Formal Verification of DEV&DESS Formalism using Symbolic Model Checker HyTech

Han Choi, Sungdeok Cha, Jae Yeon Jo, Junbeom Yoo, Hae Young Lee, and Won-Tae Kim
Abstraction

• Hybrid system
  – a combination of discrete and continuous dynamics

• Various algorithmic verification tools for model checking
  – e.g. HyTech: model checking tool for linear hybrid automata

• Widely used formalism for modeling hybrid systems - DEV&DESS
  – no verification tools for DEV&DESS formalism

→ We translated an example of hybrid system modeled in DEV&DESS formalism into linear hybrid automata and verified it using HyTech.
Background – DEV&DESS formalism

<An Overview of Discrete Event & Differential Equation System Specification>
Background – Linear Hybrid Automata

• Hybrid automata
  – finite state automata with conditions on real-valued variables

• Linear hybrid automata
  – restricted class of hybrid automata
**HyTech – Model Checker for Linear Hybrid Automata**

- **HyTech**
  - symbolic model checker for linear hybrid automata
  - model checking of safety requirements and parametric analysis

**Safety requirement**

![Diagram of safety requirement](image)
HyTech – Model Checker for Linear Hybrid Automata

- HyTech
  - symbolic model checker for linear hybrid automata
  - model checking of safety requirements and parametric analysis

**Parametric analysis**

- On
  - $t \leq 3$
  - $\dot{x} = 1$
  - $t = 1$

- Off
  - $t \leq 3$
  - $\dot{x} = -3$
  - $t = 1$

$X > 3$

error

Parameter

Unsafe state
Example model – Barrel Filler System

- Characteristics of the barrel filler system
  - continuous input ‘inflow’: 0.5 (valve - open), 0.25 (valve - closing)
  - 1 time unit for closing the valve
  - 10-liter barrel
DEV&DESS model for the barrel filler system

- Correctness of the model's behavior
  - simulation using scenarios
  - draw trajectories for the barrel filler model
Translation DEV&DESS model into Linear hybrid automata

- Parallel composition of automata for input ports

- Translation the barrel filler model into linear hybrid automata used for validation of translation (specific scenario)

- ‘e’ and ‘σ’ for time events

- Transition : events in DEV&DESS model

node : Phase in DEV&DESS model

2011-12-12
Verification of Barrel Filler System using HyTech (1)

- Statement for the safety requirement

‘Content of a barrel should be under 10 liters’

Checking whether the unsafe state can be reached

The unsafe state is unreachable

Safety property satisfied

HyTech commands for safety requirement:

```plaintext
unsafe := loc[BF]=error;
reached := reach forward from init_reg andreach;
if not empty(reached & unsafe)
    then print trace to unsafe using reached;
    else prints "Safety property satisfied";
endif;
```

The result of HyTech execution
Verification of Barrel Filler System using HyTech (2)

- Statement for parametric analysis

  ‘When should the valve start closing to avoid overflowing?’

  changing the state event condition ‘contents = cutoff’ using parameter ‘cutoff’

  checking the condition of the ‘cutoff’ value to enter the unsafe state

  unsafe := loc[BF]=error;
  reached := reach forward from init_reg andreach;
  bad_cutoff_values :=
      hide non_parameters in reached & unsafe endhide;
  prints "Spec. violated for parameter values",
  print bad_cutoff_values;

  get the right ‘cutoff’ value by negating the result ‘cutoff > 9.75’

  4cutoff < 41 & 4cutoff > 40
  | 4cutoff > 39 & 4cutoff <= 81
  | 4cutoff <= 83 & 4cutoff > 39
  | cutoff > 10

  <HyTech commands for parametric analysis>

  <The result of parametric analysis>
Further considerations on the translation

- Expressing the confliction between events in linear hybrid automata
  - lack of ability to assign the order of priority between transitions in hybrid automata

- Preprocessing of the continuous input trajectories
  - limitation of using variable in the expression of flow condition in HyTech

- Problem of the state space explosion
  - parallel composition of input automata
Conclusion and Future Work

- Formal verification of atomic DEV&DESS model
  - translation atomic DEV&DESS model into linear hybrid automata
  - performing model checking by using existing tool, HyTech

- Future work
  - translation for coupled DEV&DESS model
  - translation rules for the broad applications
  - development of automatic translation tool
Thank you for listening