Symbolic temporal constraint analysis, an approach for verifying hybrid systems

Nicolas Rivière, Hamid Demmou, Robert Valette, Malika Medjoudj

LAAS-CNRS, F-31077 Toulouse Cedex 4 France

IFAC 6 July 2005
Introduction and presentation of the approach
The objective of this presentation is:

- provide an illustration of an approach for proving some properties of hybrid systems

The property considered here is:

- compute maximal duration of a scenario

Continuous aspect is taken into account by means:

- of a temporal abstraction with parameters attached to tokens

Provide an aid to the designer:

- obtain the values (domain) of some parameters ensuring that a property is true
The modeling tool is:

- Predicate-transition-differential Petri nets (basically $p$-temporal + data attached to tokens)

The approach is based on:

- an exploration of **scenarios** and not a state enumeration
- the equivalence between reachability and linear logic provability of some sequents, **preserving causal relations**
- the **analysis** of the causal relations / precedence (partial order) between events (transition firings)
- **simple temporal networks** to represent the constraints
- keeping **parameters** within the temporal abstraction in order to take into account the hybrid aspect
A complex system is represented by the composition of simple Petri nets
- necessary to cope with industrial system complexity

Compute place invariants
- in order to derive logical constraints on the place token loads

Start from the final marking (or better a partial final marking)
- backward reasoning with the possible introduction of new tokens (when new subsystems are implied in the scenario)
- build the partial order among the events by labeling the proof tree
Principles of the approach (2)

- Building complex scenarios from simple ones
- Taking into account temporal constraints
  - hybrid aspect is taken into account by a parametrized temporal abstraction
- Search the longest scenarios
  - parameters are replaced by numerical values only when strictly necessary
- Derive a parametrized condition ensuring that the property is true
Description of the case study
Description of the system

- It is a simplified (non actual) version of a Benchmark
  - control of three landing gears of a military airplane
  - even after a series of contradictory commands, the maximal duration for extending the gears has to be smaller than a given bound

- Sequence:
  - open the 3 gear doors
  - extend the 3 landing wheels
  - close the 3 gear doors

- It is assumed that the 3 gears are independent
(Mod. 1) Global view of the Petri net

Modelling of the Petri net:
- Places:
  - $p_1$: Retracted
  - $p_2$: Extended
  - $p_{i0}$
  - $p_{i4}$
  - $p_{i5}$
  - $p_{i9}$

- Transitions:
  - $t_1$, $t_2$, $t_3$, $t_4$

- Arcs:
  - $p_1$ to $t_1$
  - $t_1$ to $p_{i0}$
  - $p_{i0}$ to $p_{i4}$
  - $p_{i4}$ to $t_2$
  - $t_2$ to $p_{i5}$
  - $p_{i5}$ to $p_{i9}$
  - $p_{i9}$ to $p_2$
  - $p_2$ to $t_3$
  - $t_3$ to $p_{i4}$
  - $p_{i4}$ to $t_1$
  - $t_4$ to $p_{i9}$
  - $p_{i9}$ to $p_1$

Legend:
- Retracted
- Extended
- Landing gear 1
- Landing gear 2
- Landing gear 3

Nicolas Rivièr, Hamid Demmou, Robert Valette, Malika Medjoudj (LAAS-CNRS, F-31077 Toulouse Cedex 4 France)

Symbolic temporal constraint analysis, an approach for verifying hybrid systems

IFAC 6 July 2005 9/26
A delay before any movement

The gear position is ill-known but located between two linear envelopes

\[
\frac{dl_i}{dt} = c_i \text{ avec } c_i \in [a_i, b_i] \text{ et } a_i \geq 0
\]
(Mod. 3) Landing wheel extending

\[
dl_i/dt = c_i \text{ avec } c_i \in [a_i, b_i]
\]
is attached to place \( p_{i1} \)
Analysis in order to derive the parametrized condition ensuring that the property is true
(Ana. 1) Invariants

- A unique token for each wheel
- It is impossible that a wheel dynamics be represented by two different equations
Initially the wheels are retracted: \( l_i = 0 \)

By using the place invariants and the conditions attached to transitions \( t_{i2} \) and \( t_{i7} \), it can be derived that:

\[ \forall M \text{ reachable marking}, \forall i, 0 \leq l_i \leq l_{0i} \]
Initially the wheels are retracted: \( l_i = 0 \)

By using the place invariants and the conditions attached to transitions \( t_{i2} \) and \( t_{i7} \), it can be derived that:

\[ \forall M \text{ reachable marking}, \forall i, 0 \leq l_i \leq l_{0i} \]
(Ana. 3) First scenario

Starting from the final state: the 3 gears are extended.
(Ana. 3) First scenario

It is necessary to produce one token (extending Petri nets) in each of the 3 places $p_{i4}$.

$$s_2 : \ p_{14} \otimes p_{24} \otimes p_{34}, \ t_2 \vdash \ p_2$$
It is necessary to produce one token (extending Petri nets) in each of the 3 places $p_{i4}$.

$s_2 : p_{14} \otimes p_{24} \otimes p_{34}, t_2 \vdash p_2$
(Ana. 4) Second scenario

An example of scenario producing one token in place $p_{i4}$.

$s_3 : p_{i0}, t_{i0}, t_{i1}, t_{i2}, t_{i3} \vdash p_{i4}$
(Ana. 4) Second scenario

An example of scenario producing one token in place $p_{i4}$.

$s_3 : p_{i0}, t_{i0}, t_{i1}, t_{i2}, t_{i3} \vdash p_{i4}$
To each precedence relation (one token in a place) a quantitative constraint is attached.

A parametrized Simple Temporal Network is derived (STN)

For $p_{i2}$ it is the following parametrized one:

$$d_{2mi} = \frac{l_{0i}}{b_i} \text{ et } d_{2Mi} = \frac{l_{0i}}{a_i}$$

$$\frac{dl_i}{dt} = c_i \text{ with } c_i \in [a_i, b_i]$$
(Ana. 6) Comparison

For each scenario the longest path is calculated
- if possible without replacing the parameters by numerical values (max)

The max duration values are compared
- if possible preserving the parameters

The condition ensuring that the property is true is derived

\[ \delta_m = \max_{i=1,3} (D_{mi} + d_{mi} + d_{2mi}) \]  \hspace{1cm} (2)

\[ \delta_M = \max_{i=1,3} (2D_{Mi} + d_{Mi} + d_{2Mi}) \]  \hspace{1cm} (3)

\[ \max_{i=1,3} (2D_{Mi} + d_{Mi} + l_{0i}/a_i) \leq \Delta \]  \hspace{1cm} (4)
(Ana. 6) Comparison

For each scenario the longest path is calculated

- if possible without replacing the parameters by numerical values (max)

The max duration values are compared

- if possible preserving the parameters

The condition ensuring that the property is true is derived

\[ \delta_m = \max_{i=1,3}(D_{mi} + d_{mi} + d_{2mi}) \]  \hspace{1cm} (2)

\[ \delta_M = \max_{i=1,3}(2D_{Mi} + d_{Mi} + d_{2Mi}) \]  \hspace{1cm} (3)

\[ \max_{i=1,3}(2D_{Mi} + d_{Mi} + l_{0i}/a_i) \leq \Delta \]  \hspace{1cm} (4)
(Ana. 6) Comparison

For each scenario the longest path is calculated
  - if possible without replacing the parameters by numerical values (max)

The max duration values are compared
  - if possible preserving the parameters

The condition ensuring that the property is true is derived

\[
\delta_m = \max_{i=1,3} (D_{mi} + d_{mi} + d_{2mi}) \tag{2}
\]

\[
\delta_M = \max_{i=1,3} (2D_{Mi} + d_{Mi} + d_{2Mi}) \tag{3}
\]

\[
\max_{i=1,3} (2D_{Mi} + d_{Mi} + l_{0i}/a_i) \leq \Delta \tag{4}
\]
Conclusion
Conclusions

- It has been possible to determine the longest scenario without replacing any parameter by a numerical value.
- Another benchmark (3 on board redundant computers) for controlling left and right steerings.
- With an automated model checking tool, parameters have to be assigned numerical values.
  - many proofs for many values would be necessary
  - combinatorial explosion of the search space may largely vary in function of the numerical values (typically small with same values and small domains and very large with very different dynamics)
Thank you for your attention

Any questions?
(Mod. 4) Landing wheel retracting

\[
\frac{dl_i}{dt} = -c_i \text{ avec } c_i \in [a_i, b_i]
\]

is attached to place \( p_{i7} \)

\[\text{is attached to place } p_{i7}\]
There is a unique scenario
There are 125 markings = states
There are thousands of sequences
Scenario with another temporal constraint

We still have:

\[ \frac{dl_i}{dt} = c_i \quad \text{with} \quad c_i \in [a_i, b_i] \]

However for this scenario:

\[ d_{2mi} = 0 \quad \text{and} \quad d_{2Mi} = 0 \]

Because \( l_i = l_{0i} \) when the token arrives in \( p_{i2} \)
Comparison with model checking

- There are 3 similar Petri nets in parallel
- The parameters may be different for each wheel
  - (at least for the front wheel)
- Duration values slightly different for concurrent activities produce an explosion of the state space.
- By model checking only one upper bound will be known for the longest scenario, not necessarily the lowest one.

- How to introduce hybrid in model checking
- How composing constraints in an abstract class graph (any modification of the net implies a new generation, there is no composition approach, no concatenation of scenarios)