]

\[ \text{Im}_\Pi(b) := \pi(\text{Im}(C_\Pi(b))) : \text{Discretized Image of abstract state } b \]

\[ \Delta(v_1, \cdots, v_n, v_1', \cdots, v_n') := \bigvee_{b \in B} \left( b(v_1, \cdots, v_n) \land \text{Im}_\Pi(b)(v_1', \cdots, v_n') \right) \]
Approximated computation (1)

Enlarged abstract states $B = \{ b_i \}$

$b_1 = [1, 1, 1, dc, dc, dc]$

$dc :$ don’t care

$b_2 = [dc, dc, dc, 1, 1, 1]$

$S_1 = b_1 \land b_2$

Conjunction complete: Each abstract state is represented by conjunction of enlarged abstract states.
Approximated computation (2)

\[ b(v_1, \ldots, v_n) : \text{enlarged abstract state with state variables } v_1, \ldots, v_n \]
\[ B : \text{the set of enlarged abstract states} \]
\[ \text{Im}_\Pi(C_\Pi(b)) : \text{discretized image of } b \]

\[ \Delta^\sim(v_1, \cdots, v_n, v'_1, \cdots, v'_n) := \bigwedge_{b \in B} (b(v_1, \cdots, v_n) \rightarrow \text{Im}_\Pi(b)(v'_1, \cdots, v'_n)) \]
Approximated computation (3)

\[ \text{Im}_{\Pi}(b_1) \]
\[ \text{Im}(C_{\Pi}(b_1)) \]
\[ C_{\Pi}(b_1) \]

\[ \text{Im}_{\Pi}(b_2) \]
\[ \text{Im}(C_{\Pi}(b_2)) \]
\[ C_{\Pi}(b_2) \]
Approximated computation (4)

Over-approximation:
\[ \text{Im}_\Pi(b_1 \land b_2) \subseteq \text{Im}_\Pi(b_1) \land \text{Im}_\Pi(b_2) \]
Justification of the Idea (1)

- Discrete-time autonomous system: \( x(t_{k+1}) = f(x(t_k)) \).
- If \( f \) is injective (one-to-one), then \( \text{Im}(Q_1 \cap Q_2) = \text{Im}(Q_1) \cap \text{Im}(Q_2) \). [This holds for discrete-time linear/affine systems.]
- Even if \( \text{Im}(Q_1 \cap Q_2) = \text{Im}(Q_1) \cap \text{Im}(Q_2) \), \( \pi(\text{Im}(Q_1 \cap Q_2)) = \pi(\text{Im}(Q_1)) \cap \pi(\text{Im}(Q_2)) \) does not necessarily hold (discretization error).
- However, the error occurs \textit{only around correct boxes}.
  - If \( \| f^{-1}(x_1) - f^{-1}(x_2) \| / \| x_1 - x_2 \| \leq K \) for any \( x_1, x_2 \) (Lipschitz continuity of \( f^{-1} \)), then \( \| x_1 - x_2 \| \leq K \| f(x_1) - f(x_2) \| \). [This holds for discrete-time linear/affine systems.]
  - Suppose that \( x_1 \in Q_1 - Q_2, x_2 \in Q_2 - Q_1 \), but \( f(x_1) \) and \( f(x_2) \) are in the same box.
  - Then, there exists a positive real \( R \) s.t. \( \| f(x_1) - f(x_2) \| \leq R \).
  - We have \( \| x_1 - x_2 \| \leq KR \).
Justification of the Idea (2)

\[ \| x_1 - x_2 \| \leq KR \]

Same box \( \rightarrow \) Discretization error
Complexity

- $h_i$: the number of predicates in the $i$-th axis.
- The number of abstract states is
  \[ |B| = \prod_{i=1}^{n} (h_i + 1) = O((1 + m/n)^n). \]
- The number of enlarged abstract states is
  \[ |\mathcal{B}| = \sum_{i=1}^{n} (h_i + 1) = O(m + n). \]
Discretization of Polyhedra: how to compute $\text{Im}_\Pi(b)$ from $\text{Im}(C_\Pi(b))$

- Since $\text{Im}(C_\Pi(b))$ is much larger than $\text{Im}(C_\Pi(b))$, the approximated computation requires more time at this step, provided that the computation time for the discretization depends on the size of polyhedra. As a result, the approximated computation is not very fast.

- We have develop an efficient algorithm, called the beam method, for this step. The algorithm uses convexity of regions.

- The beam method is compared with
  - Direct comparison: computing intersection between polyhedron $P$ and each box in the axis-aligned bounding box of $P$,
  - Shannon expansion.
Beam Method for 2D Space

\[ x_2 \]

\[ bm((j, 0), P) \]

\[ pceil_2(high((j, 0), P)) \]

\[ pfloor_2(low((j, 0), P)) \]

\[ line((j, 0)) \]

\[ c^1_{j-1} \quad c^1_j \quad c^1_{j+1} \]

\[ x_1 \]
Systems with Inputs

\[ x(t_{k+1}) = Ax(t_k) + Bu(t_k) \]

\[
\begin{pmatrix}
  x(t_{k+1}) \\
  u
\end{pmatrix} = 
\begin{pmatrix}
  A & B \\
  0 & I
\end{pmatrix}
\begin{pmatrix}
  x(t_k) \\
  u
\end{pmatrix}
\]

We embed the input in the state space. Then the matrix is nonsingular, provided that \( A \) is nonsingular.
Computation Results (1)

\[ x(t_{k+1}) = Ax(t_k) + \left( \begin{array}{c} -0.1 \\ \vdots \\ -0.1 \end{array} \right) \]

where \( A \) is an \( n \)-dimensional square matrix that represents the following rotations:

- \( n = 2 \): \( \pi/3 \) around the origin.
- \( n = 3 \): \( \pi/3 \) around the origin on \( x_{23} \)-plane, \( x_{13} \)-plane, and \( x_{12} \)-plane.
- \( n = 4 \): \( \pi/3 \) around the origin on \( x_{12} \)-plane, \( x_{23} \)-plane, and \( x_{31} \)-plane.
- \( n = 5 \): \( \pi/3 \) around the origin on \( x_{12} \)-plane, \( x_{23} \)-plane, \( x_{34} \)-plane, and \( x_{45} \)-plane.
Computation Results (2)

- $\tau_\Pi$: the exact transitions.
- $\tau_\Pi\sim$: the approximated transitions.
- Evaluation criteria:
  - Ratio $\gamma\sim = |\tau_\Pi\sim| / |\tau_\Pi|$.
  - The number of error transitions classified by hamming distance. Let $#e_i$ be the number of transitions in $\tau_\Pi\sim - H_i(\tau_\Pi)$, where $H_i(\tau_\Pi)$ is the set of all transitions whose hamming distance to at least one of transitions in $\tau_\Pi$ is no more than $i$. 
### Computation Results (3)

<table>
<thead>
<tr>
<th>( h )</th>
<th>( n = 2 ), Exact</th>
<th>( h ) : the number of predicates in each axis</th>
</tr>
</thead>
<tbody>
<tr>
<td>( h )</td>
<td>CPU time (sec.)</td>
<td>(</td>
</tr>
<tr>
<td></td>
<td>Direct</td>
<td>Shannon</td>
</tr>
<tr>
<td>3</td>
<td>0.02</td>
<td>0.03</td>
</tr>
<tr>
<td>5</td>
<td>0.04</td>
<td>0.07</td>
</tr>
<tr>
<td>10</td>
<td>0.12</td>
<td>0.37</td>
</tr>
<tr>
<td>15</td>
<td>0.24</td>
<td>0.95</td>
</tr>
<tr>
<td>20</td>
<td>0.5</td>
<td>2.42</td>
</tr>
<tr>
<td>30</td>
<td>1.4</td>
<td>8.02</td>
</tr>
<tr>
<td>40</td>
<td>3.13</td>
<td>19.22</td>
</tr>
<tr>
<td>50</td>
<td>6.05</td>
<td>37.78</td>
</tr>
<tr>
<td>60</td>
<td>10.54</td>
<td>66.77</td>
</tr>
<tr>
<td>70</td>
<td>17.14</td>
<td>108.41</td>
</tr>
<tr>
<td>80</td>
<td>26.69</td>
<td>164.85</td>
</tr>
<tr>
<td>90</td>
<td>39.03</td>
<td>240.69</td>
</tr>
<tr>
<td>100</td>
<td>56.5</td>
<td>338.98</td>
</tr>
</tbody>
</table>
## Computation Results (4)

| $h$ | CPU time (sec.) | $|\tau_\Pi|$ | $\gamma^\sim$ | $\#e_1$ |
|-----|----------------|-------------|-------------|---------|
|     | Direct | Shannon | Beam |           |          |          |
| 3   | 0.02   | 0.02    | 0.01  | 67       | 1.14    | 0        |
| 5   | 0.04   | 0.06    | 0.02  | 162      | 1.16    | 0        |
| 10  | 0.14   | 0.56    | 0.07  | 555      | 1.16    | 0        |
| 15  | 0.29   | 0.23    | 0.11  | 1,190    | 1.17    | 0        |
| 20  | 0.72   | 1.4     | 0.17  | 2,060    | 1.18    | 0        |
| 30  | 2.26   | 4.57    | 0.38  | 4,488    | 1.18    | 0        |
| 40  | 5.42   | 10.88   | 0.73  | 7,898    | 1.18    | 0        |
| 50  | 10.53  | 21.34   | 1.29  | 12,252   | 1.18    | 0        |
| 60  | 18.67  | 37.57   | 2.13  | 17,530   | 1.18    | 0        |
| 70  | 30.4   | 60.76   | 3.16  | 23,718   | 1.18    | 0        |
| 80  | 46.02  | 91.79   | 4.7   | 30,913   | 1.18    | 0        |
| 90  | 67.13  | 133.34  | 6.45  | 38,943   | 1.18    | 0        |
| 100 | 95.2   | 188.06  | 9.01  | 48,037   | 1.18    | 0        |

$n = 2$, Approx.
## Computation Results (5)

| $\ell$ | CPU time (sec.) | $|\tau_\Pi|$ | $|\tau_\Pi|$ | $\gamma$ | $#c_1$ | $#c_2$ |
|-------|-----------------|------------|------------|--------|------|------|
| 3     | 0.16            | 450        | 574        | 1.28   | 4    | 0    |
| 5     | 0.7             | 1,679      | 2,129      | 1.27   | 3    | 0    |
| 10    | 4.96            | 10,896     | 14,029     | 1.29   | 8    | 0    |
| 15    | 14.11           | 34,044     | 44,605     | 1.31   | 93   | 0    |
| 20    | 40.33           | 77,265     | 101,552    | 1.31   | 399  | 0    |
| 30    | 152.64          | 248,912    | 327,702    | 1.32   | 1,222| 0    |

$n = 3$, Exact/Approx.
Computation Results (6)

| $h$ | CPU time (sec.) | $|\tau_\Pi|$ | $|\tilde{\tau}_\Pi|$ | $\gamma^\sim$ | $#e_1$ | $#e_2$ | $#e_3$ |
|-----|-----------------|--------------|-----------------|-------------|--------|--------|--------|
| 3   | 3.67            | 3,927        | 6,095           | 1.55        | 71     | 0      | 0      |
| 5   | 15.08           | 22,322       | 36,673          | 1.64        | 468    | 0      | 0      |
| 7   | 43.91           | 72,957       | 123,526         | 1.69        | 1,738  | 0      | 0      |
| 10  | 196.55          | 265,111      | 459,607         | 1.73        | 7,050  | 1      | 0      |

$n = 4$, Exact/Approx.
# Computation Results (7)

| $h$ | CPU time (sec.) | $|\tau_{\Pi}|$ | $|\tau_{\Pi}^{|}$ | $\gamma^{|}$ | $\#e_1$ | $\#e_2$ | $\#e_3$ |
|-----|-----------------|----------------|-----------------|-----------|--------|--------|--------|
| 2   | 10.98           | 6,233          | 10,997          | 1.76      | 412    | 0      | 0      |
| 3   | 44.04           | 32,338         | 61,282          | 1.90      | 2,294  | 8      | 0      |
| 4   | 172.24          | 110,703        | 220,908         | 2.00      | 9,697  | 62     | 0      |
| 5   | 443.49          | 284,518        | 578,721         | 2.03      | 26,034 | 150    | 0      |
| 7   | -               | -              | -               | -         | -      | -      | -      |
| 10  | -               | -              | -               | -         | -      | -      | -      |

$n = 5$, Exact/Approx.
Future Work

- Application to parameter design of hybrid dynamical systems.
- Development of method for general predicates.