Difference Bound Matrices
Lecture #18 of Advanced Model Checking

Joost-Pieter Katoen
Lehrstuhl 2: Software Modeling & Verification
E-mail: katoen@cs.rwth-aachen.de

July 8, 2009
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:

  \[
  \text{Post}_e(z) = \{ \eta' \in \mathbb{R}^n_{\geq 0} \mid \exists \eta \in z, \, d \in \mathbb{R}_{\geq 0}. \, \eta + d \models g \land \eta' = \text{reset } D \text{ in } (\eta + d) \} \\
  \text{Pre}_e(z) = \{ \eta \in \mathbb{R}^n_{\geq 0} \mid \exists \eta' \in z, \, d \in \mathbb{R}_{\geq 0}. \, \eta + d \models g \land \eta' = \text{reset } D \text{ in } (\eta + d) \} 
  \]

- Intuition:
  - \( \eta' \in \text{Post}_e(z) \) if for some \( \eta \in z \) and delay \( d \), \( (\ell, \eta) \xrightarrow{d} \ldots \xrightarrow{e} (\ell', \eta') \)
  - \( \eta \in \text{Pre}_e(z) \) if for some \( \eta' \in z \) and delay \( d \), \( (\ell, \eta) \xleftarrow{d} \ldots \xleftarrow{e} (\ell', \eta') \)
Zones

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

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

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

- 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
Operations on zones

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

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

- **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:
  \[ \text{reset}^{-1} D \text{ in } z = \{ \eta \mid \text{reset } D \text{ in } \eta \in z \} \]
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:

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

and

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

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

zones: \( Z \)

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

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

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

\[ Z \]

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

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

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

$$e = \left( \ell \xrightarrow{g: \alpha, D} \ell' \right) \quad z' = \text{Post}_e(z)$$

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

Iterative forward reachability analysis computation schemata:

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

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

$$\ldots \ldots$$

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

$$\ldots \ldots$$

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:

$$e = \left( \ell \xleftarrow{g;\alpha,D} \ell' \right) \quad z' = Post_e(z)$$

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

Iterative forward reachability analysis computation schemata:

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

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

$$\cdots \quad \cdots$$

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

$$\cdots \quad \cdots$$

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:

\[ y := 0, \]
\[ x := 0 \]

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

\( \Rightarrow \) 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:

\[
\begin{align*}
(\ell, z) & \Rightarrow (\ell', z') \\
& \text{such that } z = \gamma(z) \\
(\ell, z) & \Rightarrow \gamma(\ell', \gamma(z'))
\end{align*}
\]

Iterative forward reachability analysis computation schemata:

\[
\begin{align*}
T_0 &= \{ (\ell_0, \gamma(z_0)) | \forall x \in C. z_0(x) = 0 \} \\
T_1 &= T_0 \cup \{ (\ell', z') | \exists (\ell, z) \in T_0 \text{ such that } (\ell, z) \Rightarrow \gamma(\ell', z') \} \\
& \ldots \\
T_{k+1} &= T_k \cup \{ (\ell', z') | \exists (\ell, z) \in T_k \text{ such that } (\ell, z) \Rightarrow \gamma(\ell', z') \} \\
& \ldots
\end{align*}
\]

with inclusion check and termination criteria as before
Soundness and correctness

- **Soundness:**

\[
\langle \ell_0, \gamma(z_0) \rangle \Rightarrow^* \gamma \langle \ell, z \rangle \quad \text{implies} \quad \exists \langle \ell_0, \eta_0 \rangle \rightarrow^* \langle \ell, \eta \rangle \quad \text{with } \eta \in z
\]

abstract symbolic reachability

reachability in \( TS( TA) \)

- **Completeness:**

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

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 sequel when considering zone representations
Representing zones

• Let 0 be a clock with constant value 0; let \( C_0 = C \cup \{ 0 \} \)

• Any zone \( z \) over \( C \) can be written as:
  
  – conjunction of constraints \( x - y < n \) or \( x - y \leq n \) for \( n \in \mathbb{Z} \), \( x, y \in C_0 \)
  
  – when \( x - y \leq n \) and \( x - y \leq m \) take only \( x - y \leq \min(n, m) \)

  \[ \Rightarrow \text{ this yields at most } |C_0| \cdot |C_0| \text{ constraints} \]

• Example:

  \[
  x - 0 < 20 \land y - 0 \leq 20 \land y - x \leq 10 \land x - y \leq -10 \land 0 - z < 5
  \]

• Store each such constraint in a matrix

  – this yields a difference bound matrix [Berthomieu & Menasche, 1983]
Difference bound matrices

• Zone $z$ over $C$ is represented by DBM $Z$ of cardinality $|C+1| \cdot |C+1|$
  
  - for $C = \{ x_1, \ldots, x_n \}$, let $C_0 = \{ x_0 \} \cup C$ with $x_0 = 0$, and:

  $$Z(i, j) = (c, \prec) \text{ if and only if } x_i - x_j \prec c$$

  - so, rows are used for lower, and columns for upper bounds on clock differences

• Definition of DBM $Z$ for zone $z$:

  - $Z(i, j) := (c, \prec)$ for each bound $x_i - x_j \prec c$ in $z$
  - $Z(i, j) := \infty$ (= no bound) if clock difference $x_i - x_j$ is unbounded in $z$
  - $Z(0, i) := (0, \leqslant)$, i.e., $0 - x_i \leqslant 0$ all clocks are positive
  - $Z(i, i) := (0, \leqslant)$, i.e., each clock equals itself
Example

\[(x_1 \geq 3) \land (x_2 \leq 5) \land (x_1 - x_2 \leq 4)\]

\[
\begin{pmatrix}
    x_0 \\
    x_1 \\
    x_2 \\
\end{pmatrix} = \begin{pmatrix}
    +\infty & -3 & +\infty \\
    +\infty & +\infty & 4 \\
    5 & +\infty & +\infty \\
\end{pmatrix}
\]

all clock constraints in the above DBM are of the form \((c, \leq)\)
The need for canonicity

\[(x_1 \geq 3) \land (x_2 \leq 5) \land (x_1 - x_2 \leq 4)\]

\[
\begin{bmatrix}
  x_0 & x_1 & x_2 \\
x_0 & +\infty & -3 & +\infty \\
x_1 & +\infty & +\infty & 4 \\
x_2 & 5 & +\infty & +\infty \\
\end{bmatrix}
\]

Existence of a normal form

\[
\begin{pmatrix}
  0 & -3 & 0 \\
  9 & 0 & 4 \\
  5 & 2 & 0 \\
\end{pmatrix}
\]
Canonical DBMs

- A zone $z$ is in canonical form if and only if:
  - no constraint in $z$ can be strengthened without reducing $[z] = \{ \eta \mid \eta \in z \}$

- For each zone $z$:
  - there exists a zone $z'$ such that $[z] = [z']$, and $z'$ is in canonical form
  - moreover, $z'$ is unique

how to obtain the canonical form of a zone?
Turning a DBM into canonical form

• Represent zone $z$ by a **weighted digraph** $G_z = (V, E, w)$ where
  - $V = C_0$ is the set of vertices
  - $(x_i, x_j) \in E$ whenever $x_j - x_i \preceq c$ is a constraint in $z$
  - $w(x_i, x_j) = (c, \preceq)$ whenever $x_j - x_i \preceq c$ is a constraint in $z$

• DBMs are thus (transposed) adjacency matrices of the weighted digraph

• Observe: deriving bounds = adding weights along paths

• Zone $z$ is in **canonical form** if and only if DBM $Z$ satisfies:
  - $Z(i, j) \leq Z(i, k) + Z(k, j)$ for any $x_i, x_j, x_k \in C_0$
Operations on DBM entries

Let $\leq \in \{<, \leq\}$.

- **Comparison** of DBM entries:
  - $(c, \leq) < \infty$
  - $(c, \leq) < (c', \leq')$ if $c < c'$

- **Addition** of DBM entries:
  - $c + \infty = \infty$
  - $(c, \leq) + (c', \leq) = (c+c', \leq)$
  - $(c, <) + (c', \leq) = (c+c', <)$
Example
Computing canonical DBMs

Deriving the **tightest constraint** on a pair of clocks in a zone
is equivalent to finding the **shortest path** between their vertices

- apply **Floyd-Warshall**’s all-pairs shortest-path algorithm
- its worst-case time complexity lies in \( \mathcal{O}(|C_0|^3) \)
- efficiency improvement:
  - let all frequently used operations preserve canonicity
Minimal constraint systems

- A (canonical) zone may contain many *redundant* constraints
  - e.g., in $x - y < 2$, $y - z < 5$, and $x - z < 7$, constraint $x - z < 7$ is redundant

- Reduce memory usage $\Rightarrow$ consider *minimal* constraint systems
  - e.g., $x - y \leq 0$, $y - z \leq 0$, $z - x \leq 0$, $x - 0 \leq 3$, and $0 - x < -2$
    is a minimal representation of a zone in canonical form with 12 constraints

- For each zone: $\exists$ a unique and equivalent minimal constraint system

- Determining minimal representations of canonical zones:
  - $x_i \xrightarrow{(n, \preceq)} x_j$ is redundant if a path from $x_i$ to $x_j$ has weight at most $(n, \preceq)$
  - fact: it suffices to consider alternative paths of length two only

\[ \text{complexity in } \mathcal{O}(|C_0|^3); \text{ zero cycles require a special treatment} \]
Example
DBM operations: checking properties

- **Nonemptiness**: is $\llbracket Z \rrbracket \neq \emptyset$?
  - $Z = \emptyset$ if $x_i - x_j \leq c$ and $x_j - x_i \leq' c'$ and $(c, \leq) < (c', \leq')$
  - search for negative cycles in the graph representation of $Z$, or
  - mark $Z$ when upper bound is set to value $< \text{its corresponding lower bound}$

- **Inclusion test**: is $\llbracket Z \rrbracket \subseteq \llbracket Z' \rrbracket$?
  - for DBMs in canonical form, test whether $Z(i, j) \leq Z'(i, j)$, for all $i, j \in C_0$

- **Satisfaction**: does $Z \models g$?
  - check whether $\llbracket Z \land g \rrbracket = \emptyset$
DBM operations: delays

- **Future**: determine $\vec{Z}$
  - remove the upper bounds on any clock, i.e.,
    
    $$\vec{Z}(i, 0) = \infty \quad \text{and} \quad \vec{Z}(i, j) = Z(i, j) \text{ for } j \neq 0$$
  - $Z$ is canonical implies $\vec{Z}$ is canonical

- **Past**: determine $\hat{Z}$
  - set the lower bounds on all individual clocks to $(0, \preceq)$
    
    $$\hat{Z}(i, 0) = \infty \quad \text{and} \quad \hat{Z}(i, j) = Z(i, j) \text{ for } j \neq 0$$
  - $Z$ is canonical does not imply $\hat{Z}$ is canonical
Final DBM operations

- **Conjunction**: $\llbracket Z \rrbracket \land (x_i - x_j \leq n)$
  - if $(n, \leq) < Z(i, j)$ then $Z(i, j) := (n, \leq)$ else do nothing
  - put $Z$ into canonical form (in time $O(|C_0|^2)$ using that only $Z(i, j)$ changed)

- **Clock reset**: $x_i := d$ in $Z$
  - $Z(i, j) := (d, \leq) + Z(0, j)$ and $Z(j, i) := Z(j, 0) + (-d, \leq)$

- **$k$-Normalization**: $\text{norm}_k(Z)$
  - remove all bounds $x - y \leq m$ for which $(m, \leq) > (k, \leq)$, and
  - set all bounds $x - y \leq m$ with $(m, \leq) < (-k, <)$ to $(-k, <)$
  - put the DBM back into canonical form (Floyd-Warshall)
$k$-Normalization of DBMs

Fix an integer $k$ (* represents an integer between $-k$ and $+k$)

\[
\begin{pmatrix}
* & > k & * \\
* & * & * \\
< -k & * & *
\end{pmatrix}
\sim
\begin{pmatrix}
* & +\infty & * \\
* & * & * \\
- k & * & *
\end{pmatrix}
\]

"intuitively", erase non-relevant constraints

remove all upper bounds higher than $k$ and lower all lower bounds exceeding $-k$ to $-k$