A Petri net based approach for the analysis of hybrid systems

Emilia Villani : Escola Politecnica da USP, Sao Paulo, Brazil
Jean-Claude Pascal : LAAS-CNRS, Toulouse, France
Paulo Eigi Miyagy : Escola Politecnica da USP, Sao Paulo, Brazil
Robert Valette : LAAS-CNRS, Toulouse, France

http://www.laas.fr/~robert

Objective

Define a method for property verification:

- Compatible with existing proof techniques
- Compatible with specification tools used in practice
- Not necessarily an automated approach (no decidability)
- Can be applied to relatively complex systems
- For hybrid systems
Example

Air conditioning system

Way to proceed (1)

"Divide and conquer"

- Proving by composing elementary proofs
- Start from an UML based object decomposition
- Discrete and continuous dynamics are separated
- Petri nets are used for the discrete aspect
  - Hybrid systems for which the discrete dynamics is significant
  - Concurrency = object independence
  - Objects with Petri nets / Petri nets with objects
Way to proceed (2)

Hybrid (dynamic) Objects:

- **Behavior**: A Petri net (discrete dynamics)
- **Methods**: Differential algebraic systems / RdP places (continuous dynamics) : methods phases
- **Interactions**: continuous / discrete (thresholds \(\Rightarrow\) transitions)
- **Communications**: Transitions available/required methods
- **Internal variables**: (continuous and discrete)

Object example

\[ P_{16}: \quad \theta_{aux} = 0 \]
\[ P_{17}: \quad \frac{\theta_{aux}}{1} = \left(1 - \frac{1}{\theta_{aux} + 1}\right) \left(\frac{2 \times m_{air}}{m_{air} + m_T}\right) \]

\( m_{air} \)

computed by object fan 2

\( Q_{ec} \)

used by object surgery room

\( t_17 : \quad \theta_{aux} = 0 \)
\( t_18 : \quad \theta_{aux} = 0 \)

\( t_17 \) et \( t_18 \) are two available methods (used by switcher)

Object "cooling device"
Two contradictory requirements

• A contradiction between:
  – A very large descriptive power
  – An easy analysis and formal proof

• No shared variables between the objects
  – Share constant parameters (at least variables which are constant during some phases)
  – Using continuous variables which are computed in other objects (no causal cycle)

• Rare communications which are statically defined
  – Only point to point, no broadcast, no dynamic definition of the receiver

The objects

• Switch/supervisory control
  – defines the configurations (fans 1 et 2, cooling device)

• Cooling device

• Fans (1 et 2)

• Surgery room
  – compute the temperature
Modular proof

List of necessary hypotheses

\[ H_{el}, \ldots, H_{ej}, \ldots, H_{dk}, \ldots, D_{ml}, \ldots \vdash C \]

- \( H_{el} \): global environment, validity domain
- \( H_{ej} \): property of global used continuous variables (domains for ex.)
- \( H_{dk} \): property of global discrete dynamics
- \( D_{ml} \): deduction and proof techniques available in the studied object

=> Proof obligations for all the \( H \) (excepted \( H_{el} \))

Proof example 1

- Fan 2 has to be always in operation when the cooling device is on (corresponds to a \( H_{dj} \))
- A global Petri net encapsulating 3 objects is built
- Proof is based on a p-invariant (positive and negative weights)
Proof example 2 (1)

- $T_f$ is reachable from $T_0$ before $\theta_i$ (object "surgery room")
- $H_{ei}$: Initial state: object "switch" is not commanded off
- $H_{c1}$: $\int Q_{ec} < K$ in "cooling device" (=> proof obligation)

Proof example 2 (2)

- $C$: $\int Q_{ec} < K$ in "cooling device"
- $H_{ei}$: Initial state: object "switch" is not commanded off
- $m_{air}$ is a constant: proof 1 ($H_d$ and proof obligation)
Conclusion

• Break down a complex proof into a set of simple proofs
• Allow addressing problems for which there is no decidability

BUT

• "Manual" proofs

• It is necessary to limit the descriptive power
  – Static transition merging
  – No causal cycle among the shared continuous variables