A Zone-based Reachability Analysis for Nested Timed Automata

Seiichirou Tachi[1], Shoji Yuen[1], and Mizuhito Ogawa[2]

[1] Graduate School of Informatics, Nagoya University, Japan
[2] Japan Advanced Institute of Science and Technology¡ Japan

1 Introduction

2 Timed Automata

$\mathbb{R}^{\geq 0}$ denotes the set of non-negative real numbers. Given a set of clocks X an *atomic clock guard* is in the form of either $x \triangleleft c$ or $x - y \triangleleft c$ where $x, y \in X$, $\triangleleft \in \{<, \leq\}$ and $c \in \mathbb{N}$. A *clock guard* is a conjunction of atomic clock guards, and we write $\mathcal{B}(X)$ for the set of clock guards. A set of clock valuations for clocks X is written as $V_X : X \to \mathbb{R}^{\geq 0}$.

Definition 1 (Timed Automata) *A timed automaton is a tuple* $\mathcal{A} = (Q, q_0, X, \Delta)$ *where*

- Q *is a finite set of control locations with the initial location* $q_0 \in Q$*,*
- X *is a finite set of clocks,*
- $\Delta \subseteq Q \times \mathcal{B}(X) \times 2^X \times Q$*,*
- $F \subseteq Q$ *is the set of accepting locations.*

A clock valuation over X is a map from X to $\mathbb{R}^{\geq 0}$. The set of clock valuations over X is written as N_X. The clock valuation assigning 0 to X is denoted by 0_X.

Definition 2 (Semantics of Timed automata) *Given a timed automaton* $\mathcal{A} = (Q, q_0, X, \Delta, F)$*, a configuration of* $\mathcal{A}$ *is* (q, ν) *where* $q \in Q$ *and* $\nu \in V_X$*. A transition* $(q_1, \nu_1) \xrightarrow{t} (q_2, \nu_2)$ *where* t *is either* $d \in \mathbb{R}^{\geq 0}$ *or* ε *with:*

- $(q_1, \nu_1) \xrightarrow{d} (q_1, \nu_1 + d)$*;*
- $(q_1, \nu_1) \xrightarrow{g,R} (q_2, [R](\nu_1))$ *where* $(q_1, g, R, q_2) \in \Delta$ *and* $\nu_1 \models g$*.*

3 Nested Timed Automata

Definition 3 *Given a disjoint pair of clocks* X_g *and* X_ℓ*, let a set of timed automata be* $T = \{\mathcal{A}_0, \cdots, \mathcal{A}_n\}$ *where* $\mathcal{A}_i$ *is a timed automaton* $(Q_i, q_i^0, X_\ell \cup X_g, \Delta_i)$*. We assume* $Q_i \cap Q_j = \varnothing$ *if* $i \neq j$ *and we write* $Q = \cup_i Q_i$ *and* $Q^0 = \cup_i \{q_0^i\}$*. A* nested timed automaton *(NeTA) is given by* $\mathcal{N} = (T, \mathcal{A}_0, \Delta, X_g)$ *where*

- $A_0 \in T$ *is the initial timed automaton,*
- X_g *is the set of global clocks, and*
- $\Delta_g \subseteq (Q \times \{\mathsf{push}\} \times Q^0) \cup (Q \times Q \times \{\mathsf{pop}\} \times Q)$

For simplicity, every A_i has the same set of local clocks X_ℓ.

Note that since Q_i is disjoint to each other, each push rule specifies the pushed automaton A_i with $q \in Q(A_i)$. Similarly, each pop rule specifies a pair of automata A_i and A_j and A_j is popped. To explicitly show which automaton is involved, we write $q(\mathcal{A}_i)$ when $q \in Q(\mathcal{A}_i)$.

Definition 4 *A* configuration *of NeTA is given by* (c, μ) *where* $c \in \mathcal{C}^*$ *with* $\mathcal{C} = \bigcup_i (Q(\mathcal{A}_i) \times V_{X_\ell})$ *and* $\mu \in V_{X_g}$.

- $(c_1, \mu_1) \xrightarrow{t} (c_2, \mu_2)$ *where* $t \in \mathbb{R}_{\geq 0}$, $c_2 = c_1 + t$ *and* $\mu_2 = \mu_1 + t$*;*
- $(c(q_1, \nu_1), \mu_1) \xrightarrow{g,R} (c(q_2, \nu_2), \mu_2)$ *if* $(q_1, \nu_1 \cup \mu_1) \xrightarrow{g,R} (q_2, \nu_1 \cup \mu_2) \in \Delta(\mathcal{A}_i)$*;*
- $(c(q, \nu), \mu) \xrightarrow{\mathsf{push}} (c(q, \nu)(q_0(\mathcal{A}_i), 0_{X_\ell}), \mu)$ *if* $q \xrightarrow{\mathsf{push}} q_0(\mathcal{A}_i) \in \Delta_g$*; and*
- $(c(q_1, \nu_1)(q_2, \nu_2), \mu) \xrightarrow{\mathsf{pop}} (q_3, \nu_1), \mu)$ *if* $q_1 q_2 \xrightarrow{\mathsf{pop}} q_3 \in \Delta_g$

where $c + t$ *for* $(c + t)[i] = (q^i, \nu^i + t)$ *with* $c[i] = (q^i, \nu^i)$ *where* $c[i]$ *is the* i*-th element in* c *for* $1 \leq i \leq |c|$.

The *reachability problem* of NeTA is to check if there is a sequence of transitions from $((q_0(\mathcal{A}_0), 0_{X_\ell}), 0_{X_g})$ to $(c(q, \nu), \mu)$ for some ν and μ given $\mathcal{N}$ and $q \in Q_{\mathcal{N}}$.

4 Push-down automata over Zones

Given a set of clocks X_g and X_ℓ, the set of items Y derived from X_g and X_ℓ is $\{0, \vdash, \vdash^\bullet\} \cup \{x^\bullet | x \in X_g\} \cup X_\ell \cup X_g$ and Y_{clk} for $Y\{0\}$.

For a set of items Y, A *zone* over Y is $Z \subseteq Y \times Y \times \{\leq, <\} \times (\mathbb{Z} \cup \{\infty\})$ satisfying the following conditions.

- $y \neq y'$ for $(y, y', \preceq, c) \in Z$; and
- $(y_1, y_1', \preceq_1, c_1) \in Z$ implies $y_1 \neq y_2$ or $y_2 \neq y_2'$ for all $(y_2, y_2', \preceq_2, c_2) \in Z \backslash (y_1, y_1', \preceq_1, c_1)$

For $(y, y', \preceq, c) \in Z$, we write $y - y' \preceq c$ where $\preceq \in \{<, \leq\}$. By the second condition, it is ensured that the pair (y, y') is unique in a zone. Thus, a zone can be described as a form of the *difference bound matrix* where $(\preceq, c)$ is placed in the column labelled by y' and the row labelled by y for $y - y' \preceq c$.

- $\mathsf{Test}(Z, x \in I) = Z \wedge \{x - \mathbf{0} \triangleleft \mathsf{ub}(I), \mathbf{0} - x \triangleleft -\mathsf{lb}(I)\}$;
- $\mathsf{Free}(Z, Y) = (Z \ominus Y) \oplus Y$;
- $\mathsf{Reset}(Z, Y) = \mathsf{Free}(Z, Y) \wedge \{y - \mathbf{0} \leq 0 \mid y \in Y\}$;
- $\mathsf{Copy}(Z, x \leftarrow y) = \mathsf{Free}(Z, \{x\}) \wedge \{x - y \leq 0, y - x \leq 0\}$;
- $Z(\!|y \mapsto z|\!) = \mathsf{Copy}(Z, z \leftarrow y) \ominus \{y\}$

5 Simulation

Definition 5 *A binary relation $\preceq$ on $Q \times V_{X_g} \times V_{X_\ell} \times V_{X_g^\bullet \cup \{\vdash^\bullet\}}$ is a* simulation *if, whenever $(q, \mu, \nu, \mu^\bullet) \preceq (q, \mu', \nu', \mu'^\bullet)$:*

- $(q, \mu + t, \nu + t, \mu^\bullet + t) \preceq (q, \mu' + t, \nu' + t, \mu'^\bullet + t)$;
- $(q, \mu, \nu, \mu^\bullet) \xrightarrow{g,R} (q_1, \mu_1, \nu_1, \mu_1^\bullet)$ *implies for some* $(\mu_1', \nu_1', \mu_1'^\bullet)$ $(q, \mu', \nu', \mu'^\bullet) \xrightarrow{g,R} (q_1, \mu_1', \nu_1', \mu_1'^\bullet)$ *and* $(q_1, \mu_1, \nu_1, \mu_1^\bullet) \preceq (q_1, \mu_1', \nu_1', \mu_1'^\bullet)$;
- $q \xrightarrow{\mathsf{push}} q'$ *implies* $(q', \mu, \nu_0, \bullet(\mu) \uplus [\vdash^\bullet \mapsto 0]) \preceq (q', \mu', \nu_0, \bullet(\mu') \uplus [\vdash^\bullet \mapsto 0])$ *where* $\bullet(\mu)(x^\bullet) = \mu(x)$ *for* $x \in X_g$;
- $qq'' \xrightarrow{\mathsf{pop}} q'$ *implies for all* $(\mu_1, \nu_1, \mu_1^\bullet)$ *such that* $\mu_1(X_g) + \mu^\bullet(\vdash^\bullet) = \mu^\bullet(X_g^\bullet)$ *there exists* $(\mu_1', \nu_1', \mu_1'^\bullet)$ *such that* $\mu_1'(X_g) + \mu'^\bullet(\vdash^\bullet) = \mu'^\bullet(X_g^\bullet)$, $(q'', \mu_1, \nu_1, \mu^\bullet) \preceq (q'', \mu_1', \nu_1', \mu_1'^\bullet)$, *and* $(q', \mu, \nu_1 + \mu^\bullet(\vdash^\bullet), \mu_1^\bullet + \mu^\bullet(\vdash^\bullet)) \preceq (q', \mu', \nu_1' + \mu'^\bullet(\vdash^\bullet), \mu_1'^\bullet + \mu'^\bullet(\vdash^\bullet))$

$(q, Z) \preceq (q, Z')$ if for all $(\mu, \nu, \mu^\bullet) \models Z$, there exists $(\mu', \nu', \mu'^\bullet)$ such that $(\mu', \nu', \mu'^\bullet) \models Z'$ and $(q, \mu, \nu, \mu^\bullet) \preceq (q, \mu', \nu', \mu'^\bullet)$.

If $q \neq q'$, there exists no relation between (q, v) and (q', v'). We write $v \preceq_q v'$ if $(q, v) \preceq (q, v')$. Similarly, we write $Z \preceq_q Z'$ for $(q, Z) \preceq (q, Z')$.
[The following lemma is yet to be proved]

Lemma 1. *for all $Z \preceq_q Z'$,*

- $Z_2 \odot Z \neq \bot$ *and* $qq'' \xrightarrow{\mathsf{pop}} q' \in \Delta_g$ *imply* $Z_2 \odot Z \preceq_{q'} Z_2' \odot Z'$ *for some* Z_2' *such that* $Z_2 \preceq_{q''} Z_2'$

Lemma 2. *$\sqsubseteq_{LU_q}$ is a simulation relation.*

Lemma 3. *$\sqsubseteq_{LU_q} \cap \sqsubseteq_{LU_q}^{-1}$ has a finite index.*

$$\frac{}{\mathfrak{S} := \{(A_0, Z_0)\}, \mathcal{S}_{(\mathcal{A}_0, Z_0)} := \{(q_0(\mathcal{A}_0), Z_0)\}}\ [\mathsf{start}]$$

$$\frac{(\mathcal{A}_i, Z) \in \mathfrak{S} \quad (q', Z') \in \mathcal{S}_{(\mathcal{A}_i, Z)} \quad q' \xrightarrow{g,R} q'' \quad Z'' = [R]\mathsf{Test}(Z', g)}{\mathcal{S}_{(\mathcal{A}_i, Z)} := \mathcal{S}_{(\mathcal{A}_i, Z)} \cup \{(q'', Z'')\} \quad \text{unless } \exists (q'', Z'') \in \mathcal{S}_{(\mathcal{A}_i, Z)}\ Z'' \preceq_{q''} Z'''}\ [\mathsf{local}]$$

$$\frac{\mathcal{A}_i, Z) \in \mathfrak{S} \quad (q', Z') \in \mathcal{S}_{(\mathcal{A}_i, Z)} \quad q' \xrightarrow{\mathsf{push}} q_0(\mathcal{A}_j) \quad Z'' = Reset(Z', X_c \cup \{\vdash^\bullet\})}{\mathfrak{S} := \mathfrak{S} \cup \{(\mathcal{A}_j, Z'')\} \quad \mathcal{S}_{(\mathcal{A}_j, Z'')} = \{(q_0(\mathcal{A}_j), Z'')\} \quad \text{unless } \exists (\mathcal{A}_j, Z''') \in \mathfrak{S}\ Z'' \sim_{q_0(A_j)} Z'''}\ [\mathsf{push}]$$

$$\frac{\begin{array}{c}(\mathcal{A}_i, Z) \in \mathfrak{S} \quad (q', Z') \in \mathcal{S}_{(\mathcal{A}_i, Z)} \quad q' \xrightarrow{\mathsf{push}} q_0(\mathcal{A}_j) \quad Z'' \sim_{q_0(\mathcal{A}_j)} Z_1 \quad Z'' = Reset(Z', X_c \cup \{\vdash^\bullet\}) \\ (\mathcal{A}_j, Z_1) \in \mathfrak{S} \quad (q_1', Z_1') \in \mathcal{S}_{(\mathcal{A}_j, Z_1)} \quad q'q_1' \xrightarrow{\mathsf{pop}} q_2 \quad Z_2 = Up(Z' \odot Z_1')\end{array}}{\mathcal{S}_{(\mathcal{A}_i, Z)} := \mathcal{S}_{(\mathcal{A}_i, Z)} \cup \{(q_2, Z_2)\} \quad \text{unless } \exists (q_2, Z_2') \in \mathcal{S}_{(\mathcal{A}_i, Z)}\ Z_2 \preceq_{q_2} Z_2'}\ [\mathsf{pop}]$$