

# Analysis of Timed Systems Based on Time-Abstracting Bisimulations

Paper: Stavros Tripakis and Sergio Yovine  
Slides: Martin Milata

November 17, 2010

- Behavioral equivalences (e.g. bisimulation) allow us to perform verification of state transition systems.
- Typically, system is compared to some simpler specification.
- Also can be used for reducing the size of the system.
- Not very thoroughly studied with regard to timed systems.

## Outline:

- 1 Behavioral equivalences generally.
- 2 Timed systems and time-abstracting bisimulation.
- 3 Minimization of the timed system.
- 4 Experimental results.

**Labeled Transition System** (also referred to as **model** here) is a triple  $G = \langle Q, Q^0, \rightarrow \rangle$ , where

- $Q$  is set of states,
- $Q^0 \subseteq Q$  is set of initial states and
- $\rightarrow \subseteq Q \times L \times Q$  is set of transitions labelled by  $L$ .

A relation  $R \subseteq Q \times Q$  is a **bisimulation** iff for all  $q_1 R q_2$ :

- $\forall q'_1 \in Q$  s.t.  $q_1 \xrightarrow{\ell} q'_1 \quad \exists q'_2$  s.t.  $q_2 \xrightarrow{\ell} q'_2$  and  $q'_1 R q'_2$ , and
- $\forall q'_2 \in Q$  s.t.  $q_2 \xrightarrow{\ell} q'_2 \quad \exists q'_1$  s.t.  $q_1 \xrightarrow{\ell} q'_1$  and  $q'_1 R q'_2$ .

Let  $\approx$  denote the greatest bisimulation. Two LTSes  $G_1, G_2$  are bisimilar if  $\forall q_1 \in Q_1^0, q_2 \in Q_2^0. q_1 \approx q_2$ .

# Partitions and quotient LTS (more definitions!)

A **partition** of  $\Pi$  of  $Q$  is a set of disjoint classes s.t.  $\bigcup \Pi = Q$ .

Let  $pre_\ell(B, C) = \{q \in B \mid \exists q' \in C. q \xrightarrow{\ell} q'\}$ .

The **quotient** of LTS  $G$  w.r.t. partition  $\Pi$  is another LTS  $\langle \Pi, \pi, \rightarrow \rangle$ , where  $\pi = \{B \in \Pi \mid B \cap \Pi \neq \emptyset\}$  and  $B \xrightarrow{\ell} C$  iff  $pre_\ell(B, C) \neq \emptyset$ .

Class  $B$  is stable w.r.t.  $C$  if  $\forall \ell \in L. pre_\ell(B, C) \in \{B, \emptyset\}$ . Partition  $\Pi$  is stable if all classes are stable w.r.t. each other.

Let  $\Pi_\approx$  be the partition induced by  $\approx$ . The **minimal model** of  $G$  modulo bisimulation is the quotient of  $G$  w.r.t.  $\Pi_\approx$ , denoted  $G_\approx$ .

# Computing reachable part of $G_{\approx}$

```
 $\Pi := \Pi_0; \quad \alpha := \{B \in \Pi_0 \mid B \cap Q^0 \neq \emptyset\}; \quad \sigma := \emptyset$   
while  $\exists B \in \alpha \setminus \sigma$  do  
   $C_B := Split(B, \Pi)$   
  if  $C_B = \{B, \emptyset\}$  then  
     $\sigma := \sigma \cup \{B\}$   
     $\alpha := \alpha \cup Succs(B)$   
  else  
     $\alpha := \alpha \setminus B$   
     $\Pi := (\Pi \setminus \{B\}) \cup C_B$   
     $\sigma := \sigma \setminus Preds(B)$   
  end if  
end while
```

Here,  $Split(B, \Pi)$  refines the class  $B$  by choosing a class  $C$  w.r.t. which  $B$  is potentially unstable, then computing  $B_1 = pre(B, C)$ ,  $B_2 = B \cap \overline{pre(B, C)}$ .

# Avoiding set complementation

Set complementation is very expensive in context of timed systems. We'd like to compute  $Split(B, \Pi)$  without using it.

Solution: split  $B$  directly w.r.t. all of its successors:

$$Ref(B) = \{B' \mid \exists C \in Succs(B). B' = pre(B, C) \wedge B' \neq \emptyset\}$$

$Ref$  must satisfy two conditions:

- 1 **coverness**:  $\bigcup Ref(B) = B$ .
- 2 **disjointness**:  $\forall B', B'' \in Ref(B), \text{ if } B' \neq B'' \text{ then } B' \cap B'' = \emptyset$ .

$Split$  without set complementation:

$$Split(B, \Pi) = \begin{cases} Ref(B) & \text{if } Ref(B) \notin \{\emptyset, \{B\}\} \\ \{B\} & \text{otherwise} \end{cases}$$

**Timed automaton** is a quintuple  $\langle S, s_0, E, I, \Omega \rangle$ , where

- $S$  is a finite set of control states,
- $s_0 \in S$  is the initial state,
- $E$  is finite set of arcs of the form  $(s, a, s', \psi, \mathcal{X})$ , where
  - $s, s' \in S$  are source and destination state,
  - $a \in L$  a label,
  - $\psi$  a clock constraint and
  - $\mathcal{X} \subseteq \Omega$  subset of the clocks to be reset.
- $I$  is a function associating an invariant with each state and
- $\Omega$  is the set of clocks.

**Both constraints and invariants are conjunctions of atoms of the form  $x \sim c$ , where  $\sim \in \{<, \leq, =, \geq, >\}$ .**

# Timed automata – semantics

Semantics of TA are given by LTS  $G = \langle Q, Q^0, \rightarrow \rangle$ , where

- $Q = \{ \langle s, v \rangle \mid s \in S, v \in I(s) \}$ ,
- $Q^0 = \{ \langle s_0, v \rangle \mid v \in I(s_0) \}$ , and
- $\rightarrow \subseteq Q \times (E \cup \mathbb{R}_+) \times Q$  is defined by following rules:

$$\frac{v, (v + t) \in I(s), \quad t \in \mathbb{R}_+}{\langle s, v \rangle \xrightarrow{t} \langle s, v + t \rangle} \text{ (time passage)}$$

$$\frac{e = (s, a, s', \psi, \mathcal{X}) \in E, \quad v \in \psi, \quad v' = v[\mathcal{X} := 0]}{\langle s, v \rangle \xrightarrow{e} \langle s', v' \rangle} \text{ (action)}$$

## Time-abstracting, action-immediate.

Given  $G = \langle Q, Q^0, \rightarrow \rangle$ , define  $G_{tai} = \langle Q, Q^0, \Rightarrow_{tai} \rangle$  by replacing all labels  $t \in \mathbb{R}_+$  by the label  $\varepsilon$ :

$$\frac{q \xrightarrow{e} q'}{q \xRightarrow{\varepsilon}_{tai} q'} \qquad \frac{q \xrightarrow{t} q'}{q \xRightarrow{\varepsilon}_{tai} q'}$$

The **tai-bisimulation**, denoted  $\approx_{tai}$ , is the greatest bisimulation defined on  $G_{tai}$ :  $G \approx_{tai} G'$  iff  $G_{tai} \approx G'_{tai}$ .

- $\approx_{tai}$  is coarser than region graph equivalence.
- Therefore, partition induced by  $\approx_{tai}$  is finite.

- The set of valuations  $Z$  satisfying a clock constraint is a convex polyhedron, called **convex zone**.
- A **(non-convex) zone** is a union of convex zones.
  - Closed under complement and set difference (as opposed to convex zones).

We write  $\langle s, Z \rangle$  for the class  $\{\langle s, v \rangle \mid v \in Z\}$ .

The *initial* partitions  $\Pi$  we consider must satisfy:

- **convexity**: each class of the initial partition is convex zone.
- **enabledness**: for each class  $\langle s, Z \rangle$  and edge  $(s, a, s', \psi, \mathcal{X})$  it holds that  $Z \cap \psi \in \{Z, \emptyset\}$ .

In order for the algorithm to compute partition induced by  $\approx_{tai}$ , we must redefine  $pre$ :

$$pre_e(\langle s, Z \rangle, \langle s', Z' \rangle) = \begin{cases} \langle s, Z \cap \psi \cap (Z'[\mathcal{X} := 0]) \rangle & \text{if } e = (s, a, s', \psi, \mathcal{X}) \\ \emptyset & \text{otherwise} \end{cases}$$

- 1  $q \in pre_e(B, C)$  iff  $q \in B \wedge \exists q' \in C. q \xrightarrow{e}_{tai} q'$ .
- 2 If  $B, C$  are convex, then  $pre_e(B, C)$  is also convex.

$$pre_\varepsilon(\langle s, Z \rangle, \langle s, Z' \rangle) = \langle s, \{v \in Z \mid \exists t \in \mathbb{R}_+. (v + t) \in Z' \wedge \forall 0 < t' < t. (v + t') \in Z \cup Z'\} \rangle$$

- 1 If  $q \in pre_\varepsilon(B, C)$ , then  $q \in B \wedge \exists q' \in C. q \xrightarrow{e}_{tai} q'$ .
- 2 If  $B, C$  are convex, then  $pre_\varepsilon(B, C)$  is also convex.

Let  $G_{min}$  denote the LTS computed by the algorithm with *pre* modified as described and *Succs* and *Preds* defined in the way usual for zones. Because of the mentioned asymmetry, it is not yet equal to  $G_{\approx_{tai}}$ .

However: let  $G_{\approx_{tai}} = \langle \Pi_{\approx_{tai}}, \pi_{\approx_{tai}}, \Rightarrow_{tai} \rangle$  and  $G_{min} = \langle \Pi, \pi, \Rightarrow \rangle$ .

*Proposition:*  $\Pi = \Pi_{\approx_{tai}}$ ,  $\pi = \pi_{\approx_{tai}}$ , and for all  $B, C \in \Pi$ :

- 1  $B \xrightarrow{\epsilon}_{tai} C$  iff  $B \xrightarrow{\epsilon} C$ .
- 2  $B \xrightarrow{\epsilon}_{tai} C$  iff  $B \xrightarrow{\epsilon^*} C$ .

That is, reflexive, transitive closure of  $\xrightarrow{\epsilon}$ .

- Algorithm used to generate minimal models of several timed systems.
- Tool *ALDEBARAN* used to compare models to *untimed* specifications.
- Timed transitions considered non-observable ( $\tau$ ).
- Comparison using  $\tau^*$ -bisimulation equivalence or  $\tau^*$ -simulation preorder.
- It should be possible to check TCTL formulas on the minimal model.

# Experiments

Example	N	TA		M		$C_{tot}$	splittings			time (secs)
		states	arcs	states	trans		total	$\epsilon$	e	
CSMA-CD	2	9	21	26	52	62	112	18	15	0.4
	3	26	90	340	1,055	559	1,264	150	173	3.8
	4	72	312	3,828	16,066	4,855	13,592	1,070	1,797	90.9
FDDI	3	19	25	525	933	1,873	3,202	377	637	8.5
	4	25	33	1,606	2,859	7,760	10,980	1,341	2,264	57.4
	5	31	41	4,621	8,801	26,900	32,385	3,878	6,755	315
Tick-Tock	1	24	64	78	121	202	223	31	15	1
	2	72	240	585	976	1,663	1,658	243	163	8.7

Example	N	TA		M		$C_{tot}$	splittings			time (secs)		
		states	arcs	states	trans		total	$\epsilon$	e	*	MAI	MAII
TGC		24	69	25	50	125	113	30	17	0.2	6	12
	†			62	138	159	201	36	27	0.5	57	155
FMX	2	24	34	22	26	34	34	2	0	0	1	2
	2†			47	85	63	113	7	13	0	3	6
	3	119	213	77	108	182	133	15	0	0	8	146
	3†			402	1,117	708	1,379	157	172	1.5	893	⊥
	4			548	1,164	252	420	872	493	76	0	2.1
	4†	4,437	17,902			7,850	16,144	1,931	2,022	40.4	⊥	⊥
	5	2,402	5,850			807	1,590	3,887	1,785	325	0	16.3
5†										⊥	—	—