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 $\mathbf{0}$ be a clock with constant value 0; let $C_0 = C \cup \{ \mathbf{0} \}$
- Any zone z over C can be written as:
  - conjunction of constraints $x - y < n$ or $x - y \leqslant n$ for $n \in \mathbb{Z}$, $x, y \in C_0$
  - when $x - y \preceq n$ and $x - y \preceq m$ take only $x - y \preceq \min(n, m)$

  $\Rightarrow$ this yields at most $|C_0| \cdot |C_0|$ constraints
- Example:

$$x - \mathbf{0} < 20 \;\wedge\; y - \mathbf{0} \leqslant 20 \;\wedge\; y - x \leqslant 10 \;\wedge\; x - y \leqslant -10$$

- 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 $x_0 = \mathbf{0}$, and:

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

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

- Definition of DBM **Z** for zone z:
  - $\mathbf{Z}(i,j) := (c, \prec)$ for each bound $x_i - x_j \prec c$ in z
  - $\mathbf{Z}(i,j) := \infty$ (= no bound) if clock difference $x_i - x_j$ is unbounded in z
  - $\mathbf{Z}(0,i) := (0, \leqslant)$, i.e., $\mathbf{0} - x_i \leqslant 0$, or: all clocks are non-negative
  - $\mathbf{Z}(i,i) := (0, \leqslant)$, i.e., each clock is at most itself

Example

$$(x_1 \geq 3) \wedge (x_2 \leq 5) \wedge (x_1 - x_2 \leq 4)$$

$$\begin{array}{cc} & \begin{array}{ccc} x_0 & x_1 & x_2 \end{array} \\ \begin{array}{c} x_0 \\ x_1 \\ x_2 \end{array} & \begin{pmatrix} +\infty & \mathbf{-3} & +\infty \\ +\infty & +\infty & \mathbf{4} \\ \mathbf{5} & +\infty & +\infty \end{pmatrix} \end{array}$$

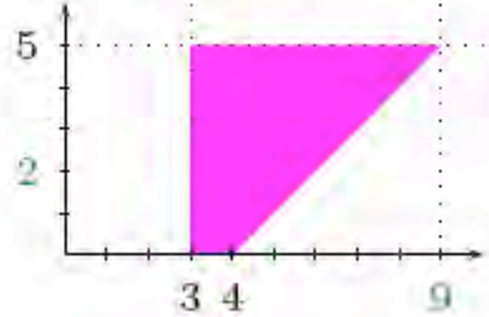
all clock constraints in the above DBM are of the form $(c, \leqslant)$

The need for canonicity

$$(x_1 \geq 3) \wedge (x_2 \leq 5) \wedge (x_1 - x_2 \leq 4)$$

$$\begin{array}{cc} & \begin{array}{ccc} x_0 & x_1 & x_2 \end{array} \\ \begin{array}{c} x_0 \\ x_1 \\ x_2 \end{array} & \begin{pmatrix} +\infty & -3 & +\infty \\ +\infty & +\infty & 4 \\ 5 & +\infty & +\infty \end{pmatrix} \end{array}$$

- 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:
  - $\mathbf{Z}(i, j) \leqslant \mathbf{Z}(i, k) + \mathbf{Z}(k, j)$ for any $x_i, x_j, x_k \in C_0$

Operations on DBM entries

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

- Comparison of DBM entries:
  - $(c, \preceq) < \infty$
  - $(c, \preceq) < (c', \preceq')$ if $c < c'$
  - $(c, <) < (c, \leqslant)$
  - $(c, \leqslant) \not< (c, <)$
- Addition of DBM entries:
  - $(c, \preceq) + \infty = \infty$
  - $(c, \leqslant) + (c', \leqslant) = (c{+}c', \leqslant)$
  - $(c, <) + (c', \leqslant) = (c{+}c', <)$

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., $x - y \leqslant 0$, $y - z \leqslant 0$, $z - x \leqslant 0$, $x - \mathbf{0} \leqslant 3$, and $\mathbf{0} - x < -2$ 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

complexity in $\mathcal{O}(|C_0|^3)$; zero cycles require a special treatment

Example

DBM operations: checking properties

- *Nonemptiness*: is $[\![\, \mathbf{Z} \,]\!] \neq \varnothing$?
  - $\mathbf{Z} = \varnothing$ if $x_i - x_j \preceq c$ and $x_j - x_i \preceq' c'$ and $(c, \preceq) < (c', \preceq')$
  - 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 $[\![\, \mathbf{Z} \,]\!] \subseteq [\![\, \mathbf{Z}' \,]\!]$?
  - for DBMs in canonical form, test whether $\mathbf{Z}(i,j) \leqslant \mathbf{Z}'(i,j)$, for all $i, j \in C_0$

- *Satisfaction*: does $\mathbf{Z} \models g$?
  - check whether $[\![\, \mathbf{Z} \wedge g \,]\!] = [\![\, \mathbf{Z} \,]\!] \cap [\![\, g \,]\!] = \varnothing$

DBM operations: delays

- *Future*: determine $\overrightarrow{\mathbf{Z}}$
  - remove the upper bounds on any clock, i.e.,

$$\overrightarrow{\mathbf{Z}}(i,0) = \infty \quad \text{and} \quad \overrightarrow{\mathbf{Z}}(i,j) = \mathbf{Z}(i,j) \text{ for } j \neq 0$$

  - $\mathbf{Z}$ is canonical implies $\overrightarrow{\mathbf{Z}}$ is canonical

- *Past*: determine $\overleftarrow{\mathbf{Z}}$
  - set the lower bounds on all individual clocks to $(0, \preceq)$

$$\overleftarrow{\mathbf{Z}}(0,i) = (0, \preceq) \quad \text{and} \quad \overleftarrow{\mathbf{Z}}(i,j) = \mathbf{Z}(i,j) \text{ for } j \neq 0$$

  - $\mathbf{Z}$ is canonical does not imply $\overleftarrow{\mathbf{Z}}$ is canonical

Final DBM operations

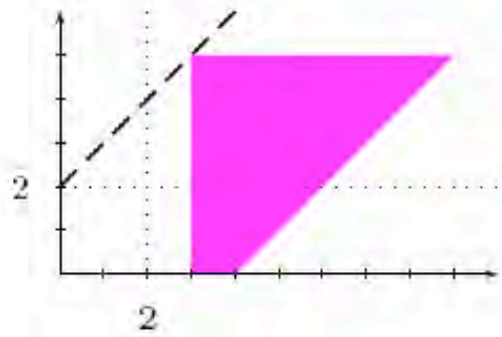
- *Conjunction*: $[\![\, \mathbf{Z} \,]\!] \wedge (x_i - x_j \preceq n)$
  - if $(n, \preceq) < \mathbf{Z}(i,j)$ then $\mathbf{Z}(i,j) := (n, \preceq)$ else do nothing
  - put $\mathbf{Z}$ into canonical form (in time $\mathcal{O}(|C_0|^2)$ using that only $\mathbf{Z}(i,j)$ changed)
- *Clock reset*: $x_i := d$ in $\mathbf{Z}$
  - $\mathbf{Z}(i,j) := (d, \leqslant) + \mathbf{Z}(0,j)$ and $\mathbf{Z}(j,i) := \mathbf{Z}(j,0) + (-d, \leqslant)$
- *k-Normalization*: *norm*$_k(\mathbf{Z})$
  - remove all bounds $x - y \preceq m$ for which $(m, \preceq) > (k, \leqslant)$, and
  - set all bounds $x - y \preceq m$ with $(m, \preceq) < (-k, <)$ 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 $+k$)

$$\begin{pmatrix} * & \boxed{>k} & * \\ * & * & * \\ \boxed{<-k} & * & * \end{pmatrix} \rightsquigarrow \begin{pmatrix} * & \boxed{+\infty} & * \\ * & * & * \\ \boxed{-k} & * & * \end{pmatrix}$$

- "intuitively", erase non-relevant constraints



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