Zone-Based Reachability Analysis
Lecture #18 of Advanced Model Checking

Joost-Pieter Katoen
Lehrstuhl 2: Software Modeling & Verification

E-mail: katoen@cs.rwth-aachen.de

February 7, 2017
TCTL model checking

- Verifying timed reachability on timed automata is **decidable**
  - example timed reachability property: $\forall \Diamond \leq 10 \text{goal}$

- Key ingredient for decidability: finite quotient wrt. a bisimulation
  - bisimulation = equivalence on clock valuations
  - equivalence classes are called **regions**

- Region automaton is highly impractical for tool implementation
  - the number of regions lies in $\Theta(|C|! \cdot \prod_{x \in C} c_x)$

- In practice, coarser abstractions than regions are used
  - this lecture considers time-bounded reachability using **zones**
Reachability analysis

- **Forward** analysis:
  - starting from some initial configuration
  - determine configurations that are reachable within 1, 2, 3, \ldots steps
  - until either the goal configuration is reached, or the computation terminates

- **Backward** analysis:
  - starting from the goal configuration
  - determine configurations that can reach the goal within 1, 2, 3, \ldots steps
  - until either the initial configuration is reached, or the computation terminates

how can these approaches be realized for timed automata?
Symbolic reachability analysis

• Use a symbolic representation of timed automata configurations
  – needed as there are infinitely many configurations
  – example: state regions $\langle \ell, [\eta] \rangle$

• For set $z$ of clock valuations and edge $e = \ell \xleftarrow{g: \alpha, D} \ell'$ let:

  \[
  \begin{align*}
  Post_e(z) &= \{ \eta' \in \mathbb{R}_n^{\geq 0} \ | \ \exists \eta \in z, \ d \in \mathbb{R}_{\geq 0}. \ \eta + d = g \land \eta' = \text{reset } D \text{ in } (\eta + d) \} \\
  Pre_e(z) &= \{ \eta \in \mathbb{R}_n^{\geq 0} \ | \ \exists \eta' \in z, \ d \in \mathbb{R}_{\geq 0}. \ \eta + d = g \land \eta' = \text{reset } D \text{ in } (\eta + d) \} 
  \end{align*}
  \]

• Intuition:
  – $\eta' \in Post_e(z)$ if for some $\eta \in z$ and delay $d$, $\ell, \eta \xrightarrow{d} \ldots \xrightarrow{e} \ell', \eta'$
  – $\eta \in Pre_e(z)$ if for some $\eta' \in z$ and delay $d$, $\ell, \eta \xrightarrow{d} \ldots \xrightarrow{e} \ell', \eta'$
Zones

- Clock constraints are *conjunctions* of constraints of the form:
  
  - \( x < c \) and \( x - y < c \) for \( < \in \{<, \leq, =, \geq, >\} \), and \( c \in \mathbb{Z} \)

- A *zone* is a set of clock valuations satisfying a clock constraint
  
  - A clock zone for \( g \) is the set of clock valuations satisfying \( g \)

- Clock zone of \( g \):
  
  \[
  [g] = \{ \eta \in \text{Eval}(C) \mid \eta \models g \}
  \]

- The *state zone* of \( s = \langle \ell, \eta \rangle \) is \( \langle \ell, z \rangle \) with \( \eta \in z \)

- For *zone* \( z \) and edge \( e \), \( \text{Post}_e(z) \) and \( \text{Pre}_e(z) \) are *zones*

  state zones will be used as symbolic representations for configurations
Example zones

on the black board

zones are convex polyhedra
Operations on zones

- **Future** of $z$:
  - $\rightarrow z = \{ \eta + d \mid \eta \in z \land d \in \mathbb{R}_{\geq 0} \}$

- **Past** of $z$:
  - $\leftarrow z = \{ \eta - d \mid \eta \in z \land d \in \mathbb{R}_{\geq 0} \}$

- **Intersection** of two zones:
  - $z \cap z' = \{ \eta \mid \eta \in z \land \eta \in z' \}$

- **Clock reset** in a zone:
  - $\text{reset } D \text{ in } z = \{ \text{reset } D \text{ in } \eta \mid \eta \in z \}$

- **Inverse clock reset** of a zone:
  - $\text{reset}^{-1} D \text{ in } z = \{ \eta \mid \text{reset } D \text{ in } \eta \in z \}$
Operations on zones: examples

on the black board

zones are closed under all aforementioned operations
Symbolic successors and predecessors

Recall that for edge $e = \ell \xleftarrow{g: \alpha, D} \ell'$ we have:

$Post_e(z) = \{ \eta' \in \mathbb{R}_{\geq 0}^n \mid \exists \eta \in z, d \in \mathbb{R}_{\geq 0}. \eta + d \models g \land \eta' = \text{reset } D \text{ in } (\eta + d) \}$

$Pre_e(z) = \{ \eta \in \mathbb{R}_{\geq 0}^n \mid \exists \eta' \in z, d \in \mathbb{R}_{\geq 0}. \eta + d \models g \land \eta' = \text{reset } D \text{ in } (\eta + d) \}$

This can also be expressed symbolically using operations on zones:

$Post_e(z) = \text{reset } D \text{ in } (\vec{z} \cap [g])$

and

$Pre_e(z) = \text{reset}^{-1} D \text{ in } (z \cap [D = 0]) \cap [g]$
Zone successor: example

\[ \ell \rightarrow g, \ alpha, \ C := 0 \rightarrow \ell' \]

zones

\[ Z \]

\[ Z' \]

\[ [C \leftarrow 0](\overline{Z} \cap g) \]

\[ Z \]

\[ \overline{Z} \]

\[ \overline{Z} \cap g \]

\[ [y \leftarrow 0](\overline{Z} \cap g) \]
Zone predecessor: example

\[ \ell \xrightarrow{g, a, C := 0} \ell' \]

\[
\left[ C \leftarrow 0 \right]^{-1} (Z \cap (C = 0)) \cap g
\]

\[ Z \]

\[ [C \leftarrow 0]^{-1} (Z \cap (C = 0)) \]

\[ \left[ C \leftarrow 0 \right]^{-1} (Z \cap (C = 0)) \cap g \]
Backward symbolic transition system (1)

Backward symbolic transition system of $TA$ with $|C| = n$ is inductively defined by:

\[
    e = \ell \xleftarrow{g:\alpha,D} \ell' \quad z = \text{Pre}_e(z')
\]

\[
    (\ell', z') \leq (\ell, z)
\]

Iterative backward reachability analysis computation schemata:

\[
    T_0 = \{ (\ell, R^n_n_{\geq 0}) \mid \ell \text{ is a goal location} \}
\]

\[
    T_1 = T_0 \cup \{ (\ell, z) \mid \exists (\ell', z') \in T_0 \text{ such that } (\ell', z') \leq (\ell, z) \}
\]

\[
    \ldots \ldots
\]

\[
    T_{k+1} = T_k \cup \{ (\ell, z) \mid \exists (\ell', z') \in T_k \text{ such that } (\ell', z') \leq (\ell, z) \}
\]

\[
    \ldots \ldots
\]

until either the computation stabilizes or reaches an initial configuration $(\ell_0, z_0)$
Backward symbolic transition system (2)

Backward symbolic transition system of $TA$ is inductively defined by:

$$
\begin{array}{c}
\ell = e \xleftarrow{g: \alpha, D} \ell' \quad z = Pre_e(z') \\
(\ell', z') \iff (\ell, z)
\end{array}
$$

Iterative backward reachability analysis computation schemata:

$$
\begin{align*}
T_0 &= \{ (\ell, R^n_{\geq 0}) \mid \ell \text{ is a goal location} \} \\
T_1 &= T_0 \cup \{ (\ell, z) \mid \exists (\ell', z') \in T_0. (\ell', z') \iff (\ell, z) \text{ and } \ell' = \ell \text{ implies } z \nsubseteq z' \} \\
& \vdots \\
T_{k+1} &= T_k \cup \{ (\ell, z) \mid \exists (\ell', z') \in T_k. (\ell', z') \iff (\ell, z) \text{ and } \ell' = \ell \text{ implies } z \nsubseteq z' \} \\
& \vdots
\end{align*}
$$

until either the computation stabilizes or reaches an initial configuration $(\ell_0, z_0)$
The backward computation terminates and is correct wrt. reachability properties

Because of the bisimulation property, it holds:
Every set of valuations which is computed along the backward computation is a finite union of regions
Forward reachability analysis (1)

Forward symbolic transition system of $TA$ is inductively defined by:

$e = \ell \xleftarrow{\alpha, D} \ell'$ \quad $z' = \text{Post}_e(z)$

$(\ell, z) \Rightarrow (\ell', z')$

Iterative forward reachability analysis computation schemata:

$T_0 = \left\{ (\ell_0, z_0) \mid \forall x \in C. \ z_0(x) = 0 \right\}$

$T_1 = T_0 \cup \left\{ (\ell', z') \mid \exists (\ell, z) \in T_0 \text{ such that } (\ell, z) \Rightarrow (\ell', z') \right\}$

$\ldots \quad \ldots$

$T_{k+1} = T_k \cup \left\{ (\ell', z') \mid \exists (\ell, z) \in T_k \text{ such that } (\ell, z) \Rightarrow (\ell', z') \right\}$

$\ldots \quad \ldots$

until either the computation stabilizes or reaches a symbolic state containing a goal configuration
Forward reachability analysis (2)

Forward symbolic transition system of $TA$ is inductively defined by:

\[
e = \ell \xleftarrow{g: \alpha, D} \ell' \quad z' = \text{Post}_e(z) \quad (\ell, z) \Rightarrow (\ell', z')
\]

Iterative forward reachability analysis computation schemata:

\[
T_0 = \{ (\ell_0, z_0) \mid \forall x \in C. z_0(x) = 0 \}
\]

\[
T_1 = T_0 \cup \{ (\ell', z') \mid \exists (\ell, z) \in T_0. (\ell, z) \Rightarrow (\ell', z') \text{ and } \ell = \ell' \text{ implies } z \not\subseteq z' \}
\]

\[
. . . . .
\]

\[
T_{k+1} = T_k \cup \{ (\ell', z') \mid \exists (\ell, z) \in T_k. (\ell, z) \Rightarrow (\ell', z') \text{ and } \ell = \ell' \text{ implies } z \not\subseteq z' \}
\]

\[
. . . . .
\]

until either the computation stabilizes or reaches a symbolic state containing a goal configuration
Forward reachability analysis: intuition

\[ x := 1 \quad y \leq 2 \quad x \geq 2 \]

leaving initial

entering first

leaving first

entering second

leaving second

entering third
Possible non-termination

The forward analysis is correct but may **not** terminate:

\[ y := 0, \]
\[ x := 0 \]
\[ x \geq 1 \land y = 1, \]
\[ y := 0 \]

\[ y \]
\[ 2 \]
\[ 1 \]
\[ 0 \]
\[ 0 \]
\[ 1 \]
\[ 2 \]
\[ 3 \]
\[ 4 \]
\[ 5 \]

\[ x \]

\[ \text{an infinite number of steps...} \]
Solution: abstract forward reachability

Let $\gamma$ associate sets of valuations to sets of valuations

Abstract forward symbolic transition system of $TA$ is defined by:

$$
(\ell, z) \Rightarrow (\ell', z') \quad z = \gamma(z)
$$

$$(\ell, z) \Rightarrow \gamma(\ell', \gamma(z'))$$

Iterative forward reachability analysis computation schemata:

$$
T_0 = \{ (\ell_0, \gamma(z_0)) \mid \forall x \in C. z_0(x) = 0 \} \\
T_1 = T_0 \cup \{ (\ell', z') \mid \exists (\ell, z) \in T_0 \text{ such that } (\ell, z) \Rightarrow \gamma(\ell', z') \} \\
\ldots \\
T_{k+1} = T_k \cup \{ (\ell', z') \mid \exists (\ell, z) \in T_k \text{ such that } (\ell, z) \Rightarrow \gamma(\ell', z') \} \\
\ldots \\
$$

with inclusion check and termination criteria as before
Soundness and correctness

- **Soundness:**

  \[ \langle \ell_0, \gamma(z_0) \rangle \Rightarrow^* \langle \ell, z \rangle \]

  implies

  \[ \exists \langle \ell_0, \eta_0 \rangle \rightarrow^* \langle \ell, \eta \rangle \text{ with } \eta \in z \]

  abstract symbolic reachability

  reachability in \( TS(TA) \)

- **Completeness:**

  \[ \langle \ell_0, \eta_0 \rangle \rightarrow^* \langle \ell, \eta \rangle \]

  implies

  \[ \exists \langle \ell_0, \gamma(\{ \eta_0 \}) \rangle \Rightarrow^* \langle \ell, z \rangle \text{ for some } z \text{ with } \eta \in z \]

  reachability in \( TS(TA) \)

  abstract symbolic reachability

for any choice of \( \gamma \), soundness and completeness are desirable
Criteria on the abstraction operator

- **Finiteness**: \( \{ \gamma(z) \mid \gamma \text{ defined on } z \} \) is finite
- **Correctness**: \( \gamma \) is sound wrt. reachability
- **Completeness**: \( \gamma \) is complete wrt. reachability
- **Effectiveness**: \( \gamma \) is defined on zones, and \( \gamma(z) \) is a zone
Normalization: intuition

symbolic semantics has infinitely many zones:

normalization yields a finite zone graph:
**$k$-Normalization** [Daws & Yovine, 1998]

Let $k \in \mathbb{N}$.

- A $k$-bounded zone is described by a $k$-bounded clock constraint
  - e.g., zone $z = (x \geq 3) \land (y \leq 5) \land (x - y \leq 4)$ is not 2-bounded
  - but zone $z' = (x \geq 2) \land (y - x \leq 2)$ is 2-bounded
  - note that: $z \subseteq z'$

- Let $\text{norm}_k(z)$ be the smallest $k$-bounded zone containing zone $z$
Example of $k$-normalization
Facts about $k$-normalization [Bouyer, 2003]

- **Finiteness:** $\text{norm}_k(\cdot)$ is a finite abstraction operator

- **Correctness:** $\text{norm}_k(\cdot)$ is sound wrt. reachability
  
  provided $k$ is the maximal constant appearing in the constraints of TA

- **Completeness:** $\text{norm}_k(\cdot)$ is complete wrt. reachability
  
  since $z \subseteq \text{norm}_k(z)$, so $\text{norm}_k(\cdot)$ is an over-approximation

- **Effectiveness:** $\text{norm}_k(z)$ is a zone
  
  this will be made clear in the next lecture when considering zone representations