Verification

Lecture 25

Bernd Finkbeiner

Exam info

- Main exam: Oct 9, 2013, 9am
- Backup exam: Nov 25, 2013, 10am

UNIVERSITÄT DES SAARLANDES

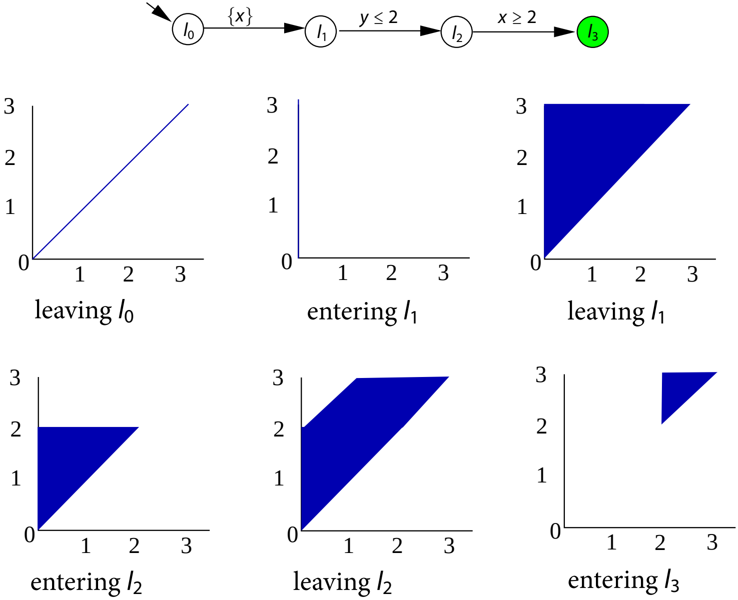
Plan for today

- Timed model checking
  - Regions
  - Zones

Zones

- Clock constraints are conjunctions of atomic constraints
  - $x \prec c$ and $x - y \prec c$ for $\prec \in \{<, \leq, =, \geq, >\}$
  - restrict to TA with only conjunctive clock constraints
  - and (as before) assume no difference clock constraints
- A clock zone is the set of clock valuations that satisfy a clock constraint
  - a clock zone for g is the maximal set of clock valuations satisfying g
- Clock zone of g: $[\![g]\!] = \{ \eta \in Eval(C) \mid \eta \models g \}$
  - use z, z' and so on to range over zones
- The state zone of $s = \langle \ell, \eta \rangle \in TS(TA)$ is $\langle \ell, z \rangle$ with $\eta \in z$

Zones: intuition



Successor and reset zones

- z' is the successor (clock) zone of z, denoted $z' = z^{\uparrow}$, if:
  - $z^{\uparrow} = \{ \eta + d \mid \eta \in z, d \in \mathbb{R}_{>0} \}$
- z' is the zone obtained from z by resetting clocks D, if:
  - $\text{reset } D \text{ in } z = \{ \text{reset } D \text{ in } \eta \mid \eta \in z \}$

Zone graph

For non-Zeno *TA* let:

$$ZG(TA, \Phi) = (S, Act, \rightarrow, I, AP', L') \quad \text{with}$$

- $S = Loc \times Zone(C)$ and $I = \{ \langle \ell, z_0 \rangle \mid \ell \in Loc_0 \}$
- $L'(\langle \ell, z \rangle) = L(\ell) \cup \{ g \mid g \in z \}$
- $\rightarrow$ consists of two types of edges:
  - Discrete transitions: $\langle \ell, z \rangle \xrightarrow{\alpha} \langle \ell', \text{reset } D \text{ in } (z \wedge g) \wedge inv(\ell') \rangle$ if $\ell \overset{g:\alpha,D}{\rightsquigarrow} \ell'$, and
  - Delay transitions: $\langle \ell, z \rangle \xrightarrow{\tau} \langle \ell, z^{\uparrow} \wedge inv(\ell) \rangle$.

Correctness

For timed automaton *TA* and any initial state $\langle \ell, \eta_0 \rangle$:

- Soundness:

$$\underbrace{\langle \ell, \underbrace{\{\, \eta_0 \,\}}_{z_0} \rangle \to^* \langle \ell', z' \rangle}_{\text{in } ZG(TA)} \quad \text{implies} \quad \underbrace{\langle \ell, \eta_0 \rangle \to^* \langle \ell', \eta' \rangle}_{\text{in } TS(TA)} \text{ for all } \eta' \in z'$$

- Completeness:

$$\underbrace{\langle \ell, \eta_0 \rangle \to^* \langle \ell', \eta' \rangle}_{\text{in } TS(TA)} \quad \text{implies} \quad \underbrace{\langle \ell, \{\, \eta_0 \,\} \rangle \to^* \langle \ell', z' \rangle}_{\text{in } ZG(TA)} \text{ for some } z' \text{ with } \eta'$$

Zone normalization

- To obtain a finite representation, the zones are normalized:
- For zone z, $norm(z) = \{ \eta \mid \eta \cong \eta', \eta' \in z \}$
  - where $\cong$ is the clock equivalence
- There can only be finitely many normalized zones
- $\langle \ell, z \rangle \rightarrow_{norm} \langle \ell', norm(z') \rangle$ if $\langle \ell, z \rangle \rightarrow \langle \ell', z' \rangle$

Forward reachability algorithm

Passed := $\varnothing$; // explored states so far

Wait := $\{ (\ell_0, z_0) \}$; // states to be explored

while Wait $\neq \varnothing$ // still states to go

do select and remove (ℓ, z) from Wait;

  if $(\ell = \text{goal} \;\wedge\; z \cap z_{goal} \neq \varnothing)$ **then return** "reachable"! **fi** ;

  if $\neg(\exists(\ell, z') \in \text{Passed}.\, z \subseteq z')$ // no "super"state explored yet

  then add (ℓ, z) to Passed // (ℓ, z) is a new state

    foreach (ℓ', z') with $(\ell, z) \rightarrow_{norm} (\ell', z')$

    do add (ℓ', z') to Wait; // add symbolic successors

  fi

od

return "not reachable"!

Representing zones

- Let $\mathbf{0}$ be a clock with constant value 0; let $C_0 = C \cup \{ \mathbf{0} \}$
- Any zone $z \in Zone(C)$ 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 $x - y \preceq n$ 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:

$$x - \mathbf{0} < 20 \;\wedge\; y - \mathbf{0} \leq 20 \;\wedge\; y - x \leq 10 \;\wedge\; x - y \leq -10 \;\wedge\; \mathbf{0} - z < 5$$

- Store each such constraint in a matrix
  - this yields a difference bound matrix

Notation: $\preceq$ stands for $<$ or $\leq$.

Difference bound matrices

- Zone z over C is represented by DBM $\mathbf{Z}$ of cardinality $(|C|+1)\cdot(|C|+1)$
  - for $C = x_1, \ldots, x_n$, let $C_0 = \{x_0, x_1, \ldots, x_n\}$ with $x_0 = \mathbf{0}$
  - $\mathbf{Z}(i,j) = (c, \preceq)$ if and only if $x_i - x_j \preceq c$
- Definition of $\mathbf{Z}$ for zone z:
  - for $x_i - x_j \preceq c$ let $\mathbf{Z}(i,j) = (c, \preceq)$
  - if $x_i - x_j$ is unbounded in z, set $\mathbf{Z}(i,j) = \infty$
  - $\mathbf{Z}(0,i) = (\leq, 0)$ and $\mathbf{Z}(i,i) = (\leq, 0)$
- Operations on bounds:
  - $(c, \preceq) < \infty$, $(c, <) < (c, \leq)$, and $(c, \preceq) < (c', \preceq)$ if $c < c'$
  - $c + \infty = \infty$, $(c, \leq) + (c', \leq) = (c+c', \leq)$ and $(c, <) + (c', \preceq) = (c+c', <)$

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: $\exists$ a unique and equivalent zone in canonical form
- Represent zone z by a weighted digraph $G = (V, E, w)$ 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
  - $w(x_i, x_j) = (\preceq, c)$ whenever $x_j - x_i \preceq c$ is a constraint in z
- Zone z is in canonical form if and only if DBM **Z** satisfies:
  - $\mathbf{Z}(i,j) \;\le\; \mathbf{Z}(i,k) + \mathbf{Z}(k,j)$ for any $x_i, x_j, x_k \in C_0$
- Compute canonical zone?
  - use Floyd-Warshall's all-pairs SP algorithm (time $\mathcal{O}(|C_0|^3)$)

Minimal constraint systems

- A zone may contain 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., $x - y \leq 0$, $y - z \leq 0$, $z - x \leq 0$, $x - \mathbf{0} \leq 3$, and $\mathbf{0} - x < -2$
  - 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:
  - $x_i \xrightarrow{(n,\preceq)} x_j$ is redundant if an alternative path from x_i to x_j has weight at most $(n, \preceq)$
  - it suffices to consider alternative paths of length two

zero cycles require a special treatment

Main operations on DBMs (1)

- Nonemptiness: is $[\![\mathbf{Z}]\!] \neq \emptyset$?
  - search for negative cycles in the graph representation of **Z**, or
  - mark **Z** when some upper bound is set to value < its lower bound
- Inclusion test: is $[\![\mathbf{Z}]\!] \subseteq [\![\mathbf{Z}']\!]$?
  - for DBMs in canonical form, test whether $\mathbf{Z}(i,j) \leq \mathbf{Z}'(i,j)$, for all $i,j \in C_0$
- Delay: determine $\mathbf{Z}^{\uparrow}$
  - remove the upper bounds on any clock, i.e.,
  - $\mathbf{Z}^{\uparrow}(i,0) = \infty$ and $\mathbf{Z}^{\uparrow}(i,j) = \mathbf{Z}(i,j)$ for $j \neq 0$

Main operations on DBMs (2)

- Conjunction: $z \;\&\; (x_i - x_j \leq n)$
  - if $(n, \leq) < \mathbf{Z}(i,j)$ then $\mathbf{Z}(i,j) := (n, \leq)$ else do nothing
  - put $\mathbf{Z}$ back into canonical form (in time $\mathcal{O}(|C_0|^2)$ using that only $\mathbf{Z}(i,j)$ changed)
- Clock reset: $x_i := 0$
  - $\mathbf{Z}(i,j) := \mathbf{Z}(0,j)$ and $\mathbf{Z}(j,i) := \mathbf{Z}(j,0)$
- Normalization
  - remove all bounds $x - y \leq m$ for which $(m, \leq) > (c_x, \leq)$, and
  - set all bounds $x - y \leq m$ with $(m, \leq) < (-c_y, <)$ to $(-c_y, <)$
  - put the DBM back into canonical form (Floyd-Warshall)