Difference Bound Matrices
Lecture #20 of Advanced Model Checking

Joost-Pieter Katoen
Lehrstuhl 2: Software Modeling & Verification

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

February 7, 2017
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 $x - y \leq \min(n, m)$
  $\Rightarrow$ this yields at most $|C_0| \cdot |C_0|$ constraints

- Example:

  $$x - 0 < 20 \land y - 0 \leq 20 \land y - x \leq 10 \land x - y \leq -10$$

- 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 $z$
  - $Z(0, i) := (0, \leq)$, i.e., $0 - x_i \leq 0$, or: all clocks are non-negative
  - $Z(i, i) := (0, \leq)$, i.e., each clock is at most 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

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

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

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 \textit{canonical form} if and only if:
  - no constraint in $z$ can be strengthened without reducing $\llbracket z \rrbracket = \{ \eta \mid \eta \in z \}$

- For each zone $z$:
  - there exists a zone $z'$ such that $\llbracket z \rrbracket = \llbracket z' \rrbracket$, 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 \textit{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 \textit{canonical form} if and only if DBM $Z$ satisfies:
  
  – $Z(i, j) \leq Z(i, k) + Z(k, j)$ for any $x_i, x_j, x_k \in C_0$
Advanced model checking

Operations on DBM entries

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

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

- **Addition** of DBM entries:
  
  - $(c, \preceq) + \infty = \infty$
  
  - $(c, \leq) + (c', \leq) = (c+c', \leq)$
  
  - $(c, <) + (c', \leq) = (c+c', <)$
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 $O(|C_0|^3)$
- 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 ⇒ 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: ∃ a unique and equivalent minimal constraint system

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

  complexity in $\mathcal{O}(|C_0|^3)$; 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 $< its ~ corresponding ~ lower ~ bound$

- **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 $\llbracket Z \land g \rrbracket = \llbracket Z \rrbracket \cap \llbracket g \rrbracket = \emptyset$
DBM operations: delays

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

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

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

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

- **\(k\)-Normalization**: \(\text{norm}_k(\mathbf{Z})\)
  
  - 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 $+k$)

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

- "intuitively", erase non-relevant constraints

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